#04

ICT Security MAGAZINE

THREAT ACTOR

PREFAZIONE DI

GIANLUCA GALASSO

Head of Operations Directorate and CSIRT
Italia, National Cybersecurity Agency, Italy

2023

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINT.ORG

FORUM ICT SECURITY

25-26 OTTOBRE 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
21ª Edizione del Forum ICT Security

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT è un'associazione scientifica senza fini di lucro, il cui obiettivo è quello di promuovere la cultura e lo studio dell'intelligence in Italia.

QUADERNI DI CYBER INTELLIGENCE

La presente collana, frutto della collaborazione tra ICT Security Magazine e la Società Italiana di Intelligence (SOCINT), inaugura una serie di contenuti volti ad arricchire e approfondire il dibattito scientifico sulla Cyber Intelligence.

Indice

Prefazione a cura di **Gianluca Galasso**, *Head of Operations Directorate and CSIRT Italia, National Cybersecurity Agency, Italy*

Introduzione a cura di **Mattia Siciliano**, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

PREFAZIONE

È inevitabile, a mio avviso, aprire la prefazione di questa interessante raccolta di scritti sul tema della Cyber Threat Intelligence prendendo le mosse dalla guerra in atto alle porte dell'Unione Europea ed ai confini con la NATO.

In un'epoca in cui la cybersecurity rappresenta un'emergenza globale, nel tragico conflitto in atto vediamo infatti, per la prima volta in maniere così palese, l'utilizzo dell'arma cyber quale strumento distruttivo ai danni delle infrastrutture critiche e degli strumenti digitali di governo del paese aggredito, e non solo. Dal gennaio del 2022 tutti gli esperti hanno potuto osservare come le fenomenologie cyber riconducibili alla guerra abbiano subito un'impennata nei numeri e nella varietà. Ad esempio, è stato osservato un utilizzo estremamente aggressivo dei wiper per distruggere sistemi operativi in esercizio presso infrastrutture critiche (se ne sono contati, ad oggi, in numero a due cifre, appartenenti a famiglie diverse); anche il più banale attacco DDoS, fenomeno residuale e dagli impatti modesti, è salito agli onori delle cronache, anche italiane, poiché utilizzato dall'attivismo filorusso in campagne di natura ibrida in chiave antioccidentale.

La guerra ha inoltre creato nuove polarizzazioni nel complesso mondo cybercriminale; numerosi gruppi si sono infatti apertamente schierati a supporto della Federazione Russa, altri gruppi attivisti al contrario hanno annunciato azioni ai danni della stessa, altre realtà si sono coalizzate a supporto dell'Ucraina, e molte altre invece hanno sfruttato il nuovo caos per trarre vantaggi sotto il profilo del lucro.

Ma c'è dell'altro che non passa inosservato, ed è la quantità di informazioni dettagliate alla portata di tutti, che è possibile raccogliere su fonti aperte, che ci permette di conoscere ciò che avviene con tempi e dettagli inimmaginabili nei conflitti precedenti. I media raccontano gli sviluppi del campo di battaglia addirittura utilizzando anche immagini da satelliti spaziali commerciali, ricercatori, operatori dell'informazione specializzata e aziende di servizi di sicurezza di ogni dimensione forniscono dettagli su eventi e metodologie di attacco in gran quantità. Ciò è frutto di una trasformazione digitale che produce nuove tecnologie a ritmi vertiginosi, abilitando quindi la produzione esponenziale di dati e informazioni che i moderni analisti cyber devono saper trattare per cogliere quei segnali utili a conoscere ed anticipare la minaccia, fine ultimo delle attività di Cyber Threat Intelligence.

In questo contesto così dinamico ed in espansione, in cui anche la distinzione tra bande di cybercriminali e attori "state-sponsored" a volte svanisce, si avverte sempre più il bisogno di conoscere le minacce che insidiano i nostri servizi digitali; pertanto la Cyber Threat Intelligence, attività di ricerca informativa tipica del mondo della sicurezza militare ed intelligence in senso stretto, è ormai uno strumento a disposizione di tutti gli specialisti della sicurezza, anche di quelli meno avvezzi alla specifica materia.

Ma individuare le giuste informazioni nel mare di dati a cui è possibile accedere tra fonti aperte e servizi commerciali non è affatto cosa semplice, e diventa sempre più complicato se consideriamo la mutevolezza della minaccia, come questa vada alla ricerca di nuovi strumenti e tattiche per rendersi sempre più silenziosa.

Per fare ciò è necessario costruire l'attività in modo corretto, instaurare un processo di governance che rispetti i canoni del ciclo dell'intelligence. Una corretta pianificazione della ricerca, che risponda alla

domanda “chi e cosa voglio conoscere, ed a quale scopo”, è il punto di partenza necessario per orientare le successive fasi di raccolta ed analisi delle informazioni.

Coloro i quali si affidano alla Cyber Threat Intelligence per proteggere i propri asset tecnologici dovranno inoltre tenere sempre in mente che essa va costruita sulla propria organizzazione, sul proprio business, e deve rispondere a domande precise per capire quali minacce realmente ci interessano, poiché è impossibile collezionare intelligence per tutte le minacce in circolazione ed è estremamente impegnativo analizzare e valutare la grande quantità di informazioni disponibili, soprattutto a fronte della scarsa disponibilità di risorse umane specializzate. È importante quindi operare scelte precise, che presuppongano la piena conoscenza della propria organizzazione e del proprio business, e che tengano conto della necessità di dedicare le poche risorse specializzate alla gestione di informazioni di valore immediatamente “actionable”.

Questa raccolta di approfondimenti in materia redatti da esperti autorevoli, fornisce al lettore un’eccellente descrizione dei principali threat actors che minacciano istituzioni ed operatori privati occidentali e costituisce un’ottima panoramica divulgativa anche per coloro i quali, pur non essendo addetti ai lavori, intendano orientarsi in questo complesso ambito della cybersicurezza.

Gianluca Galasso, *Head of Operations Directorate and CSIRT Italia, National Cybersecurity Agency, Italy*

BIOGRAFIA

Gianluca Galasso

Contrammiraglio della Marina Militare Italiana, vanta un'esperienza ultratrentennale nel settore delle telecomunicazioni e della cybersecurity acquisita durante la carriera militare, nel corso della quale ha ricoperto le più importanti posizioni di settore nel campo tecnico-operativo, tra cui la direzione del Centro principale di telecomunicazioni ed informatica della Marina ed il comando di tre navi di superficie combattenti.

Dal 2017, dopo il passaggio ai ruoli di Presidenza del Consiglio dei Ministri in posizione dirigenziale, ha preso parte al processo di definizione e sviluppo dell'architettura nazionale di cybersecurity, con particolare attenzione agli aspetti tecnico-operativi del nuovo quadro normativo nazionale. In tale ruolo ha contribuito al recepimento in Italia della Direttiva NIS e alla definizione delle linee operative della legge sul Perimetro Nazionale di Sicurezza Cibernetica. Ha inoltre partecipato al processo di costituzione dell'Agenzia per la Cybersicurezza Nazionale, nei cui ruoli ha preso servizio il 15 settembre 2021 quale Direttore del Servizio Operazioni/CSIRT Italia.

INTRODUZIONE

Giunti alla quarta edizione del nostro quaderno tematico, continuiamo con gli approfondimenti in tema di Cyber Intelligence.

Questa volta la Commissione Cyber Threat Intelligence e Cyber Warfare, parte integrante della Società Italiana di Intelligence (SOCINT), ha voluto affrontare il tema dei **Threat Actors**.

La questione viene analizzata da un punto di vista sia tecnico sia geopolitico al fine di comprendere le dinamiche, le sfide, i rischi e le conseguenze dell'uso degli strumenti cyber negli scenari di conflitto, nonché come questi attori siano legati tra di loro e con i diversi Stati; senza sottovalutare il tema delle Insiders Threats.

Primo Levi diceva che "Se comprendere è impossibile, conoscere è necessario".

Gli unici elementi che abbiamo a nostro favore, in effetti, sono la conoscenza e l'approfondimento.

Quando si parla di Threat Actors, ci sono due elementi fondamentali da considerare: motivazione e attribution.

Le **motivazioni** possono essere disparate,

andando da ragioni ideologiche, di profitto o spionaggio alla soddisfazione personale dei singoli attori criminali: comprendere come questi ultimi agiscano in termini di Tecniche, Tattiche e Procedure (TTP) permette allora di avere un quadro completo di come siano organizzati, in che modo lavorino e, infine, quale sia il loro scopo/motivazione.

Questo è sicuramente uno degli aspetti fondamentali da tenere in considerazione: solo capendo quale sia la reale motivazione dietro un attacco cyber siamo in grado di attivare le corrette contromisure legali, tecnologiche e di comunicazione. E in questo senso le informazioni di Cyber Threat Intelligence, intese come report sottoposti al decisore politico o alla leadership aziendale, possono essere di grande aiuto.

L'**attribution**, intesa come capacità di comprendere chi sia l'attaccante, rimane ancora oggetto di ricerca in ambito Cyber Intelligence. Le moderne tecnologie permettono di sferrare attacchi informatici lasciando sempre meno tracce; inoltre i gruppi dediti al cybercrime mutano frequentemente nomi, linguaggi e metodologie, rendendo la loro classificazione tutt'altro che semplice. Ma solo identificare con certezza l'attaccante - e la sua eventuale affiliazione a uno Stato - permette a istituzioni e aziende di agire efficacemente, a livello nazionale e internazionale, per neutralizzare e contrastare specifiche minacce.

In conclusione possiamo affermare che la conoscenza (intesa come la combinazione degli elementi tecnologici e non), unita alla valutazione del contesto geopolitico di riferimento, resta l'unico modo per conoscere i propri avversari in un contesto di guerra cibernetica.

Mentre, da un punto di vista umano, l'unica strada rimane la salvezza della "nostra cittadella interiore"[1] .

Marco Aurelio - "Il modo migliore per difendersi da un nemico è di non comportarsi come lui".

Mattia Siciliano, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

[1] Marco Aurelio, Pensieri – LIBRO VI

BIOGRAFIA

Mattia Siciliano

L'ing. Siciliano ha oltre 15 anni di esperienza in *Cyber Security* e *Cyber Intelligence*. Attualmente è *Business Director* per una società internazionale con sede negli Emirati Arabi Uniti e docente presso le Università "Luiss Guido Carli" di Roma e "Federico II" di Napoli. In precedenza, partner e co-fondatore di DeepCyber, una società boutique focalizzata sulla *Cyber Threat Intelligence* e manager in diverse società di consulenza come EY e KPMG. Docente all'Università degli Studi di Napoli Federico II. Consulente per Ministero della Difesa (Innova Difesa), agenzie di *intelligence* e forze dell'ordine. Presidente della Commissione di Studio in *Cyber Threat Intelligence e Cyber Warfare* della Società Italiana di Intelligence.

FORUM ICT SECURITY

25-26 OTTOBRE 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
21ª Edizione del Forum ICT Security

Gli attori malevoli, la Cyber Threat Intelligence e i principali framework di analisi

«The great accomplishments of today's intelligence brotherhood have been of two sorts: collection and analysis»

Sherman Kent [1903-1986], Strategic Intelligence for American World Policy, 1965, xv-xvi

INTRODUZIONE

Come già messo in risalto in un precedente Quaderno SOCINT, l'essenza centrale di un'attività di *Cyber Threat Intelligence* (CTI) è costituita da dati e informazioni raccolte da una serie di fonti sugli attacchi attuali o potenziali contro un'organizzazione, da parte di attori malevoli[1].

Più in dettaglio, la CTI è costituita da dati e informazioni che vengono raccolti, elaborati e analizzati per comprendere le motivazioni, gli obiettivi e i comportamenti di attacco di un agente portatore di una minaccia (*Threat actor*, TA).

La CTI è importante per i seguenti motivi:

1. apporta nuove informazioni su attività malevoli che sono celate, consentendo ai team di sicurezza di approntare delle risposte basate su decisioni adeguate;
2. svela i motivi degli avversari così come le loro tattiche, tecniche e procedure (TTP) nonché gli indicatori di compromissione (IOC);
3. aiuta a comprendere meglio il processo decisionale dell'autore della minaccia;
4. responsabilizza e potenzia gli stakeholder aziendali, come Consigli di amministrazione, *Chief information security officer* (CISO), *Chief information officer* (CIO) e *Chief technology officer* (CTO) così da mitigare il rischio, diventare più efficienti e prendere decisioni più rapide basate sui dati disponibili. In questo senso, lo scopo principale della CTI è rendere consapevoli le organizzazioni dei vari rischi che devono affrontare a causa di minacce esterne, come le minacce *zero-day* e le minacce persistenti avanzate (*Advanced persistent threat*, APT).

Tra i vari strumenti che sono stati messi a punto, nel corso degli ultimi decenni, al fine di mitigare tali minacce vi sono senz'altro i framework per l'identificazione dei TA, importanti poiché forniscono un modello comune per analizzare e categorizzare le minacce informatiche, rendendo più facile per le organizzazioni comprendere e rispondere agli attacchi. Inoltre, i framework

[1] Achille Pierre Paliotta, Una riflessione preliminare sul processo di Istituzionalizzazione della Cyber Intelligence (CYBINT), in Quaderni di Cyber Intelligence #1, ICT Security Magazine, novembre 2022, https://bit.ly/3OqTXT1

forniscono un linguaggio comune per la collaborazione e la condivisione delle informazioni tra le diverse organizzazioni e le forze dell'ordine, il che a sua volta migliora la capacità di identificare e neutralizzare i TA.

Tutto ciò si inserisce all'interno di un risoluto e ultradecennale processo di standardizzazione che la comunità CTI ha inteso portare avanti per raggiungere i fini anzidetti e che è consistita, sostanzialmente, di tre fasi principali, qui necessariamente succinte:

1. identificare i principali elementi dei dati, quali informazioni sul tipo di minaccia, sulla gravità della stessa, sulla fonte della minaccia, sull'impatto potenziale, ecc.;
2. sviluppare un modello di dati mediante la creazione di una tassonomia o di un'ontologia per classificare i diversi tipi di minacce e i loro attributi;
3. definire i formati dei dati che verranno utilizzati, i più importanti dei quali possono essere considerati i framework STIX (*Structured Threat Information eXpression*) e TAXII (*Trusted Automated eXchange of Indicator Information*).

STIX è un linguaggio standardizzato per descrivere le informazioni sulle minacce informatiche sviluppato da MITRE Corporation nel 2012 ed è arrivato, ad oggi, alla versione 2.0, progettata per essere più flessibile, estensibile e facile da usare rispetto al suo predecessore 1.0. STIX 2.0 include una serie di nuove funzionalità e miglioramenti, tra cui: un'architettura più modulare che consente una più facile personalizzazione ed estensione; un modello di dati semplificato che facilita la rappresentazione di informazioni complesse sulle minacce; un supporto migliorato per gli indicatori di compromissione (IOC) e altri tipi di dati sulle minacce; un migliore supporto per la condivisione e la collaborazione tra le diverse organizzazioni utilizzatrici.

TAXII è, invece, un protocollo che consente lo scambio di informazioni sulle minacce informatiche tra diverse organizzazioni. Lo standard TAXII specifica i dettagli tecnici per lo scambio di informazioni quali il formato dei dati, i protocolli per la loro trasmissione e le misure di sicurezza che devono essere adottate per proteggere le informazioni in transito. Sono ricomprese in TAXII anche delle linee guida per l'implementazione dello stesso in diversi ambienti quali i sistemi di rilevamento delle intrusioni (IDS) e i sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM).

Lo sforzo di sintesi che viene compiuto in questo testo è, dunque, finalizzato a dar conto dei framework più importanti per l'identificazione dei threat actors nella cybersecurity, considerando che non esiste un elenco esaustivo di questi ma che i più influenti e consigliati possono essere considerati i seguenti:

1. *Intrusion Lifecycle Model*;
2. *Indicator Types Model*;
3. *Attributional Model*.

La breve illustrazione di questi framework, a scopo prettamente divulgativo, con esempi specifici di alcuni modelli, è in grado di fornire una veloce panoramica su quali sono le principali modalità che la comunità della *cyber intelligence* si è data

nel corso degli ultimi decenni al fine di provare a individuare e classificare la natura delle minacce informatiche e, di conseguenza, su come meglio proteggere le reti, i processi e i dati.

1. INTRUSION LIFECYCLE MODEL (ILM)

L'ILM è un framework utilizzato per descrivere e analizzare le fasi di un attacco cyber. Questo modello è assai utile perché fornisce una visione complessiva del processo di intrusione dei TA, permettendo ai responsabili della sicurezza informatica di identificare e comprendere i punti deboli nella difesa del sistema e di pianificare una risposta più efficace. Questo modello può essere utilizzato anche per la formazione e la sensibilizzazione degli utenti, per la valutazione del rischio e per la pianificazione della sicurezza. Qui di seguito verranno brevemente illustrate le caratteristiche di quelli più utilizzati quali The Cyber Kill-Chain e il MITRE ATT&CK.

THE CYBER KILL-CHAIN (CKC)

La CKC è un modello concettuale, attribuito alla *corporation* Lockheed Martin, divulgato in un paper del 2009, mediante il quale vengono illustrate le varie fasi eseguite da un avversario nel raggiungimento dei propri obiettivi di attacco. L'idea sottostante al framework, derivato dall'intelligence militare, è che il difensore deve cercare di interrompere un anello della catena, una volta individuata la fase di attacco, perché poi i passaggi sarebbero abbastanza prevedibili e passibili di contrasto e mitigazione. *«The phrase "kill chain" describes the structure of the intrusion, and the corresponding model guides analysis to inform actionable security intelligence. Through this model, defenders can develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes. Kill chain analysis illustrates that the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary. Through intelligence-driven response, the defender can achieve an advantage over the aggressor for APT caliber adversaries»*[2].

Le varie fasi della CKC sono illustrate nella figura seguente:

Fonte: immagine tratta dal web.

La CKC è assai utile per avere una valutazione delle proprie capacità di difesa, ovvero può permettere di evidenziare le proprie lacune strutturali

[2] Eric M. Hutchins, Michael J. Cloppert, M. Rohan, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Bethesda (MD), Lockheed Martin Corporation, Technical Report, 2009.

nel contrasto di minacce portate da poderosi attori quali gli APT. Una seconda ragione è che essa può essere assai utile nelle analisi post-incidente in quanto fornisce un quadro realistico di come si è svolto l'attacco, permettendo di sezionare ogni fase e di profilare il comportamento dell'avversario e del suo eventuale successo, ovvero di fornire una vasta comprensione dell'attacco, dell'attore e di ciò che dovrebbe essere fatto, di conseguenza, per mitigare future minacce. La terza ragione è di carattere comunicativo ma non meno importante delle altre due, in quanto il framework offre un modo semplice e potente per comunicare, con una storia lineare e con un livello di concettualizzazione semplice ed efficace, una situazione molto complessa, in cui sono presenti molti tecnicismi, sia se ci si deve relazionare ai vertici societari, oppure ai decisori pubblici o alla stampa di opinione[3]. Per tutte queste ragioni, la CKC si è largamente diffusa nella comunità InfoSec. Come tutti gli strumenti, nondimeno, essa non può coprire tutto il campo di analisi in quanto, soprattutto nella fase 7 ("*Actions on Objectives*"), la quale può durare anche molti mesi, si apre un campo davvero vasto in cui molto deve essere ancora svolto in termini di approfondita elaborazione teorica. Su queste basi, di conseguenza, non sono mancate critiche al riguardo[4]. «*Lockheed Martin's model is intrusion-centric, which was the focus of cyber security when it was created, and is indeed still the focus of (too) much cyber security effort today. […] Then we have the fact that the Chain is completely malware-focused. But malware is only one threat vector facing today's networks. What about the insider threat? Social engineering? Intrusion based on remote access, in which no malware or payload is involved? The list of threat vectors facing today's networks is far, far longer than those covered by the Chain*»[5].

A seguito di tali critiche si sono proposti dei modelli migliorativi, quale la CKC unificata con l'*Adversarial Tactics, Techniques & Common Knowledge for Enterprise* (ATT&CK), quest'ultimo messo a punto dal centro di ricerca non-profit MITRE Corporation e fatto oggetto di successiva analisi.

Dalla congiunzione di questi due modelli è stato messo a punto un framework unificato, il quale consiste di 18 fasi e prevede tre punti di sintesi:

1. ***Initial Foothold*** *(Compromised System);*
2. ***Network Propagation*** *(Internal Network);*
3. ***Actions on Objectives*** *(Critical Asset Access)*[6].

Fonte: immagine tratta dal web.

[3] Sean Mason, Leveraging The Kill Chain For Awesome, 2 December 2014, https://bit.ly/3ixdFMr.

[4] Matt Devost, Every Cyber Attacker is an Insider, 19 February 2015, https://bit.ly/2Z0bY2t.
Marc Laliberte, A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack, 21 September 2016, https://bit.ly/3f2j0sX.
Tim Greene, Why the 'cyber kill chain' needs an upgrade, 5 August 2016, https://bit.ly/38saXDk.

[5] Giora Engel, Deconstructing The Cyber Kill Chain, 18 November 2014, https://bit.ly/2Z1xuUE.

[6] Paul Pols, The Unified Kill Chain. Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks, Cyber Security Academy, 2017.

MITRE ATT&CK

L'*Adversarial Tactics, Techniques & Common Knowledge for Enterprise* (ATT&CK)[7], divulgato nel 2013, prevede 14 "tattiche" Enterprise le quali rappresentano il più alto livello di astrazione; esse non hanno, tuttavia, un ordine prestabilito di esecuzione e non costituiscono, quindi, una catena di eventi come la CKC.

Le "tattiche" sono le seguenti:

1. Reconnaissance ("the adversary is trying to gather information they can use to plan future operations");
2. Resource Development ("the adversary is trying to establish resources they can use to support operations");
3. Initial access ("the adversary is trying to get into your network");
4. Execution ("the adversary is trying to run malicious code");
5. Persistence ("the adversary is trying to maintain their foothold");
6. Privilege escalation ("the adversary is trying to gain higher-level permissions");
7. Defense evasion ("the adversary is trying to avoid being detected");
8. Credential access ("the adversary is trying to steal account names and passwords");
9. Discovery ("the adversary is trying to figure out your environment");
10. Lateral movement ("the adversary is trying to move through your environment");
11. Collection ("the adversary is trying to gather data of interest to their goal");
12. Command and Control ("the adversary is trying to communicate with compromised systems to control them");
13. Exfiltration ("the adversary is trying to steal data");
14. Impact ("the adversary is trying to manipulate, interrupt, or destroy your systems and data").

Ogni "tattica" è poi composta di numerose "tecniche" così come è dato evincere dall'immagine seguente.

In generale, il MITRE ATT&CK è uno strumento assai utile per analizzare e contrastare le minacce informatiche, ma presenta anche alcuni limiti. Tra i punti di forza del framework si può qui citare, in primo luogo, l'ampia copertura di tecniche e tattiche usate dagli attaccanti, basata su dati reali e verificabili. In secondo luogo, grazie alla sua struttura modulare e flessibile, vi è la possibilità di adattarlo a diversi contesti e scenari operativi. Infine, esso è facilmente integrabile con altri strumenti e fonti di informazione, anche grazie alla sua natura aperta e collaborativa.

Tra i punti di debolezza, invece, può essere qui sottolineata la sua complessità e vastità, il che può renderne difficile la comprensione e gestione da parte degli utenti meno esperti. Un altro aspetto critico può essere considerato la sua potenziale esposizione a manipolazioni o abusi da parte degli attori malevoli, i quali possono sfruttarlo al fine

[7] https://attack.mitre.org/tactics/enterprise/.

Fonte: immagine tratta dal web.

di nascondere o simulare le proprie attività. In ultimo, infine, come tutti questi tipi di modelli, vi può essere una difficoltà di applicazione a minacce emergenti o sconosciute; le quali richiedono, evidentemente, una continua revisione e aggiornamento delle relative tattiche e tecniche.

2. INDICATOR TYPES MODEL (ITM)

Gli ITM sono modelli utilizzati per classificare i segnali o le tracce lasciati dagli attaccanti durante un attacco informatico. Questi indicatori possono essere utilizzati per identificare la presenza di una minaccia e per aiutare a determinare la natura e le intenzioni dell'attaccante. Qui di seguito viene presentato il framework più conosciuto, The Pyramid of Pain.

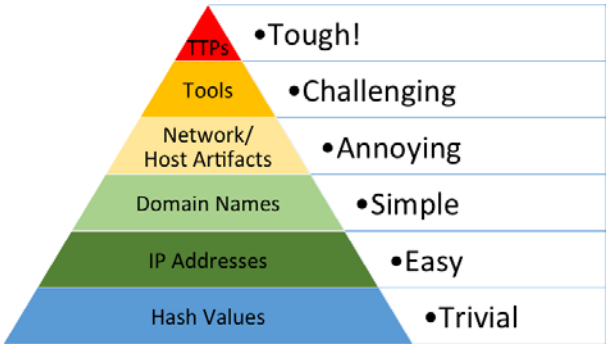
[8] https://bit.ly/3f1UBUh.

The Pyramid of Pain (PoP)

PoP nasce, nell'elaborazione del suo autore David J. Bianco, nel 2013[8], per rispondere agli incidenti e alla necessità di individuazione delle minacce al fine di migliorare il campo di applicazione degli indicatori di attacco. La "piramide" misura la potenziale utilità della propria sicurezza cibernetica, così come la difficoltà di ottenere tale livello di sicurezza, in quanto più in alto si è sulla piramide e più risorse devono essere spese dagli avversari per attaccarla.

La "Piramide del Dolore" è assai utile, perché aiuta a identificare le fasi critiche dell'attacco e a pianificare la difesa del sistema in modo più effi-

cace. Inoltre, aiuta a valutare il potenziale danno causato da un attacco e a prioritizzare la risposta all'emergenza.



Fonte: immagine tratta dal web.

In ogni fase di azione, si ha la possibilità di rilevare le azioni dell'avversario utilizzando determinati indicatori. Ed è qui che entra in gioco la PoP: essa funge da guida per sapere come dare priorità alle proprie risorse, spesso limitate, al fine di arrecare il massimo danno ai piani dell'avversario.

Le definizioni fornite dall'autore sono le seguenti:

1. *Hash Values: "SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files";*
2. *IP Addresses;*
3. *Domain Names;*
4. *a) Network Artifacts: "Observables caused by adversary activities on your network";*
5. *b) Host Artifacts: "Observables caused by adversary activities on one or more of your hosts";*
6. *Tools: "Software used by the adversary to accomplish their mission";*
7. *Tactics, Techniques and Procedures (TTPs): "How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between".*

L'articolo del blog in cui Bianco presenta la PoP nasce a margine di un rapporto di ricerca curato dalla società Mandiant e relativo all'entità malevola APT1: l'autore si chiede perché non vi sia stata nessuna discussione pubblica sui dati/osservabili messi a disposizione dal rapporto e sembra avallare l'utilizzo consapevole degli indicatori di compromissione (IOC).

Bianco, difatti, così chiude l'articolo: «*Whenever you receive new intel on an adversary (whether it be APT1/Comment Crew or any other threat actor), review it carefully against the Pyramid of Pain.* ***For every paragraph, ask yourself "Is there anything here I can use to detect the adversary's activity, and where does this fall on the pyramid?"*** *Sure, take all those domains and IPs and make use of them if you can, but keep in mind that* ***the amount of pain you cause an adversary depends on the types of indicators you are able to make use of****, and create your plan accordingly*» [in grassetto nell'originale].

3. ATTRIBUTIONAL MODEL

Un *Attributional Model* è un modello utilizzato nella cybersecurity per identificare la fonte di un attacco informatico. Il modello mira a raccogliere e ad analizzare informazioni sulle caratteristiche tecniche, le motivazioni e le opportunità degli attaccanti al fine di identificare la loro provenienza; a tal fine considera diversi fattori, come ad esempio la lingua utilizzata nel codice dell'at-

tacco, l'ora del giorno in cui è stato effettuato, il modello di elaborazione utilizzato e altri dettagli tecnici. Queste informazioni sono confrontate con database esistenti e analizzate in base a schemi di attacchi noti per determinare la provenienza dell'attacco e l'identità degli attaccanti.

L'attribuzione degli attacchi informatici è importante perché permette di comprendere le motivazioni e le opportunità degli attaccanti, nonché di identificare eventuali tendenze e schemi ricorrenti. Inoltre può aiutare a prevenire futuri attacchi, poiché le organizzazioni possono utilizzare le informazioni ottenute per pianificare la difesa contro degli attaccanti specifici. Tuttavia, deve essere qui messo in rilievo che l'attribuzione degli attacchi, soprattutto quelli da parte di attori *nation-state*, può essere molto complessa e che non sempre è possibile determinare con certezza la fonte di un attacco informatico. Ciò premesso, uno dei principali modelli utilizzati dalla comunità InfoSec è quello del Diamond Model.

The Diamond Model (DM)

L'approccio del DM si concentra molto più sulla comprensione dell'attaccante – quali strumenti e infrastrutture usa e quali siano le sue motivazioni – rispetto ad altri modelli finora presentati (in primis, la CKC).

Il DM presenta un nuovo modello concettuale di analisi delle intrusioni basato sull'elemento atomico dell'attività di intrusione, l'evento, a cui corrisponde un singolo "diamante", da cui è stato derivato il nome di questo framework.

Dell'evento vengono mostrate, nello schema riassuntivo, le funzionalità principali di ogni attività dannosa:

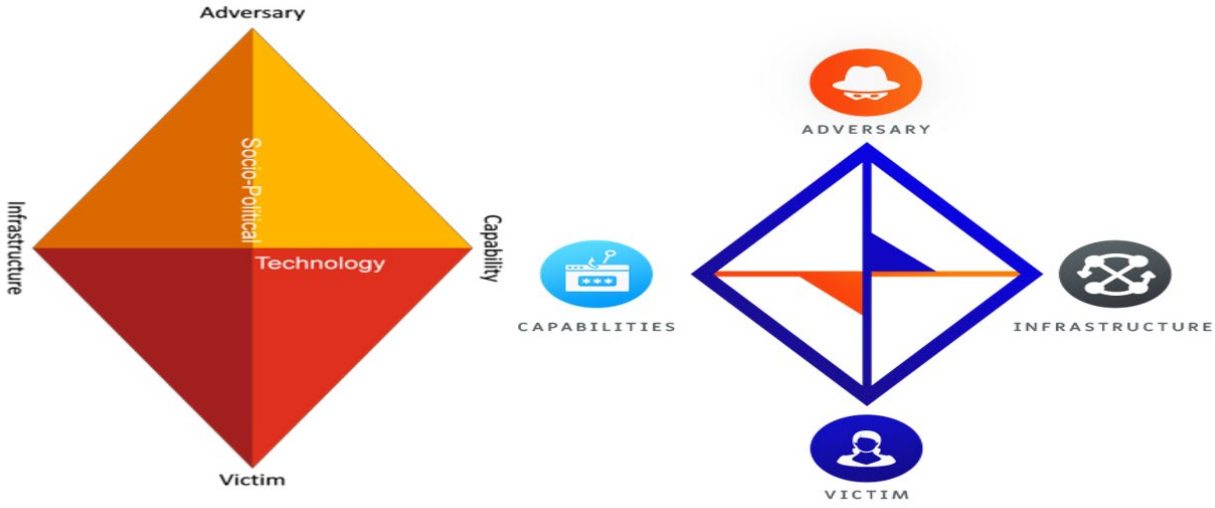
1. l'avversario (*badguy, email addresses, handles, network assets*);
2. la vittima (*personas, network assets, email addresses*);
3. le capacità (*malwares, exploits, hacker tools, stolen certs*);
4. l'infrastruttura (*IP addresses, domain name, email addresses*).

Come viene specificato, «*for every intrusion **event** there exists an **adversary** taking a step towards an intended goal by using a **capability** over **infrastructure** against a **victim** to produce a result*»[9].

Questi 4 concetti principali (*core-features*) sono connessi tra di loro mediante dei vertici i quali rappresentano una relazione unica tra gli stessi concetti e possono dar luogo a un pivoting analitico per cui, da ogni vertice, si possono raggiungere gli altri vertici. In questo senso, una vittima può "vedere" come le capacità vengono usate contro una determinata infrastruttura. Dal vertice dell'infrastruttura si può "vedere", difatti, l'avversario manovrare le capacità contro le vittime facendo uso di determinate infrastrutture.

È evidente il ricorso alla teoria dei grafi, in quanto si fa esplicita citazione di relazioni e di vertici.

[9] Sergio Caltagirone, The Diamond Model of Intrusion Analysis. A Summary, Hanover (MD), Center for Cyber Threat Intelligence and Threat Research, Technical Report, 2013.



Fonte: immagine tratta dal web.

Il framework prevede anche delle meta-caratteristiche (*meta-features*) quali *timestamp, phase (reconnaissance, weaponization, exploitation), result (success, failure, confidentiality compromised, integrity compromised), direction (from or to the victim, bidirectional), methodology (spear-phishing, denial of service attack)* e delle *external resources* necessarie per completare con successo l'attività degli eventi *(the target's email address or IP address, the vulnerability to exploit)*[10]. Queste meta-caratteristiche non formano parte costitutiva del modello e, pertanto, possono essere aggiunte o rimosse, a seconda delle esigenze contingenti.

Altra peculiarità del framework è che esso è volutamente ad alto livello di generalità in modo da permetterne la taratura in ogni situazione, così come l'aggiunta di ulteriori sotto-caratteristiche (*sub-features*); a solo titolo esemplificativo, la vittima può essere ulteriormente caratterizzata come *IP address, hostname*, organizzazione, ecc.

Il modello, infine, può essere ulteriormente espanso con altri due strati di meta-caratteristiche: l'asse *technology*, che connette le infrastrutture alle capacità favorendone l'effettiva interazione; l'asse *social-political*, che descrive le complesse interrelazioni tra vittima e avversario.

«Analytically, the Diamond allows concepts from criminology and victimology to be applied to intrusion analysis allowing one to understand the reason a victim was chosen, the value the victim brings to the adversary, and ultimately how that relationship can be influenced and manipulated to enhance mitigation» (Caltagirone, 2013:4).

L'avversario opera in fasi multiple, utilizzando due o più eventi al fine di ottenere un risultato dannoso sulla vittima; e tale corso di azione (*activity threads*) può essere attentamente analizzato

[10] https://www.activeresponse.org/wp-content/uploads/2013/07/diamond_summary.pdf.

da un analista. «*Threads not only span vertically along a single adversary-victim pair, but horizontally as adversaries take advantage of knowledge and access gained in one operation to enable other operations*» (Caltagirone, 2013:4).

In ultimo, il framework permette di effettuare analisi mediante altre concettualizzazioni quali *activity-attack graph, adversary processes, activity groups, activity group families* ma ciò richiederebbe ben altro spazio a disposizione e, infine, potrebbe inutilmente complicare la presentazione, a soli fini didascalici, del modello stesso.

