#02

ICT Security MAGAZINE

CYBER CRIME

PREFAZIONE DI

IVANO GABRIELLI

Direttore del Servizio Polizia Postale e delle Comunicazioni

2022

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINIT.ORG

WWW.CYBER40.IT

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SOCINT Società Italiana di Intelligence

ICT Security MAGAZINE

QUADERNI DI CYBER INTELLIGENCE

Questo secondo numero, che affronta argomenti inerenti il Cyber Crime, nasce dalla collaborazione tra ICT Security Magazine, la Società Italiana di Intelligence (SOCINT) e il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity (Cyber 4.0).

SOCINT Società Italiana di Intelligence

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

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

CENTRO DI COMPETENZA NAZIONALE AD ALTA SPECIALIZZAZIONE PER LA CYBERSECURITY

Cyber 4.0 è il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, uno degli 8 centri di competenza ad alta specializzazione finanziati dal Ministero dello Sviluppo Economico.
La missione del Centro è accompagnare policy maker, imprese e PA in un percorso di crescita verso una digitalizzazione sicura, grazie a soluzioni concrete, strategiche e sostenibili basate su conoscenze, tecnologie innovative e servizi abilitanti sviluppati con le competenze del proprio network, che valorizzino le eccellenze del Paese nel contesto europeo e internazionale.

Indice

Prefazione a cura di **Ivano Gabrielli,** *Direttore del Servizio Polizia Postale e delle Comunicazioni*

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

14

Operazioni di cyber spionaggio nel conflitto tra Russia e Ucraina

Il cyber spionaggio è un tipo di attacco informatico che ha come fine quello di accedere l'accesso a dati sensibili e informazioni su attività o progetti futuri di agenzie governative e non per ottenerne vantaggi a livello economico.

Francesco Schifilliti

32

Cognitive Security (COGSEC)

Contenuti ingannevoli, fuorvianti, falsificati o fabbricati ad arte vengono regolarmente creati e diffusi online con l'intento di creare confusione e ampliare le divisioni politiche-sociali, o di commettere crimini.

Francesco Arruzzoli

46

Il potenziamento della cooperazione internazionale in materia di cybercrime e prove elettroniche

Evento centrale del semestre di Presidenza Italiana del Consiglio d'Europa, il 13 maggio 2022 si è tenuta a Strasburgo la cerimonia di apertura per la firma del Secondo Protocollo Addizionale alla Convenzione di Budapest.

Matteo Lucchetti

56 **Cybercrime-as-a-Service (CaaS). Il ruolo delle transazioni in criptovalute nel Darknet**

Tra tutti i servizi offerti sui mercati darknet quello attualmente di maggior successo, oltre alla vendita di stupefacenti, è indubbiamente il Ransomware-as-a-Service (RaaS)

Achille Pierre Paliotta

80 **Insider Threat o minaccia interna**

Le minacce interne presentano un rischio complesso e dinamico che colpisce i domini pubblici e privati di tutti i settori, incluse le infrastrutture critiche.

Giuseppe Maio

88 **Il furto di identità e come non facilitarlo – il luogo comune "non ho nulla da nascondere"**

In generale esistono due tipi di attacco informatico: "a pioggia" e "mirato". Nei primi si è attaccati per il semplice fatto di essere utenti di Internet; nei secondi invece l'attacco è legato al nostro ruolo, status o funzione e integra un'azione espressamente studiata per noi. intelligence

Fabrizio d'Amore

PREFAZIONE

Tra le varie declinazioni della cybersicurezza le statistiche di settore confermano, anno dopo anno, come la dimensione criminale alla base degli attacchi informatici costituisca ancora la matrice di gran lunga prevalente.

Una matrice cui si associa, in maniera certamente non meno preoccupante, la proliferazione di attività ostili motivate da ragioni di *cyber-warfare*: specie nel corso di fasi storiche, come quella attuale, caratterizzate da tensione e conflitti internazionali che vedono nel dominio cibernetico uno dei principali terreni di elezione.

La materia dell'**anticrimine informatico** richiede, dunque, un'attenzione privilegiata, non soltanto da parte delle autorità pubbliche ma anche degli operatori della cybersicurezza, professionisti, ricercatori e funzionari del settore privato.

Nell'occuparci di cybercrime, tuttavia, sappiamo di agire in un ambito caratterizzato da estrema complessità, non soltanto a causa della mole notevolissima di minacce esistenti: è soprattutto sotto il

profilo qualitativo che emergono infatti le maggiori criticità, abilitate dall'intervento di vari e concomitanti fattori, sia interni sia esterni rispetto alla minaccia stessa.

Dal primo punto di vista, l'evidente considerazione dell'intrinseca complessità tecnica della materia si lega alla presenza di tecnologie, sempre più performanti, di alterazione, camuffamento ed eliminazione delle tracce informatiche lasciate da parte dell'autore di un attacco a un sistema, come pure delle tracce di pagamenti elettronici eseguiti per assicurarsi (o per riciclare) il profitto di un reato.