CONCLUSIONI

Per contrastare le minacce provenienti dagli attori malevoli sempre più diffusi nell'ecosistema digitale attuale, è necessaria una strategia di *cyber threat intelligence* che si basi su una raccolta e analisi efficace delle informazioni relative al contesto, alle motivazioni e alle capacità degli avversari.

Esistono diversi framework di analisi che possono aiutare i professionisti della CTI a organizzare e interpretare i dati raccolti e in questo breve testo si è cercato di fornire un'iniziale categorizzazione degli stessi, individuati in: 1) *Indicator Types Model*; 2) *Intrusion Lifecycle Model;* 3) A*ttributional Model*. All'interno di queste macro tipologie si sono velocemente presentati alcuni modelli principali, tra i quali i più conosciuti e utilizzati sono senz'altro:

- The Cyber Kill Chain;
- MITRE ATT&CK;
- The Diamond Model;
- The Pyramid of Pain.

Questa veloce presentazione non è esaustiva, pertanto, di tutti essi e ha sole funzioni di carattere esemplificativo e divulgativo, al fine di promuovere una cultura crescente dell'*awareness* in campo cyber security. Come si è cercato di mettere in luce nel corso del testo, questi framework forniscono una struttura concettuale per identificare gli elementi chiave di un'operazione malevola, come gli obiettivi, le fasi, le tecniche e le contromisure. In questo senso l'utilizzo esteso di questi framework, da parte della comunità di *cyber intelligence*, può migliorare la qualità e l'efficienza delle analisi delle minacce, facilitando la comunicazione e la collaborazione tra gli analisti e gli altri *stakeholder* coinvolti nella difesa dei sistemi informatici mediante la condivisione di una modellistica e di un linguaggio comune. Un esempio di tale processo di standardizzazione, in atto da decenni, nel campo della comunità CTI, oltre ai framework già citati, è anche quello relativo a STIX 2.0 e a TAXII, i quali sono stati brevemente presentati nell'introduzione di questo articolo.

Tutti questi modelli, considerati in maniera olistica, rappresentano quanto di più avanzato l'attuale comunità CTI sia riuscita a mettere a punto e rappresenta, assai bene, quel percorso di crescita e istituzionalizzazione che l'intero ecosistema della cybersecurity sta portando avanti in Italia e nel resto del mondo, sia in campo civile che militare, sia in campo accademico che tra i sempre più numerosi addetti ai lavori.

Achille Pierre Paliotta, *Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL).*

BIOGRAFIA

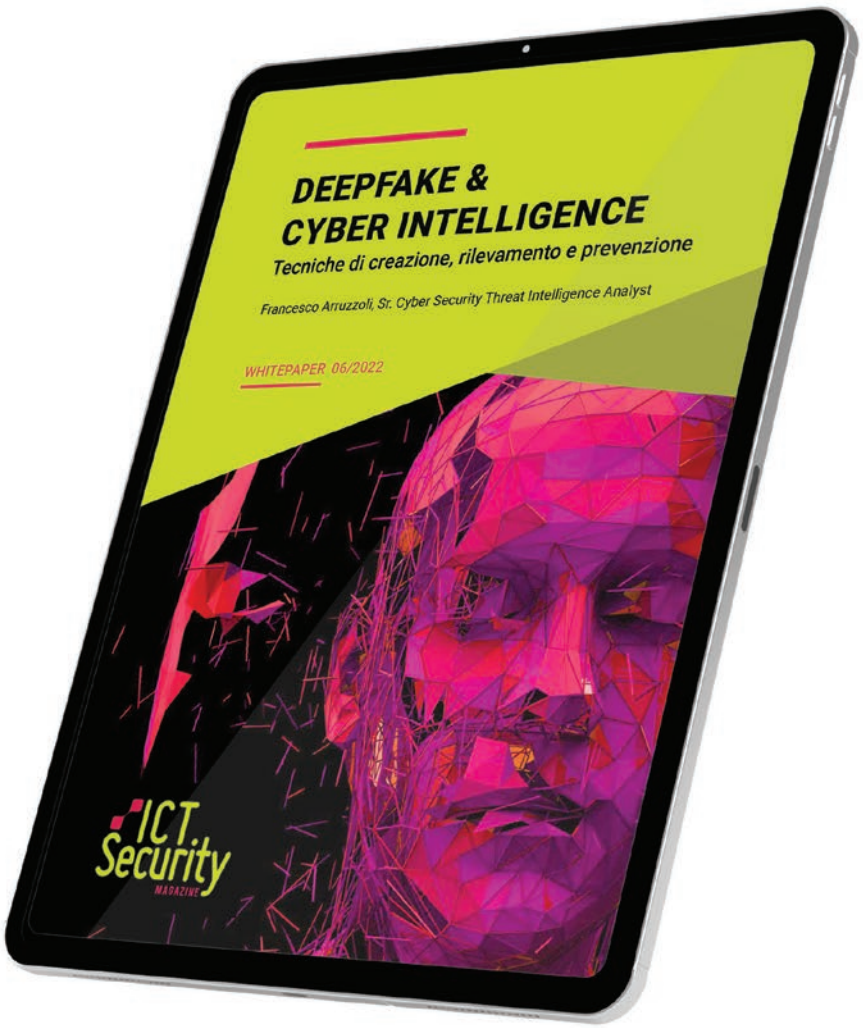
Achille Pierre Paliotta

Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL). Laurea in Sociologia all'Università di Roma "La Sapienza", Master in Data Science (DS) all'Università di Roma "Tor Vergata" nel 2015 e Master in Cybersecurity (SIIS) all'Università di Roma "La Sapienza" nel 2021. Svolge studi e ricerche sull'innovazione tecnologica, sulla *cyber intelligence*, sulla cybersicurezza, sulle professioni, sull'incrocio tra domanda ed offerta di lavoro, sulla formazione continua, sull'invecchiamento attivo, sulla contrattazione collettiva e, in generale, su tematiche di sociologia economica. Sta attualmente svolgendo il I Dottorato nazionale in Cybersecurity presso IMT Lucca e IIT CNR.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com



Overview dei principali Threat Actor legati agli Hostile Nation-State

Nel presente articolo si vuole ripercorrere la nascita dei concetti di minaccia cyber e di t*hreat actor,* avvenuta davvero da pochi anni e che giustifica tutti gli sforzi che attualmente si stanno compiendo per stabilire framework con cui definire lo svolgimento di un attacco e classificare/categorizzare al meglio un avversario. Successivamente, saranno analizzati i principali governi che sono oggi considerati ostili e i *threat actor* a loro legati, fino a introdurre una metodologia che permetta di farne una valutazione.

Dal punto di vista storico, le prime menzioni di *targeted cyber threats* e, in particolare, di cyber threat al di fuori degli ambiti governativi sono apparse nel 2001 durante un briefing non classificato della National Security Agency del 2010. Il termine APT[1] (o Advanced Persistent Threat) è stato invece utilizzato per la prima volta durante una discussione all'Air Force Intelligence Agency in cui si cercava un termine per classificare una specifica tipologia di attaccanti, molto ben addestrati, che con ogni probabilità erano finanziati e addestrati da enti governativi.

Una definizione attualmente condivisa di A*dvanced Persistent Threat* è fornita dal NIST SP 800-39[2], che li descrive come "*an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives*".

Una caratteristica chiave di un attacco APT è l'uso congiunto di tecniche manuali e automatizzate per raggiungere i propri obiettivi, che possono consistere nella compromissione di computer e di dispositivi mobili. Gli APT sono generalmente associati ad attacchi sponsorizzati dai governi, ma sono utilizzati anche da organizzazioni criminali e da singoli individui.
Generalmente – data la loro complessità – gli APT sono attacchi multi-stage, possono richiedere anche molto tempo per essere preparati e l'aspettativa degli attaccanti è che la compromissione non sia rilevata per molto tempo (o addirittura anni).

[1] Il concetto di Advanced Persistent Threat si riferisce al fatto che gli APT mostrano un alto livello di sofisticazione, difficile da raggiungere con strumenti automatizzati; inoltre gli attacchi utilizzano un'ampia varietà di tecniche per mantenersi offuscati e sono spesso mirati a individui specifici all'interno dell'organizzazione.

[2] https://doi.org/10.6028/NIST.SP.800-39

Le fasi che compongono un attacco APT sono le seguenti:

- **Observation/Social Engineering**: ricerca e raccolta di dati sul target dell'attacco;
- **Section**: delivery del malware che sarà utilizzato nell'attacco attraverso la tattica scelta (Phishing, Exploit Public-Facing Application, Drive-by Compromise, etc.);
- **Discovery**: dopo aver ottenuto l'accesso, gli attaccanti devono agire rapidamente per evitare il loro riconoscimento;
- **Catch & Exfiltration**: i dati riservati del target raccolti durante l'attacco sono inviati ai server dagli attaccanti. Questa fase può essere molto lunga e può contemplare l'interazione continua tra l'attaccante e l'infrastruttura target.

Un attacco basato su APT si differenzia moltissimo dagli attacchi informatici di base e possiamo considerare almeno i seguenti aspetti distintivi:

- un APT è più complesso di una generica minaccia online, in quanto la realizzazione degli strumenti impiegati e l'esecuzione dell'attacco comportano che il gruppo di attaccanti lavori a tempo pieno per realizzarla. Nel setup dell'attacco deve essere anche considerato il tempo in cui gli avversari – dopo aver trovato il primo punto di accesso all'infrastruttura target – svolgono le attività manuali necessarie a garantirne la miglior persistenza;
- gli APT sono creati per perseguire specifici obiettivi (come, ad esempio, specifiche organizzazioni o determinati settori industriali) e quindi non rappresentano una minaccia generale. Per questa caratteristica, gli APT si definiscono tailored.

Nella Figura 1 sono mostrate tutte le fasi che compongono un attacco di tipo APT:
Gli attori di Advanced Persistent Threat possono

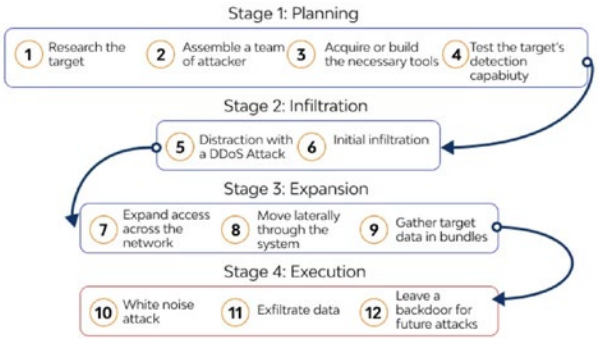


Fig. 1 - Advanced Persistent Threat (APT) Attack Lifecycle

appartenere ad una (a volte più d'una) tra le seguenti categorie:

- Terrorists
- Corporate espionage actor
- Nation-state actor
- Organized criminal actor
- Hacktivist

Le motivazioni alla base degli attacchi APT possono variare notevolmente, ma le finalità primarie di solito rientrano tra le seguenti:

- raccogliere informazioni;
- ottenere un punto di ingresso per realizzare successive fasi di un attacco o all'accesso indiretto a una società legata al target o a un suo affiliato;
- ottenere un guadagno finanziario;
- ottenere un vantaggio competitivo su altre

nazioni;

- danneggiare la reputazione di un'organizzazione;
- produrre interferenze a livello politico;
- mettere fuori uso sistemi, dispositivi o intere infrastrutture;
- condurre operazioni di Cyber Espionage (furto di proprietà intellettuali e accesso alle credenziali, finanziarie, informazioni classificate o sensibili);
- condurre operazioni di Cyber Warfare;
- controllare le attività di singoli o di gruppi di persone.

Solo nel 2016[3] il Segretario generale della NATO Jens Stoltenberg, nonostante gli attacchi di tipo APT siano già stati riconosciuti come minacce di alto livello che possono coinvolgere apparati e infrastrutture governativi o privati, riconosce il cyberspazio come dominio operativo.

Dopo l'attacco del 2015[4] alla rete elettrica dell'Ucraina, realizzato utilizzando il malware Black Energy, gli attacchi cyber sono equiparati per pericolosità a quelli fisici.

*"**We also turned our attention to cyberspace[5]. We agreed that we will recognise cyberspace as an operational domain. Just like air, sea and land. Cyber defence is part of collective defence. Most crises and conflicts today have a cyber dimension. So treating cyber as an operational domain would enable us to better protect our missions and operations.**"*

Nella conferenza stampa che si è tenuta a seguito dell'intervento, alla domanda di un giornalista riguardo all'implicazione del considerare gli attacchi cyber al pari dei "kinetic attack" rispetto all'attivazione dell'articolo 5[6] per la NATO, alla capacità di identificare gli autori e alla necessità di sviluppare capacità informatiche offensive all'interno della NATO, il Segretario Generale risponde in questi termini:

*"**We have decided that a cyber attack can trigger Article 5, meaning that a cyber attack can***

[3] https://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

[4] Va segnalato che l'attacco del 2015 alla rete elettrica dell'Ucraina non è stato il primo tra quelli più conosciuti e di alta rilevanza, in quanto già nell'aprile del 2007 era stato accertato l'attacco mirato (molto probabilmente di matrice russa) contro diverse infrastrutture governative e private in Estonia; tra questi anche l'Operation Aurora, attribuita all'Elderwood Group per conto del PLA cinese, che nel 2009 ebbe l'obiettivo principale di ottenere l'accesso (e potenzialmente modificare) i repository dei codici sorgenti di diverse società – principalmente statunitensi – del campo IT, Network Security e Internet Provider.

[5] Possiamo definire il cyberspace come "all of the computer networks in the world and everything they connect and control. It's not just the Internet [...] cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet." (da"Cyber War: The Next Threat to National Security and What to Do About It" di Clarke, Knake - 2010)

[6] "Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell'esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall'art. 51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'uso della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali", https://www.nato.int/cps/en/natohq/topics_110496.htm

trigger collective defence, because we regard cyber attacks as something that can cause a lot of damage and can be very dangerous. *As I said, it's hard to imagine a conflict without a cyber dimension. So, yes, cyber can trigger Article 5, but the same time I think it's also important to understand that cyber is not something that always triggers Article 5. […] What we do is defensive, but it is important to develop our defensive capabilities, and it* ***is important to be able to attribute because one of the challenges when we speak about cyber is that it's not always easy to tell exactly who is attacking you****. So everything related to attribution is one of the issues which are high on our agenda and we are developing capabilities to be better able to attribute different kinds of cyber attacks."*

Sebbene la decisione di inserire anche il cyberspazio come dominio operativo sia stata fondamentale, le tempistiche della NATO nel riconoscere tali attacchi come altamente dannosi possono apparire faziosi se si pensa che, nei primi mesi del 2010, gli esperti della National Security Agency (NSA), in collaborazione con l'Israel Defense Force (IDF), crearono il malware Stuxnet[8].

Tale malware fu in grado di agire sui PLC Siemens Simatic S7-300 adibiti al controllo delle centrifughe utilizzate per produrre l'uranio arricchito. Si stima che l'attacco potrebbe aver messo fuori uso almeno 1.000 delle 5.000 centrifughe iraniane, causando un ritardo di alcuni anni nel programma nucleare iraniano.

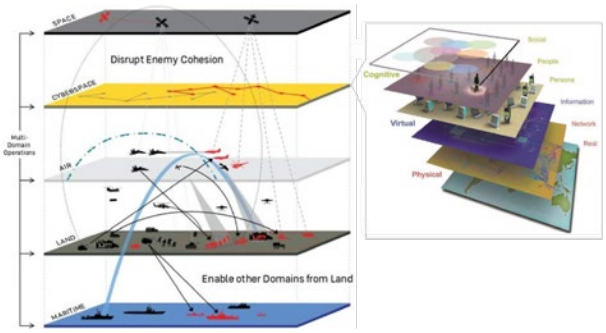


Fig. 2 - Advanced Persistent Threat (APT) Attack Lifecycle

Naturalmente, sebbene in misura e con modalità diverse, i governi delegano parte delle attività cyber di tipo offensivo a diversi "stakeholder" che possono essere aziende, freelance o università.

L'attuale conflitto russo-ucraino sta mostrando, nella maniera più ampia possibile, quanti soggetti possano essere disposti sullo scacchiere del cyber warfare: gruppi governativi che si avvalgono di aziende private per la progettazione e sviluppo di strumenti offensivi, ransomware gang e gruppi cybercrime che collaborano con attori governativi e creano per loro uno smokescreen, gruppi (o freelance) che supportano le fasi iniziali di un attacco, quali gli Initial Access Broker (IAB)[8].

Tra le figure non governative generalmente utilizzate nello svolgimento di un attacco vi è quella dei cyber proxy.

[7] Per approfondire tecnicamente l'attacco Stuxnet si consiglia l'articolo "W32.Stuxnet Dossier" reperibile al link https://www.01net.it/wp-content/uploads/sites/14/2014/10/symantec_stuxnet_dossier.pdf, mentre per un approfondimento sugli effetti economici e politici dell'attacco si rimanda all'articolo "Hotspot Analysis: Stuxnet" reperibile al link https://www.researchgate.net/publication/323199431_Stuxnet

[8] Per un approfondimento sugli Initial Access Broker si può consultare il report "Initial Access Brokers Are Key to Rise in Ransomware Attacks" https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf e il post https://www.cyfirma.com/outofband/inside-the-world-of-initial-access-broker-iab-insights-and-trends

Questi[9] conducono o contribuiscono direttamente nelle Offensive Cyber Operation che possono avere una varietà di effetti e di finalità. Oltre ad offrire la plausibile negabilità del coinvolgimento di un governo in un attacco informatico, l'utilizzo dei cyber proxy permette di incrementare la complessità/sofisticazione di un attacco, in quanto questi dispongono generalmente di elevate capability.

La Figura 3 mostra una gerarchia distinta su sei livelli (I = livello più basso, VI = livello più alto) delle minacce informatiche definita dello US Defense Science Board
Il grafico riassume le distinzioni fatte confrontando le capacità degli attori statali e non statali: i cyber proxy che conducono operazioni informatiche offensive hanno spaziato dal livello I al IV. I proxy possono anche contribuire alle operazioni informatiche offensive condotte da attori governativi di livello V e VI (quali Stati Uniti, Russia e Cina).

Il Defense Science Board[10] formula due osservazioni particolarmente importanti al riguardo. In primo luogo, "gli attori di livello superiore useranno i metodi e le tecniche al livello più basso necessario per raggiungere i loro obiettivi... per evitare di esporre le loro tecniche più sofisticate" e, in secondo luogo, "gli Stati potrebbero impiegare attori non statali come delegati (proxy). In tali situazioni, le organizzazioni di livello intermedio ottengono l'accesso a capacità di livello superiore".

Prima di indicare i governi a cui risulta associabile il numero più alto di gruppi APT, è bene fare almeno le seguenti precisazioni:

- la conoscenza dei gruppi APT legati ai vari governi è sicuramente incompleta, ovvero l'attribution potrebbe essere errata o ancora in corso di approfondimento. La difficoltà prin-

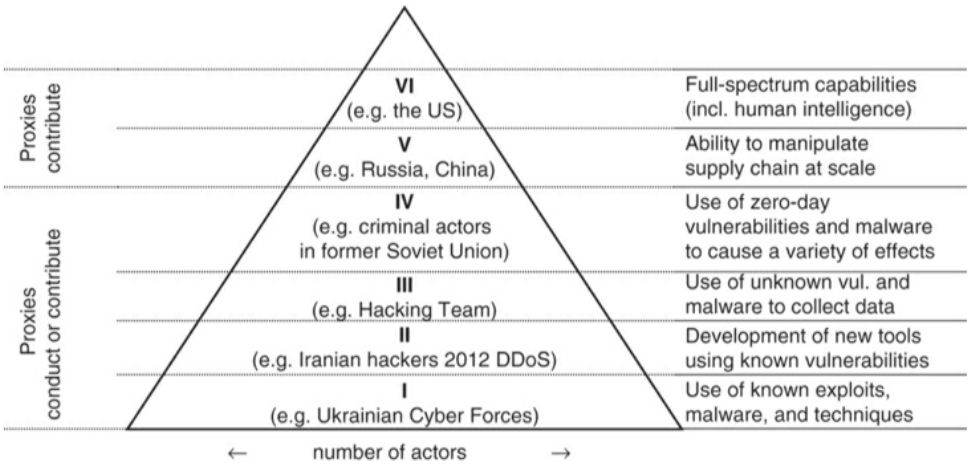


Fig. 3 - Collocazione dei cyber proxy nella tassonomia delle minacce

[9] Per approfondire il tema si possono consultare gli articoli reperibili ai link https://www.lawfareblog.com/states-proxies-cyber-operations

[10] US Defense Science Board, Resilient Military Systems and the Advanced Cyber Threat (2013)

cipale deriva dall'assenza di una completa conoscenza e associazione tra governi e APT e occorre considerare pure la fase di attribuzione è svolta mentre sono in corso continui cambiamenti politici e le tecniche di attacco diventano più avanzate.

- quand'anche un governo non abbia le risorse per sostenere le attività di gruppi APT, non vuol dire che questo non possa disporre di strumenti che – forniti ad operatori legati al governo e opportunamente addestrati – realizzino attività compatibili con quelle svolte da un gruppo APT. A titolo di esempio si può citare lo strumento Pegasus, prodotto dall'azienda israeliana NSO Group e introdotto nel mercato globale nel 2011, poi acquistato e utilizzato – per fini molto differenti – da decine di governi di tutto il mondo.

Sin da quando i governi hanno iniziato a utilizzare i cyber threat actor per incrementare la loro potenza offensiva, alcuni tra questi si sono distinti per un loro uso estensivo[11]. Tra gli Stati che devono principalmente essere presi in considerazione sono Russia, Cina, Nord Corea e Iran, visto che si stima che il 77% delle attività state-sponsored siano a loro associabili[12] [13] .

Naturalmente, di seguito saranno evidenziate le caratteristiche dei threat actor di questi Stati senza approcciare le loro attività in una visione complessiva e senza, quindi, esaminare eventuali motivazioni politiche.

Come mostrato nelle figure seguenti, a partire dal 2016 la numerosità degli attacchi realizzati dai threat actor di questi quattro governi (a volte indicati come big-four tra gli Stati ostili) è sempre cresciuta e la vittimologia è anche mutata al variare degli scenari e delle condizioni socio-politiche:
Nella Figura 4 si riporta la stima, aggiornata al 2022, delle CybOp eseguiti dai diversi gruppi APT di questi quattro governi:

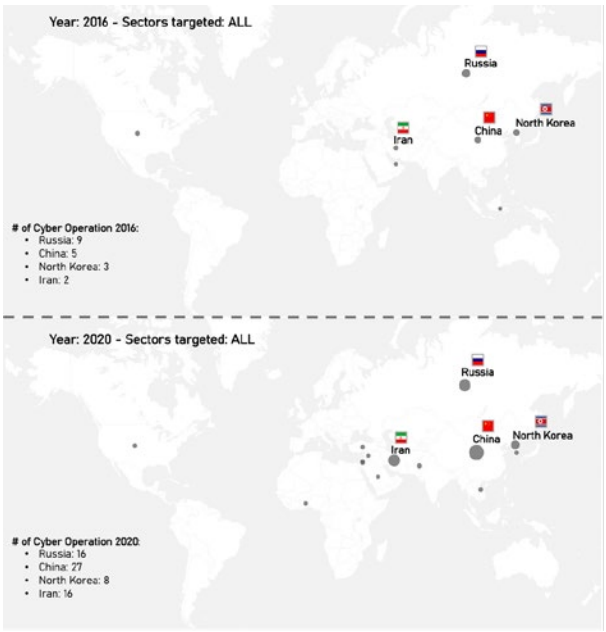


Fig. 4 – Incremento delle Cyber Operation tra il 2016 e il 2020 da parte di Russia, Cina, Nord Corea e Iran

Sebbene l'elevato impiego di operazioni cyber offensive non sia la sola caratteristica comune ai quattro governi sopra indicati, in diverse situazioni

[11] L'articolo "Cyber Capabilities and National Power: A Net Assessment" analizza le capacità cyber di 15 governi ed è reperibile al link https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power

[12] https://www.cfr.org/cyber-operations

[13] Per maggiori dettagli: https://www.cisa.gov/russia

Fig. 5 – Stima delle Cyber Operation da parte di Russia, Cina, Nord Corea e Iran eseguite nel 2022

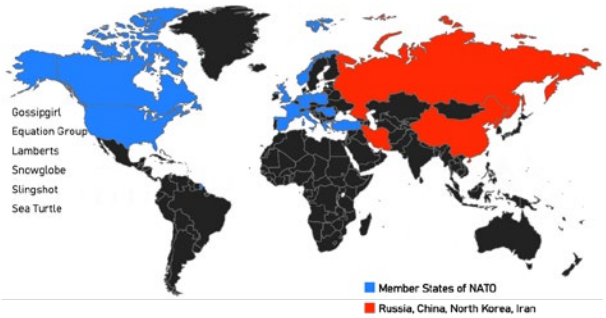


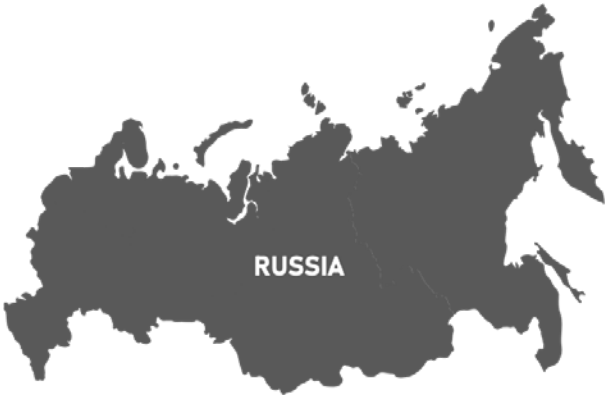
Fig. 6 – Suddivisione tra gli stati della coalizione NATO e gli stati China, Russia, Iran e North Korea

(vedi ad esempio il conflitto russo-ucraino in cui sono apertamente schierati con la Russia) essi rappresentano anche una coalizione (con sfaccettature sicuramente diverse al proprio interno) che si oppone alle politiche della NATO.

Su questo aspetto sono disponibili molti report dell'Unione Europea, del Regno Unito, degli Stati Uniti[14] e del Canada, che descrivono le minacce (anche da un punto di vista multi-domain) rappresentate da questi Paesi[15].

Nella Figura 6 è mostrata una mappa degli Stati che appartengono alle due coalizioni ed è riportata la lista dei principali threat actor legati a governi NATO[16]:

Di seguito, per ciascuno dei quattro Stati prima indicati, si riporta una breve sintesi delle caratteristiche principali e motivazioni dei threat actor a loro legati:



Motivazioni Principali degli APT russi:

- Espionage
- Hybrid Warfare

Principali attori attivi nel 2022:

- APT28 (alias Sofacy e Fancy Bear)
- APT29 (alias Cozy Bear e Dukes)

[14] Annual Threat Assessment of the U.S. Intelligence Community del 2022 (https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community)

[15] "Multi-Domain Integration in Defence - Conceptual Approaches and Lessons from Russia, China, Iran and North Korea" (https://www.rand.org/pubs/research_reports/RRA528-1.html)

[16] La lista dei threat actor è stata acquisita da "APT Groups and Operations", consultabile al link https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pub?output=xlsx

- Callisto
- Gamaredon
- The Dukes
- Sandworm

Le avanzate capacità informatiche della Russia sono principalmente dirette a supportare gli obiettivi della sua politica estera per contrastare l'influenza occidentale in patria e a promuovere la sua posizione di leader a livello globale. La Russia considera l'Occidente, in particolare l'alleanza dell'Organizzazione del Trattato del Nord Atlantico (NATO), come una minaccia continua e centrale per gli interessi nazionali della Federazione Russa.

Motivazioni Principali degli APT cinesi:

- Cyber Espionage
- Intellectual Property
- Theft

Principali attori attivi nel 2022:

- Mustang Panda
- Goblin Pand
- MirrorFace
- LuckyMouse
- APT10
- APT41

I gruppi APT sponsorizzati dal governo cinese rappresentano – nell'intero panorama internazionale – alcune delle minacce più prolifiche e ricche di risorse. Il governo di Pechino utilizza le sue capacità informatiche, tipicamente gestite o incaricate dal Ministero della Sicurezza di Stato (MSS) o dall'Esercito popolare di liberazione (PLA) per raccogliere informazioni politiche e militari, svolgere attività di cyber espionage e spiare individui di interesse.

Negli ultimi anni il governo cinese ha intrapreso iniziative legate alla modernizzazione e innovazione del Paese e, in linea con questa finalità, sono state impiegate le sue capacità informatiche offensive. Inoltre, negli ultimi dodici mesi c'è stata una tendenza continua degli APT cinesi a condurre operazioni che siano difficili da ricondurre a loro e rivolte contro una gamma più selezionata di obiettivi. Tuttavia questi attacchi sono spesso condotti per apparire come opportunistici, ad esempio utilizzando tecniche più spesso impiegate dai gruppi cyber criminali come, ad esempio, le ransomware gang. Va sottolineato che, tra tutti i casi di spionaggio gestiti dal Dipartimento di Giustizia degli U.S.A. tra il 2011 ed il 2018, si stima che il 90% abbia coinvolto attori connessi alla Cina. Il cyber espionage posto in essere dalla Cina è fonte di preoccupazione anche per numerose agenzie di intelligence europee.

Motivazioni Principali degli APT nordcoreani:

- Financial Gain
- Espionage

Principali attori attivi nel 2022:

- Konni
- Lazarus
- Andariel
- APT37

Per la maggior parte dei gruppi APT nordcoreani, l'utilizzo della criminalità rimane la principale priorità per fornire reddito allo stato e rafforzare il proprio apparato militare. La necessità di fare cassa attraverso attacchi informatici è legata principalmente alle sanzioni delle Nazioni Unite (ONU) imposte alla Corea del Nord a causa del continuo impegno in un programma di armi nucleari. Inoltre, la crisi economica si è aggravata con l'evento della pandemia di COVID-19 e ha isolato la RPDC dalla Cina, il suo partner commerciale più vicino. Gli obiettivi prima esposti sono ottenuti dagli APT nordcoreani attraverso operazioni di cyber spionaggio. In aggiunta a queste finalità primarie, gli APT nordcoreani hanno anche agito nella raccolta di informazioni di intelligence nell'ambito nucleare e dello spionaggio diplomatico, presumibilmente al fine di mantenere l'attuale regime al potere.

Motivazioni Principali degli APT iraniani:

- Espionage
- Monitoring dissidents
- Sabotage

Principali attori attivi nel 2022:

- APT34 (alias Helix kitten e OilRig)
- APT35
- MuddyWater
- POLONIUM
- Cutting Kitten
- APT33
- APT39

Le attività informatiche offensive dell'Iran,quasi esclusivamente supervisionate dalle Islamic Revolutionary Guard Corps (IRGC), sono commissionate a diverse strutture che possono essere completamente legate al governo, ad organizzazioni proxy come pure ad appaltatori indipendenti che mescolano lavoro di sicurezza, frode criminale e sviluppo di software.

Sebbene i funzionari statunitensi abbiano ipotizzato che Teheran abbia ricevuto assistenza tecnica da paesi come la Russia e la Corea del Nord, il livello di sofisticazione è commisurato alle pratiche consolidate delle comunità di hacker amatoriali.

L'attività dei gruppi APT iraniani è rimasta, nel complesso, concentrata su obiettivi tradizionali quali Israele, alcuni Paesi del Medio Oriente e i dissidenti in patria e all'estero tra la sua comunità della diaspora. In particolare i settori della difesa, delle telecomunicazioni e relativi alla tecnologia dell'informazione sono candidati ad essere, nel prossimo futuro, i probabili target dei gruppi connessi al regime iraniano, soprattutto con riferimento a entità pubbliche e private nell'area MENA (Medio Oriente e Nord Africa) e negli Stati Uniti. Una caratteristica di alcuni gruppi APT iraniani è l'impiego di tecniche di pseudo-ransomware e di tunneling in un'ampia varietà di attacchi.

Nell'ipotesi che un'azienda/organizzazione sia un target per più di un gruppo APT, una questione che ci si può porre è come dare una priorità sull'adeguamento ad un loro eventuale attacco. Chiaramente la questione vale indipendentemente che gli attaccanti siano gruppi APT, cybercrime, hacktivist, etc. Dunque, la necessità di ogni organizzazione è di disporre di una metodologia di Threat Actor Assessment.

Sebbene ogni organizzazione possa definirne una propria, possono essere utilizzate delle metodologie già disponibili che si prestano anche ad essere personalizzate.

Alla base di ciascuna metodologia occorre che si esplicitino due elementi fondamentali: una Threat Matrix e una categorizzazione delle tecniche di attacco potenzialmente impiegate dagli avversari.

Per avere una categorizzazione delle tecniche di attacco, generalmente si dovrebbe prediligere la creazione di un Cyber Threat Landscape[17] specifico per il settore industriale in cui opera l'organizzazione e, opzionalmente, si possono utilizzare strumenti di Adversary Emulation dotati di una Threat Actor Profile Knowledge-Base.

Un esempio di Data Model su cui basare il Cyber Threat Landscape è quello proposto dal CERT-EU[18] che mette in relazione i threat actor (con le informazioni ad essi connesse), le TTP (Tactics, Techniques & Procedure)[19] e i settori/target.

[17] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

[18] https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cert-eu-presentation

[19] Le TTP descrivono come un threat actor tenta di raggiungere l'obiettivo desiderato. Le Tattiche descrivono l'obiettivo delle azioni eseguite da un attaccante. Le Tecniche forniscono una descrizione più dettagliata delle azioni stesse, mentre le Procedure dettagliano in maniera approfondita le istruzioni che l'attaccante sta utilizzando per implementare una tecnica specifica.

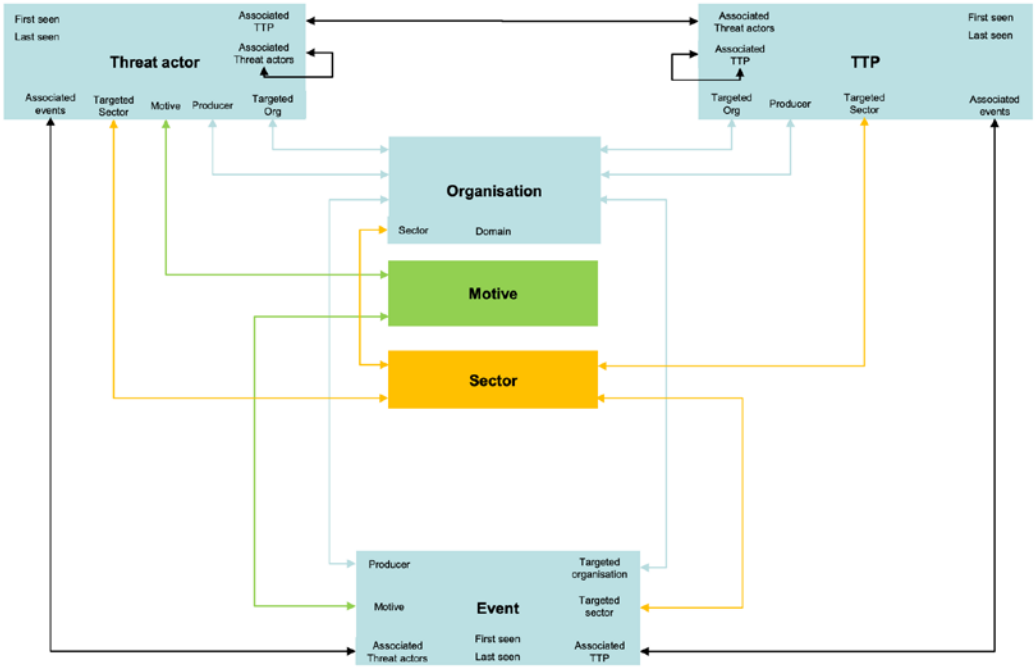


Fig. 7 - Esempio di Data Model

A titolo esemplificativo, tra le varie metodologie (o strumenti) che possono essere utilizzate si segnalano le seguenti:

- il Threat Assessment and Remediation Analysis (TARA)[20] sviluppato dal MITRE;
- le metodologie basate sui cosiddetti FAIR (Factor Analysis of Information Risk) Factors[21]. In Figura 2 è mostrata una esemplificazione di Threat Matrix basata sulle categorie FAIR;
- la metodologia di Threat Actor Assessment basata su Threat Box[22], che si pone l'obiettivo di valutare intenzioni e capacità e produrre un'unica rappresentazione grafica di immediata comprensione.

Al fine di offrire un esempio concreto di Threat Actor Assessment si è creata una rappresentazione utilizzando Threat Box[23]. Per semplicità, si è sviluppato l'esempio prendendo in considerazione solo un threat actor tra tutti quelli sopra citati e legati – rispettivamente – alla Russia, alla Cina, all'Iran e alla Corea del Nord. In particolare, sono stati scelti i gruppi APT28, APT33, APT37 e APT41.

Nella Tabella 1 sono riportati i target di questi gruppi e nella Figura 8 sono mostrate in maniera comparata le principali tecniche di attacco (espresse in termini di Tactics & Techniques della MITRE ATT&CK ver. 12).

[20] https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara

[21] Il modello FAIR è descritto dal FAIR Institute https://www.fairinstitute.org/what-is-fair, mentre per un esempio di applicazione al Threat Actor Assessment si può consultare https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats#12

[22] https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11

[23] Per l'esempio riportato si è utilizzato il progetto tbat, disponibile al link https://tbat.app

Threat Actor	Suspected Attribution	Target Sectors
APT28	Russia	The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organization (NATO) and other European security organizations and defense firms
APT41	China	Healthcare, telecoms, and the high-tech sector, and have historically included stealing intellectual property, higher education, travel services, and news/media firms. Their cybercrime intrusions are most apparent among video game industry targeting (including the manipulation of virtual currencies) and attempted deployment of ransomware.
APT33	Iran	Aerospace, energy
APT37	North Korea	Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

Tab. 1 – Settori target dei gruppi APT28, APT33, APT37 e APT41

Figure 2—Threat Metrics by FAIR Category

FAIR Category	Evidence-Based Threat Category	Metric
Contact frequency	Past incident time series	Incident count within a period
		Trend change in the incident count
		Proportion of attacks by the actor over total attacks of the same type
		Trend change in the proportion of attacks by the actor over total attacks of the same type
	Past victims' geosectoral profile	Average match ratio of past victims' region within a period
		Trend change in the average match ratio of past victims' region within a period
		Average match ratio of past victims' country political alliance
		Average match ratio of past victims' country development level
		Average match ratio of past victims' country language
		Average match ratio of past victims' sector
		Trend change in the match ratio of past victims' sector
Probability of action	Threat actor's objective	Match ratio of an objective
		Trend change in the match ratio of the objective
	Threat actor's commitment	Days since the campaign started
		Days since the last attack
		Average number of days between attempts within a period
		Trend change in number of days between attempts within a period
Threat capability	Threat actor's skills	Sophistication level within a period
		Trend change in sophistication level
		ATT&CK coverage
		Trend change in ATT&CK coverage
		Efficiency
		Trend change in efficiency
Resistance strength	Detection capabilities	Campaign analysis: average kill chain detection phase
		Campaign synthesis: kill chain detection coverage
		DETT&CT overall coverage
		DETT&CT campaign coverage
	Exploitation surface	General exploitation surface
		Campaign exploitation surface
	Postdetection capabilities	Average investigation time
		Average response time

Fig. 8 – Threat Metric basata sulle categorie FAIR

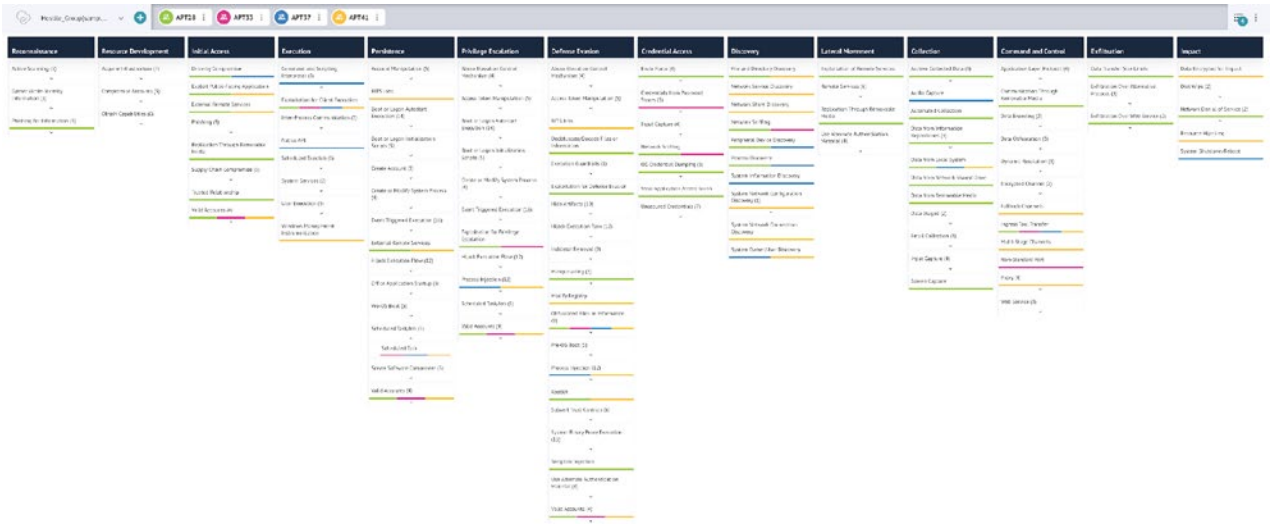


Fig. 9 – Matrice ATT&CK con le TTP utilizzate dai gruppi APT28, APT33, APT37 e APT41

Sebbene col progetto tbat si possano ottenere automaticamente le Tactics & Techniques, si è preferito esplicitarle separatamente per evidenziare come gruppi APT diversi, che vogliono ottenere obiettivi distinti, utilizzeranno tecniche di attacco solo parzialmente sovrapponibili.

Per la creazione del report è necessario fornire – per ciascun threat actor – alcune informazioni di base, mentre quelle relative alle tecniche di attacco impiegate sono già presenti per i principali avversari.

La prima domanda è legata alla tipologia/categoria di attacchi realizzata dagli avversari.

- Espionage: attacchi che incidono sulla riservatezza dei dati o dei sistemi;
- Destructive: attacchi che hanno un impatto sull'integrità dei dati o dei sistemi;
- Disruptive: attacchi che incidono sulla disponibilità di dati o sistemi;
- Cyber-Crime: attacchi finalizzati al profitto finanziario a breve termine.

Gli altri elementi che si chiede di valutare sono relativi a:

- Intent & Willingness, in cui si identificano le motivazioni (Intent) per cui un threat actor vuole prendere di mira un'organizzazione e quali sono i vincoli (Willingness) che possono influire sull'intento dell'attaccante;
- Capabilities & Novelty, in cui si valutano le reali possibilità (Capabilities) di eseguire un certo tipo di attacco e se l'attaccante dispone di capacità di realizzare tecniche avanzate/innovative (Novelty).

Nella tabella seguente si riporta la valorizzazione delle informazioni sopra riportate rispetto ai gruppi scelti:

#	Group Identifier	Intentions	Intent	Willingness	Capability	Novelty
1	APT28	Espionage, Cyber-crime	3	-2	5	0
2	APT33	Espionage, Cyber-crime	2	0	3	-1
3	APT37	Espionage	3	0	5	0
4	APT41	Espionage, Cyber-crime	1	0	5	0

Tab. 2 – Valutazione degli elementi Intentions, Intent & Willingness e Capabilities & Novelty

Sulla base di queste informazioni e sulle tecniche di attacco impiegate dagli attori presi in considerazione, è stato prodotto il seguente report:

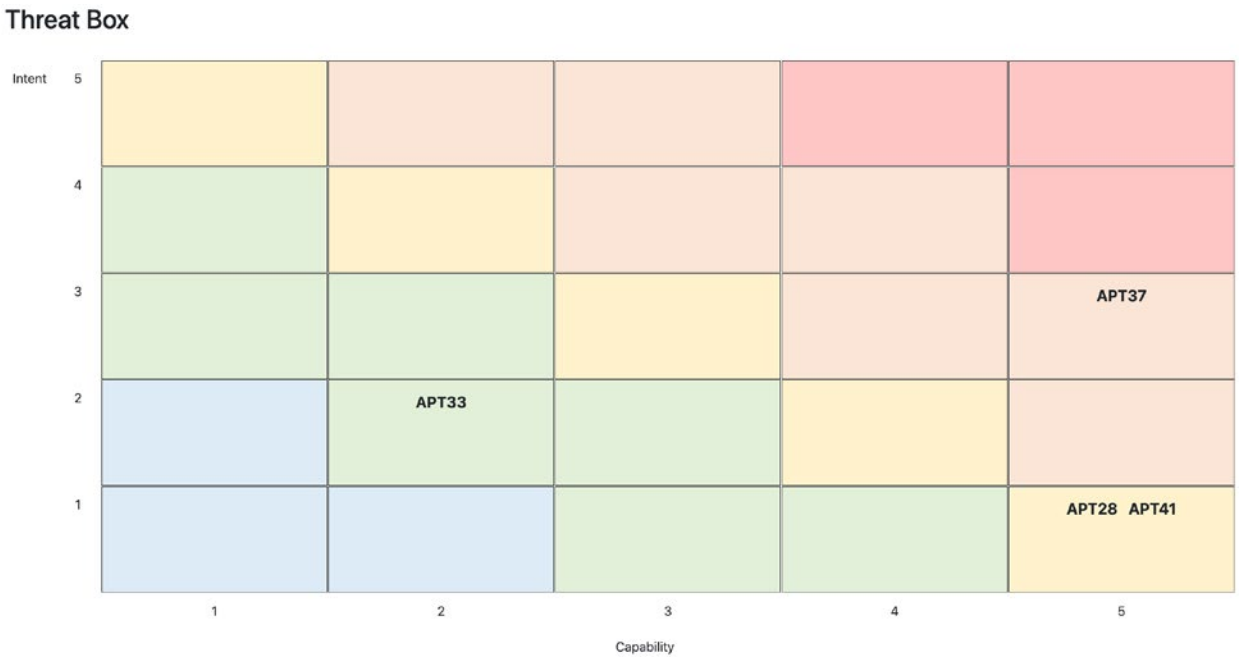


Fig. 9 – Report prodotto dal progetto tbat

Francesco Schifilliti, *Consulente in Cyber Security & Threat Intelligence*

BIOGRAFIA

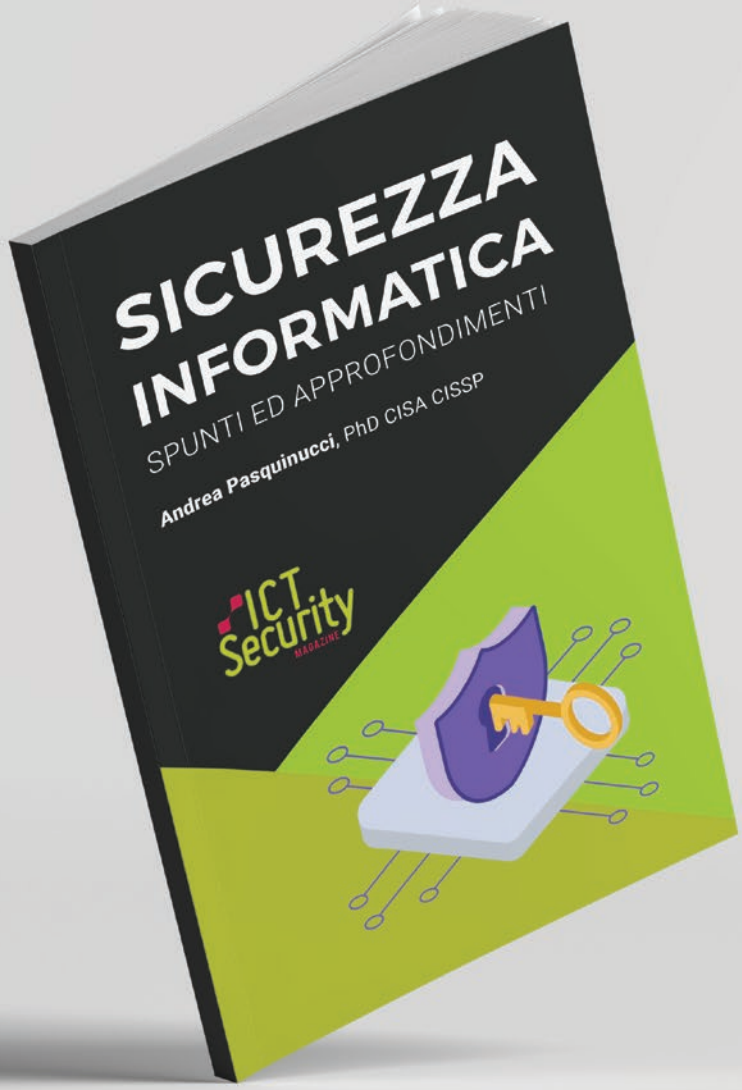
Francesco Schifilliti

Esperto in sicurezza delle informazioni, *digital forensic* e *cyber threat intelligence* per grandi aziende. È stato il *Practice Manager* di F*orensic Technology & Discovery Services* (FTDS) in Fraud Investigation & Dispute Services (EY). Ricercatore nel campo di *Malware* e *Memory Analysis*, *Structured Analytic Procedures* (SAT), OSINT, *Intelligence Investigation Techniques, Incident Responding Techniques* e *Cyber Threat Intelligence*. Laureato in Informatica presso l'Università degli Studi di Catania, è docente in corsi e master in *digital forensics* e *malware forensics*.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

Threat actors made in China

Con il processo di riforma iniziato negli anni '70 e '80 da Deng Xiaoping, la Cina ha compiuto progressivamente una trasformazione radicale che ha portato il Paese verso un futuro di grande crescita economica e di sviluppo industriale. Internet arriva in Cina negli anni '90 e il governo di Pechino intravede immediatamente le sue grandi potenzialità, tanto da concentrare impressionanti risorse sullo sviluppo delle infrastrutture di telecomunicazione e tecnologiche del Paese.

Il 2015 è un anno molto particolare per la Cina: è l'anno in cui la Cina ha mostrato al mondo il suo piano.

IL PIANO

Rilasciato nel 2015, "Made in China 2025" è il piano decennale del governo cinese per sviluppare rapidamente una politica industriale mirata a rendere la Cina dominante nella produzione high-tech globale, in particolare dieci industrie high-tech, tra cui: auto elettriche, tecnologie dell'informazione (IT) e delle telecomunicazioni di prossima generazione, robotica avanzata, intelligenza artificiale, ingegneria aerospaziale, biomedicina avanzata e nuovi materiali sintetici. Se consideriamo ciò che è scritto nel piano industriale del governo, risulta evidente che l'obiettivo strategico di Pechino è ridurre la dipendenza della Cina dalla tecnologia straniera e promuovere i produttori high-tech cinesi per conquistare la leadership tecnologica mondiale nel modo più rapido possibile. Il piano prevede un forte investimento del governo in programmi per aumentare la posizione competitiva delle aziende cinesi sul mercato globale; e sicuramente anche l'impiego di operazioni di cyber spionaggio risulta determinante nel velocizzare il raggiungimento di tale scopo.

Lo spionaggio di segreti industriali e commerciali mira principalmente ad ottenere informazioni su come realizzare nuove tecnologie, processi industriali e commerciali in tempi brevi e con risorse proprie, saltando completamente la catena del valore, senza quindi dover investire in risorse economiche e umane necessarie a inventarle e progettarle: una pratica che nei fatti la Cina sta sempre più dimostrando di attuare, in particolar modo, attraverso il cyber spionaggio.

LA CINA ENTRA PUBBLICAMENTE NEI RADAR DELLE AGENZIE

Il 6 luglio 2022 il direttore dell'FBI Christopher Wray e il capo dell'MI5 Ken McCallum, in una conferenza congiunta senza precedenti svoltasi nella sede dell'MI5 a Thames House (Londra), hanno evidenziato come le attività di contrasto di entrambi i governi, inglese e statunitense, alle azioni di spionaggio del governo cinese siano più che raddoppiate negli ultimi tre anni.

Wray ha affermato in particolare che la Cina ha sviluppato il più grande programma di cyber spionaggio per rubare know-how mai realizzato da qualsiasi altro paese; e McCallum ha reso note attività di contrasto a diverse cyber-minacce cinesi, come quella che nel maggio 2022 l'MI5 ha bloccato contro il settore aerospaziale.

Wray ha inoltre affermato che la Cina sta traendo

molte informazioni dal conflitto tra Russia e Ucraina, dalla sperimentazione di nuove tecniche di cyber spionaggio alle strategie per evitare qualsiasi tipo di sanzione nel caso invadesse Taiwan: evento che causerebbe una crisi economica molto più grave di quella avuta con la produzione dei chip nel 2022, sia per l'acquisizione indebita di know-how tecnologico sia perché causerebbe l'interruzione delle catene di approvvigionamento e gli investimenti occidentali in Cina verrebbero così trasformati in "ostaggi".

Wray ha infine affermato che il governo cinese "rappresenta la più grande minaccia a lungo termine" alla sicurezza economica e nazionale per il Regno Unito, gli USA e gli alleati europei.

Nei mesi successivi alla conferenza gli Stati Uniti hanno cominciato a rallentare i progressi della Cina nell'industria chiave dei semiconduttori, vietando ai cittadini statunitensi di lavorare per aziende di chip cinesi, incrementando i controlli sulle esportazioni nonché richiedendo licenze e autorizzazioni alle aziende che esportano chip in Cina e che utilizzano strumenti o software statunitensi, suscitando notevoli malumori da parte del governo cinese.

La particolarità di questa conferenza – oltre al fatto di essere stata indetta per la prima volta congiuntamente da Stati Uniti e Regno Unito – è di fatto un ultimatum ufficiale per richiamare la Cina all'accordo del 2015 (fatto proprio in concomitanza della presentazione del piano industriale cinese), in cui Stati Uniti e Cina si impegnavano comunemente a non effettuare "furti informatici di proprietà intellettuale, inclusi segreti commerciali o altre informazioni commerciali riservate per vantaggio commerciale". Accordo che, secondo gli Stati Uniti, ebbe fin da subito un risultato blando, in quanto gli attacchi di cyber spionaggio cinesi diminuirono in termini quantitativi, ma proseguirono invece quelli più sofisticati.

CYBER ESPIONAGE ESCALATION

Da diversi anni ormai sempre più campagne di cyber spionaggio sono attribuite alla Cina, che sembra continuare le proprie operazioni in maniera sempre più "disinvolta". E mentre l'abbattimento del sospetto pallone spia cinese, il 4 febbraio 2023, nello spazio aereo canadese, rimane ancora un mistero da svelare, l'India ha cautelativamente attivato il 6 marzo 2023 un protocollo operativo militare per abbattere ad alta quota eventuali palloni spia cinesi che dovessero sorvolare i propri cieli.

Un mese prima, nel gennaio 2023, Zheng Xiaoqing, un ex dipendente del conglomerato energetico General Electric Power (GE), è stato condannato dalla Corte di Giustizia americana a due anni di carcere per spionaggio di segreti industriali: Zheng inviava sui social foto di paesaggi naturalistici che in realtà contenevano all'interno file riservati rubati alla GE, attraverso una tecnica denominata steganografia[1].

[1] Steganografia: evoluzione digitale dell'antica arte di occultare le informazioni, da strumento di riservatezza a strumento di offesa per dispositivi mobili, Francesco Arruzzoli, settembre 2017 (https://www.ictsecuritymagazine.com/articoli/steganografia-evoluzione-digitale-dellantica-arte-occultare-le-informazioni-strumento-riservatezza-strumento-offesa-dispositivi-mobili/)

Basta effettivamente verificare la cronaca degli ultimi anni, relativa alle operazioni di cyber spionaggio, per constatare la massiccia attività che la Cina sta sviluppando non solo verso gli Stati Uniti (dove l'attribuzione arriva al 90% dei casi totali) ma anche verso altri Paesi.

Ovviamente il settore delle telecomunicazioni risulta essere particolarmente esposto alle attenzioni delle campagne di cyber spionaggio cinesi, sia come target da colpire sia come vettore per le loro attività di spionaggio. A titolo di esempio vale la pena citare il caso del malware MESSAGETAP, sviluppato nel 2019 dal gruppo di spionaggio Wicked Panda (APT41), sponsorizzato dallo Stato cinese, che monitorava il traffico globale di messaggi SMS selezionando specifiche parole chiave, numeri di telefono e IMSI (International Mobile Subscriber Identity), relativamente a target operanti in settori come: difesa, governativo, energia, finanza, trasporti.

SPIONAGGIO ELEVATO A SISTEMA

Un errore da non commettere è considerare il modello di spionaggio cinese simile a quello dei governi occidentali. La cultura dello spionaggio in Cina ha origini antichissime, si ritrova nella dottrina di Confucio e negli scritti di Sun Tzu. Lo spionaggio è parte del sistema sociale cinese. Ogni cittadino cinese è tenuto a mantenere riservate le informazioni sulla propria attività lavorativa e contestualmente educato a riferire qualsiasi informazione possa essere di interesse per il governo di Pechino; e, nonostante i meccanismi di funzionamento dei servizi segreti cinesi siano noti, rimane ancora incomprensibile come una tale mole di informazioni fornita da miliardi di fonti possa essere vagliata e classificata.

Ancor prima dell'ambizioso piano "Made in China 2015", da oltre 50 anni l'autoritario governo della Repubblica Popolare Cinese ha fortemente investito nello sviluppo delle tecnologie digitali connesse ad Internet, sviluppo che non ha mai rallentato e che ha prodotto una capacità di spiare e applicare una sorveglianza di massa sempre maggiore, che oggi risulta tra le più avanzate del mondo.

Analizzando il tasso di penetrazione della connettività Internet sulle popolazioni degli Stati, notiamo che ad oggi la Cina, nonostante abbia un tasso del 64.1% – di molto inferiore a quello di altri Stati, come ad es. il Nord America con il 93.4% o l'Europa con l'88.4% (fonte Atlas VPN) – con il suo miliardo di utenti in rete è al primo posto in termini di utenti connessi ad Internet, seguita dall'India e con notevole distacco dall'Europa e dagli USA.

L'e-commerce nel Paese ha raggiunto un livello di maturità superiore a quello italiano e degli Stati europei. La sua politica autoritaria permette di controllare l'immenso mercato online da oltre 1 miliardo di persone: lo fa addirittura piegando i "modus operandi" dei mercati americani e occidentali, comprese le "Big Tech" GAFA (acronimo di Google, Apple, Facebook e Amazon), alle regole imposte dal governo di Pechino. Ad es. nel 2019 Google, pur di poter essere presente sul territorio cinese, è stato costretto a sviluppare una versione riveduta e corretta del suo motore di ricerca (progetto Dragonfly) secondo i voleri del governo cinese.

Ma il governo di Pechino è andato oltre, svilup-

pando i suoi "Gafa" sotto l'acronimo di BAT (Baidu, Alibaba, Tencent). Per avere successo e competere nel mercato cinese si deve utilizzare il motore di ricerca Baidu, primo motore di ricerca in Cina e terzo tra i più usati nel mondo. Baidu è molto di più di un semplice motore di ricerca: è un'enorme realtà tecnologica specializzata in servizi e prodotti, che sta sempre più utilizzando l'intelligenza artificiale nelle proprie soluzioni, diventando di fatto una delle più grandi società mondiali di Internet e intelligenza artificiale.

Alibaba è una piattaforma che opera nel segmento dell'e-commerce, l'equivalente cinese di Amazon; mentre Tencent è il gruppo cinese che, tra le sue varie attività, ha sviluppato e gestisce app di messaggistica e comunicazione come QQ e WeChat, una piattaforma di instant messaging che unisce al suo interno funzioni per lo shopping, prenotazioni, pagamenti digitali, richiesta documenti, etc., estremamente più evoluta dell'americana WhatsApp o Messenger (di proprietà di Meta).

BAT rappresenta uno strumento di cyber spionaggio multifunzionale efficientissimo e sotto il completo controllo di Pechino, in grado di spiare tanto i cittadini cinesi quanto le attività delle aziende estere che commerciano con la Cina e di bloccare qualsiasi informazioni vada contro il pensiero del governo cinese.

La crescita del potere di mercato globale delle società tecnologiche cinesi attraverso le politiche di finanziamento del governo si trasforma in un vantaggio tecnologico anche a grazie ai prezzi particolarmente accessibili sul mercato estero; inoltre, l'applicazione di una politica interna preferenziale nel trattamento dei fornitori nazionali permette il controllo del mercato interno (oltre il 75%) e imbattibili economie di scala. L'influenza cinese nel mercato globale delle tecnologie è cresciuta anche nelle organizzazioni per la normazione come ad es. ITU, 3G Partnership Project, etc. permettendogli di ricoprire, attraverso i suoi rappresentanti, posizioni decisionali chiave.

QUANDO L'ALLIEVO SUPERA IL MAESTRO

E se l'ex NSA Edward Snowden, nel 2019, aveva fatto delle rivelazioni riguardo le piattaforme social come Facebook e Instagram che spiavano gli utenti, anche la Cina sta dimostrando le sue capacità di spionaggio pervasivo di massa ben oltre i suoi confini, utilizzando sofisticate tecnologie di spionaggio cognitivo: in questo senso, uno dei migliori strumenti di "story telling" è senza dubbio TikTok.

Nel 2016 la società cinese ByteDance sviluppa l'app Douyin, una piattaforma social, per gli utenti cinesi. L'anno seguente l'app cambia nome in TikTok e la ByteDance acquista l'americana Musical.ly per entrare nel mercato americano, migrando così tutti gli account di Musical.ly su TikTok. L'app di TikTok ha la medesima versione software sia in Cina che nel resto del mondo ma i dati e i contenuti vengono mantenuti su reti separate, per rispettare le restrizioni alla censura dei diversi governi, in particolare quello cinese.

Nonostante questo, nel dicembre 2022 TikTok è arrivato all'attenzione della cronaca internazionale per aver spiato alcuni giornalisti di Forbes che stavano raccogliendo informazioni per de-

gli articoli riguardanti proprio il social network. La vicenda ha poi acceso un riflettore su TikTok, facendo emergere successivamente ulteriori preoccupazioni e indizi di attività di spionaggio governative condotte attraverso la sede in Cina di TikTok, che avrebbe così avuto accesso ai dati degli utenti statunitensi (oltre 100 milioni) e di altri utenti stranieri.

La paura principale è che Pechino, supervisionando tutte le società tecnologiche nel suo Paese, possa richiedere a TikTok, essendo una società cinese, di trasferire all'intelligence nazionale tutti i dati richiesti, senza bisogno di un ordine del tribunale.

Sull'onda sensazionalistica delle vicende di spionaggio di TikTok da parte del governo cinese, a partire dalla metà di marzo 2023, funzionari e rappresentanti dell'UE (Parlamento e Commissione Europea) non potranno più utilizzare TikTok sui propri dispositivi di lavoro. Stessa sorte per i dipendenti del governo canadese (che ha già bandito l'app dai dispositivi mobili governativi) e degli Stati Uniti, dove il Congresso sta inoltre lavorando ad un disegno di legge che potrebbe portare al suo divieto totale entro il 2023.

Oggettivamente TikTok non rappresenta alcun rischio aggiuntivo rispetto ad altre piattaforme come Facebook, Instagram, etc.: TikTok è stata progettata prendendo spunto da quelle americane, migliorata e potenziata in termini cognitivi, cosa che l'ha resa molto più "avvincente" nell'utilizzo, più fluida nella comunicazione e nell'interazione. Sicuramente anch'essa è in grado di spiare o veicolare disinformazione e probabilmente lo fa meglio delle sorelle americane ma – in questo specifico momento storico – il divieto dell'utilizzo di TikTok nelle istituzioni governative da parte degli USA e degli Stati occidentali ha soprattutto una lettura geopolitica: gli Stati Uniti e l'UE stanno cercando di limitare il potere tecnologico della Cina anche per paura di un suo coinvolgimento nella guerra in Ucraina. Ma questa tensione tecno-politica, soprattutto tra Washington e Pechino, potrebbe portare i governi stranieri a dover scegliere se commerciare con gli Stati Uniti o con la Cina, istituendo una sorta di nuova "cortina di ferro" tecnologica.

HUAWEI: "FORZA CINA"

La Cina ha da decenni capito che gestendo la produzione tecnologica del mondo occidentale, che gliel'ha delegata per via dei suoi bassi costi di produzione, poteva sfruttare questa sua posizione per sviluppare politiche di spionaggio su tutti i livelli dell'ambito ICT, dagli utenti finali alle grandi infrastrutture, fino ai governi stranieri. Uno dei primi casi noti è quello di Huawei. In cinese antico, la parola Huawei significa "forza Cina": e mai un nome è stato più adeguato a rappresentare un'azienda cinese. Huawei Technologies Co. Ltd è una multinazionale cinese che fornisce tecnologie dell'informazione e della comunicazione (ICT) a più di 3 miliardi di persone in tutto il mondo. Conta oltre 180.000 dipendenti in oltre 170 paesi e nel 2022 ha fatturato 91,53 miliardi di dollari.

Nonostante il successo a livello internazionale, Huawei ha incontrato difficoltà su alcuni mercati stranieri a causa del fin troppo evidente e indebito sostegno statale nonché per via dei suoi stretti collegamenti con il Ministero della sicurezza statale (MSS) cinese, che hanno generato preoccu-

pazioni sul fatto che i dispositivi Huawei potessero consentire attività di spionaggio da parte del governo cinese. Huawei non produce solamente dispositivi per il mercato consumer ma è il più grande produttore al mondo di apparecchiature per le telecomunicazioni di reti infrastrutturali come ad es. router, switch, centralini telefonici, etc., quindi sistemi progettati per essere installati anche su infrastrutture aziendali, governative e critiche di un Paese. Le reti di comunicazione di base costituiscono un'infrastruttura fondamentale, con evidenti implicazioni per la sicurezza nazionale. Il fatto che la tecnologia Huawei venga impiegata ad es. per le reti di comunicazione backbone implica che Huawei fornirebbe componenti critici in sistemi di importanza strategica per la società di uno Stato, tra cui i servizi di sicurezza o le funzioni sociali ed economiche principali.

Huawei negli anni ha sollevato diversi sospetti casi di spionaggio: nel 2003 fu accusata dalla CISCO Systems di copia illegale della proprietà intellettuale, avendo immesso sul mercato apparati di networking simili a quelli della CISCO sia in termini di hardware che software. Nel 2018 è tornata alla ribalta delle cronache di spionaggio soprattutto per via della tecnologia 5G. Gli intrinseci aspetti tecnologici legati alle vulnerabilità del 5G e i dubbi sul fornitore della stessa, che si traducono nella stretta relazione con gli apparati di intelligence di Pechino, hanno spinto diversi governi a vietare l'utilizzo della tecnologia Huawei. All'inizio del 2018 il governo australiano vietò a Huawei di prendere parte al lancio dell'infrastruttura mobile 5G per motivi di sicurezza nazionale, esempio seguito poi anche dall'agenzia per la sicurezza nazionale della Nuova Zelanda e dagli Stati Uniti. Nel 2020 il governo di Boris Johnson ha ordinato l'esclusione delle forniture 5G di Huawei in UK, con l'obiettivo di smantellare entro il 2027 l'esistente. Nello stesso periodo, anche l'Italia ha bloccato l'accordo in base al quale Fastweb avrebbe dovuto ricevere da Huawei apparecchiature per la sua rete core 5G.

THE BIG HACK: IL CHICCO DI RISO CHE HA FATTO RABBRIVIDIRE LA COMUNITÀ DELL'INTELLIGENCE

Le posizioni di divieto imposte da diversi Stati nei confronti della tecnologia 5G della Huawei non sono frutto di particolari atteggiamenti paranoici da parte delle agenzie di intelligence o della propaganda politica dei governi. In realtà esistono fondate motivazioni per sospettare dei dispositivi realizzati dalle aziende cinesi: e più questi sistemi e dispositivi vanno a occupare ruoli strategici nella riservatezza delle informazioni di una nazione, più è probabile che l'interesse del governo di Pechino "stimoli" le sue aziende ad operare in modo da acquisire quelle informazioni.

Nel 2018 Bloomberg pubblicò un'inchiesta relativa ad Amazon Inc. che nel 2015 aveva iniziato la valutazione di una startup chiamata Elemental Technologies per una potenziale acquisizione. L'Elemental aveva sviluppato un software di compressione e streaming video che interessava ad Amazon per un suo servizio di entertainment, oggi noto come Amazon Prime Video. L'Elemental aveva utilizzato il suo software per trasmettere in streaming i Giochi Olimpici, per comunicare con la Stazione Spaziale Internazionale e grazie ad una partnership di sviluppo con In-Q-Tel Inc., società d'investimento della CIA, per la gestione di flussi video di droni alla Central Intelligence Agency. I

contratti di sicurezza nazionale di Elemental erano un ulteriore valore aggiunto per le attività governative che Amazon stava implementando per la CIA attraverso la creazione di un cloud sicuro con Amazon Web Services (AWS). Durante l'attività di due diligence propedeutica all'acquisizione della Elemental, i consulenti preposti da AWS rilevarono delle anomalie sui server che Elemental aveva venduto ai suoi clienti e che utilizzavano il loro software di streaming video.