Tali tecnologie - neutre dal punto di vista della loro liceità e persino necessarie se utilizzate a fini di progresso economico e sociale o a protezione dei diritti individuali - mutano completamente qualificazione quando vengono asservite al compimento di attività illecite, risolvendosi in ostacoli rilevanti per l'identificazione di un attore ostile.

Ma gli ostacoli, si diceva, sono anche di carattere esterno e in questo senso richiamano, in primo luogo, l'elemento della costante transnazionalità delle condotte criminose: persino nelle ipotesi in cui vittima e autore di un attacco risiedano nel medesimo territorio, percorrere a ritroso le tracce che dalla seconda riconducono al primo realizza un'attività destinata a valicare inevitabilmente i confini della giurisdizione domestica, coinvolgendo *provider, server,* nodi di rete e servizi installati all'estero che richiedono, per essere efficacemente approfonditi, la collaborazione di autorità e soggetti privati operanti al di fuori dell'ambito di intervento dell'autorità nazionale inquirente.

A fronte di tale scenario è possibile erigere efficaci difese solo a patto di concentrare, in chiave sinergica e collaborativa, gli sforzi di tutti gli operatori della sicurezza – istituzionali, privati e della ricerca – verso lo sviluppo di risorse utili al contrasto ma, più ancora, alla prevenzione.

Una prevenzione che sia frutto di una rinnovata attenzione ai temi della *cybersecurity* e della *cyber hygiene*, coinvolgendo tanto il piano degli operatori privati - chiamati all'implementazione e al costante aggiornamento delle risorse

umane e tecnologiche interne alla propria organizzazione – quanto degli studiosi e ricercatori, destinati a misurarsi con scenari complessi e rapidamente mutevoli, quanto soprattutto delle autorità pubbliche le quali, in uno sforzo di costante *capacity-building*, si dedicano quotidianamente alla protezione di organizzazioni, imprese e cittadini.

Ivano Gabrielli, Direttore del Servizio
Polizia Postale e delle Comunicazioni

BIOGRAFIA

Ivano Gabrielli

Laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, il Dr. Ivano Gabrielli è nella Specialità Polizia Postale e delle Comunicazioni dal 2006. Dopo 3 anni in forza al Compartimento Polizia Postale e delle Comunicazioni di Genova, dal 2009 è al Servizio Polizia Postale del Dipartimento della PS.

Dal maggio 2012 è il Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC).

Dal luglio 2017 è il Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, a cui fanno riferimento il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC, la Sezione Cyber Terrorismo e la Sezione per il contrasto al Financial Cyber Crime e dal gennaio 2022 è anche il Direttore del Servizio Polizia Postale e delle Comunicazioni.

INTRODUZIONE

La Commissione *Cyber Threat Intelligence* e *Cyber Warfare* (di seguito "Commissione"), parte integrante della SOCINT (Società Italiana di Intelligence), è giunta alla sua seconda edizione di questo quaderno tematico, stavolta con un focus sul tema del *Cybercrime*.

Utilizzando una famosa frase del filosofo cinese Sun Tzu - "*conosci il tuo nemico*" - possiamo sostenere che, per analizzare a fondo il fenomeno del *cybercrime*, bisogna prima di tutto comprendere le motivazioni che muovono questi gruppi criminali. Al riguardo abbiamo deciso di adottare un approccio multidisciplinare, che ne evidenzia la complessità da più punti di vista: giuridico, tecnico e d'impatto sociale.

Esistono molti elementi ancora da considerare, ma di certo in questo quaderno si è cercato di sottolineare l'importanza delle attività d'*intelligence* per il contrasto al crimine informatico, in modo da comprendere le dinamiche, le sfide, i rischi e le "opportunità" del fenomeno stesso.

Ciò detto, pur con i limiti concettuali

sopra esposti, gli obiettivi generali della ricerca possono essere così declinati:

- evidenziare le carenze normative e definire nuove linee guida per il contrasto al *cybercrime*;
- analizzare le principali minacce in corso e le azioni di possibili rimedi in ottica di *intelligence*;
- comprendere il fenomeno da un punto di vista multidisciplinare, giuridico-sociologico-tecnico;
- suggerire le possibili soluzioni/azioni, tecnologiche e non, ritenute utili.

Il lavoro complessivo che ne è scaturito può essere visto come una proposta rivolta all'Agenzia di Cybersicurezza Nazionale (ACN), nonché un utile strumento per gli organismi investigativi o altre associazioni e istituzioni italiane.

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

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. 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 CyberWarfare della Società Italiana di Intelligence.

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**

Operazioni di cyber spionaggio nel conflitto tra Russia e Ucraina

La domanda più difficile per un analista di *intelligence* riguarda spesso le motivazioni che si celano dietro un attacco informatico. Risulta infatti molto più semplice, nella maggior parte dei casi, ricostruire le varie fasi di un attacco piuttosto che comprendere perché sia stato sferrato.