In particolare, nei server che i clienti (Dipartimento della Difesa, NASA, CIA, etc.) avevano installato nelle loro reti e che erano stati assemblati per Elemental dalla Super Micro Computer Inc. (Supermicro), società con sede a San Jose in California e tra i maggiori fornitori al mondo di schede madri per server, fu individuato – proprio nelle schede madri – un minuscolo microchip, grande quanto la punta di una matita (Fig.1), che non faceva parte del design originario delle schede. Amazon segnalò l'anomalia alle autorità, cosa che portò subito l'attenzione delle agenzie di intelligence statunitensi ai massimi livelli; FBI e CIA aprirono un'indagine top secret che durò oltre tre anni. Gli investigatori stabilirono che i chip consentivano agli aggressori di creare una backdoor per accedere in modalità stealth in qualsiasi rete che includesse le macchine alterate e, seguendo la catena di produzione, gli investigatori scoprirono inoltre che i chip erano stati inseriti in fabbriche gestite da subappaltatori di componenti di produzione in Cina. Secondo Bloomberg gli investigatori arrivarono alla conclusione che un'unità militare cinese aveva progettato i microchip per assomigliare a comuni transistor ma che incorporavano all'interno componenti di memoria, capacità di rete e potenza di elaborazione sufficiente per un cyber attacco; inoltre piccole differenze nella dimensione dei chip "canaglia" rivelavano che la produzione degli stessi era stata fatta in aziende diverse. Il caso fece emergere tutti i timori ipotizzati, cioè che i server della Elemental erano solo alcuni rispetto alle migliaia di clienti che aveva Supermicro in tutto il mondo. L'inchiesta di Bloomberg rivelò che questa attività di cyber spionaggio altamente sofisticata e orchestrata con successo aveva compromesso silenziosamente la catena di fornitura globale di hardware per computer, infiltrandosi in quasi 30 società statunitensi tra cui Amazon e Apple. Nei mesi successivi molte delle aziende coinvolte negarono i fatti descritti da Bloomberg, ma nessuno mosse mai alcuna azione legale nei confronti della testata.

Questo (presunto) attacco è stato più grave degli incidenti basati su malware e a cui siamo ormai abituati:, gli attacchi basati sull'hardware sono più difficili da realizzare, richiedono ingenti risorse, infrastrutture e soggetti "autorizzati" nella catena di produzione, sono potenzialmente più devastanti, producono effetti a lungo termine e qualsiasi agenzia di spionaggio è disposta ad investire milioni di dollari pur di ottenere le informazioni a cui possono dare accesso.

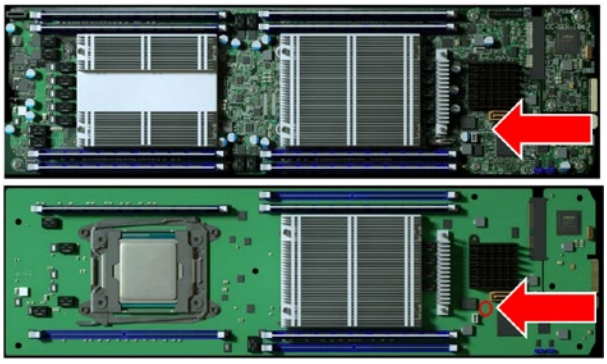


Fig. 1

Inoltre, a differenza dei software di spionaggio, la manipolazione dell'hardware richiede una pianificazione sofisticata, in quanto lascia tracce nel mondo reale. I componenti hardware hanno specifiche catene di approvvigionamento, bolle di spedizione, fatture, numeri di serie che identificano specifiche fabbriche. Per individuare la fonte dei chip "canaglia", le agenzie di intelligence statunitensi analizzarono l'intera supply chain di Supermicro fino ad appurare che i tre produttori principali che costruivano le sue schede madri, due con sede a Taiwan e una a Shanghai, avevano subappaltato le forniture a quattro fabbriche già da due anni prima dell'attacco. Le agenzie di intelligence statunitensi, spiando le comunicazioni delle persone chiave delle varie aziende, identificarono quindi come responsabile un'unità dell'Esercito popolare di liberazione specializzata in attacchi hardware. I responsabili delle aziende sub-appaltanti erano contattati da persone che affermavano di rappresentare Supermicro o che ricoprivano posizioni che suggerivano un legame con il governo. Gli intermediari avrebbero richiesto le modifiche ai progetti originali delle schede madri, offrendo anche tangenti in caso di resistenza.

L'episodio causò un notevole imbarazzo diplomatico tra Stati Uniti e Cina, in quanto l'attribuzione dell'attacco, almeno per quanto riguardava la fonte geografica, risultava inequivocabile. Il Ministero degli Affari Esteri cinese smentì fermamente le accuse di spionaggio e diffuse una dichiarazione che si concludeva in maniera evasiva:

"Speriamo che le parti facciano accuse e sospetti meno gratuiti, ma conducano colloqui e collaborazioni più costruttivi in modo da poter lavorare insieme alla costruzione di un cyberspazio pacifico, sicuro, aperto, cooperativo e ordinato".

LA CINA E IL "CYBER SUPERPOWER"

Nel recente congresso nazionale del Partito Comunista Cinese, il Segretario Generale Xi Jinping ha sottolineato che i funzionari del PCC che attuano le politiche cibernetiche devono avere una visione "corretta" del cyberspazio perché "le idee determinano le azioni" e che l'aspirazione della Cina è diventare una superpotenza cibernetica, nonché controllare il cyberspazio per proteggere la sicurezza nazionale e come luogo di competizione strategica internazionale.

L'espressione "superpotenza cibernetica" è sia uno slogan politico che un concetto strategico fondamentale in ambito di cyber warfare e di guerra asimmetrica[2], ambito in cui la Cina sta focalizzando sempre maggiori risorse. Parte integrante di questa strategia è la costituzione di gruppi di hacker apparentemente indipendenti, ma che spesso rivelano collegamenti con l'Esercito di liberazione cinese (PLA), la Forza di supporto strategico (SSF) e l'intelligence cinese. Ad avvalorare l'ipotesi di forti legami tra questi gruppi e il governo cinese è l'utilizzo delle risorse durante gli attacchi, la collaborazione tra gruppi e i Paesi target, che rivelano un unico profilo comune come attore di minaccia. Questi gruppi si concentrano quasi esclusivamente su Stati che hanno legami conflittuali con il governo cinese: Paesi occidentali (ad es. Stati Uniti) e asiatici (ad es. Taiwan, Giappone) che sono percepiti come una minaccia po-

[2] CYBER-ENABLED INFORMATION WARFARE, Francesco Arruzzoli, aprile 2022, pag. 48 (https://www.ictsecuritymagazine.com/pubblicazioni/quaderni-di-cyber-intelligence-1/)

litica e industriale per la Cina.

Un'altra caratteristica è che tali gruppi spesso operano congiuntamente e quando un gruppo viene individuato, spesso si ferma e cambia alias (cosa piuttosto inconsueta per gruppi hacker che perseguono una ideologia) e i membri non attivi si spostano ad operare in altri gruppi: questo denota un'organizzazione centrale che dirige le risorse di tutti i gruppi.

Uno studio dell'International Institute for counter terrorism IDC HERZLIYA ha effettuato una classificazione dei gruppi hacker cinesi in base al livello di priorità delle loro attività. Di seguito i principali gruppi operativi in Cina per azioni di cyber spionaggio con evidenti collegamenti all'intelligence nazionale cinese.

APT1 aka Unit 61398, Comment Crew: il gruppo, ritenuto collegato al PLA e più specificamente al General Staff Department's (GSD) 3rd Department, ha capacità che denotano un gruppo numeroso, focalizzato principalmente su obiettivi di tecnologia di difesa e di alta tecnologia, compreso il sistema israeliano Iron Dome, situati in particolare negli Stati Uniti, a Taiwan e in Giappone.

APT3 aka Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110: è considerato uno dei più sofisticati gruppi di hacker cinesi ed è collegato al gigante tecnologico Huawei. Il gruppo, i cui obiettivi includono un'ampia gamma di Paesi e industrie bersaglio, è sospettato di essere finanziato dallo Stato e conduce attività di spionaggio informatico.

APT12 aka Calc Team, DynCalc, DNSCALC, Numbered Panda: il gruppo è focalizzato su varie organizzazioni governative, dei media e dell'alta tecnologia. Nel 2013 APT12 è stato responsabile di una serie di attacchi al New York Times: il gruppo si è infiltrato nelle reti e nei sistemi informatici della testata, esfiltrando dati dei giornalisti e di altri dipendenti. Il mandante fu associato al governo cinese in quanto all'epoca un'inchiesta del New York Times riguardava la raccolta di miliardi di dollari da parte dei parenti dell'allora primo ministro cinese Wen Jiabao.

APT18 aka DYNAMITE PANDA, TG-0416, SCANDIUM, PLA Navy, Wekby, G0026: gruppo attivo da diversi anni che si rivolge a vari settori come le telecomunicazioni, l'aerospaziale, la difesa, l'alta tecnologia e la biotecnologia. Noto per sfruttare gli exploit zero-day, come nel caso dell'exploit Flash di HackingTeams, è anche sospettato di aver preso di mira il gruppo terroristico Daesh in Iraq nel 2014 per proteggere gli interessi petroliferi nella regione.

APT27 aka GreedyTaotie, TG-3390, EMISSARY PANDA, TEMP.Hippo, Red Phoenix, Budworm, Gruppo 35, ZipToken, Iron Tiger, BRONZE UNION, Lucky Mouse, G0027, Iron Taurus: gruppo cinese finanziato dallo stato, altamente sofisticato, prende di mira gli Stati Uniti, i sistemi di difesa dei Paesi asiatici e la tecnologia dei droni europea.

APT41 aka WINNTI UMBRELLA: gruppo identificato come divisione dell'intelligence cinese. È attivo da molto tempo e i suoi obiettivi principali sono politici di vari Paesi, inclusi Stati Uniti, Tibet, Giappone e Corea del Sud. Il nome Umbrella identifica una raccolta di gruppi di hacker sponsorizzati dallo Stato cinese che include un certo numero di sin-

goli gruppi (tra cui LEAD, BARIUM, Wicked Panda, GREF, PassCV e altri).

ELDERWOOD aka Beijing Group, Sneaky Panda: è un gruppo di spionaggio informatico cinese che sarebbe stato responsabile dell'intrusione di Google del 2009 nota come Operazione Aurora[3]. Il gruppo ha preso di mira organizzazioni di difesa, produttori di catene di approvvigionamento, organizzazioni per i diritti umani non governative (ONG) e fornitori di servizi IT.

HIDDEN LYNX: è stato collegato al Gruppo di Elderwood con una serie di importanti attacchi, inclusa l'Operazione Aurora e gli attacchi "VOHO" a banche e siti web di servizi, istruzione e politiche pubbliche nel 2012.

DRAGONOK: gruppo di minaccia specializzato nelle organizzazioni giapponesi, noto per gli attacchi con e-mail di phishing e l'utilizzo di malware come Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog e NewCT, è stato associato anche al gruppo Moafee con cui condivide stesse tecniche e target.

I LIMITI DEL DIRITTO INTERNAZIONALE IN TEMA DI SPIONAGGIO

L'influenza esercitata sulle aziende cinesi dal governo di Pechino pone la problematica di dover limitare il comportamento della Cina in attività di carattere spionistico anche attraverso la normativa internazionale, al fine di offrire maggiori garanzie di sicurezza ai governi occidentali.

Gli atti di spionaggio all'interno di un Paese in cui si opera sono normalmente puniti in base alla relativa legge nazionale e lo spionaggio in quanto tale non è direttamente disciplinato dal diritto internazionale. Questo, in generale, limita significativamente le azioni legali da Stato a Stato: uno Stato esercita in modo esclusivo la sua sovranità all'interno del proprio territorio e questo include la sua autorità su infrastrutture informatiche, persone e attività informatiche nel suddetto territorio, nel rispetto dei suoi obblighi giuridici internazionali. Di conseguenza, le azioni di uno Stato che ignorano od ostacolano l'esercizio della sovranità di un altro Stato costituiscono una violazione del diritto internazionale.
Affinché una particolare operazione cibernetica di spionaggio venga identificata come violazione della sovranità è però necessario valutare il grado di violazione dell'integrità territoriale dello Stato vittima, nonché il grado di coinvolgimento dello Stato attaccante nell'operazione di spionaggio: elementi, questi, decisivi per determinare se l'attività costituisca una violazione del diritto internazionale. La presenza di vulnerabilità (come ad es. backdoor) all'interno di prodotti di aziende cinesi avrebbe quindi poco significato dal punto di vista del diritto internazionale; l'autorità cinese, sui propri affari interni, può imporre obblighi alla propria industria anche a fini di collaborazione con l'intelligence nazionale. Viceversa la sovranità degli Stati occidentali può vietare la vendita e l'utilizzo dei prodotti cinesi sul proprio territorio, rispettando i loro obblighi nell'ambito degli accordi commerciali internazionali, in particolare l'Accordo generale sulle tariffe e il commercio (GATT) dell'OMC che riguarda il commercio internaziona-

[3] OPERAZIONE AURORA. STORIA, ANALISI ATTACCO, OBIETTIVI, PERPETRATORI
(https://italiawiki.com/pages/virus-informatico/operazione-aurora-storia-analisi-attacco-obiettivi-perpetratori.html)

le di beni. L'articolo XXI del GATT contiene infatti un'eccezione che consente a una parte di adottare le azioni o le misure "che ritiene necessarie per la sicurezza".

CONCLUSIONI

Le notizie sulle cyber minacce rappresentate dalla Cina appaiono regolarmente. La comunità dell'intelligence statunitense (IC) ha recentemente presentato la sua nuova valutazione annuale delle minacce 2023[4], identificando come principali minacce informatiche predominanti alla sicurezza nazionale la Cina, la Russia, l'Iran e la Corea del Nord.

Per quanto riguarda la Cina, ancora una volta il rapporto dell'IC conferma che Pechino utilizza una serie di strumenti – dagli investimenti pubblici allo spionaggio – per cercare di far progredire le proprie capacità tecnologiche, proteggere le imprese nazionali dalla concorrenza straniera e facilitare la loro tecnologia per facilitarne l'espansione sul mercato globale. La volontà di Pechino è di utilizzare lo spionaggio, i sussidi e la politica commerciale per cercare di dare un vantaggio competitivo alle proprie imprese tale da assumere la leadership del progresso tecnologico e degli standard mondiali.

Il sospetto sulle capacità e le intenzioni delle cyber minacce cinesi potrebbe portare a un conflitto tra Stati, in particolare tra Cina e Stati Uniti, a causa del ruolo che gli strumenti informatici possono svolgere nelle operazioni militari. Per questo è necessario approfondire alcuni aspetti delle strategie cinesi sulla guerra informatica da una prospettiva diversa rispetto alla narrazione secondo cui la Cina starebbe usando il potere informatico per crescere e infine conquistare il dominio globale.

La Cina di oggi è difficile da definire: ha il capitalismo senza la democrazia, lo sviluppo economico senza libertà politiche, fonde la modernizzazione cosmopolita con il nazionalismo. La più grande economia di mercato a livello mondiale, governata da un regime autoritario che limita la libertà di espressione e non ammette opposizioni. Questa situazione permette di avere però una guida stabile e di definire strategie economiche e politiche a lungo termine, a differenza degli Stati occidentali dove ormai, da circa 40 anni, assistiamo al continuo avvicendamento delle forze politiche al governo che operano strategie di "sopravvivenza" a brevissimo termine e che, soprattutto, lasciano il completo controllo delle politiche del Paese alle influenze delle lobbies economiche e della finanza, che spesso sono manifestazioni dell'influenza di Super potenze straniere.

L'assoluta centralità che riveste la stabilità nella politica di Pechino si palesa ad esempio in ambito di controllo del cyber spazio. Da quando, negli anni '90, la Cina è rimasta stupita dall'applicazione delle tecnologie delle forze armate statunitensi nella Guerra del Golfo e nelle successive operazioni in Kosovo, Afghanistan e Iraq, ha sviluppato una precisa strategia riguardo l'uso delle tecnologie dell'informazione nei ruoli più critici, strategia che ha poi per la prima volta esposto pubblicamente nel 2013 con uno studio dell'Accademia

[4] ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY, February 6, 2023 (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf)

delle scienze militari, "The Science of Military Strategy". Uno studio dove veniva affrontata la guerra cibernetica da un punto di vista olistico, dove il cyberspazio diventava un nuovo ed essenziale dominio militare nel mondo moderno. Visione rafforzata nel documento del Ministero della Difesa Nazionale del 2015 intitolato "China's Military Strategy" proprio in concomitanza con della pubblicazione del piano decennale "Made in China 2025". La "China's Military Strategy" affrontava per la prima volta il tema della sicurezza informatica in un documento militare ufficiale, definendo il cyberspazio come nuovo pilastro dello sviluppo economico e sociale e nuovo dominio della sicurezza nazionale, dichiarando apertamente che la sicurezza dell'infrastruttura cibernetica cinese era a rischio, poiché la concorrenza internazionale nel cyberspazio stava sviluppando forze militari cibernetiche.

Un altro aspetto fondamentale è che le infrastrutture critiche della Cina, comprese quelle della Difesa, come in tutti gli Stati sono sempre più dipendenti dalle infrastrutture informatiche. Nonostante disponga di un'industria tecnologica su larga scala, potenzialmente in grado di competere con gli Stati Uniti in alcuni settori, la maggior parte delle tecnologie cinesi sono ancora fornite da società statunitensi. Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle e Qualcomm sono le principali aziende da cui la Cina è fortemente dipendente e che cerca di superare con lo sviluppo dell'industria tecnologica nazionale, al fine di rendere più sicura l'infrastruttura Internet interna del Paese: cosa che fa pensare che il suo obiettivo principale nel cyberspazio sia difensivo e non offensivo.

Nei fatti, ad oggi, non esistono prove inconfutabili che dimostrino che la Cina sia stata coinvolta in cyber attacchi mirati a distruggere altri Stati; mentre lo spionaggio informatico a scopo economico è un'accusa a cui il governo cinese ha spesso risposto motivando le relative attività come rientranti nella sicurezza nazionale, un'azione comunemente condotta anche dalla maggior parte degli altri Paesi.

Come descritto nel documento "China's Military Strategy" del 2015, la Cina ha sviluppato una linea guida strategica nel cyberspazio mirata alla difesa attiva e questo comprende anche campagne di cyber spionaggio. La strategia ha quindi come obiettivo principale, nella guerra informatica, quello di migliorare le capacità di difesa per sopravvivere e contrastare un attacco cibernetico offensivo. Nel cyberspazio il principio secondo cui la migliore difesa è l'attacco non è applicabile: infatti nella prima fase di un attacco cibernetico la parte attaccata potrà rispondere con un preciso contrattacco solo se dispone di una forte difesa e l'attaccante, a sua volta, subirà esiti sfavorevoli se la sua difesa non sarà sufficientemente robusta.

Francesco Arruzzoli, *Resp. R&D e Centro Studi Cyber Defense Cerbeyra*

BIOGRAFIA

Francesco Arruzzoli

Con oltre 30 anni di esperienza nell'ambito della sicurezza delle informazioni Francesco Arruzzoli è Sr. Cyber Security Threat Intelligence Analyst presso la Winitalia di cui è cofondatore. Responsabile del Centro Studi Cyber Defense Cerbeyra presso il polo di cyber security del Gruppo Vianova, coordina le attività di R&D, analisi delle cyber minacce e progettazione di nuove soluzioni per la cyber security di aziende ed enti governativi. Progettista di sistemi esperti, software developer, network e system engineer, è stato tra i primi ethical hacker italiani certificati. Autore di libri ed articoli sue riviste del settore, in passato ha lavorato per multinazionali, aziende della sanità italiana, enti governativi e militari. In qualità di esperto di Cyber Intelligence e contromisure digitali ha svolto inoltre attività di docenza presso alcune università italiane.

Quaderno di Cyber Intelligence #2

CYBER CRIME

White paper gratuito su www.ictsecuritymagazine.com

Corea del Nord, un piccolo Stato che ambisce a divenire una cyber potenza

Negli ultimi anni la Corea del Nord si è distinta nel panorama delle minacce per la persistenza e l'efficacia delle sue operazioni cyber, che hanno colpito organizzazioni governative, infrastrutture critiche e aziende private in tutto il mondo.

Il governo di Pyongyang ha avviato un programma cyber estremamente articolato che può contare su numerosi gruppi APT (Advanced Persistent Threat) i quali rispondono al Reconnaissance General Bureau e al Ministero della Sicurezza di Stato.

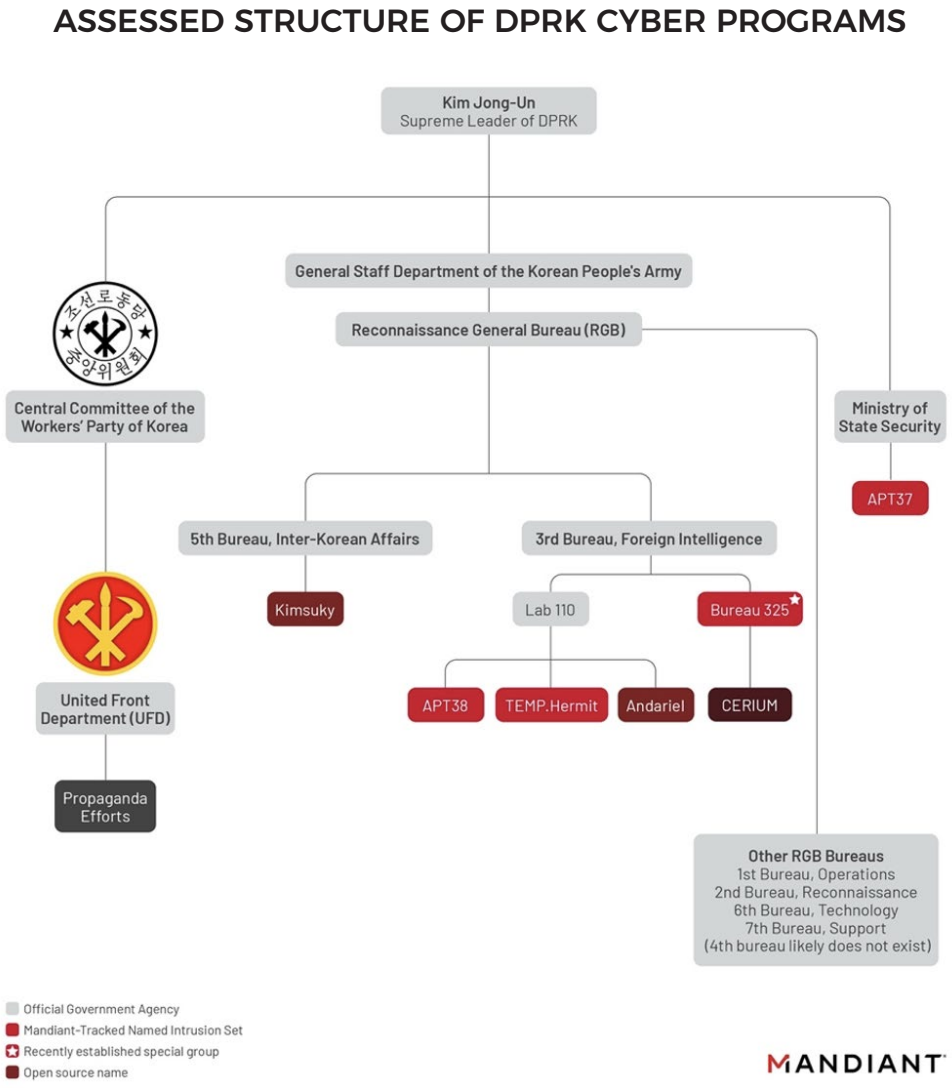


Figura 1 - Organizzazione Infrastruttura Cyber della Corea del Nord (Fonte Mandiant[1])

[1] Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations, Mandiant, marzo 2022 (https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government)

Secondo stime degli analisti di intelligence, l'esercito cyber del paese potrebbe contare su più di 6500 specialisti che operano principalmente sotto la direzione dell'Unità 180 dell'agenzia d'intelligence nazionale (Reconnaissance General Bureau, RGB). Secondo gli esperti dell'azienda di threat intelligence Mandiant, la struttura cyber del Paese asiatico è caratterizzato da grande flessibilità e per questo in grado di modificare la propria organizzazione secondo le esigenze dettate dagli eventi.

L'Unità 180, o Reconnaissance General Bureau (RGB), è il vero motore della strategia cyber nordcoreana P : il suo compito è di reclutare talenti, definire programmi formativi idonei e, ovviamente, coordinare le operazioni nello spazio cibernetico.

Ad oggi non esistono dati ufficiali sulla struttura dei vari gruppi che compongono l'esercito cyber del Paese, trattandosi di informazioni classificate e per questo motivo non pubblicamente disponibili.

L'unica certezza è una crescente capacità riscontrata negli ultimi anni degli attori nation-state che operano per conto del governo nordcoreano.
Tutto ciò è possibile solo grazie al forte commitment del leader supremo Kim Jong Un, che ha sempre sostenuto a pieno il programma militare del paese dando priorità allo sviluppo di nuove capacità militari, comprese le operazioni cibernetiche.

I diversi gruppi operano secondo una strategia condivisa, perseguendo finalità di spionaggio, sabotaggio, disinformazione e anche obiettivi economici, con l'intento di finanziare le proprie operazioni militari.

Oltre alle attività condotte dal Reconnaissance General Bureau, il Ministero della Sicurezza di Stato e il Dipartimento del Fronte Unito (UFD) supportano le operazioni del governo nordcoreano specializzandosi rispettivamente in campagne di spionaggio nei confronti di obiettivi di altro profilo e in attività di propaganda.

Sebbene le i diversi gruppi APT operino spesso sotto la direzione di Dipartimenti e/o Bureau differenti, le analisi condotte da agenzie cyber governative e da aziende di sicurezza informatica hanno dimostrato un'intensa collaborazione tra le varie entità della struttura cyber nazionale. Sono state più volte dimostrate sovrapposizioni delle strutture di comando e controllo, così come una condivisione dei malware presenti nell'arsenale dei vari gruppi.

IL GENERAL STAFF DEPARTMENT (GSD)

Il GSD è sicuramente la principale agenzia all'interno delle milizie del governo della Corea del Nord, che pianifica e coordina la quasi totalità delle operazioni condotte dall'esercito del Paese, ivi incluse le operazioni nel cyberspazio.
Compito del GSD è definire gli obiettivi in linea con le strategie definite dal governo e assicurarsi che gli stessi vengano raggiunti.

Tra le principali responsabilità dell'agenzia rientrano l'addestramento, la logistica e la gestione delle comunicazioni militari dell'esercito nordcoreano.

Corea del Nord, un piccolo Stato che ambisce a divenire una cyber potenza

Il Reconnaissance General Bureau (RGB) dipende direttamente dal General Staff Department (GSD), sebbene si tratti di fatto di due agenzie separate e con ruoli distinti all'interno delle forze armate della Corea del Nord.

RECONNAISSANCE GENERAL BUREAU

Il Reconnaissance General Bureau è l'unità all'interno dell'esercito nordcoreano che si specializza in attività di cyber spionaggio, di intelligence e persino di sabotaggio in un contesto di information warfare. Si ritiene siano almeno 6 gli uffici afferenti all'agenzia per lo svolgimento delle operazioni nel cyberspazio, tuttavia il 3rd Bureau (Foreign Intelligence) e il 5th Bureau (Inter-Korean Affairs) sono sicuramente le divisioni a cui si afferiscono la quasi totalità degli APT responsabili delle campagne condotte negli ultimi anni.

Quando si analizzano le operazioni di spionaggio attribuite al governo nordcoreano, spesso si cade nell'errore di attribuirle al più popolare gruppo di hacking del Paese, noto come Lazarus.

Lazarus è un gruppo APT che opera direttamente sotto il controllo del RGB, la cui attività è aumentata in maniera significativa dal 2014. Si riconoscono al gruppo elevate competenze tecniche che consentono ai suoi membri di disporre di un'ampia gamma di malware e custom tools utilizzati in attacchi mirati.

Si ritiene che il gruppo sia attivo dal 2009 (probabilmente già nel 2007 si sarebbe reso responsabile di alcuni attacchi di difficile attribuzione) ed è stato coinvolto sia in campagne di spionaggio informatico che in attività di sabotaggio volte a distruggere i sistemi presi di mira.

Il gruppo è considerato responsabile del massiccio attacco ransomware WannaCry, di una serie di attacchi contro il sistema interbancario internazionale SWIFT nel 2016 e del clamoroso attacco a Sony Pictures nel 2014.

Lazarus ha mostrato con continuità la capacità di condurre operazioni complesse e di accrescere le proprie capacità cyber: gli attacchi sono diventati negli anni più insidiosi e si sono avvalsi di tecnologie in grado di eludere i sistemi avversari a mano a mano che gli stessi venivano adattati per individuare la minaccia nordcoreana.

Proprio la capacità camaleontica del gruppo ha spesso ingannato gli analisti di cybersecurity, facendo attribuire le campagne individuate al popolare APT.

Approfondendo l'analisi della struttura cyber nordcoreana si individuano due componenti principali del 3rd Bureau, rispettivamente identificate come il Lab 110 e il Bureau 325.

Secondo gli esperti, il Lab 110 si concentrerebbe su attacchi con motivazione finanziaria e si comporrebbe di tre distinti gruppi APT identificati come TEMP.Hermit, APT38 e Andariel. Le operazioni di questi tre gruppi sono spesso identificate sotto il nome Lazarus; tuttavia, parliamo di tre distinte unità militari operanti sotto un medesimo coordinamento.

Il gruppo APT38, ad esempio, è stato spesso identificato come responsabile di attacchi contro isti-

tuzioni finanziarie che hanno portato al furto di centinaia di milioni di dollari dalle banche di tutto il mondo.

Attivo almeno dal 2014, secondo gli esperti internazionali sarebbe coinvolto direttamente negli attacchi contro il sistema SWIFT, in particolare l'attacco alla Vietnam's TP Bank nel 2015, alla Bangladesh's Central Bank nel 2016, alla Taiwan's Far Eastern International nel 2017, a Bancomext in Mexico nel 2018 e al Banco de Chile nel 2018.

Pur trattandosi di attacchi protratti nel tempo, vale la pena sottolineare come questo gruppo sia sempre riuscito a eludere i sistemi di sicurezza a protezione delle strutture finanziarie, sebbene le sue operazioni fossero state precedentemente riportate da diverse aziende di sicurezza.

Il gruppo negli anni si è anche specializzato nell'utilizzo di ransomware e ha sviluppato framework come MATA, in grado di colpire sistemi basati su sistemi operativi Windows, Linux e macOS.

Nel 2018 gli esperti dell'azienda FireEye hanno prodotto un report[2] dettagliato sulle operazioni dell'APT38 sottolineando come lo stesso, invece di ottenere semplicemente accessi ai sistemi obiettivo per trasferire fondi il più rapidamente possibile, operi in modo più simile alle operazioni di spio-

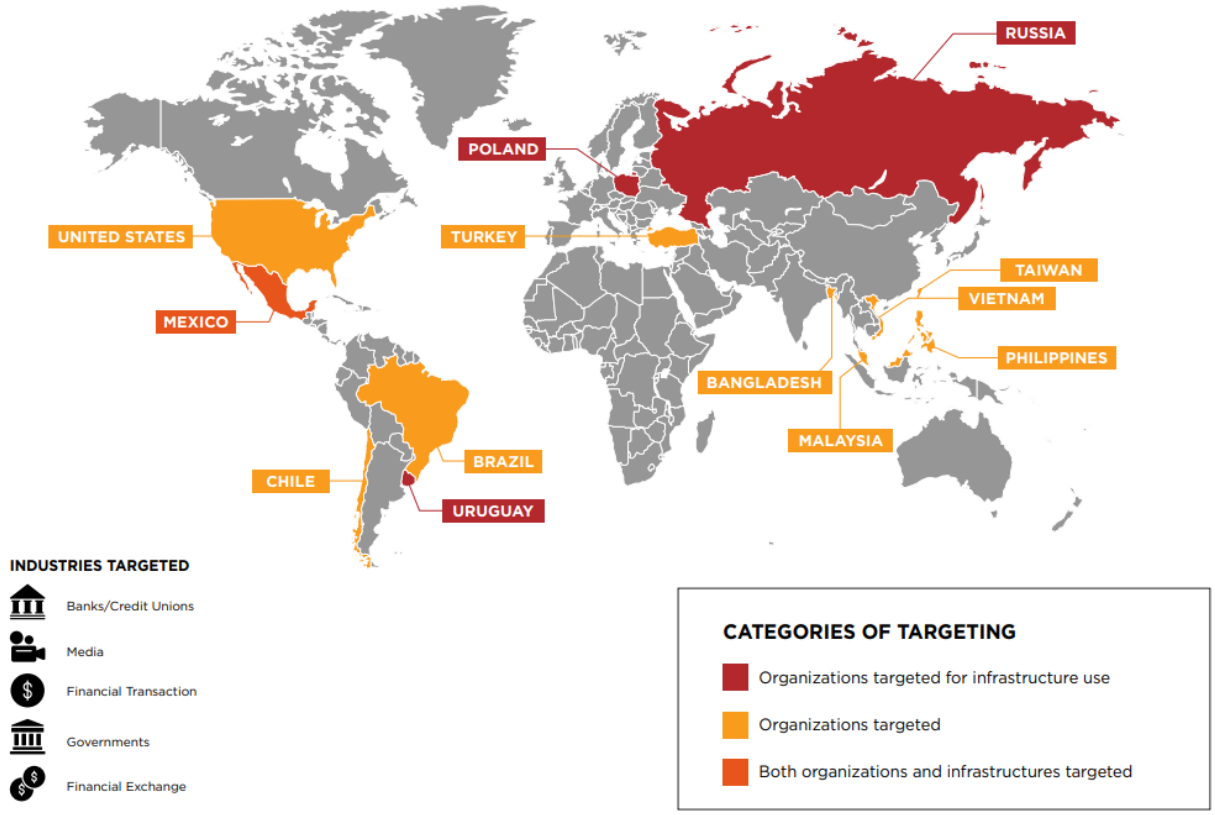


Figura 2 - Attività APT38 al 2018 (rapporto FireEye[2])

[2] APT28 Un-usual Suspects, FireEye, dicembre 2015 (https://content.fireeye.com/apt/rpt-apt38)

naggio, caratterizzate da minuziose ricognizioni all'interno di istituzioni finanziarie compromesse e bilanciando obiettivi motivati finanziariamente con l'analisi dei sistema di difesa usati dalle vittime. APT38 condivide il proprio arsenale con l'unità TEMP.Hermit.

Gli attacchi con motivazione finanziaria da parte del gruppo sono arrivati ai giorni nostri: all'inizio del 2023 l'FBI ha confermato che nel giugno 2022 una operazione congiunta da parte del gruppo Lazarus APT e del gruppo APT38 ha portato al furto di criptovalute per un valore di 100 milioni di dollari alla società Blockchain Harmony Horizon Bridge.

Il 27 giugno 2022, gli hacker nordcoreani hanno iniziato a trasferire[3] i fondi (circa 39 milioni di dollari) attraverso il servizio di mixer Tornado Cash per riciclare i profitti illeciti.

La società di sicurezza blockchain Elliptic è stata in grado di analizzare le transazioni anche dopo l'utilizzo del servizio mixer e ha confermato l'attribuzione alle unità del governo di Pyongyang.

Gli esperti dell'FBI hanno riferito che il 13 gennaio 2023 gli hacker nordcoreani hanno utilizzato il protocollo RAILGUN per riciclare oltre 60 milioni di dollari in ethereum (ETH) rubati in giugno. Quindi gli attaccanti hanno inviato una parte dei fondi rubati a exchange e li hanno convertiti in bitcoin (BTC).

Il livello di complessità dell'attacco e il coordinamento mostrato in occasione dell'intrusione forniscono una dimostrazione delle capacità di queste unità nel cimentarsi con nuove tecnologie e protocolli al fine di condurre attacchi sempre più complessi e difficili da individuare.

Anche il gruppo Andariel è stato collegato ad attacchi finanziariamente motivati; tuttavia ad esso si attribuiscono anche attacchi contro le infrastrutture critiche.

Nel 2022 i ricercatori di Kaspersky hanno attribuito al gruppo il ransomware Maui, usato in attacchi contro le strutture sanitarie.

Gli esperti notarono che, circa dieci ore prima della distribuzione del ransomware all'interno nelle reti delle aziende prese di mira, gli attaccanti avevano distribuito una variante del noto malware DTrack, riconosciuto come un codice malevolo in disponibilità esclusiva proprio dell'APT Andariel.

Kaspersky ha poi scoperto che la variante DTrack impiegata negli attacchi contro le società giapponesi, russe, indiane e vietnamite ha una somiglianza del codice dell'84% con i campioni utilizzati nelle campagne di spionaggio informatico attribuite all'APT Andariel.

L'ultimo dei gruppi afferenti al Lab 110 è l'APT TEMP. Hermit, che diversamente dai precedenti gruppi si specializza in attività di intelligence con attacchi rivolti principalmente a strutture governative, alla difesa e a organizzazioni operanti nel settore finanziario e delle telecomunicazioni.

Di recente costituzione è il Bureau 325, istituito probabilmente nel gennaio 2021 per rispondere a nuove esigenze del RGB. Si ritiene ad esempio

[3] Harmony Incident Analysis, Certik, giugno 2022 (https://www.certik.com/resources/blog/2QRuMEEZAWHx0f16kz43uC-harmony-incident-analysis)

che l'unità sia stata creata dopo lo scoppio della pandemia di Coronavirus e che tra i compiti della stessa vi siano state campagne di intelligence mirate alle attività di spionaggio nei confronti delle organizzazioni di ricerca e produzione di vaccini anti COVID-19.

Secondo le rivelazioni di disertori, all'interno del Bureau 325 è stata creata un'unità nota come "CERIUM".

Gli esperti di sicurezza di Microsoft sostengono[4] che il gruppo APT Cerium si è impegnato in attacchi di spear-phishing a tema Covid-19 fingendosi l'Organizzazione Mondiale della Sanità.

Come sottolineato il direttivo RGB è responsabile anche delle attività afferenti al Bureau 5, all'interno del quale si colloca il gruppo APT Kimsuky.

Il gruppo Kimsuky (noto anche come ARCHIPELAGO, Black Banshee, Thallium, Velvet Chollima, APT43) è stato individuato per la prima volta da Kaspersky nel 2013. Alla fine di ottobre 2020, l'US-CERT ha pubblicato un rapporto sulle attività di Kimusky che ha fornito informazioni sulle loro tecniche, tattiche e procedure (TTP) e sulle infrastrutture utilizzate nelle sue campagne.

Il gruppo APT prende di mira principalmente think tank e organizzazioni in Corea del Sud, oltre a diverse entità negli Stati Uniti, in Europa e in Russia. Negli anni Kimsuky ha colpito organizzazioni militari, manifatturiere, accademiche e think tank con competenze specifiche in materia di difesa e sicurezza (in particolare sicurezza nucleare e politiche di non proliferazione). Il gruppo si è distinto in attività di intelligence e furto di dati finanziari, con particolare riferimento ad organizzazioni attive in Corea del Sud. Le informazioni acquisite sono poi utilizzate per la raccolta di dati e la creazione di infrastrutture di attacco per future operazioni di spionaggio informatico.

In una recente campagna[5], il gruppo si è concentrato sui programmi nucleari tra Cina e Corea del Nord, rilevanti per la guerra in corso tra Russia e Ucraina.

IL UNITED FRONT DEPARTMENT (UFD) ED IL MINISTRY OF STATE SECURITY (MSS), DALLA PROPAGANDA AL CONTROSPIONAGGIO

Lo United Front Department (UFD) è un'agenzia il cui compito principale è l'attività di propaganda a livello internazionale. UFD promuove la dottrina del Partito del Lavoro della Corea del Nord, esaltando la figura del leader supremo Kim Jong Un e auspicando una riunificazione con la Corea del Sud sotto il suo controllo.

Al MSS è assegnata la funzione di controspionaggio del governo nordcoreano sul fronte interno e internazionale. Il gruppo APT37 rappresenta l'unità operativa della divisione per la raccolta di informazioni di interesse strategico, militare, politico ed economico del Paese.

[4] Cyberattacks targeting health care must stop, Microsoft, novembre 2020 (https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/)

[5] Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign, SentinelOne, maggio 2023 (https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/)

Corea del Nord, un piccolo Stato che ambisce a divenire una cyber potenza

APT37 è attivo almeno dal 2012 e negli anni le sue operazioni sono state probabilmente tra le più sofisticate attribuite alla Corea del Nord. Il gruppo ha dimostrato la capacità di sviluppare e utilizzare zero-day exploit in popolari software, come Adobe Flash Player, per compromettere i sistemi presi di mira.

Le campagne di spionaggio condotte dal gruppo APT37 hanno preso di mira principalmente organizzazioni governative, nel settore della difesa e dei media della Corea del Sud.

Altri obiettivi del gruppo sono organizzazioni in Giappone, Vietnam e Medio Oriente.

L'arsenale impiegato comprende molteplici malware, tra cui il wiper RUHAPPY, lo strumento di esfiltrazione CORALDECK, i downloader GELCAPSULE e HAPPYWORK, i loader MILKDROP e SLOWDRIFT, l'infostealer ZUMKONG e le backdoor tracciate come DOGCALL, KARAE, POORAIM, WINERACK, ROKRAT, BLUELIGHT, DOLPHIN e SHUTTERSPEED.

RELAZIONE CON LA CINA

Secondo la testimonianza di un alto funzionario dell'intelligence sudcoreana, il leader Kim Jong Un avrebbe affermato che «La guerra informatica, insieme alle armi nucleari e ai missili, è una "spada multiuso" che garantisce la capacità dei nostri militari di colpire senza sosta».

La Corea del Nord considera le campagne di hacking un pilastro della sua strategia militare.
Sabotaggio, intelligence e attacchi condotti contro istituzioni finanziarie rendono il piccolo Stato una concreta minaccia per qualunque Paese ritenuto ostile dal suo leader.

Nel biennio 2021-2022, gli hacker nordcoreani avrebbero rubato poco meno di un miliardo di dollari in criptovalute offrendo al Paese un sostentamento economico cruciale per la sua sopravvivenza.

Ma com'è possibile che una nazione con un accesso apparentemente limitato a Internet possa rendersi responsabile di campagne di hacking così efficaci e pericolose?

Sebbene i principali governi occidentali abbiano cementato un'alleanza, anche sotto il profilo cyber, per contrastare le operazioni della Corea del Nord, il Paese può contare sul supporto strategico offerto dal Partito Comunista Cinese (PCC) alle sue campagne cyber.

Gli analisti di intelligence occidentali sono al corrente che proprio il governo cinese ha ospitato unità hacking di élite della Corea del Nord in città di confine come Shenyang. Diverse unità all'interno dell'esercito cyber sono state addirittura formate presso prestigiose università tecnologiche e istituti di ricerca cinesi, tra cui l'Harbin Institute of Technology, che ospita regolarmente studenti di informatica nordcoreani.

Il governo cinese continua a sostenere la crescita delle capacità informatiche nordcoreane con l'intento di far sviluppare un "asse cibernetico" in grado di minacciare e indebolire interessi degli Stati Uniti.

A dimostrazione di tutto ciò, nel 2019 il Ministro dell'Istruzione cinese ha firmato un accordo con

il governo nordcoreano sulla continuazione degli scambi e dei partenariati educativi dal 2020 al 2030.

Nel 2016, un ricercatore di sicurezza informatica sudcoreano ha stimato[6] che in Cina operano da 600 a 1000 hacker appartenenti a unità impiegate del governo nordcoreano e specializzate in operazioni cibernetiche di guerra informatica. È noto, inoltre, che il traffico proveniente dal Paese transita attraverso le reti di provider cinesi.

Nell'ottobre 2020 John Demers, allora assistente procuratore generale degli Stati Uniti per la sicurezza nazionale, ha affermato nel corso di un evento che «c'è supporto attraverso l'infrastruttura informatica cinese. Probabilmente c'è supporto in termini di condivisione di competenze e formazione da parte cinese».

Le unità cyber nordcoreane possono beneficiare di questo supporto e delle informazioni fornite dagli esperti di Pechino per camuffare l'origine dei loro attacchi e adottare false flag con l'intento di renderne difficile l'attribuzione. A differenza di quanto accade per armamenti convenzionali, lo sviluppo di capacità informatiche offensive non dipende dall'approvvigionamento di attrezzature specializzate difficili da ottenere per un Ppaese sotto perenne embargo, né tantomeno risulta particolarmente costoso.

Un rapporto[7] pubblicato nel 2017 dall'azienda di threat intelligence Recorded Future rivelò anche una significativa presenza fisica e virtuale di unità nordcoreane anche in India. Secondo gli esperti quasi il 20% di tutta l'attività Internet nordcoreana osservata da aprile a luglio 2017 coinvolse l'India.

UNO SGUARDO AL PRESENTE PER ANTICIPARE IL FUTURO

La Corea del Nord negli ultimi anni si è resa protagonista di un numero significativo di operazioni cibernetiche, continuando a perseguire una aggressiva strategia cyber.

Le varie unità descritte si sono avvicendate in molteplici campagne di spionaggio e in operazioni con finalità estorsive, con l'intento di raccogliere fondi per sovvenzionare l'ambizioso programma militare del Paese.

Numerose sono le campagne malware contro le istituzioni governative in tutto il mondo, così come attacchi ad istituzioni finanziarie e operatori nel settore delle criptovalute.

Un elemento di forte preoccupazione da parte dei governi occidentali è una escalation in attacchi che hanno preso di mira organizzazioni operanti in settori critici, come banche e strutture sanitarie. Il ricorso a ransomware in attacchi contro infrastrutture critiche ha indotto le agenzie statunitensi (NSA, FBI, CISA) e della Corea del Sud (il Dipartimento della salute e dei servizi umani, il Servizio di intelligence nazionale della Repubblica di Corea - ROK e l'Agenzia per la sicurezza della difesa della

[6] North Korea Knows How Important Its Cyberattacks Are, Foreign Policy, febbraio 2022 (https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/)

[7] North Korea's Ruling Elite Are Not Isolated, Recorded Future, luglio 2017 (https://www.recordedfuture.com/north-korea-internet-activity)

Corea del Nord, un piccolo Stato che ambisce a divenire una cyber potenza

ROK) a emettere emesso un avviso congiunto[8] su attacchi ransomware in corso contro le organizzazioni della sanità pubblica e altre entità nel settore delle infrastrutture critiche.

Nell'ultimo anno i gruppi Lazarus e Kimsuky si sono rivelati i più attivi nel panorama nazionale e internazionale. Gli APT nordcoreani hanno dimostrato la capacità di potenziare il proprio arsenale cyber, ad esempio con lo sviluppo di nuovi malware concepiti per colpire anche piattaforme macOS oppure exploit in grado di sfruttare vulnerabilità zero-day per compromettere i sistemi obiettivo.

Lazarus, ad esempio, ha utilizzato nuovi malware sviluppati per colpire sistemi Linux e MacOS nell'ambito dell'operazione tracciata come Operation Dream Job.

Il gruppo APT è inoltre sospettato di essere il principale responsabile dell'attacco alla supply chain del software 3CX, che ha consentito di colpire società operanti nel settore delle criptovalute così come almeno due infrastrutture critiche nel settore dell'energia.

Ad inizio anno, l'FBI ha confermato che nel giugno 2022 il Gruppo Lazarus, in collaborazione con l'unità APT38, ha rubato 100 milioni di dollari in criptovalute dall'azienda Harmony Horizon Bridge.

A conferma dell'intensa attività da parte di attori nation-state nordcoreani contro il comparto delle criptovalute, in dicembre l'agenzia di spionaggio della Corea del Sud, il National Intelligence Service, ha stimato che gli APT legati alla Corea del Nord hanno rubato circa 1,5 trilioni di won (circa 1,2 miliardi di dollari) in criptovalute e altre risorse virtuali negli ultimi cinque anni.

Secondo l'agenzia di spionaggio, più della metà delle risorse (circa 800 miliardi di won, 626 milioni di dollari) sono state rubate nel solo 2022.
Sul fronte domestico risulta intensa anche l'attività del gruppo Kimsuky che grazie ad una nuova collezione di strumenti, come il tool di ricognizione ReconShark, ha preso di mira varie entità nella Corea del Sud.

Interessante anche l'utilizzo di attacchi di credential harvesting da parte del gruppo APT38 contro aziende di differenti settori. Gli analisti evidenziano come le unità della Corea del Nord per la prima volta hanno cominciato ad utilizzare questa modalità di attacco su larga scala dalla fine dello scorso anno.

Nei prossimi mesi, i gruppi APT nordcoreani continueranno incessanti nelle proprie operazioni: preoccupano soprattutto attacchi con finalità estorsiva basati su ransomware, soprattutto se indirizzati a infrastrutture critiche. Questi attacchi consentono al governo di Pyongyang di raccogliere fondi tramite attacchi di difficile attribuzione.

Le capacità cyber del Paese aumentano con l'intensificarsi delle operazioni, grazie anche alla grande flessibilità e all'elevato livello di collaborazioni tra le varie articolazioni che compongono la struttura cyber all'interno dell'apparato militare nazionale.

Pierluigi Paganini, *Membro del Gruppo Ad-Hoc Working Group on Cyber Threat Landscape dell'agenzia eu-ropea ENISA*

[8] #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities, US CISA, FBI, NSA, febbraio 2023 (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a)

BIOGRAFIA

Pierluigi Paganini

Pierluigi Paganini è Ceo di CYBHORUS e Membro del Gruppo Ad-Hoc Working Group on Cyber Threat Landscape dell'agenzia europea ENISA. E' Adjunct Professor in Cyber Security presso l'Università Luiss Guido Carli e Coordinatore scientifico del Master in Cyber Security del Sole24Ore Formazione. Ha fondato Cybaze, uno dei principali poli privati di cyber security poi acquisito dal gruppo Tinexta. Pierluigi Paganini è fondatore di Security Affairs, tra i primi blog al mondo di Cyber Security e collabora con le principali testate giornalistiche nazionali ed internazionali. Gestisce la rubrica "Sicuri nella Rete" per la Repubblica ed è autore per la rubrica VERIFIED dell'agenzia ANSA. Nel 2017 è stato membro del gruppo italiano "Ise-Shima Cyber Group" (ISCG) in occasione del G7 Italia, un nuovo Working Group del G7 sulle tematiche che riguardano il Cyberspace. E' co-autore della dichiarazione di Lucca, approvato dai Ministri del G7, concernente la dichiarazione sulle norme di comportamento degli stati nel Cyberspace.

Quando la minaccia eversiva evolve

INTRODUZIONE

Negli ultimi decenni abbiamo assistito, a livello globale, alla progressiva digitalizzazione di un mondo originariamente analogico. L'alto livello di informatizzazione e interconnessione che caratterizza la società odierna ha determinato il cedimento dei tradizionali perimetri di sicurezza e ciò ha esposto gli Stati a una molteplicità di potenziali minacce, da prevenire e affrontare. La dipendenza da computer, network e infrastrutture ICT (Information and Communication Technologies) ha fatto crescere il timore che il terrorismo non si limiti a usare il cyberspace solo come uno strumento per condurre propaganda o proselitismo, raccogliere fondi e organizzare attentati (comunicando anche tramite cifratura e steganografia) ma come vero e proprio veicolo di attacchi terroristici, che potrebbero avere delle conseguenze rilevanti per l'integrità degli Stati.

La presente ricerca nasce dalla volontà di contribuire a produrre conoscenza su un fenomeno attualmente molto dibattuto e complesso per quanto mai ancora realizzatosi in concreto, anche per la difficoltà tecnica di classificare un attacco informatico come terroristico a meno che non vi sia un'esplicita e inequivocabile rivendicazione dello stesso da parte di un gruppo terroristico. A tal fine sono state integrate metodologie, nozioni e tecniche in uno scenario multidisciplinare per fornire un contributo metodologico a prevenzione e contrasto alla potenziale metamorfosi della minaccia eversiva e, in particolare, terroristica.
Si è partiti dunque dallo studio del concetto generale per poi contestualizzarlo nell'analisi di uno specifico gruppo del terrorismo di matrice jihadista. È stata selezionata la metodologia OSINT (Open Source Intelligence)[1] con l'ausilio della SOCMINT (Social Media Intelligence)[2] per la raccolta delle informazioni: le evidenze sono state poi sfruttate come punto di partenza per un'analisi che rispondesse alla richiesta se un'organizzazione terroristica, mediante la sua transizione dal mondo fisico a quello virtuale, possa sfruttare il dominio cibernetico come vettore per condurre un attacco con finalità terroristiche, minando per esempio le infrastrutture critiche nazionali e mettendo così in pericolo la sicurezza della nostra Repubblica.

Il documento termina con alcune conclusioni.

IL TERRORISMO CIBERNETICO

Per tracciare lo Stato dell'arte del terrorismo cibernetico è stata condotta un'indagine sia sul piano internazionale che nazionale e a tal fine è stato selezionato un considerevole numero di documenti (libri, ricerche accademiche, ricerche governative, articoli, analisi, sondaggi, siti web ecc.) provenienti da molteplici aree geografiche, per un periodo che va dal 1999 al 2022. È risultato che non esiste una definizione di terrorismo cibernetico generalmente riconosciuta e che la valutazione e la definizione del concetto è mutata e si è sviluppata con l'evolversi di Internet.

[1] https://en.wikipedia.org/wiki/Open-source_intelligence

[2] https://en.wikipedia.org/wiki/Social_media_intelligence

Un elemento interessante è che sia per il terrorismo tradizionale che per il terrorismo cibernetico esistono differenti percezioni e definizioni, inevitabilmente influenzate da una serie di variabili sussistenti in maniera differente in ogni Paese. Trattando il concetto di terrorismo cibernetico è importante evidenziare alcuni punti fondamentali: in primo luogo il fenomeno è etimologicamente la convergenza tra lo spazio cibernetico e il terrorismo, in secondo si tratta di un tema complesso, motivo per il quale non esiste nemmeno una definizione universale di terrorismo "tradizionale". Si è rilevata inoltre una tendenza ad associare il termine terrorismo cibernetico e sinonimi alle organizzazioni terroristiche di matrice jihadista; tuttavia, il terrorismo cibernetico si riferisce a una eterogeneità di gruppi terroristici di cui alcuni esempi potrebbero essere i rivoluzionari e gli estremisti di destra, i separatisti etno-nazionalisti, terroristi c.d. New Age, anarco-insurrezionalisti come anche i gruppi del terrorismo di matrice jihadista. Per chiarezza è essenziale non confondere il terrorismo cibernetico con la criminalità informatica e l'hacktivism[3]. I criminali informatici sono mossi generalmente da ragioni economiche, pertanto operano per trarre benefici finanziari, per autocompiacimento, per sfida o vendetta. Gli hacktivist sono invece alimentati da un'ideologia, praticano resistenza sociopolitica, agiscono in modo creativo per mettere in discussione l'operato di governi e multinazionali (Zampetti, 2015) attraverso petizioni online, siti web e operazioni c.d. di defacement[4].

Le radici della nozione di terrorismo cibernetico possono essere fatte risalire agli anni Novanta, quando la rapida crescita dell'uso di Internet e il dibattito sull'emergente società dell'informazione diedero vita a numerosi studi sui potenziali rischi scaturenti dall'alta interconnessione e dalla dipendenza dalla tecnologia informatica. Da allora, diversi gruppi terroristici hanno dimostrato di avere piena consapevolezza del potenziale degli attacchi informatici e di come questi ultimi possano effettivamente essere eseguiti. Difatti, a differenza dei primi anni Duemila, oggi gli allarmismi su una possibile transizione dei terroristi nel mondo cibernetico sono diventati palesemente una realtà. Nonostante i tradizionali metodi per condurre attentati terroristici rappresentino la minaccia maggiore, così come all'inizio del nuovo secolo gli eventi dell'11 settembre colsero di sorpresa l'intero pianeta – rimanendo nella storia come un evento spartiacque con implicazioni globali di vasta portata – allo stesso modo potrebbe presentarsi un attentato di terrorismo cibernetico la cui gravità aumenterebbe se l'attacco informatico venisse combinato con un attacco fisico (Weimann 2004). Dai molteplici tentativi di definire questo fenomeno è risultato che esistono due macro-tendenze. Da un lato vi sono studiosi che definiscono il terrorismo cibernetico in senso restrittivo (o puro) e dall'altro chi invece ne dà una definizione più ampia, includendovi le azioni che vengono definite di supporto al cyberterrorismo; e questo dipende dall'uso che fanno i terroristi del cyberspace per il perseguimento delle loro attività. A tal proposito si riporta un'interessante distinzione pubblicata sull'argomento da Anna-Maria Talihärm (2010) tra comprensione orientata all'obiettivo (stretta) e orientata agli strumenti (ampia). La prima identi-

[3] https://en.wikipedia.org/wiki/Hacktivism

[4] https://en.wikipedia.org/wiki/Website_defacement

fica come terrorismo cibernetico tutti gli attacchi motivati politicamente o socialmente contro computer, reti e informazioni condotti attraverso altri computer o fisicamente, quando provocano ferite, spargimenti di sangue o gravi danni o terrore (target-oriented cyberterrorism). La seconda etichetta tutte le azioni che utilizzano Internet o i computer per organizzare attacchi terroristici come cyberterrorism (tool-oriented cyberterrorism). Secondo questo approccio le attività come raccolta fondi, ricognizione, comunicazione e propaganda si qualificano tutte potenzialmente come cyberterrorism se condotte online con fini terroristici. Secondo Nelson et al. (1999) invece queste azioni rappresenterebbero un supporto al terrorismo cibernetico, non essendo tese di per sé ad avere un effetto coercitivo su un pubblico target ma a potenziare altri atti terroristici: per cui, secondo questa visione, l'uso terroristico della tecnologia dell'informazione nelle attività di supporto non si dovrebbe caratterizzare come cyberterrorismo.

Dalla ricognizione svolta per delineare il quadro nazionale circa la definizione di terrorismo cibernetico è risultato che in Italia gli sforzi accademici e non, volti a dare una definizione di terrorismo cibernetico, sembrano essere pubblicamente pochi (o comunque non facilmente raggiungibili dalla maggioranza) e gran parte di essi riconducono a un'interpretazione più "ampia", alludendo a quanto già menzionato. Dallo studio dei documenti si evince che tra la molteplicità di sfumature esistenti per cyber terrorismo, cyber-terrorismo, cyber-terrorism o cyberterrorism ecc. viene sottintesa genericamente l'attività di routine dei terroristi nello spazio cibernetico. È stata notata inoltre una propensione a connettere il termine a movimenti terroristici di matrice jihadista, tra i quali i più citati sono Al-Qā'ida (AQ) e l'Islamic State (IS). Sebbene siano presenti dei validissimi articoli o ricerche che hanno l'intento di scindere tra l'uso che fanno i terroristi di Internet come fattore abilitante e l'uso di strumenti informatici come capacità offensiva, sembra difficile comprendere l'orientamento italiano nell'interpretazione di questo fenomeno. Si pensa che questo potrebbe dipendere dall'attuale inesistenza di una fattispecie legale che tipizzi il terrorismo cibernetico (Florio 2023).

METODOLOGIA DI ANALISI DEL CASO SPECIFICO

Verrà nel seguito proposta una metodologia di analisi che potrebbe essere applicata anche ad altri gruppi terroristici riconosciuti, per comprendere a che punto siano nella loro transizione dal fisico al virtuale nonché se possano, sulla base delle loro attività e delle loro capacità tecniche, intraprendere azioni di terrorismo cibernetico minando così la sicurezza nazionale. Ogni gruppo terroristico possiede delle specifiche peculiarità che lo differenzia, in termini di ideologia, di struttura interna, di modus operandi e capacità, di auditorio bersaglio, di contesto storico e geografico ecc. Pertanto, prima di intraprendere qualsiasi sforzo analitico bisognerebbe avere contezza del gruppo terroristico su cui si vuole indagare attraverso lo studio del contesto storico, sociale e culturale nel quale si sviluppa ed entrare nelle logiche e nelle dinamiche che lo caratterizzano.

Partendo dal presupposto che il terrorismo cibernetico è un fenomeno del mondo virtuale per raccogliere e analizzare informazioni su di esso bisogna utilizzare all'interno del ciclo di intelligence delle metodologie di raccolta appropriate come

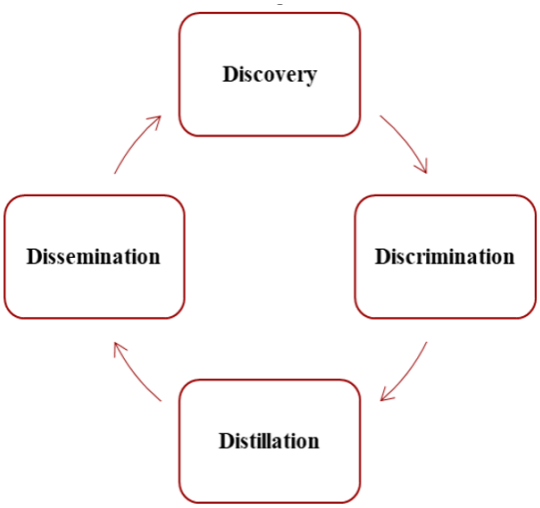


Figura 1: Le fasi del ciclo OSINT
Fonte: NATO Open Source Intelligence Handbook (2001).

l'OSINT, la SOCMINT o la VIRTUAL HUMINT (Virtual Human Intelligence)[5] che in questo caso verrà tralasciata. Posta la rete Internet come fonte principale su cui basare le operazioni di ricerca e raccolta delle informazioni, le fonti aperte di intelligence (OSINT) comprendono le informazioni appositamente cercate, selezionate, distillate e destinate a un gruppo selezionato per affrontare una richiesta specifica di intelligence (Figura 1). L'approccio analitico del processo OSINT si applica al ciclo di intelligence tradizionale [«il ciclo OSINT può sostituirsi, o innestarsi, in qualsiasi momento del ciclo di intelligence generale, in funzione del supporto informativo da garantire (integrazione, aggiornamento, approfondimento specialistico, riscontro informativo)», d'Amore 2020]. La SOCMINT è una delle metodologie di reperimento di informazioni utili al ciclo di intelligence tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i social media (Burato 2015); la differenza tra OSINT e SOCMINT è che quest'ultima ha come oggetto delle sue attività unicamente le informazioni che vengono scambiate mediante i social media, che non si limitano ai social network.

L'analisi OSINT potrebbe poi essere utilizzata per lo svolgimento di un'analisi strutturata che dia come risultato un prodotto di intelligence. L'analisi qualitativa scelta nel caso della metodologia proposta è l'ACH (Analysis of Competing Hypotheses)[6]: trattasi di un processo analitico che inizia con l'identificazione di un insieme di spiegazioni o risultati alternativi che si escludono a vicenda, chiamate "Ipotesi"; l'analista valuta la consistenza o l'inconsistenza di ogni evidenza con ciascuna ipotesi che meglio si adatta alle informazioni rilevanti (Pherson and Heuer 2021).

ANALISI OSINT E DIGITAL JIHAD: IL CASO DELL'ISLAMIC STATE (IS)

Dalla trattazione del terrorismo cibernetico nella sua accezione generale si passerà ad approfondire un caso di studio incentrato sul digital jihad dell'Islamic State (IS). Nel web di superficie e nel deep web esistono moltissimi siti pro-AQ e pro-IS (Figura 2); queste due organizzazioni riconosciute di terrorismo di matrice jihadista, secondo le ricerche effettuate, hanno avviato una vera e propria transizione spaziale dallo spazio fisico a quello virtuale dal 1998 circa e questo ha comportato un loro crescente utilizzo di Internet e delle TIC (tecnologie dell'informazione e della comunicazione) che ha contributo allo sviluppo di competenze sempre migliori per propaganda, reclutamen-

[5] https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)

[6] https://en.wikipedia.org/wiki/Analysis_of_competing_hypotheses

to, finanziamento, comunicazione, pianificazione, coordinamento e anche campagne d'influenza, favorendo una notevole produzione di materiale utilissimo per condurre un'analisi OSINT. È cruciale tenere presente che i terroristi di matrice jihadista, sia nello spazio fisico che in quello virtuale, si muovono secondo la logica d'imparare, innovare e adattarsi. In linea di massima il cyberspace offre la possibilità di svolgere attività relativamente sicure, redditizie e difficili da rilevare grazie alla pervasività e all'ubiquità che caratterizzano Internet. Inoltre, concede ai terroristi l'elemento dell'interscambiabilità tra spazio fisico e spazio cibernetico, per cui l'attività che avviene in una dimensione può benissimo espandersi all'altra dove effettivamente sussistono dei vincoli limitati per le attività di supporto o per le attività finalizzate al terrorismo. L'anonimato, come ha scritto Victoria J. Correia (2022) ha incentivato l'effetto dell'inibizione cognitiva che, unito alla mancanza della deterrenza, genera la dissociazione tra l'azione e il risultato finale incoraggiando il comportamento terroristico. Oltretutto, il sempre e maggiore uso dei social media da parte dei jihadisti ha contribuito allo sviluppo di un jihad visivo che punta alla costruzione del "buon musulmano online," sfruttando il potenziale delle immagini che hanno un effetto importante sia sulla percezione che sulla persuasione mediante l'uso di immagini emozionali e simbolismo (Macdonald et al. 2021). Facendo leva su una combinazione di fattori come la propaganda online si crea la logica dell'appropriatezza, ossia la scelta in base al sé percepito dai jihadisti e l'altra identità, pertanto si installa il "noi-contro-loro" in cui l'in-group è il noi e l'out-group è il loro, ossia il nemico (Macdonald et al. 2014), in perfetto accordo con quella che è l'ideologia jihadista. La tecnologia avvantaggia la continua comunicazione tra le diverse parti dei gruppi e questo rappresenta, come i fatti hanno dimostrato, un efficace mezzo di auto radicalizzazione di individui e gruppi in tutto il mondo. Sia AQ che IS sviluppano la loro capacità organizzativa per migliorare la propria sicurezza operativa (OPSEC) mediante comando e controllo decentralizzati nei confronti dei gruppi che li sostengono ai fini di una vera e propria resistenza senza leader, sfruttando le tecnologie emergenti e sviluppando nuove soluzioni tecniche nel caso in cui le loro comunicazioni e infrastrutture organizzative venissero attaccate (per esempio dalle operazioni di contrasto al terrorismo). Nel complesso, secondo questa impostazione, si

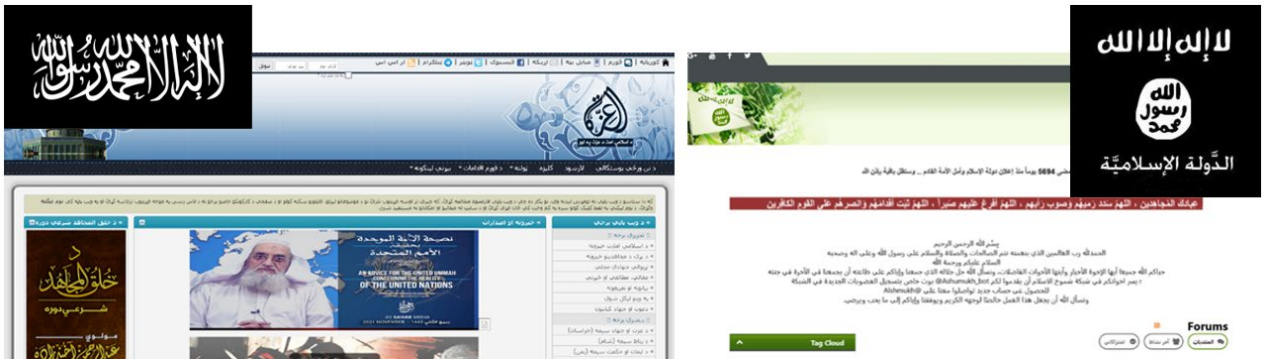


Figura 2: Snapshot di un sito web pro-AQ (sinistra) e uno pro-IS (destra).

viene a creare una vera e propria Ummah digitale[7], quasi globale, svincolata dal mondo fisico, che permette l'interconnessione tra compagni jihadisti di varie comunità come Asia, Medio Oriente, Europa e Americhe (Rudner 2017). Per evitare di raccogliere informazioni sul gruppo sbagliato è opportuno prestare molta attenzione a una serie di elementi caratterizzanti, tra i quali molto importante è quello della simbologia utilizzata dai vari gruppi jihadisti; quest'ultimo, infatti, potrebbe già rappresentare un ottimo elemento di scrematura. Una volta inquadrato quanto il cyberspace offre ai due gruppi per l'espletamento delle loro attività e approfondite le differenze esistenti si riporteranno di seguito i risultati ottenuti dall'analisi OSINT svolta sul solo digital jihad perpetrato dallo Stato Islamico (IS).

Il key customer ipotizzato per l'analisi è la Repubblica italiana. L'analisi puntava a produrre conoscenza su:

- uso dello spazio cibernetico da parte dell'organizzazione terroristica IS;
- capacità tecniche dell'IS inerenti al dominio cibernetico.

L'audience è un pubblico eterogeneo, in possesso di un background che va dal settore tecnico-scientifico a quello economico, politico-sociale e giuridico. Le fonti utilizzate sono siti istituzionali (Occidente e Medio Oriente), siti web di testate giornalistiche internazionali e locali (mediorientali), siti web satellite utilizzati dall'organizzazione terroristica stessa e legati ai siti ufficiali (deep web), organizzazioni pro-IS, forum, fonti derivanti dalla ricerca nel dark web, social network (Twitter, Facebook). Per il supporto metodologico è stata utilizzata la SOCMINT, per accedere ai social media è stato creato un apposito indirizzo e-mail usando l'applicazione open source di posta elettronica Tutanota, che sfrutta la crittografia end-to-end, mediante la quale sono stati creati due profili fake sui social network Twitter e Facebook per meri fini esplorativi.

Di seguito un elenco degli strumenti utilizzati per la ricerca:

- Browser: Firefox, TOR (The Onion Router);
- Motore di ricerca: Google, Duckduckgo, Duckduckgo.onion;
- Siti utili: https://osintframework.com/, https://osint.link/;
- Piattaforme: Internet Archive[8], Torch[9], JustPaste.it[10] (popolare tra le organizzazioni di IS per la diffusione di materiale propagandistico), Webmii[11], PasteThis.To[12] ;
- Verifica siti web: Wayback Machine[2];

[7] Comunità dei musulmani digitale

[8] https://web.archive.org/

[9] http://torch4st4l57l2u2vr5wqwvwyueucvnrao4xajqr2klmcmicrv7ccaad.onion. Solo su Tor.

[10] https://justpaste.it/

[11] https://webmii.com/

[12] https://pastethis.to/

[13] https://seotochecker.com/domain-to-ip/

- Verifica indirizzi IP: SEO To checker[13], Rankwatch[14], IpVoid[15];
- Verifica immagini: Google Immagini[16], Tineye[17];
- Traduzione: App Google traduttore (lettore ottico, microfono).

Per la creazione di un piano di raccolta strutturato si è scelto di selezionare un bacino limitato di fonti e di informazioni che rispondessero il più possibile alla richiesta. Si è partiti con la selezione delle parole chiave studiando l'IS e le sue province, la bandiera, la simbologia usata, i colori più frequenti, le lingue maggiormente utilizzate, i nomi più ricorrenti, le applicazioni sfruttate per la comunicazione online, i nomi delle principali piattaforme che distribuiscono prodotti mediatici, le applicazioni che vengono usate per la disseminazione dei prodotti mediatici, i magazine, le parole che utilizzano per identificarsi (per esempio se fosse ricorrente Ummah, Califfato, هفالخا, Khalifa, islam, jihad, cyberjihad ecc.), se venisse usato il termine terrorismo elettronico o cibernetico o addirittura non utilizzato. Il risultato è stato un piccolo glossario diviso in ordine alfabetico di parole chiave principalmente in due lingue: arabo e inglese.

RACCOLTA DELLE INFORMAZIONI

L'indagine OSINT è stata divisa in tre parti, per le quali sono state usate differenti tecniche.

La prima parte puntava a raccogliere fonti quanto più affidabili (siti istituzionali, centri studio, siti web dediti al monitoraggio dei gruppi estremisti, centri di ricerca specializzati nel contrasto al terrorismo, pagine web sulla cybersecurity ecc.) e a tal fine sono state impostate le opzioni di ricerca avanzata di Google grazie alla combinazione di parole chiave prevalentemente in lingua inglese relative alla sfera jihadista salafita.

Per la seconda parte è stato utilizzato l'OSINT framework, dal quale si è avuto accesso a utili forum, search engine, blog search engine ecc. ottenendo così le coordinate delle piattaforme maggiormente utilizzate dai gruppi sostenitori dello Stato Islamico per la condivisione di materiale propagandistico (news, video, nasheed e condivisione di link), tra cui Internet Archive, JustPaste.it e PasteThis.to. In questa fase si è avuto accesso a una vasta mole di materiale tramite la combinazione di un campo ristretto di parole chiave in arabo e inglese. Si è passati poi all'utilizzo di TOR perché la ricerca, a questo punto, necessitava di un maggiore livello di privacy e protezione ed è stato consultato e verificato manualmente un archivio aggiornato di link di gruppi estremisti (attivi e inattivi). Da qui si sono aperte le porte di una costellazione di siti jihadisti indistinti (quasi tutti in lingua araba o urdu) e, grazie allo studio della simbologia, si è riusciti a selezionare i siti pro-Stato Islamico e raccogliere importanti notizie finalizzate alla richiesta. Attraverso l'uso di TOR e duckduckgo.onion è stata

[14] https://www.rankwatch.com/free-tools/domain-to-iP-converter-tool

[15] https://www.ipvoid.com/find-website-ip/

[16] https://images.google.com

[17] https://tineye.com

individuato un URL apparentemente "tradizionale" ma che in realtà era un link .onion (dark web) pro-IS, dal quale si è avuto accesso a una vasta mole di materiale come news, articoli, magazine come «Al-Naaba'», nasheed, ma soprattutto a un altro link .onion che a sua volta raccoglieva una lista di siti pro-IS e rimandava a un terzo link di questo tipo nel dark web.

La terza fase si riferisce alla ricerca SOCMINT, per la quale ci si è avvalsi di due fake account per meri fini esplorativi. Non è stato aggiunto o contattato alcun utente, sono stati fatti dei tentativi su Facebook ma ai fini della richiesta la ricerca si è spostata su Twitter, dove è stato utilizzato un repository anonimo che raccoglie ID Twitter di possibili estremisti jihadisti, utili sono stati, inoltre, i contatti trovati nelle pagine pro-IS in arabo. Alcuni tentativi di ricerca sono stati svolti utilizzando parole chiave o nomi non offuscati catturati dai video tutorial di alcune pagine pro-IS. Uno strumento molto utile è stato Webmii, un people search engine che aiuta a trovare informazioni pubbliche. Nel caso specifico per questa analisi si è riusciti a raggiungere, tramite un preciso nome, un archivio relativamente recente (2019) di un gruppo di InfoSec pro-IS che disponeva di una pagina web ufficiale (e non) oggi inattiva. Oltretutto Webmii ci ha portati a Tgstat.com (catalogo online di canali Telegram) dal quale sono state ricavate alcune risorse di Telegram condivise dal gruppo in questione, strettamente inerenti alla richiesta dell'analisi. Tgstat rappresenta un buon escamotage laddove l'uso diretto di applicazioni come Telegram non sia possibile, per esempio potrebbe essere utile cercare su questo tool gli ID dei canali Telegram forniti nelle pagine web pro-IS per ottenere i link .onion e così, tramite tentativi, creare una rete.

PIANO DI RACCOLTA

Il piano di raccolta strutturato della ricerca OSINT è stato sviluppato su un foglio di Microsoft Excel che conteneva 41 fonti provenienti dal Web di superficie, deep e dark web. L'affidabilità della maggior parte delle fonti è stata valutata secondo il modello della Canadian Checklist per la valutazione delle fonti su Internet, per cui la valutazione è condotta attraverso una lista di controllo composta da diverse domande alle quali gli analisti devono rispondere e assegnare un punteggio compreso tra 0 e 3. Il punteggio totale corrisponderà a una valutazione sintetica (espressa attraverso A, B, C, D, E, F) che definisce l'affidabilità della fonte (molto alta, alta, media, bassa, molto bassa, non valutabile). Per alcune fonti del deep web e dark web di cui risultava difficile la valutazione si è usato il sistema Admiralty/NATO[18], un esempio sono i siti web pro-IS completamente anonimi o alcuni utenti Twitter. La credibilità delle informazioni è stata valutata seguendo uno schema di domande guida collegato al sistema Admiralty/NATO.

È stata poi svolta un'analisi statistica sul piano di raccolta OSINT di quante notizie più o meno affidabili si sono ottenute (Figura 3) ed è risultato che,

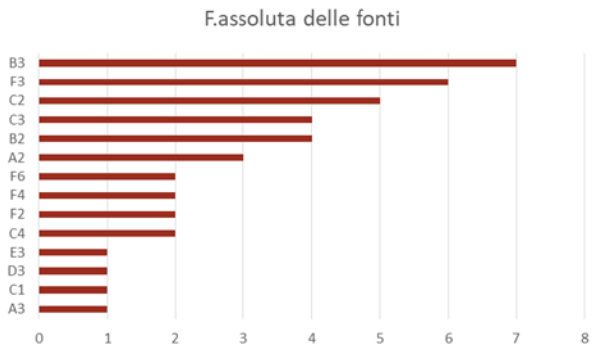


Figura 3: Frequenza assoluta delle fonti.

per questo piano di raccolta, a prevalere di poco è un livello di affidabilità e credibilità B3 (solitamente affidabile / forse vero), ma degno di nota è il secondo posto occupato da fonti F3 (affidabilità non giudicabile / forse vero). Questo risultato si crede dovuto alla tipologia di richiesta per la quale la maggior parte della raccolta si è spostata nel deep web, quindi verso siti la cui affidabilità non era giudicabile, nonostante gli strumenti a disposizione. Nel caso del dark web la ricerca è stata ardua nonostante l'uso di search engine quali Torch e altri o l'esplorazione di forum come Libreddit. Difatti, mediante l'uso di parole chiave in arabo e inglese, non si sono ottenuti risultati soddisfacenti coerenti con la richiesta. In questo caso i metodi risultati più proficui per ottenere link .onion sono l'attenta disamina dei siti web satellite che potrebbero rimandare a delle reti di link (link che collegano ad altri link e così via) oppure ottenerli accedendo ai canali Telegram (o altre applicazioni simili come Element) tramite i contatti forniti dalle pagine in questione; per questo piano di raccolta si è potuta seguire solo la prima opzione. Un altro elemento da tenere in considerazione è la raccolta fatta su Twitter, dove gli account erano difficili da valutare, poiché in questi casi è facile cadere nel vortice degli account fake creati, per esempio, dai governi per il monitoraggio e il contrasto al terrorismo. Proprio per questo per ognuno dei profili è stata condotta una verifica sull'affidabilità, in alcuni casi ottenendo dei risultati e in altri no.

Un'ulteriore analisi statistica è stata generata sulla frequenza assoluta, relativa e percentuale del Topic (Figura 4), quindi sono stati prima scelti un massimo di tre argomenti nel caso specifico (Cyberterrorism, Jihad, Digital Jihad), da cui è emerso che la raccolta si è concentrata per il 44% sul Digital jihad e per il 34% sul Jihad, mentre il Cyberterrorism ha ottenuto la percentuale minore. Il fatto che il topic Digital Jihad abbia ottenuto la percentuale maggiore indica che il piano di raccolta è coerente con la richiesta fatta. Per quanto riguarda invece il 22% ottenuto per il Cyberterrorism, potrebbe essere collegato anche al fatto che il topic venga usato solitamente ad alto livello. Infatti, più l'indagine veniva canalizzata nel deep web, meno le parole chiave usate nella prima fase della ricerca funzionavano e meno affidabili risultavano le fonti, nonostante sia stato possibile confutare la credibilità di buona parte delle notizie raccolte.

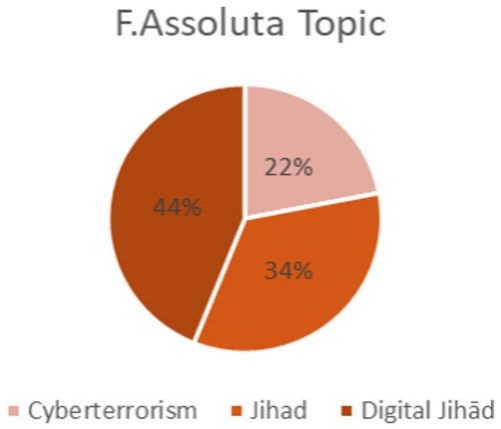


Figura 4: Frequenza assoluta del topic.

[18] https://en.wikipedia.org/wiki/Admiralty_code

RISULTATI

L'analisi puntava a produrre conoscenza su:

a) Uso dello spazio cibernetico da parte dell'organizzazione terroristica IS

L'analisi ha dimostrato che lo Stato Islamico ha integrato e implementato le sue attività nello spazio cibernetico. L'organizzazione si dirama in una costellazione di gruppi satellite resilienti e questo consente sia ai simpatizzanti che agli estremisti di non perdere la rete di contatti ove questa venisse attaccata da operazioni di contrasto al terrorismo. Dal totale delle fonti esaminate, risultano più attivi sul web i gruppi jihadisti pro-IS rispetto all'organizzazione centrale stessa. Nonostante lo Stato Islamico abbia affrontato un periodo di crisi dopo il collasso del Califfato avvenuto nel 2019, sembra che in tempi recenti abbia sfruttato l'evento del COVID-19 per rilanciare e migliorare la sua attività online sfruttando i social media e incitando, sul campo sia fisico che digitale, l'azione dei suoi sostenitori sparsi per tutto il globo tramite le sue piattaforme ufficiali decentralizzate per la diffusione della propaganda e della narrazione jihadista. Il fattore della decentralizzazione risulta considerevole ai fini dell'uso dello spazio cibernetico poiché i gruppi jihadisti o i gruppi pro-IS si stanno espandendo a livello intellettuale più di quanto non lo sia l'organizzazione centrale stessa e questo gli permette di avere successo nel consolidare l'ideologia ed espandere la conoscenza su larga scala senza limiti territoriali; quest'ultimo è un fattore rilevante, perché potrebbe generare un problema interno allo Stato italiano. Dalle fonti osservate è emerso che la sfera dei "soldati" che si muove nel mondo virtuale è fluida, anonima e resiliente nel perpetrare il digital jihad, pertanto è diversa da quella che opera sul campo fisico. Alcuni dei social media maggiormente sfruttati dai gruppi dello Stato Islamico rilevati dalla ricerca OSINT sono: SoundCloud, Youtube, Vimeo, DailyMotion SendVid, Wikr, Tam Tam, Telegram, Element, Threema, Riot, Rocket Chat, Reddit, Twitter e Facebook. Inoltre, la disseminazione dei prodotti mediatici può essere trovata prevalentemente nel deep e dark web. L'analisi delle notizie raccolte ha evidenziato che l'uso dello spazio cibernetico non si limita alla propaganda, narrazione, reclutamento o finanziamento; durante la sua esistenza l'IS, anche a causa delle operazioni governative di contrasto al terrorismo, ha sviluppato una sempre maggiore capacità difensiva nonché una volontà offensiva.

b) Capacità tecniche dell'IS inerenti al dominio cibernetico

Dall'analisi è emerso che un buon metodo per intendere le capacità tecniche di IS e dei suoi seguaci è monitorare le loro pubblicazioni focalizzate sulla cybersecurity e information security, nonché le dichiarazioni, ove vi fossero, di gruppi hacker o di esperti tecnici che si schierano con l'IS. Il gruppo jihadista dimostra continuamente che ha bisogno, per il suo jihad globale, di essere presente nel dominio cibernetico mediante il digital jihad; quindi, produce e distribuisce contenuti senza limiti di tempo e di spazio per informare e rendere consapevole la Ummah delle minacce che la circondano. L'analisi ha dimostrato che i gruppi pro-IS possiedono effettivamente delle competenze tecniche in evoluzione di cui non si conosce il livello reale, che tuttavia potrebbe essere valutato da professionisti del settore mediante il metodo succitato. Un ulteriore elemento

rilevante è la controsservazione posta in essere dai gruppi jihadisti nei confronti degli Stati che li monitorano e li combattono; infatti è anche grazie a questa attività che stanno implementando le loro capacità di difesa in ambito tecnico e stanno avanzando campagne di awareness verso la Ummah. Da quando l'organizzazione è stata fondata si sono verificati casi di gruppi di hacker dichiaratisi pro-IS, come per esempio, nel 2015, quello di Jumaid Hussain c.d. "TriCk", cittadino britannico che andò a combattere per l'allora ISIS e che divenne leader della Cyber Caliphate Army, prima squadra di hacking legata all'IS; il suo successore fu Siful Haque Sujan, di cittadinanza bangladese. Dalle fonti sono stati individuati altri gruppi simili, come l'Islamic State Hacking Division o The United Cyber Caliphate (UCC), anche se dall'indagine svolta risulta che questi gruppi non solo non siano più attivi ma che non abbiano nemmeno condotto attività minacciose. Si segnala però la volontà offensiva, che – se identificata e monitorata – potrebbe rappresentare un buon sensore di sviluppo dell'intenzione di condurre attività con finalità terroristiche nello spazio cibernetico da parte di gruppi decentralizzati dello Stato Islamico. L'analisi delle fonti consente di comprendere la capacità difensiva nel cyberspace di cui i gruppi jihadisti (IS) sono e potrebbero essere in possesso, in tal senso una delle capacità rilevate risiede nell' Information Security (in particolare nell'uso della crittografia) ma anche nella conoscenza dell'uso delle Virtual Private Network (VPN)[19]. Inoltre, dai link controllati è stata osservata la capacità di sfruttare la tecnica dei link-shortener[20], che comprime un URL originale e lo rende impossibile da interpretare a vista. Anche nel caso della documentazione inerente alla sicurezza delle informazioni su Internet e alla cybersecurity in generale tali gruppi produ-

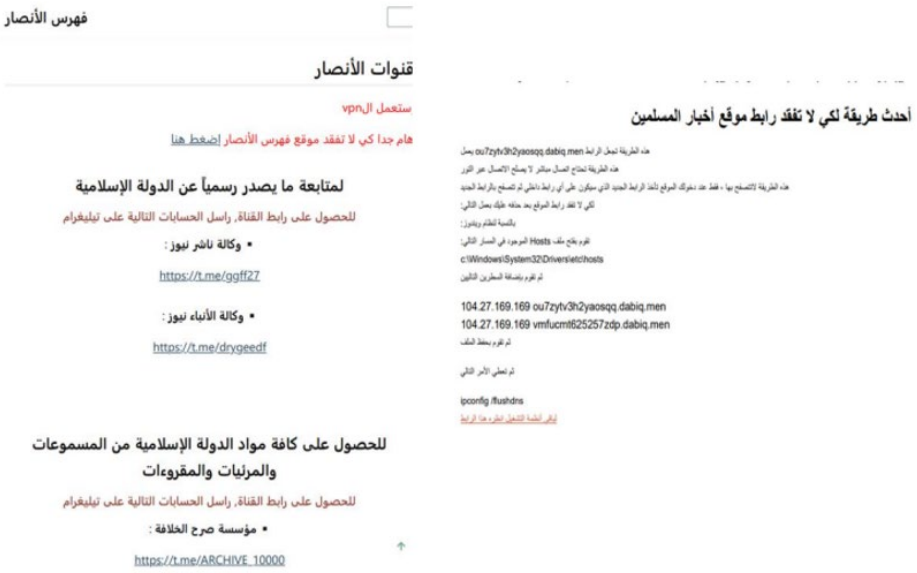


Figura 5: Snapshot di due siti pro-IS nel dark web.

[19] https://en.wikipedia.org/wiki/Virtual_private_network

[20] https://en.wikipedia.org/wiki/URL_shortening

Figura 6: Snapshot siti web pro-IS Deep Web.

cono e disseminano manuali, video tutorial, testi esplicativi, articoli ecc.

Di seguito (Figura 5) alcuni snapshot esplicativi a sostegno dei risultati dell'analisi OSINT.

Entrambe le acquisizioni provengono dal dark web e forniscono indici aggiornati e indicazioni utili per non perdere l'attività dell'IS. Nell'immagine a destra il titolo si traduce come "Ultimo modo per non perdere il collegamento al sito di news musulmane" mentre l'altra, a sinistra, fornisce una serie di link utili per non perdere il materiale e le pubblicazioni ufficiali dello Stato Islamico, incluso un link di collegamento a Web Archive. La Figura 6 rappresenta due fonti che producono notizie nell'ambito delle scienze, della tecnologia e dell'informazione: alcuni argomenti trattati sono per esempio sul come specializzarsi in programmazione (website development o database development, application

Figura 7: Snapshot dimostrativo del materiale pubblicato da EHF.

development, mobile application development). La fonte di destra è un sito pro-IS impegnato nella diffusione delle competenze informatiche per fini difensivi, i temi maggiormente trattati sono come imparare a scoprire se l'account personale è stato hackerato e come proteggersi, social media, legal espionage, guida sulla protezione dei cellulari, rischi per la sicurezza dei cellulari, lezioni sull'IP e sulla crittografia, come usare Telegram, METADA, metodi e tecniche di information gathering, come progettare un sito web, come crittografare la memoria di un cellulare Android, la differenza tra cybersecurity e information security.

Un gruppo pro-IS degno di nota è l'Electronic Horizons Foundation, che ha dimostrato mediante le sue pubblicazioni un'ampia conoscenza delle materie inerenti all'ambito dell'informatica (in particolare information security e cybersecurity), ha prodotto moltissimo materiale e nel 2021 ha dichiarato di aver sviluppato la Horizons Cloud Platform; tuttavia, dai controlli effettuati momentaneamente le sue pagine sono inattive. In un archivio della loro produzione di materiale tecnico trovato su PasteThis.to (ultima pubblicazione risale al 2019) vengono illustrate le tecniche di raccolta delle informazioni [cookies[21], active web contents,

Traduzione del testo in arabo:

They are intelligence alliance between a number of countries in the word that work together to monitor the Internet to collection and share the largest number of data that presets its analysis, so it acts as a global monitoring entity to monitor any and record your activities. Therefore, we note that security precautions must be taken when present in these countries or using sensitive services that take their headquarters of servers such as hosting services and VPN services.

Figura 8: Snapshot punto 8 di un articolo della EHF intitolato "The Fourteen eyes".

[21] https://en.wikipedia.org/wiki/HTTP_cookie

JavaScript[22], Browser Fingerprinting[23], Browser history and cache, Web bugs and banner[24], ADS TCP Timestamps, IP (Internet Protocol)[25]].

Sono presenti, inoltre, molte guide per l'installazione e l'uso di TOR anche su sistema Android (Figura 7, immagine a destra), nonché consigli sull'installazione di proxy di TOR nell'app di Twitter. Molto interessante è la lista di un buon numero di servizi VPN gratuiti (Figura 7, immagine al centro) che violano la privacy degli utenti sfruttando i loro dati a scopi commerciali.

L'ultimo elemento ritenuto rilevante a sostegno del fatto che i gruppi in questione monitorano a loro volta, nei limiti delle loro capacità, il nemico (USA e alleati) è la Figura 8, parte di un articolo sull'InfoSec nel quale è inclusa anche l'Italia. L'articolo si intitola «The Fourteen eyes» e mette in guardia la Ummah dagli occhi di 14 stati tracciando uno schema che rappresenta un'intelligence alliance. Il core è costituito dagli USA, UK, Australia, Nuova Zelanda, Canada seguono Francia, Svizzera, Norvegia, Olanda. L'Italia si trova nel cerchio esterno insieme a Svezia, Spagna, Belgio e Germania.

IL DIGITAL JIHAD ACTIVITY FRAMEWORK (DJAF)

Il Framework in Figura 9 è stato selezionato dalla ricerca di Victoria Janada Correia intitolata «An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom» del 2022. Sebbene il TAF (Terrorist Activity Framework) sia basato su uno studio condotto per il Regno Unito, lo si crede utile ai fini di una comprensione più chiara di alcune tipologie di attività terroristiche che si verificano o si potrebbero verificare nel cyberspace, nonché per mettere in luce i collegamenti tra terrorismo tradizionale e terrorismo cibernetico. Correia (2022) ha proposto un modello ternario, vale a dire l'incrocio tra tre categorie di terrorismo (Traditional Terrorism, Cyber Enabled Terrorism, Cyber Dependent Terrorism) e quattro tipologie di attività terroristica (Recruitment, Organisation and Planning, Preparatory Conduct, Terrorist Act). Il TAF mette in evidenza le somiglianze tra i tre tipi di terrorismo e mediante le frecce accentua ulteriormente i collegamenti che possono sussistere tra l'uno e l'altro. I differenti percorsi hanno tutti come output un terrorist act e una tipologia di vittima. Tuttavia non è detto che le prime tre fasi si susseguano sistematicamente, in quanto potrebbero verificarsi simultaneamente.

Si richiama l'attenzione poi sulla categoria del Cyber Enabled Terrorism, le cui attività hanno alla terza fase la possibilità di diramarsi sia nei percorsi tradizionali sia in quelli Cyber Dependent in quanto l'attività del Cyber Enabled Terrorism può essere di supporto per gli altri due percorsi. Per quanto riguarda l'attività di Recruitment, sia per il terrorismo tradizionale che per quello cibernetico, ha la capacità di rimanere attiva in background durante l'intero processo, indipendentemente dall'attacco terroristico. Per ciò che concerne gli effetti

[22] https://en.wikipedia.org/wiki/JavaScript

[23] https://en.wikipedia.org/wiki/Device_fingerprint

[24] https://en.wikipedia.org/wiki/Web_beacon

[25] https://en.wikipedia.org/wiki/Internet_Protocol

dell'atto di terrorismo cibernetico – e quindi la vittimologia – dal TAF si evince che per il Traditional Terrorism l'attentato ha come risultato le human victim, per il Cyber Enabled Terrorism il processo potrebbe deviare nella fase tre (Preparatory Conduct) e quindi concludersi o come un atto di terrorismo tradizionale o come un atto di terrorismo cibernetico. Il Cyber Dependent Terrorism invece si sviluppa interamente nel Quinto dominio ed è l'unico che ha come risultato dell'atto terroristico sia vittime umane sia i sistemi informatici. Incrociando le informazioni derivanti dell'analisi OSINT della sezione precedente e il Terrorist Activity Framework è possibile, a questo punto, provare a posizionare lo Stato Islamico in una delle tre categorie sulla base delle sue attività nel perseguimento del digital jihad. Seguendo questo framework lo Stato Islamico, che comprende le sue province e tutti i gruppi simpatizzanti, va classificato come Cyber Enabled Terrorism, le cui attività, come si può notare, hanno alla terza fase la possibilità di diramarsi sia nei percorsi tradizionali sia in quelli del Cyber Dependent Terrorism.

ANALYSIS OF COMPETING HYPOTHESES (ACH): IL DIGITAL JIHAD RAPPRESENTA UNA MINACCIA PER LE INFRASTRUTTURE CRITICHE ITALIANE?

Dopo aver quindi compreso a che punto si trova l'IS nella sua evoluzione e averlo posizionato in un framework, la metodologia proposta prevede l'utilizzo di tali informazioni per un'analisi di intelligence. Visto che generalmente un terrorista punta al danneggiamento o alla distruzione dei settori essenziali che costituiscono un ordinamento nazionale, ai fini della ricerca si è ritenuto interessante analizzare quali siano le infrastrutture critiche (materiali e immateriali) italiane che potrebbero rappresentare un potenziale target per il digital jihad, provocando gravi effetti sulla sicurezza del nostro Paese sia a livello cibernetico che fisico. Considerando che le ICN (infrastrutture critiche nazionali) sono completamente gestite da sistemi informatici, interconnesse dalla rete Internet e fortemente interdipendenti, il verificarsi di un attacco di terrorismo cibernetico potrebbe danneggiare o distruggere non solo l'infrastruttura stessa, ma anche l'erogazione di un servizio vitale al cittadino. Un esempio sono i servizi non immagazzinabili come le telecomunicazioni e l'elettricità, la cui fruizione potrebbe cessare se dovesse verificarsi un grave attacco alle infrastrutture che le erogano. Dopo aver individuato le infrastrutture critiche nazionali ci si è avvalsi di una tecnica di analisi strutturata, in questo caso l'Analysis of Competing Hypotheses (ACH)[26], il cui key customer ipotizzato è la Repubblica italiana.

La richiesta era: "Il Digital jihad rappresenta una minaccia per le infrastrutture critiche italiane?"

Il principio scientifico alla base di questa tecnica è di procedere cercando di confutare quante più ipotesi ragionevoli possibili, piuttosto che confermare quella che inizialmente sembra essere l'ipotesi più probabile. L'ipotesi più probabile è quindi quella con la minor quantità di informazioni inconsistenti, non quella con un'abbondanza di informazioni rilevanti a supporto. Si è scelto di svolgere l'analisi manualmente usando un file Excel impo-

[26] https://en.wikipedia.org/wiki/Analysis_of_competing_hypotheses

H:1	H:2	H:3
IS sta sviluppando la sua capacità tecnica offensiva	IS potrebbe essere sponsorizzato da uno Stato per un atto di terrorismo cibernetico	IS ha solo una capacità tecnica difensiva

Tabella 1: Le tre ipotesi (H) dell'analisi ACH.

stato in maniera molto simile al famoso modello proposto dal software PARC ACH 2.0.5 sviluppato dal Palo Alto Research Center. La prima fase del processo è la formulazione ragionata e quanto più oggettiva di potenziali ipotesi, le quali costituiscono il fondamento principale su cui si basa tutta l'analisi (Teti 2015). In questo caso ne sono state identificate 3, riportate nella tabella 1.

Le ipotesi rappresentano tre proposte di scenario basate su ciò che è vero, su ciò che esiste o che accadrà e riguardano tutte delle ragionevoli possibilità che possono verificarsi, incluse quelle che sembrano improbabili ma non impossibili. L'ipotesi due (H:2) era quella con un minor numero di informazioni a sostegno, ma si è potuta comunque inserire perché esistevano almeno due prove che la supportassero. Come si può notare dalla formulazione, le ipotesi si escludono a vicenda; infatti, se H:1 è vera, H:3 e H:2 devono essere false. Le ipotesi fanno parte di una matrice di cui un esempio è la Figura 10.

Tutte le ipotesi sono correlate da prove (Evidence) che in questo caso derivano dal piano di raccolta OSINT: queste ultime devono poi essere aggiunte alla matrice per valutarne la Credibilità e la Rilevanza. Per ogni ipotesi (H1/H2/H3) bisogna fare una diagnosi valutando se ogni singolo elemento di Evidence è N (Neutral/Not Applicable), C (Consistent), CC (Very Consistent), I (Inconsistent), II (Very Inconsistent). Per assegnare uno di questi valori ci si è posti questa domanda: «l'informazione è consistente con l'ipotesi, è inconsistente con l'ipotesi o non applicabile o non rilevante?». Una volta completata la valutazione risulteranno dei numeri sotto ogni ipotesi. Nel caso di questa analisi si è applicato il Weighted Inconsistency Score, che valuta l'inconsistenza tenendo conto del valore di ogni punteggio calcolato sulla base della credibilità e della pertinenza con l'elemento di prova. In questa analisi la più plausibile è la H:2 "IS potrebbe essere sponsorizzato da uno Stato per un atto di terrorismo cibernetico", perché possiede il numero di (I) Inconsistent o (II) Very Inconsistent minore. Questo risultato è stato poi sfruttato per un'analisi di intelligence previsionale a breve e lungo termine, il cui risultato è riportato di seguito.

A. Nel breve termine non dovrebbero verificarsi attacchi di terrorismo cibernetico alle infrastrutture critiche (materiali e immateriali) italiane che mettano in pericolo la sicurezza della Repubblica, poiché lo Stato Islamico e i gruppi pro-IS sono dotati, al momento, di una capacità tecnica difensiva, nonostante si segnali una crescente capacità tecnica offensiva. Per condurre atti di terrorismo cibernetico illegali, violenti e politicamente motivati che sortiscano effetti di vasta portata e che quindi intacchino i servizi essenziali mettendo così

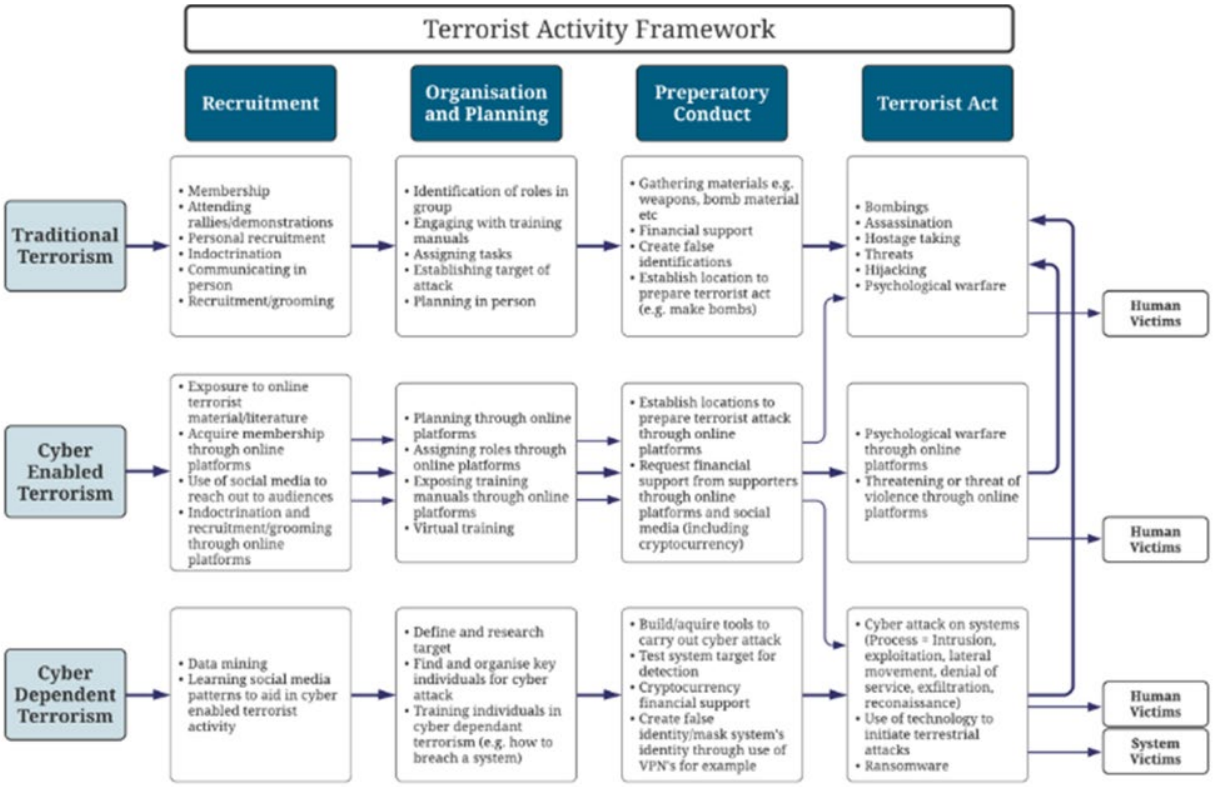
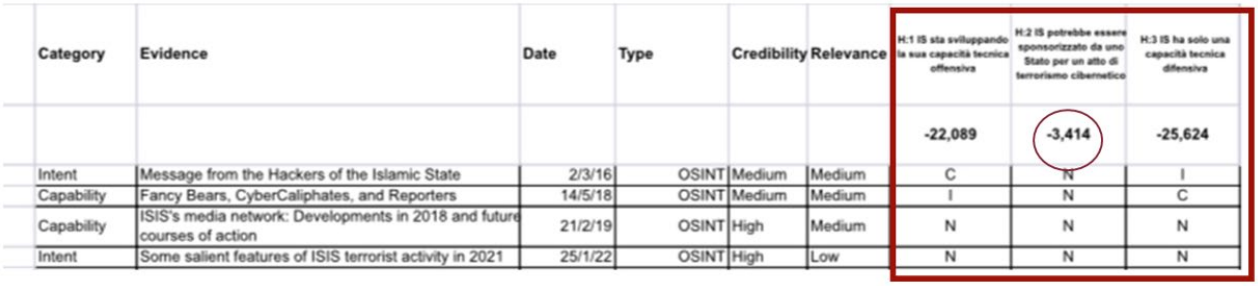


Figura 9: Terrorist Activity Framework entailing cyber terrorism
Fonte: Correia, J. V. (2022), An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, in Computer Science, vol.3, n. 84, p.83

in discussione gli interessi strategici della nostra nazione (politici, militari, economici, scientifici e industriali), l'IS potrebbe essere sponsorizzato da uno Stato e quindi agire con il sostegno, il supporto o l'istigazione di una potenza straniera nel perseguimento di un attacco di terrorismo cibernetico contro le ICN (infrastrutture critiche nazionali) maggiormente colpite da attacchi cibernetici. Tra le ICN che potrebbero rappresentare un obiettivo, coerentemente con la richiesta, si riportano per il settore pubblico le infrastrutture IT riferibili a enti locali e strutture sanitarie; per il settore privato quello energetico, dei trasporti e delle telecomunicazioni. Particolare attenzione dovrebbe essere indirizzata inoltre alle tecnologie di automazione industriale e ai sistemi cyber fisici, in quanto le reti di molte infrastrutture critiche del Paese dipendono in modo strategico da sistemi SCADA (Supervisory Control and Data Acquisition) che, se attaccati nella loro mansione di sistemi informatici per il monitoraggio e il controllo di sistemi industriali, potrebbero provocare seri danni anche ai cittadini.

B. Nel lungo termine si ipotizza che l'IS, nel perseguimento del suo digital jihad, possa sviluppare sempre di più una capacità offensiva dovuta anche alla particolare decentralizzazione che lo caratterizza, difatti i gruppi pro-IS che operano nel cyberspace sono fluidi, dinamici e resilienti e potrebbero essere composti da soggetti di differente nazionalità aventi capacità tecniche avan-



	Category	Evidence	Date	Type	Credibility	Relevance	H:1 IS sta sviluppando la sua capacità tecnica offensiva	H:2 IS potrebbe essere sponsorizzato da uno Stato per un atto di terrorismo cibernetico	H:3 IS ha solo una capacità tecnica difensiva
							-22,089	-3,414	-25,624
	Intent	Message from the Hackers of the Islamic State	2/3/16	OSINT	Medium	Medium	C	N	I
	Capability	Fancy Bears, CyberCaliphates, and Reporters	14/5/18	OSINT	Medium	Medium	I	N	C
	Capability	ISIS's media network: Developments in 2018 and future courses of action	21/2/19	OSINT	High	Medium	N	N	N
	Intent	Some salient features of ISIS terrorist activity in 2021	25/1/22	OSINT	High	Low	N	N	N

Figura 10: Esempio matrice analisi ACH.

zate. Pertanto, si prevede che nell'arco di 20 anni l'IS possa giungere ad avere efficaci ed efficienti competenze offensive transnazionali incentrate maggiormente nell'ambito della programmazione, della sicurezza delle informazioni e della cybersecurity. Secondo l'analisi svolta lo Stato Islamico farà leva sempre di più sul perseguimento del digital jihad da parte del singolo jihadista, il quale potrebbe trovarsi sia al di fuori dei confini italiani sia al suo interno.

CONCLUSIONI

Avevamo l'obiettivo di studiare il fenomeno del terrorismo cibernetico, mettere in pratica una metodologia e dimostrarla con lo studio di un caso specifico, nonché di proporre un contributo innovativo per la ricerca. La revisione della letteratura ha evidenziato che non esiste in Italia una definizione di terrorismo cibernetico e una sua relativa categorizzazione. Formulare una definizione di un fenomeno complesso e mai verificatosi potrebbe essere controproducente; tuttavia, se ne proporrà una seguendo il principio filosofico del «rasoio di Occam» secondo il quale occorre circoscrivere il problema al nucleo essenziale, senza aggiungere elementi interpretativi non necessari e preferendo le interpretazioni più semplici rispetto a quelle più astratte (Caligiuri 2019). Ciò non implica che la spiegazione più semplice sia sempre quella più corretta, ma occorre trovare il giusto bilanciamento tra semplicità ed efficacia. Nel proporre una definizione di terrorismo cibernetico si seguirà una rappresentazione che sia coerente con la realtà, con lo scopo di tracciare le linee generali di un fenomeno mai verificatosi finora.

"Terrorismo cibernetico" è l'insieme di azioni illegali e violente perpetrate da singoli o da gruppi che agiscono clandestinamente nello spazio cibernetico spinti da motivi ideologici, politici o confessionali allo scopo di compiere atti terroristici mediante strumenti informatici o telematici contro gli assetti informatici del bersaglio che vogliono colpire, distruggendo o destabilizzando la popolazione civile, uno Stato e i suoi interessi o un'organizzazione internazionale per diffondere terrore e condizionare orientamenti e scelte (Florio 2023).

La definizione del fenomeno spiana la strada per un ulteriore tentativo di innovazione che nasce da una necessità dovuta alla metamorfosi che i gruppi terroristici stanno subendo. Nel caso in cui si dovesse verificare un attacco cibernetico, a meno che non sussista un'inequivocabile rivendicazione da parte del gruppo terroristico agente, sarebbe difficile per un tecnico etichettarlo come terroristico. Per limitare il campo di indagine e creare

un quadro statico si propone un esempio di categorizzazione empirica (Mantici 2019) alla quale si tenterà di includere il terrorismo cibernetico sia come sottocategoria del terrorismo tradizionale sia come nuova categoria a sé stante. La madre di tutte le categorie terroristiche è l'eversione, tuttavia sotto quest'ultima si posizionano anche altri fenomeni come la violenza politica e la guerriglia (nei casi più estremi). Il terrorismo tradizionale si dirama in terrorismo nazionale (es. Brigate Rosse, Prima Linea ecc.) e terrorismo internazionale (es. terrorismo internazionale di matrice jihadista), terrorismo di Stato e terrorismo sponsorizzato da uno Stato, a loro volta caratterizzate da sottocategorie che non verranno approfondite in questo documento. In generale nel caso del terrorismo cibernetico queste distinzioni diventano difficilmente applicabili, a causa della natura transnazionale del fenomeno e della difficoltà, oltretutto, di identificare i colpevoli grazie non solo alle caratteristiche dell'ubiquità e della pervasività che offre Internet ma anche all'anonimato.

Per "eversione" si intende l'insieme delle attività che mirano ad alterare gli assetti istituzionali di un Paese con atti violenti, illegali e politicamente motivati.

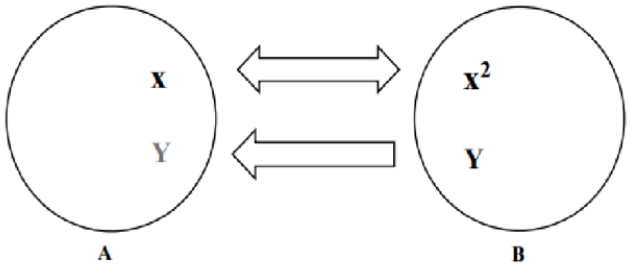
Il "terrorismo" deve essere un insieme di azioni politicamente motivate, violente e illegali, perpetrate da singoli o da gruppi che agiscono perfettamente mimetizzati all'interno della società che vogliono colpire e che puntano all'attenzione di un auditorio bersaglio, il quale rappresenta l'obiettivo dell'azione terroristica.

Le categorie succitate fanno chiaramente riferimento al terrorismo "tradizionale" che si muove e si sviluppa nel mondo reale. Se volessimo categorizzare il terrorismo cibernetico basandoci sull'esperienza non potremmo farlo, poiché il fenomeno inteso nel senso più "puro" non si è ancora realizzato, ecco perché nel titolo si fa riferimento all'evolversi della minaccia eversiva. Dunque, alla luce di quanto osservato, il fenomeno potrebbe essere trattato in due modi, come sottocategoria del terrorismo tradizionale o come categoria a sé stante. Il "terrorismo cibernetico come sottocategoria del terrorismo tradizionale" potrebbe essere un insieme di azioni politicamente motivate, violente e illegali perpetrate da singoli o da gruppi che agiscono clandestinamente nello spazio cibernetico, al fine di perpetrare condotte e/o atti che hanno finalità terroristiche sfruttando strumenti informatici o telematici (Florio 2023).

Il "terrorismo cibernetico propriamente detto" potrebbe essere un insieme di azioni politicamente motivate, violente e illegali perpetrate da singoli o da gruppi che agiscono clandestinamente e totalmente nel mondo cibernetico al fine di compiere atti terroristici mediante strumenti informatici e telematici contro gli assetti istituzionali digitalizzati del bersaglio che vogliono colpire (Ibidem).

Si vuole sottolineare che entrambi gli esempi puntano all'attenzione di un auditorio bersaglio il quale rappresenta l'obiettivo dell'attività terroristica.

Visto il quadro teorico nazionale tracciato fin qui e tenendo conto della legge vigente in Italia, dalla Figura 11 si può intuire che il terrorismo tradizionale, così come erano per esempio le Brigate Rosse degli anni Settanta, nasce, si sviluppa e agisce nel mondo reale (A). Nel momento in cui i gruppi del terrorismo tradizionale iniziano a transitare nel-



A: Mondo fisico;

B: Spazio cibernetico;

X: Singolo o gruppo terroristico che nasce, si sviluppa e agisce nel mondo A;

X^2: Singolo o gruppo terroristico che nasce e si sviluppa nel mondo A, ma che sfrutta in mondo B e agisce in esso provocando delle conseguenze o nel mondo A o nel mondo B;

Y: Singolo o gruppo terroristico che nasce e si sviluppa nel mondo B (completamente appartenente allo spazio cibernetico) e agisce nel mondo B provocando delle conseguenze anche nel mondo A.

Figura 11: Schema logico dell'esempio di categorizzazione.
Fonte: P. Florio (2023), Terrorismo cibernetico e sicurezza nazionale, p.49.

lo spazio cibernetico (B) per perpetrare condotte prodromiche alla prestazione di atti di terrorismo (propaganda, finanziamento, reclutamento, addestramento per finalità terroristiche ecc.) o per condurre attentati terroristici che hanno delle effettive conseguenze nel mondo A o nel mondo B, inevitabilmente mutano e diventano x2. Tuttavia, per parlare di terrorismo cibernetico puro sarebbe forse erroneo legarlo a una sottocategoria del terrorismo tradizionale poiché – pur trattandosi di due fenomeni con caratteristiche molto simili (terrorismo) – essi nascono, si sviluppano e agiscono in due mondi differenti, per cui bisognerebbe riflettere se considerare lo studio di una segmentazione del terrorismo cibernetico stesso. Come si evince dalla figura in questione, Y nasce, si sviluppa e agisce mediante condotte e atti nello spazio cibernetico e i suoi effetti devono essere diretti sia al mondo cibernetico B che al mondo reale A al fine di generare implicazioni di vasta portata; questo è uno dei fattori che lo distingue da x2. Si ritiene importante ribadire che diverso è il supporto al terrorismo cibernetico (Nelson et al. 1999), che è l'uso altrimenti legale di sistemi informativi da parte di terroristi o loro sostenitori non inteso, di per sé, ad avere un effetto coercitivo su un pubblico target. Il supporto al terrorismo cibernetico aumenta o migliora altri atti terroristici: l'atto supportato potrebbe essere il terrorismo tradizionale o il terrorismo cibernetico.

Pertanto, un attacco di terrorismo cibernetico per definirsi tale deve innanzitutto ricadere sotto l'ombrello dell'eversione, che è la madre di tutte le categorie terroristiche. Per cui se un attacco cibernetico non è violento, illegale e politicamente motivato (secondo la categorizzazione seguita) non può definirsi eversivo. Una volta che l'attacco cibernetico è stato inquadrato come eversivo, bisogna indagare se si tratta di terrorismo cibernetico o di un altro fenomeno eversivo che potrebbe essere, per esempio, l'hacktivismo nei casi più estremi. Si precisa che le categorie dell'eversione, così come quelle del terrorismo, non si escludono a vicenda. A questo punto ci si potrebbe rifare alla definizione scritta precedentemente e poi inda-

gare più a fondo, classificando l'atto di terrorismo cibernetico o come sottocategoria del terrorismo tradizionale o come terrorismo cibernetico propriamente detto. Una definizione generale come quella proposta, a causa della sua semplicità, potrebbe richiamare più matrici di terrorismo cibernetico; tuttavia l'indagine del caso specifico e quindi lo studio, la profilazione e la contestualizzazione del singolo gruppo è obbligatoria se si vogliono impiegare delle buone pratiche di prevenzione e contrasto.

Pertanto, si dovrebbe applicare una distinzione all'interno del terrorismo cibernetico eversivo che si presuppone riferito a tipologie di terrorismo come quelle di matrice anarco-insurrezionalista, di estrema destra, di estrema sinistra o etnico-separatista, compresa quella confessionale. Poiché ogni singolo gruppo, pur perpetrando atti di terrorismo cibernetico potenzialmente identici, per gli analisti del campo, ha delle peculiarità in termini di ideologia dalla quale sono spinti, di struttura interna, di modus operandi, di auditorio bersaglio, di contesto storico e geografico ecc.

Quindi il terrorismo cibernetico di matrice jihadista è un fenomeno differente e totalmente distinto, per esempio, da un gruppo di terrorismo cibernetico anarco-insurrezionalista.

Un esempio è lo studio svolto per questa ricerca: si è partiti dalla macro-categoria – ossia il terrorismo cibernetico – e si è arrivati allo studio del caso dell'IS (Islamic State), gruppo riconosciuto di terrorismo di matrice jihadista. Una volta studiato, contestualizzato e profilato il fenomeno, le sue attività e le sue capacità, grazie all'analisi si è compreso che l'IS non può essere classificato come appartenente al terrorismo cibernetico propriamente detto, ma va invece inserito nella categoria del terrorismo cibernetico come sottocategoria del terrorismo tradizionale (cfr. DJAF) e quindi, richiamando lo schema logico (figura 11), attualmente è una x2 (singolo o gruppo terroristico che nasce e si sviluppa nel mondo A, ma che sfrutta e agisce nel mondo B provocando delle conseguenze o nel mondo A o nel mondo B). Questo esercizio, dunque, potrebbe essere potenzialmente ripetuto anche per le altre matrici.

Fabrizio d'Amore, *Docente presso l'Università degli Studi di Roma "La Sapienza", membro del Cyber Intelligence and Information Security Center*

Pasqualina Florio, *Cyber security senior analyst*

BIBLIOGRAFIA

Burato, A. (2015), Sicurezza, Terrorismo e Società, in «International Journal, Italian Team for Security, Terroristic Issues & Managing Emergencies», EDUCatt- Università Cattolica del Sacro Cuore, Milano. ISSN 2421-4442.

Caligiuri, M. (2019), Come i pesci nell'acqua. Immersi nella disinformazione, Rubbettino Editore.

Correia, J. V. (2022), An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, in «Computer Science», vol. 3, n. 84. https://doi.org/10.1007/s42979-021-00962-5.

d'Amore, F. (2020), in AA.VV. "Studiare l'intelligence in Italia". Rubbettino Editore, 2023. ISBN: 9788849873795. Il master di II livello in: Sicurezza delle informazioni e informazione strategica, il DIS e l'OSINT.

Florio, P. (2023), Terrorismo cibernetico e sicurezza nazionale. Potenziale metamorfosi della minaccia eversiva, Tab edizioni.

Macdonald, S., Lorenzo-Dus, N. (2021), Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines, in «Studies in Conflict & Terrorism», vol. 44, n. 5, pp. 363-386. DOI: 10.1080/1057610X.2018.1559508.

Macdonald, S., Jarvis, L., Lavis, M. S. (2014), Cyberterrorism Today? Findings from a Follow-on Survey of Researchers, in «Studies in Conflict & Terrorism». DOI: 10.1080/1057610X.2019.1696444.

Mantici, A. (2019), lezioni universitarie di Buone pratiche di contrasto alla criminalità, UNINT (Università degli Studi Internazionali di Roma).

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, G. (1999), Cyber Prospects and Implications, Center on Terrorism and Irregular Warfare Naval Postgraduate School. URI: http://hdl.handle.net/10945/27344.

Pherson, R. H., Heuer, JR. J. (2021), Structured Analytic Techniques for Intelligence Analysis, SAGE, CQ Press, Thousand Oaks.

Rudner, M. (2017), "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror, in «Studies in Conflict & Terrorism», vol. 40, n. 1, pp. 10-23. DOI:10.1080/1057610X.2016.1157403.

Talihärm, A. M. (2010), Cyberterrorism: in Theory or in Practice?, in «Defence Against Terrorism Review», vol.3, n. 2, Fall 2010, pp. 59-74.

Teti, A. (2015), Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza, Rubbettino Editore.

Weimann, G. (2004), Cyberterrorism: How Real is the Threat?, Special Report, disponibile su https://www.usip.org/sites/default/files/sr119.pdf, consultato il 19 febbraio 2022.

Zampetti, R. (2015), Sicurezza nazionale e spazio cibernetico. Una minaccia "invisibile" nell'era digitale, disponibile su https://www.archiviodisarmo.it/view/ylWJuVUoQfdaM5gqeM_x7V3yPWolExD_9pRLrgHyH04/sis-gennaio-2015.pdf, consultato il 10 aprile 2023.

BIOGRAFIA

Fabrizio d'Amore

Romano, docente di Cybersecurity alla Sapienza Università di Roma. Ha trascorso periodi di studio e ricerca all'estero (Zurigo, Buenos Aires, Berkeley, UMIACS a College Park Maryland). Insegna inoltre corsi di crittografia, sicurezza delle informazioni, sicurezza applicativa e steganografia presso alcuni master ed altre iniziative di alta formazione. Direttore del master di 2° livello in Sicurezza delle informazioni e informazione strategica, in collaborazione con il DIS. Svolge attività di verificatore e di consulente tecnico di parte. Referente scientifico di contratti di ricerca applicata, studio e analisi fra università ed enti istituzionali e privati. Dal 2015 la sua attività di ricerca si concentra sul campo della steganografia/watermarking, sicurezza del software (antiplagio), cybersecurity del volo aero civile e delle infrastrutture, modelli di autenticazione, protezione dei dati & privacy e OSINT.

BIOGRAFIA

Pasqualina Florio

Pasqualina Florio è un Cyber security senior analyst presso una società di consulenza nel settore dell'Information Technology. Laureata in Investigazione, criminalità e sicurezza internazionale all'Università degli studi internazionali di Roma (UNINT), nell' anno accademico 2020 – 2021 ha frequentato il Master di II livello in Sicurezza delle informazioni e informazione strategica (SIIS) nel Dipartimento di ingegneria informatica, automatica e gestionale della Sapienza di Roma.

Gli attori della minaccia ransomware

Gli attacchi ransomware sono in continua evoluzione e rappresentano uno strumento funzionale al perseguimento degli obiettivi di un crescente numero di attori della minaccia cyber che si specializzano nello sviluppo e nell'utilizzo di specifiche tattiche, tecniche e procedure, oppure fanno ricorso a servizi resi disponibili da terze parti in cambio di un corrispettivo in denaro.

Ransomware[1] è un termine che deriva dalla sincrasi delle parole malware[2] e ransom (riscatto) e fa riferimento all'utilizzo di codice malevolo per condurre attacchi cyber con finalità estorsiva. Originariamente l'estorsione si basava esclusivamente sulla cifratura dei dati della vittima per renderli indisponibili e sulla conseguente richiesta del pagamento di un riscatto, per l'ottenimento della chiave crittografica necessaria per decifrarli. Attualmente il termine ha assunto un'accezione più ampia, includendo anche altri tipi di cyber extortion basati, ad esempio, sulla compromissione della disponibilità dei sistemi e servizi ICT e della riservatezza dei dati[3].

Gli attacchi ransomware nascono e si evolvono come strumento utilizzato dalla criminalità per l'ottenimento di guadagni illeciti. Tuttavia nel tempo anche altre tipologie di attori della minaccia cyber, come ad esempio gli hacktivist e organismi statuali (nation-state), hanno iniziato ad impiegare attacchi ransomware con finalità diverse, sfruttandone le capacità estorsive e/o distruttive.
Con l'intento di poter qualificare i più importanti attori della minaccia ransomware, in Tabella 1 si riportano le principali categorie di threat actor, classificate in base a intento e capacità.

L'individuazione e la profilazione degli attori della minaccia ransomware è un'attività particolarmente complessa che risente delle difficoltà connesse con il problema dell'attribuzione, ovvero l'individuazione a posteriori dell'autore di un attacco cyber.

Questa attività presenta diversi fattori critici, come ad esempio:

- la limitatezza e la volatilità delle evidenze digitali disponibili ex post,
- la transnazionalità del dominio cyber,
- l'utilizzo da parte degli attaccanti di tecniche di anonimizzazione, offuscamento e anti-forensics.

Inoltre, le caratteristiche del cyber-spazio consentono a threat actor con adeguate capacità di porre in essere strategie per dissimulare l'origine de-

[1] Ransomware: malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento e altri oggetti similari. Fonte: Glossario ACN CSIRT Italia: https://www.csirt.gov.it/glossario/23

[2] Malware: contrazione di malicious software. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. Fonte: Glossario ACN CSIRT Italia: https://www.csirt.gov.it/glossario/22

[3] Cfr. Articolo "Lo scenario evolutivo della minaccia ransomware" in Rapporto Clusit 2023.

	Categoria	Descrizione
	Insider threat	Dipendenti o contractor che, utilizzando autorizzazioni e conoscenze aziendali, impiegano impropriamente informazioni o sistemi informatici dell'organizzazione per cui lavorano al fine di arrecarvi danno o per un vantaggio personale
	Cyber-terrorist	Gruppi o singoli terroristi in grado di sfruttare le opportunità offerte dal cyberspazio con la finalità di fare propaganda, proselitismo, radicalizzazione e/o per la diffusione del terrore attraverso la minaccia o l'interruzione di servizi critici mediante attacchi cyber
	Hacktivist	Gruppi o singoli attivisti che organizzano e conducono attacchi cyber con movente ideologico e principalmente con finalità dimostrativa
	Cyber-criminal	Criminali che, attraverso l'utilizzo abusivo di sistemi informatici o telematici, perpetrano azioni di matrice criminale con il fine di ottenere un vantaggio economico
	State-sponsored	Soggetti dotati di elevate capacità che conducono azioni illecite nel cyberspazio per conto e negli interessi di uno Stato, che li sostiene e/o finanzia
	Nation-state	Individui appartenenti ad apparati statuali in grado di organizzare e condurre cyber operation di tipo offensivo nell'interesse nazionale, sotto l'egida del proprio vertice politico

Tabella 1 – Tassonomia delle principali categorie degli attori della minaccia cyber

gli attacchi, come ad esempio l'ingaggio di terze parti per la conduzione di cyber-operation (proxy warfare[4]) o l'adozione di tecniche di disinformazione e operazioni volte a far ricadere la paternità dell'attacco verso altri threat actor (false flag operation[5]).

A queste si affiancano le difficoltà di tipo tecnico e giuridico che consentono anche a threat actor nation-state di perseguire i propri obiettivi strategici conducendo attività ostili a bassa intensità, attraverso attacchi cyber considerabili sotto la soglia del conflitto armato e in grado di permettere agli autori dell'attacco di dichiararsi estranei allo

[4] Nel contesto del conflitto tra Stati nel dominio cibernetico, l'espressione proxy warfare identifica la strategia che prevede la conduzione di operazioni cyber offensive da parte di "forze non convenzionali", ovvero da intermediari (proxy) non appartenenti all'entità statuale che li ingaggia.

[5] Operazioni che vengono poste in essere utilizzando tecniche tali da indurre il target a ritenere che le stesse siano riconducibili ad un attore diverso da quello che ha condotto l'attacco.

stesso (plausible deniability[6]).

Gli attacchi ransomware presentano delle peculiarità che incidono sul processo di attribuzione di queste attività malevole. Al fine di portare avanti il piano estorsivo, gli attori della minaccia ransomware hanno difatti la necessità di svolgere alcune attività che potrebbero agevolare il processo di raccolta di evidenze funzionali alla loro individuazione e profilazione, come ad esempio le comunicazioni con la vittima, l'utilizzo di specifici algoritmi di crittografia e le comunicazioni con i server di Comando e Controllo o la transazione economica per la riscossione del riscatto.

In base alle loro capacità, gli attori della minaccia ransomware sviluppano e adottano specifiche tattiche per ridurre la probabilità che le sopra citate attività possano agevolare il processo di attribuzione, esponendoli alle conseguenti azioni repressive.

La Figura 1 rappresenta le attività di analisi funzionali all'attribuzione di un attacco ransomware evidenziando le conseguenti tattiche di anti-attribution attuate dagli attori della minaccia con tre livelli di profondità (Livello 1, 2 e 3).
Il Livello 1 comprende le tattiche di anti-attribution descritte di seguito in relazione a tre specifiche attività:

i. Le comunicazioni attaccante-vittima
Gli attaccanti per le comunicazioni con le vittime utilizzano specifici strumenti per garantire l'anonimato, come i servizi di posta elettronica e di messaggistica istantanea crittografati.

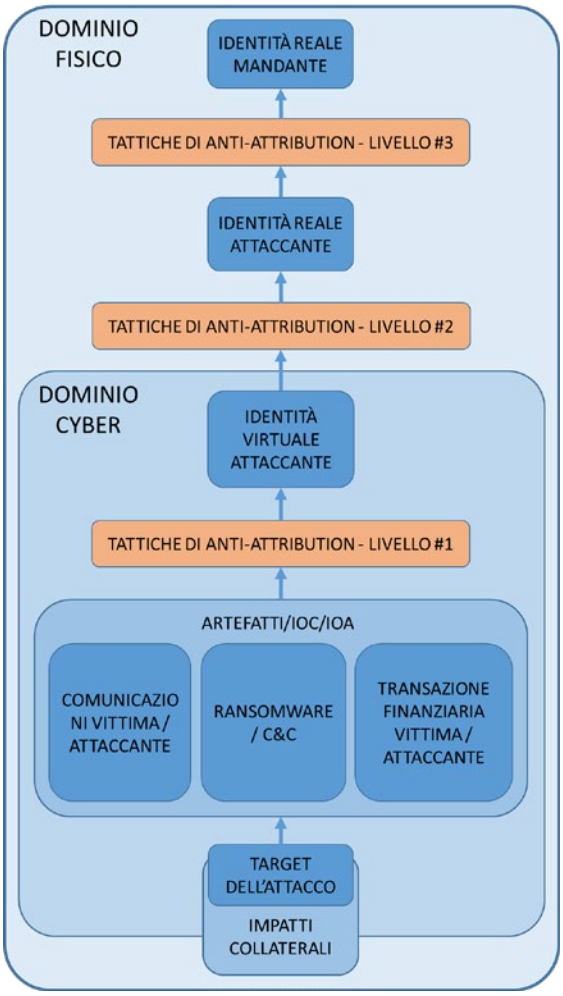


Figura 1 - Attribuzione di un attacco ransomware attraverso l'analisi retrospettiva delle evidenze raccolte

ii. Gli artefatti relativi al ransomware e ai server di Comando e Controllo
Per rendere più difficoltosa l'individuazione del server di Comando e Controllo si introducono layer di anonimizzazione (come ad esempio catene di proxy e reti decentralizzate) fra quest'ultimo e il ransomware operante nel sistema compromesso della vittima. Per rendere più complesse le attivi-

[6] L'espressione definisce i casi in cui sia possibile dichiararsi formalmente estranei a qualsivoglia fattispecie deprecabile commessa da terzi dei quali si abbia responsabilità o comando diretto.

	Ruolo	Attività specialistica
	Initial Access Broker	Ricerca, acquisizione e vendita di informazioni utili a consentire a terzi l'accesso remoto a reti aziendali precedentemente compromesse
	RaaS Admin	Amministrazione delle infrastrutture informatiche utilizzate per la gestione operativa dell'attacco ransomware
	Ransomware Developer	Sviluppo software per la produzione e personalizzazione di malware da impiegare nell'attacco ransomware
	RaaS Affiliate	Utilizzo dei servizi e degli strumenti RaaS descritti nei ruoli precedenti per la conduzione degli attacchi ransomware
	RaaS Seller	Intermediazione nella compravendita da e verso gli altri ruoli, dei servizi e degli strumenti RaaS utilizzabili nell'attacco ransomware

Tabella 2 – Principali ruoli degli attori dell'ecosistema RaaS e rispettive specializzazioni

tà di estrazione di indicatori di compromissione funzionali all'attribuzione del ransomware rispetto al proprio sviluppatore, si impiegano alcuni espedienti come l'utilizzo di librerie di cifratura standard e la compilazione del ransomware con tecniche di anti-forensics (che prevede ad esempio l'offuscamento del codice sorgente).

iii. La transazione finanziaria

Il riscatto viene solitamente richiesto in valuta virtuale, con la finalità di rendere più difficile la tracciabilità dei flussi finanziari. Una volta ricevuto il pagamento, l'importo indebitamente acquisito viene tipicamente frazionato e convertito in diverse differenti criptovalute. Ciò ad esempio avviene facendo uso dei cosiddetti "Crypto Mixer". Infine, gli attaccanti cercano di trasformare in moneta a corso legale gli importi derivanti dall'attività criminale facendo uso di intermediari (come ad esempio Crypto Exchange o money mule)[7].

Il Livello 2 delle tattiche anti-attribution fa riferimento all'impiego di tecniche di anonimizzazione dell'identità attaccante, come ad esempio l'uso di server situati nel dark web o di identità digitali di terze parti compromesse.

[7] Nonostante ciò le potenzialità derivanti dai moderni sistemi di analisi delle blockchain consentono di superare, almeno in parte, i problemi di tracciabilità di flussi finanziari in criptovalute, abilitando anche per questo tipo di investigazioni l'utilizzo del principio espresso sinteticamente con la locuzione "Follow-the-money".

Il Livello 3 è infine relativo al già citato ingaggio di terze parti per la conduzione operativa delle attività malevole.

Vi sono inoltre altri elementi che impattano in maniera trasversale il processo di attribuzione, che riguardano il rebranding dei gruppi ransomware, la crescente fluidità della loro composizione e la diffusione del paradigma del Ransomware as a Service (RaaS).

La crescente percezione di remunerativitá degli attacchi ransomware ha catalizzato l'evoluzione di questa minaccia verso logiche di mercato, industrializzazione e stratificazione della catena del valore. Si è assistito alla conseguente creazione di un indotto di servizi specializzati, funzionali all'orchestrazione di attacchi efficaci anche da parte di attori dotati di scarse capacità. Questo ha determinato una diversificazione dei cyber-criminali in sottogruppi altamente qualificati, che erogano "servizi" gli uni verso gli altri o verso terze parti, secondo il modello di business criminale denominato Ransomware as a Service. Si riportano in Tabella 2 i ruoli e le relative attività specialistiche dei principali attori che nel modello RaaS partecipano all'organizzazione e alla conduzione di un attacco ransomware.

Una delle dirette conseguenze della diffusione del modello RaaS è il riuso di strumenti e procedure fra diversi threat actor. Accade quindi che uno stesso threat actor può utilizzare più varianti di ransomware, oppure che la stessa variante può essere impiegata da diversi gruppi criminali. Mentre, quindi, in passato l'attribuzione di un attacco ransomware poteva beneficiare dell'individuazione di strumenti e TTP riconducibili ad un threat actor dotato di specifiche capacità, oggi gli indizi digitali acquisibili durante l'analisi tecnica di un attacco ransomware hanno un ruolo sempre meno determinante per le attività di analisi funzionali all'attribuzione.

La crescente efficacia delle azioni di contrasto della minaccia ransomware poste in essere a livello internazionale ha consentito, in taluni casi, la neutralizzazione delle infrastrutture tecnologiche impiegate da alcuni gruppi e il contestuale arresto di parte dei relativi membri. Questo ha contribuito a determinare il rebranding dei gruppi in questione e ad alimentare il transito di figure professionali verso altri gruppi criminali. Di seguito, e schematizzati in Figura 2, la descrizione di due casi rilevanti relativi alle dinamiche descritte[8]:

- REvil
  Nel novembre del 2021 l'FBI ha arrestato uno dei membri del gruppo REvil e ha sequestrato parte dei fondi del gruppo[9]; poco dopo, le attività malevole del gruppo cyber-criminale sono cessate; nel giro di alcuni mesi si sono rilevate campagne ransomware condotte da un nuovo attore della minaccia, al tempo non noto ma successivamente ricondotte al gruppo REvil, operante sotto altra identità.
- DarkSide
  Nel maggio del 2021 il gruppo ransomware

[8] Gli aspetti caratterizzanti dei diversi threat actor di seguito citati sono riportati in Tabella 3

[9] https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

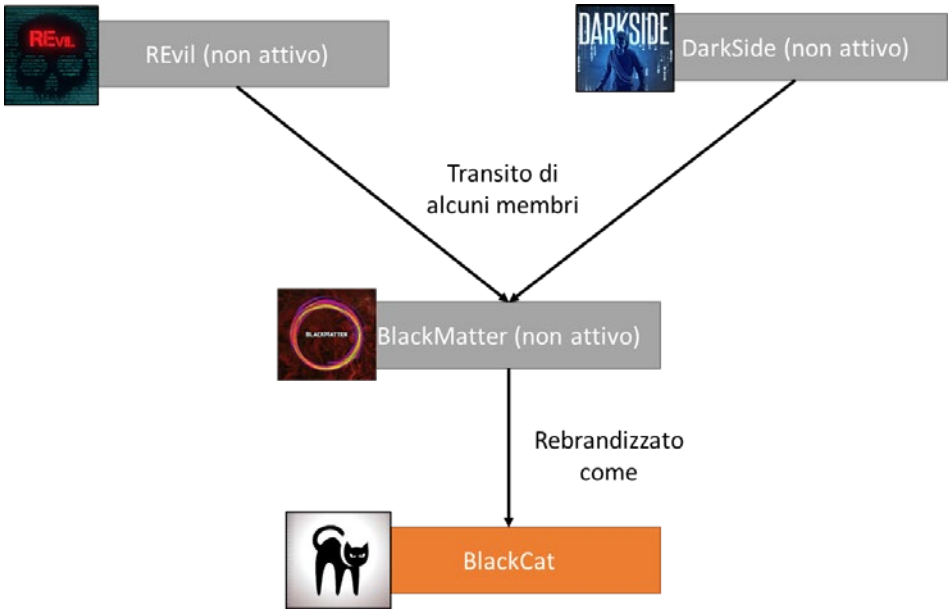


Figura 2 - Schematizzazione dei cambiamenti relativi a nomi e composizione di alcuni threat actor ransomware

DarkSide[10] ha dichiarato di aver perso l'accesso alle proprie infrastrutture tecnologiche e di voler quindi porre conseguentemente termine alle proprie attività, anche a causa della pressione ricevuta da parte del governo degli Stati Uniti[11]; alcuni mesi dopo è emerso un nuovo gruppo ransomware, denominato BlackMatter, nel quale è risultato che siano confluiti alcuni ex membri del gruppo DarkSide, unitamente a membri di REvil. In breve tempo il gruppo BlackMatter ha poi effettuato un rebranding, denominandosi BlackCat.

Al netto delle sopra elencate difficoltà nell'eseguire l'attribuzione di un attacco ransomware, l'applicazione di tecniche di cyber intelligence da parte di entità statuali e non, ha consentito nel tempo lo sviluppo di conoscenza utile per la profilazione di alcuni attori della minaccia, soprattutto con riferimento a quelli operanti con finalità economica[12]. In Tabella 3 si propone un elenco dei threat actor più attivi nel corso degli ultimi anni, con le relative caratteristiche peculiari.

Anche se i principali attori della minaccia ransomware afferiscono alla categoria del cyber-crime e agiscono con finalità economica, negli ultimi anni si riscontra un crescente utilizzo di attacchi ransomware anche per il perseguimento di obiettivi strategici nazionali.

In particolare, si osserva come alcuni attori afferenti alle categorie nation-state e state-sponsored (cfr. Tabella 1) sfruttano le potenzialità distrut-

[10] Aspetti caratterizzanti del gruppo sono riportati in Tabella 3

[11] https://www.privacy.com.sg/cybersecurity/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/

[12] Il movente economico rappresenta la principale vulnerabilità per l'attribuzione di un attacco ransomware in considerazione degli aspetti di dettaglio descritti in Figura 1.

Threat Actor	Attivo da - a	Nazione di appart-enenza	Aspetti caratterizzanti
DarkSide	2013 - 2021	Russia	Presumibilmente composto da ex membri del gruppo FIN7. A partire dall'agosto 2020, DarkSide ha sviluppato una piattaforma per attacchi Ransomware-as-a-Service (RaaS) che consente di veicolare, eseguire e controllare il malware durante le fasi dell'attacco, negoziare il riscatto mediante un canale anonimo di messaggistica e ricev-ere l'eventuale pagamento in valuta digitale. Per l'utilizzo dei servizi offerti, DarkSide richiede una quota compresa tra il 10% e il 25% dei proventi realizzati. Tra ottobre 2020 e maggio 2021, DarkSide avrebbe riscosso riscatti da oltre 47 vittime per un ammontare di circa 90 milioni di dollari, di cui 15.5 milioni come sua quota di profitto. Il gruppo è noto per l'attacco alla società di gestione dell'infrastruttu-ra di distribuzione del carburante Colonial Pipeline, che ha causato elevati impatti sia dal punto di vista economico che operativo[13]. Nel 2021 alcuni affiliati di DarkSide sono confluiti nel gruppo BlackMatter.
Conti	2015 - 2022	Russia	A seguito dell'invasione russa in Ucraina, il gruppo si è ap-ertamente schierato a favore di Mosca indirizzando le pro-prie offensive contro target governativi di Stati filo-ucraini. A casa di un leak di dati sensibili relativi al gruppo, lo stesso a partire da aprile 2022 ha ridotto le proprie oper-azioni fino a dismettere, il mese successivo, i siti web e le infrastrutture principali utilizzate per condurre gli attacchi. Conti ha poi avviato una profonda riorganizzazione inter-na, suddividendosi in diversi nuclei autonomi e stringendo partnership con altri gruppi di matrice cyber-criminale con l'obiettivo di eludere le forze dell'ordine e continuare a operare.

[13] A seguito dell'attacco perpetrato da DarkSide ai danni della società di gestione dell'infrastruttura di distribuzione del carburante Colonial Pipeline, per una settimana sono state interrotte forniture equivalenti a 2,5 milioni di barili al giorno di benzina, diesel e altri prodotti petroliferi, provenienti dalle raffinerie del Golfo del Messico e destinate a rifornire diversi centri nevralgici della costa atlantica. L'indisponibilità di carburante ha determinato la dichiarazione, da parte del Federal Motor Carrier Safety Administration (FCMSA), dello stato di emergenza nei 17 stati USA coinvolti. Il 19 maggio, a valle del ritorno alla normale operatività, l'amministratore delegato della società ha ammesso di aver pagato, già il giorno dopo l'attacco, un riscatto in criptovaluta (Bitcoin) equivalente a circa 4,4 milioni di dollari, parte dei quali sono stati successivamente recuperati dall'FBI. Rif. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

LockBit	2019 - oggi	Russia e Paesi dell'ex Unione Sovietica	Lockbit è un gruppo che ha sviluppato nel tempo le proprie attività criminali specializzandosi nell'offerta di servizi RaaS particolarmente evoluti. Gli affiliati di LockBit hanno la possibilità di accedere ad un pannello di amministrazione web mediante il quale possono generare, in modo autonomo, nuove varianti del ransomware, gestire le vittime, trattare i riscatti, ottenere statistiche e decifrare file. Negli ultimi mesi il gruppo ha lanciato un programma di bug bounty per ransomware, al fine di individuare prontamente eventuali vulnerabilità nel codice dei propri strumenti e poterle sanare prima che possano essere sfruttate dalle forze dell'ordine. Tra le grandi organizzazioni che sono state colpite da Lockbit si annovera l'azienda statunitense Entrust, fornitrice di servizi e prodotti di sicurezza informatica[14], colpita a giugno 2022.
REvil	2019 - 2021	Russia	Plausibilmente costituitosi in seguito allo scioglimento del gruppo GandCrab, dal quale ha ereditato gran parte delle capacità offensive, il gruppo ha sviluppato una piattaforma tecnologica che offre servizi per la conduzione degli attacchi "acquistati" e per il supporto dei "clienti" secondo il modello RaaS, a fronte di un pagamento pari al 30% dei proventi realizzati. REvil è ritenuto responsabile di attacchi ransomware che hanno permesso nel solo 2020 di sottrarre complessivamente circa 120 milioni di dollari a enti e società occidentali. Il gruppo è autore dell'attacco, perpetrato a luglio 2021, ai danni del Managed Service Provider (MSP) Kaseya[15]. Nel 2021 alcuni affiliati di REvil sono confluiti nel gruppo BlackMatter.
BlackCat (ALPHV)	2021 - oggi	Russia	Alimentato da ex appartenenti del gruppo BlackMatter, ALPHV si contraddistingue per l'utilizzo di strumenti di attacco che impiegano tecniche innovative come la crittografia intermittente e la corruzione dei dati, per ridurre il tempo necessario a completare il processo funzionale a rendere indisponibili alla vittima i dati compromessi. Tra le aziende colpite dal gruppo figura il Gestore di Servizi Energetici (GSE) italiano, che ha subìto un attacco ransomware[16] ad agosto 2022.

[14] L'azienda, a luglio 2022, ha inviato una comunicazione ai propri clienti per informarli di aver rilevato un accesso non autorizzato ai propri sistemi informatici, avvenuto il 18 giugno, non escludendo possibili impatti sulla riservatezza e/o integrità dei servizi erogati.

[15] L'offensiva, oltre ad essere di tipo ransomware, è stata classificata anche come supply chain avendo portato alla compromissione di circa 1.500 aziende correlate a Kaseya tra clienti diretti e indiretti. Rif. https://www.csoonline.com/article/3626703/the-kaseya-ransomware-attack-a-timeline.html

[16] L'attacco in questione non ha comunque causato l'interruzione di servizi critici, né impatti di tipo sistemico.

Lapsus$	2021 - oggi	Inghilterra, Russia, Turchia, Germania, Portogallo	Lapsus$ si caratterizza per l'utilizzo di insider (dipendenti, consulenti o fornitori infedeli) funzionale all'accesso abusivo ai sistemi informatici delle vittime e al perseguimento delle attività necessarie a supportare l'azione estorsiva. I potenziali insider vengono individuati e reclutati attraverso i principali canali social. L'applicazione Telegram è, invece, utilizzata per pubblicare i dati indebitamente sottratti alle vittime con finalità estorsiva. L'esfiltrazione dei dati è spesso accompagnata da azioni di sabotaggio utili a cancellare le tracce dell'attacco e a distogliere l'attenzione della vittima.
BlackBasta	2022 – oggi	Russia	Presumibilmente composto da ex membri provenienti dalle cyber-gang russofone Conti e REvil. Al pari di altri cyber-criminali, anche Black Basta ha un proprio sito accessibile nel dark web in cui vengono pubblicati i dati esfiltrati appartenenti alle organizzazioni che non hanno corrisposto la cifra richiesta. Il gruppo utilizza tipicamente email di phishing per carpire credenziali di accesso alle reti informatiche da violare e strumenti di cifratura particolarmente efficienti (ad es. la crittografia intermittente) per velocizzare le operazioni volte a rendere indisponibili i dati dei sistemi infettati dal ransomware. Sebbene di recente formazione, il gruppo si è fatto notare per la conduzione di offensive cyber ai danni di molteplici organizzazioni collocate principalmente negli Stati Uniti in Canada e in Europa (soprattutto Francia, Germania e Italia), come ad esempio l'attacco a febbraio 2023 ai danni di Acea[17].
Hive	2021-oggi	Russia, Bulgaria	Hive è un gruppo cyber-criminale russo-bulgaro a doppia estorsione, apparso per la prima volta nel giugno 2021, che opera secondo il modello di business del RaaS allo scopo di ottenere profitti economici a scapito dei target colpiti con la tattica della doppia estorsione. Gli attacchi hanno l'obiettivo di esfiltrare e cifrare i dati presenti sui dispositivi della vittima, alla quale viene richiesto il pagamento di un riscatto sia per la relativa decodifica, sia per evitare di diffondere e/o vendere illegalmente i dati e i file sottratti. Hive è un threat actor particolarmente attivo ed è stato autore di attacchi rivolti a numerose organizzazioni, tra cui si annovera l'attacco condotto a marzo 2022 nei confronti di Ferrovie dello Stato Italiane[18].

Tabella 3 - Principali threat actors correlati alla minaccia ransomware

[17] L'attacco ha comportato la non raggiungibilità di tutti i siti web pubblici di Acea a partire dalla mattina del 2 fino al 5 febbraio. Il disservizio informatico generato dall'attacco ransomware non ha interessato i servizi essenziali di distribuzione elettrica e idrica che sono stati sempre regolarmente garantiti: https://www.gruppo.acea.it/media/avvisi/2023/02/acea-dopo-attacco-cyber-ripristinata-l-operativita-dei-sistemi-it

[18] L'attacco ha provocato disservizi in tutta la penisola, bloccando temporaneamente l'acquisto dei titoli di viaggio nelle biglietterie e nei self service presenti nelle stazioni ferroviarie. Non sono stati, invece, riscontrati malfunzionamenti nei servizi di vendita online, né disservizi alla circolazione dei convogli.

tive ed estorsive degli attacchi ransomware per il perseguimento dei propri interessi strategici.

Gli attacchi ransomware possono rappresentare, infatti, un diversivo per le attività di cyber-espionage o uno strumento per l'interruzione di servizi essenziali attraverso attacchi ai danni di infrastrutture critiche. Nell'ottobre 2022, ad esempio, Sandworm[19] ha perpetrato un attacco cyber contro alcune organizzazioni ucraine e polacche del settore dei trasporti e della logistica, attraverso la campagna ransomware Prestige. Sandworm è noto soprattutto per la campagna ransomware NotPetya del 2017, che ha colpito diversi settori e infrastrutture critiche in Ucraina e in altri Paesi europei, con effetti anche a livello globale, generando danni stimati in oltre un miliardo di dollari[20].

Attori di matrice statuale ricorrono ad attacchi ransomware anche per l'acquisizione illecita di fondi funzionali a sostenere economicamente gli interessi nazionali. Un esempio è rappresentato dalla campagna del 2017 nota con il nome di WannaCry, la cui responsabilità è stata attribuita ufficialmente al threat actor nordcoreano Lazarus, che ha colpito più di 300.000 computer in 150 Paesi causando perdite globali stimate in circa 4 miliardi di dollari[21]. L'alta efficacia dell'attacco è stata garantita anche dallo sfruttamento della vulnerabilità EternalBlue[22]. Più recentemente attori della minaccia di matrice statuale nord-coreana hanno preso di mira anche obiettivi operanti nel settore sanitario statunitense colpiti con il ransomware Maui[23], con il presumibile intento di massimizzare l'effetto estorsivo degli attacchi e di conseguenza la probabilità del pagamento del riscatto.

Si rilevano anche casi in cui gli attacchi ransomware sono impiegati da attori nation-state o state-sponsored come strumento di ingerenza nelle decisioni di politica estera dei governi stranieri. Ad esempio, nella seconda metà di luglio 2022, i sistemi informativi del governo albanese sono stati oggetto di un attacco cyber rivendicato dal gruppo HomeLand Justice composto da diversi threat actor di presunta matrice statuale iraniana. Tale azione è stata portata avanti come ritorsione per il sostegno offerto, da parte di Tirana, all'Esercito di Liberazione Nazionale dell'Iran (Mojaheddin-E Khalq o più brevemente MEK), organizzazione politica iraniana tra le più attive nell'opposizione al governo di Teheran. Dal 2016 l'Albania ospita sul proprio territorio la principale sede operativa dell'Esercito di Liberazione (MEK) e da allora i rapporti diplomatici tra i due Paesi si sono progressivamente deteriorati, fino alla loro interruzione nel settembre 2022.

A fronte del mutamento dello scenario della minaccia cyber connesso al conflitto russo-ucraino, si è rilevato un crescente utilizzo di attacchi ransomware per l'ottenimento di obiettivi strate-

[19] Sandworm, noto anche come IRIDIUM, è un attore statuale ritenuto legato al GRU, il Servizio d'intelligence militare russo.

[20] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[21] https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

[22] Un exploit sviluppato dalla National Security Agency (NSA) degli Stati Uniti per i sistemi Windows. EternalBlue, è stato rubato e fatto trapelare da un gruppo chiamato The Shadow Brokers un mese prima dell'attacco.

[23] North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA

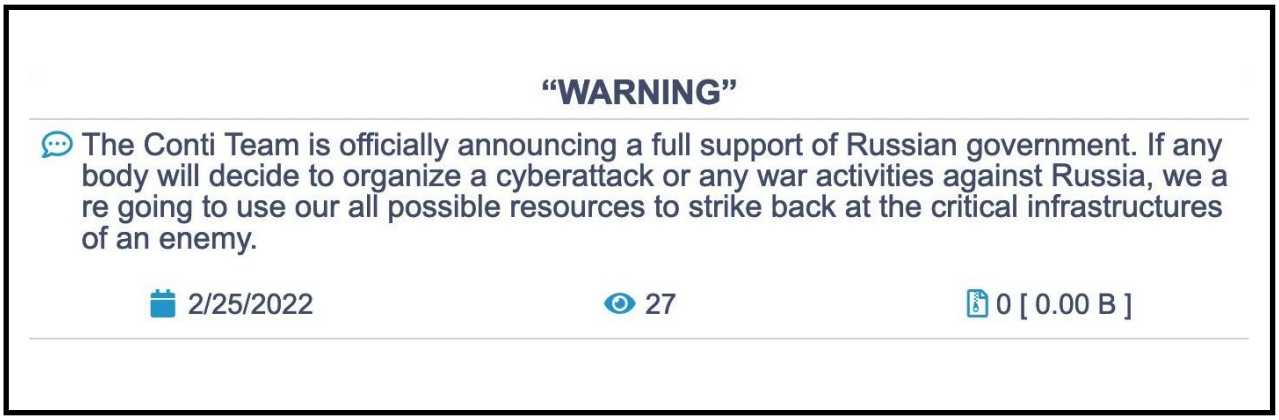


Figura 3 - Dichiarazione di supporto del gruppo Conti al governo di Mosca a seguito dello scoppio del conflitto in Ucraina

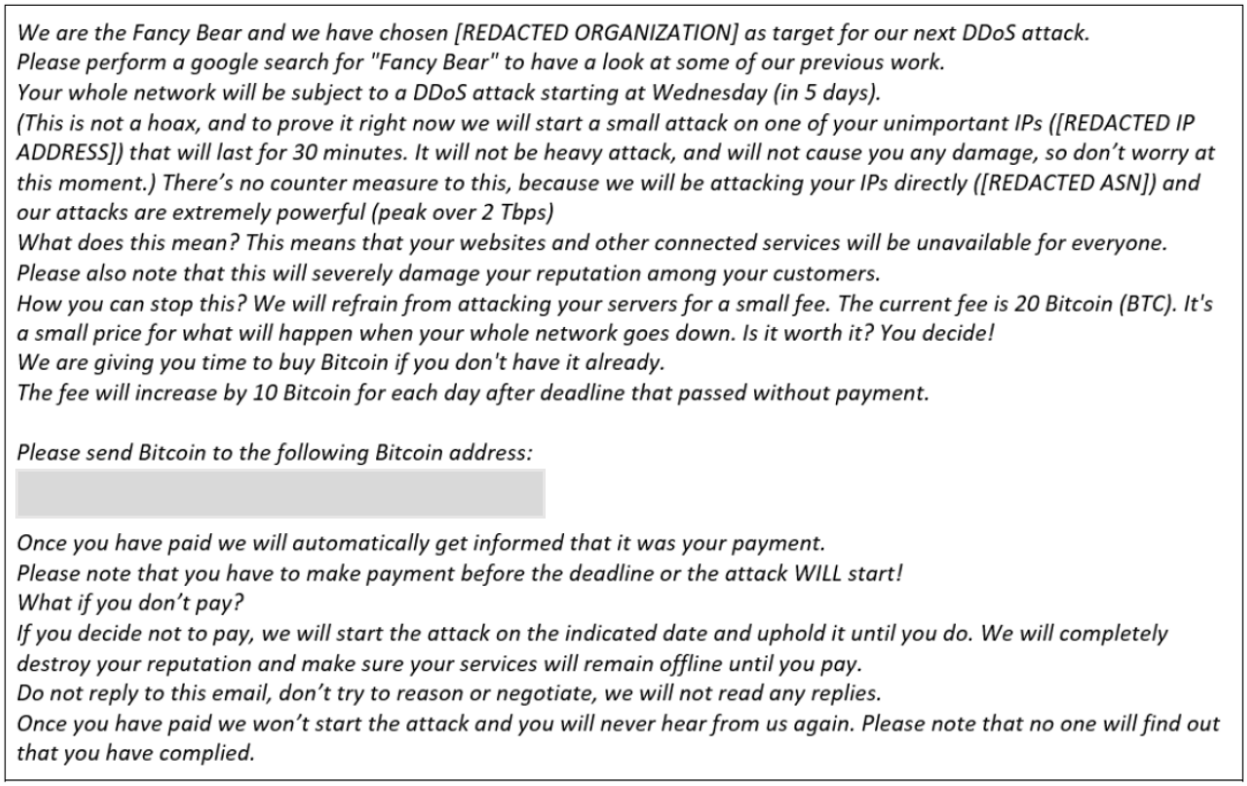
gici nazionali anche da categorie di attori della minaccia che generalmente perseguono guadagni economici. Infatti, secondo la strategia della proxy warfare, threat actor afferenti alla sfera del cybercrime hanno plausibilmente agito nell'interesse di Mosca (cfr. Figura 3). Il governo russo ha recentemente rilasciato una dichiarazione in cui afferma che si dovrebbero stabilire delle garanzie legislative per gli hacker che lavorano nell'interesse della Russia[24].

Si registrano, infine, casi di attacchi ransom rivendicati da attori della minaccia cyber che si qualificano utilizzando impropriamente identità di altri, con la finalità di ricondurre a terzi la responsabilità dell'attacco. In particolare si osserva il ricorso all'identità di un attore statuale nella fase di richiesta del riscatto con l'intento di incrementare il potere intimidatorio dell'estorsione, sfruttando la diffusa percezione di alta pericolosità di questa categoria di attaccanti. Un modus operandi comunemente impiegato prevede l'invio di una e-mail intimidatoria che informa la vittima di un imminente attacco DDoS a scopo dimostrativo, richiedendo il pagamento di un riscatto entro una scadenza stabilita per non incorrere in un attacco dagli impatti ben più rilevanti. In Figura 4 è riportato, a titolo di esempio, la rivendicazione di un attacco ransom eseguito da un gruppo criminale che si spaccia per il noto threat actor di matrice statuale Fancy Bear[25].

La minaccia ransomware è caratterizzata da una capacità, particolarmente marcata, di innovarsi ed evolvere rapidamente. Per tale ragione, al fine dicontrastare efficacemente questo fenomeno a livello locale e sistemico, è importante individuarne i principali attori e seguirne costan-

[24] https://www.vedomosti.ru/politics/news/2023/02/10/962551-v-gosdume-predlozhili-ne-nakazivat

[25] È un gruppo filogovernativo russo di matrice state-sponsored attivo almeno dal 2007 e legato a doppio filo con il GRU del Ministero della Difesa. L'avversario ha colpito con operazioni di CNE (Computer Network Exploitation) una pluralità di obiettivi di alto profilo principalmente nei Paesi NATO e dell'ex blocco sovietico, nell'ottica di reperire intelligence utile al Cremlino o influenzare opinioni ed eventi di portata internazionale, sempre in chiave anti-NATO ed anti-europeista. Risulta collegato ad altri gruppi di Mosca tra cui Sandworm e Gallmaker.



We are the Fancy Bear and we have chosen [REDACTED ORGANIZATION] as target for our next DDoS attack.
Please perform a google search for "Fancy Bear" to have a look at some of our previous work.
Your whole network will be subject to a DDoS attack starting at Wednesday (in 5 days).
(This is not a hoax, and to prove it right now we will start a small attack on one of your unimportant IPs ([REDACTED IP ADDRESS]) that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly ([REDACTED ASN]) and our attacks are extremely powerful (peak over 2 Tbps)
What does this mean? This means that your websites and other connected services will be unavailable for everyone.
Please also note that this will severely damage your reputation among your customers.
How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!
We are giving you time to buy Bitcoin if you don't have it already.
The fee will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!
What if you don't pay?
If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.
Do not reply to this email, don't try to reason or negotiate, we will not read any replies.
Once you have paid we won't start the attack and you will never hear from us again. Please note that no one will find out that you have complied.

Figura 4 - Messaggio e-mail impiegato in un tentativo di estorsione messo in atto da un gruppo criminale che, spacciandosi per il noto threat actor di matrice statuale "Fancy Bear", minaccia di effettuare un attacco ransom DDoS

temente i profili evolutivi in modo da sviluppare e mantenere un adeguato livello di situational awarenes[26]. Per questo sono essenziali le capacità di cyber threat intelligence e di difesa partecipata attraverso la cooperazione e lo scambio volontario di informazioni sulla minaccia cyber.

Considerando l'attuale scenario delle minacce cyber, è possibile desumere che l'inversione di tendenza nella continua espansione di questo genere di fenomeno potrà avvenire quando gli attaccanti considereranno meno profittevole il ricorso ad attacchi ransomware per l'ottenimento dei propri obiettivi, in termini di costi e rischi.

Pasquale Digregorio, *Capo Divisione del Computer Emergency Response Team della Banca d'Italia*[27]

Chiara Ferretti, *Cyber Security Analyst, Computer Emergency Response Team della Banca d'Italia*[27]

Daniele Filoscia, *Cyber Security Analyst, Computer Emergency Response Team della Banca d'Italia*[27]

[26] Capacità di comprendere adeguatamente l'evoluzione dello scenario della minaccia cyber in relazione alle caratteristiche dell'entità da proteggere.

[27] Le opinioni sono espresse a titolo personale e non impegnano la responsabilità dell'Istituto.

BIOGRAFIE

Pasquale Digregorio

Ex-Ufficiale d'Accademia, attualmente Capo Divisione del Computer Emergency Response Team della Banca d'Italia, dove mette al servizio dell'Istituto la sua esperienza in cyber intelligence e cybersecurity, sviluppata in 20 anni di servizio, svolti presso il Ministero della Difesa e la Presidenza del Consiglio.

Chiara Ferretti

Si è occupata per oltre 15 anni di sicurezza delle informazioni e gestione di progetti IT per aziende operanti nei settori finanziario, delle telecomunicazioni, alimentare, dei trasporti e logistico. Dal 2022 lavora presso il Computer Emergency Response Team della Banca d'Italia.

Daniele Filoscia

Ex-Ufficiale d'Accademia, specializzato in cyber threat intelligence. Ha prestato servizio presso l'Aeronautica Militare per 15 anni. Dal 2021 lavora presso il Computer Emergency Response Team della Banca d'Italia in qualità di Cyber Security Analyst.

White Paper

LA DIGITAL FORENSICS NEL PROCESSO PENALE

Download gratuito su www.ictsecuritymagazine.com

Cybercrime e spionaggio industriale

La difesa del know-how aziendale

In un'economia basata principalmente sulla conoscenza, è sempre di più il know how di un'azienda a fare la differenza in termini di competitività: tuttavia, gli investimenti fatti per migliorare le abilità operative di un'impresa rischiano di essere resi vani qualora tali conoscenze vengano sottratte e vendute ad altri operatori di mercato. Per questo motivo assume sempre maggior rilevanza la difesa dallo spionaggio industriale, al fine di non essere coinvolti in una scorretta e sfavorevole dinamica concorrenziale.

Lo spionaggio industriale si concretizza nella sottrazione illecita di informazioni industriali e commerciali ai danni di un'impresa, con l'obiettivo di sfruttare le informazioni sottratte per trarre un indebito vantaggio. Questa tipologia di reato può configurarsi secondo diverse fattispecie, a seconda che venga realizzato da un agente interno o esterno rispetto all'azienda danneggiata.

Lo spionaggio industriale c.d. "esterno" oggi si realizza prevalentemente attraverso la sottrazione delle informazioni sensibili di un'azienda, quali tecniche e procedure produttive, nominativi dei clienti e strategie di marketing. La commissione di tale reato si verifica principalmente attraverso attività di cyber spionaggio, intercettazioni telefoniche o tramite l'installazione di microspie.

Nell'ipotesi di spionaggio industriale c.d. "interno", al contrario, le informazioni e le strategie riguardanti un'azienda vengono sottratte da uno o più soggetti interni alla stessa (dipendenti, ex-dipendenti, consulenti, collaboratori, ecc.) i quali, potendo accedervi legittimamente, risultano facilitati a venderle segretamente ad altri operatori di mercato. In questo caso parleremo di "Insider Threat".

Gli insider sono soggetti che – operando con negligenza, dolo eventuale o dolo diretto – possono causare gravi pregiudizi economici agli Enti e aziende di appartenenza, favorendo la distruzione o la sottrazione di informazioni di valore e mettendo a repentaglio l'integrità della propria organizzazione. Affinché si realizzi il reato di spionaggio industriale, è sufficiente che si dimostri la sottrazione e la rivelazione del "know how" aziendale, ossia del patrimonio di conoscenze di un'impresa attinente ai metodi di progettazione e produzione caratterizzanti la sua struttura industriale.

Il Ponemon Institute (Istituto indipendente dello Stato del Michigan, USA) ha pubblicato uno studio svolto nel 2022 su un campione di 278 organizzazioni negli Stati Uniti, in cui sono stati denunciati ben 6708 incidenti di sicurezza causati da Insiders. Di questi, il 56% è stato causato

da negligenza mentre il 26% da un'azione dolosa del personale, per un totale di oltre 10 milioni di dollari di costi per le organizzazioni coinvolte.

Lo spionaggio industriale è un reato che può gravemente danneggiare un'azienda a livello finanziario e d'immagine: nominativi di clienti e fornitori, strategie di marketing, conoscenze, protocolli e procedure interne, oltre a software e brevetti, sono le principali informazioni che possono essere utilizzate dall'autore del reato per danneggiare l'azienda che ne subisce la sottrazione, traendone direttamente un indebito vantaggio o vendendole ad altri operatori di mercato in settori concorrenziali.

Lo spionaggio economico e industriale si configura in due forme:

1. acquisizione di proprietà intellettuale, come processi o tecniche di produzione, luoghi di produzione, informazioni proprietarie od operative come dati dei clienti, prezzi, vendite, ricerca e sviluppo, politiche, offerte potenziali, pianificazione o strategie di marketing;
2. furto di segreti commerciali, corruzione, ricatto o sorveglianza tecnologica con diversi tipi di malware.

Una perdita significativa della clientela, la fuga di notizie riservate, le dimissioni di dipendenti o il lancio sul mercato di una propria idea innovativa da parte di un'impresa concorrente sono solo alcune delle conseguenze negative che può subire un'azienda bersaglio dello spionaggio industriale: pertanto, è sempre più evidente l'importanza di prevenire e contrastare tale fenomeno, avvalendosi di agenzie investigative professionali e specializzate in indagini aziendali.

I veri segreti commerciali possono trovare la loro strada nel mercato attraverso diversi canali. Il dipendente sleale può cercare furtivamente i concorrenti e spacciare dati riservati al miglior offerente. Una tecnica più comune è la cospirazione di gruppo: diversi dipendenti, generalmente tecnici e altre figure di alto calibro manageriale, lasciano un'azienda e creano un'impresa competitiva, capitalizzando le confidenze acquisite mentre erano a libro paga del loro ex datore di lavoro. Una variazione di questa pratica si verifica quando un concorrente attira un prezioso dipendente offrendogli più denaro e benefici, nella speranza che il lavoratore "piratato" metta a disposizione del suo nuovo datore di lavoro il suo deposito di segreti.
Di seguito alcuni degli esempi più noti di spionaggio industriale:

- Hewlett-Packard: nel 2006 Hewlett-Packard, nel tentativo di scoprire i segreti trapelati alla stampa, ha assunto investigatori che hanno utilizzato il "pretesting", un metodo ingannevole e illegale per ottenere informazioni private, per raccogliere i tabulati telefonici di diversi giornalisti. Hewlett-Packard alla fine pagò 14,5 milioni di dollari allo stato della California e fu inoltre condannata a risarcire i giornalisti che spiava.
- General Motors: Opel, la divisione tedesca di General Motors, ha accusato la Volkswagen di spionaggio industriale nel 1993, dopo che il capo della produzione di Opel e altri sette dirigenti si erano trasferiti alla Volkswagen. Il caso è stato risolto nel 1997 con la Volkswa-

gen che ha accettato di pagare alla General Motors 100 milioni di dollari e di acquistare almeno $ 1 miliardo di parti di automobili nell'arco di anni.

- Google: il 13 gennaio 2010 Google ha annunciato che gli operatori dall'interno della Cina avevano violato la loro operazione "Google China" e rubato la proprietà intellettuale e l'accesso agli account di posta elettronica degli attivisti per i diritti umani. L'attacco, ritenuto parte di un diffuso attacco informatico alle aziende in Cina, è diventato noto come Operazione Aurora.
- Oracle: Nel 2000, Oracle è stata sorpresa a pagare degli investigatori per acquisire la spazzatura degli stabilimenti Microsoft perché sospettava che l'azienda stesse pagando due organizzazioni di ricerca apparentemente indipendenti per pubblicare rapporti in proprio favore.

Detto questo, lo spionaggio economico è orchestrato dai governi ed è di portata internazionale, mentre lo spionaggio industriale o aziendale generalmente avviene tra organizzazioni.
I governi stranieri, in particolare quelli in cui molte aziende sono di proprietà statale e hanno una forte attenzione allo sviluppo economico, sono utenti comuni dello spionaggio aziendale. Di conseguenza, anche altri governi si ritrovano coinvolti nel fenomeno.

CONCLUSIONI

Per difendere la propria azienda da comportamenti integranti il reato di spionaggio industriale, è necessario adottare strategie finalizzate al compimento di attività volte a prevenire o porre rimedio alle possibili minacce per la sicurezza delle informazioni.

Questi fenomeni hanno fatto sorgere l'esigenza, per Enti e Aziende, di dotarsi di personale con competenze non esclusivamente tecniche ma anche di tipo investigativo, in grado di analizzare dati e predisporre linee guida per prevenire azioni criminali, rendendo la cyber intelligence un nuovo baluardo per la difesa dell'integrità e degli interessi aziendali anche in settori finora non considerati a rischio, rendendo quindi di fondamentale importanza la predisposizione di una strategia di difesa che utilizzi una serie di misure su più livelli.

I dati sono diventati un obiettivo chiave dello spionaggio industriale a causa della facilità con cui possono essere copiati e trasmessi, portando molte organizzazioni ad attribuire crescente importanza alla digital forensics e all'attribuzione IP per provare a determinare se, quando, come e chi abbia causato una violazione dei sistemi o una fuga di dati.

È certamente importante dotarsi di sistemi di Loss Prevention per inibire la fuoriuscita di informazioni, definire un'architettura di Privileged Access Management (PAM) che permetta di limitare il set delle azioni disponibili per ogni utente o predisporre meccanismi di UEBA (User and Entity Behavior Analysis) che consentono di raccogliere informazioni preziose tramite l'utilizzo di machine learning per analizzare tutte le azioni compiute dal personale operante, generando prontamente avvisi nel caso in cui il comportamento di un determinato utente devii dal

comportamento standard per quel tipo di ruolo o mansione aziendale.

Non è più sufficiente che la politica di sicurezza delle informazioni si concentri solo sulle singole organizzazioni. Le minacce informatiche all'interno e all'esterno di ciascuna organizzazione, infatti, possono portare al furto di segreti commerciali; e i processi di gestione e valutazione dei rischi di sicurezza dovrebbero riflettere questo scenario.

Non è mai stato così importante disporre di una solida strategia di sicurezza informatica e organizzativa per prevenire lo spionaggio aziendale.

Giuseppe Maio, *Security Advisor in ambito Governance, Risk and Compliance (GRC)*

Gabriele Minniti, *esperto di Sicurezza Informatica e Sicurezza delle informazioni*

BIOGRAFIA

Giuseppe Maio

In qualità di Cybersecurity Governance Specialist collabora, all'interno della function di Cybersecurity, con una delle principali multinazionali italiane che opera nel settore dell'energia, occupandosi di compliance, analisi delle principali normative di settore e sviluppo relazioni con i principali stakeholders ed enti governativi.

In precedenza ha lavorato come Security Advisor in ambito Governance, Risk e Compliance per un'importante società di consulenza strategica.

A seguito del conseguimento della laurea in Giurisprudenza, ha frequentato il Master di II Livello presso l'Università LUISS in "Cybersecurity: politiche pubbliche, normative e gestione".

È membro della Commissione Cyber Threat Intelligence presso la Società Italiana di Intelligence (SOCINT) collaborando a diverse progettualità tra cui la redazione di contributi, articoli e paper; coordina il progetto "Cybersecurity Liaison" finalizzato ad attività di redazione di position paper e supporto al decisore.

BIOGRAFIA

Gabriele Minniti

È un informatico specialista in Sicurezza Informatica e Sicurezza delle informazioni con oltre 15 anni di esperienza. Ha conseguito molteplici certificazioni internazionali in ambito tecnologico ed ha lavorato in Germania ed Inghilterra per importanti aziende costruttrici di tecnologie per la Sicurezza Informatica. Nel corso della sua carriera è stato chiamato sia come consulente che come docente per entità afferenti al comparto della Difesa. Fondatore di WhySecurity srl, oggi si occupa di supporto ad indagini difensive collaborando con investigatori privati, svolge analisi di rischio economico connesso al rischio informatico e offre servizi SOC a favore dei propri clienti.

FORUM ICT SECURITY

25-26 OTTOBRE 2023

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
21ª Edizione del Forum ICT Security