La risposta a tale quesito varia a seconda dei casi; ma è un dato di fatto che i criminali informatici agiscano in maniera opportunistica, cercando di ottenere il miglior risultato con il minor sforzo possibile, usando i metodi più semplici e allo stesso tempo più efficaci, calibrati sui propri obiettivi.

Per comprendere a fondo un attacco è fondamentale analizzare, insieme ai TTP utilizzati, le diverse caratteristiche e motivazioni che permettono di creare un profilo accurato dei responsabili delle minacce.
La geopolitica gioca un ruolo fondamentale: senza un contesto politico, un'analisi puramente tecnica è insufficiente per attribuire un malware a una fonte precisa. Scoprire chi si nasconde dietro un attacco è una delle attività più complesse che un analista deve sostenere: non sempre si riescono ad attribuire con certezza le responsabilità, mentre le motivazioni spesso si intrecciano alle categorizzazioni.

Viceversa, oggigiorno una decisione politica che possa definirsi soddisfacente deve tenere in considerazione le informazioni ottenute attraverso la *Cyber Threat Intelligence*. In molti Stati (Russia, Cina, Israele, Iran, etc.) è ormai prassi utilizzare tecniche di *cyber warfare* e, in particolare, di *cyber espionage* per ottenere informazioni su altri Stati, o per danneggiare infrastrutture civili o governative e interferire con sistemi critici, con esiti che possono comportare anche perdite di vite umane.

Il cyber spionaggio[1] è un tipo di attacco informatico che ha come fine l'accesso a dati sensibili e informazioni su attività o progetti futuri di agenzie governative

e non per ottenerne vantaggi a livello economico. Questa pratica, sviluppatosi di pari passo con il web, viene utilizzata regolarmente contro obiettivi occidentali da Stati come la Russia, la Cina, l'Iran, la Corea del Nord, etc.
Va però notato che, mentre tradizionalmente gli attacchi di tipo governativo si sono sempre concentrati sullo spionaggio, sviluppi recenti includono sempre più spesso azioni distruttive, ingerenze sociali e, in molti casi, anche un tornaconto economico.

Secondo gli analisti di SecureWorks lo spionaggio industriale rimane al primo posto tra le motivazioni dei Paesi che utilizzano regolarmente tecniche di *cyber warfare*. Gli esperti hanno affermato che "*Hostile state activity will continue to focus primarily on espionage rather than on disruption and destruction. Several states, notably China, Russia, and Iran, will continue to conduct operations aimed at harvesting bulk data to support subsequent cyber operations and traditional espionage activities*".

Sul piano geopolitico, la Russia è spinta soprattutto dalla volontà di riaffermare l'influenza a livello globale di cui godeva ai tempi dell'URSS. Per raggiungere questo obiettivo, la Russia non mostra remore a ricorrere alla forza militare laddove il rischio di una reazione da parte della NATO appare debole, mentre si affida ad armi digitali in caso contrario, in modo da poter eventualmente negare ogni responsabilità. I suoi scopi principali sono tre: spiare gli altri Paesi per rimanere al passo con le loro tecnologie, raccogliere dati per poter accedere a settori critici e destabilizzare le società nemiche.

Culturalmente, la Cina è molto diversa dalla Russia. Si muove sul lungo periodo, cercando di mantenere un basso profilo, ma influenzando al contempo l'economia globale. Al contrario della Russia non ha interessi nel distruggere o sovvertire altre società, economie o governi, puntando piuttosto a dominarli e sovrastarli. Non può però raggiungere questi obiettivi senza tecnologie miglio-

[1] "*China's Cyber Espionage*" - https://www.cyber-insights.org/chinas-cyber-espionage.

ri e un sistema economico più solido. Differentemente dalla Russia appare meno interessata a negare, qualora necessario, l'evidenza di un proprio intervento in un conflitto vero e proprio: per questo motivo si ritiene che le attività cyber ostili da parte dei cinesi subiranno un'accelerazione nel prossimo futuro.

Per ora, la Cina deve recuperare terreno in entrambi i settori; e per farlo usa sempre più la *cyber information*, sfruttando il cyber spionaggio come metodo primario per rubare segreti tecnologici statali, insieme a credenziali di personalità che potrebbero essere in grado di promuovere gli interessi nazionali.
È importante ricordare, da un punto di vista storico, che quando la Cina è diventata una potenza nel cyberspazio (soprattutto tra i Paesi asiatici) il Partito Comunista Cinese (PCC) è stato colto di sorpresa e ha dovuto sviluppare un completo quadro normativo per mantenere il controllo su ciò che veniva pubblicato online. Negli ultimi vent'anni, le attività di spionaggio informatico cinesi sono aumentate progressivamente e stanno presentando nuove minacce per l'area asiatico-pacifica.
Più dettagliatamente, il Ministero della Sicurezza di Stato cinese (MSS) sta acquistando rilievo nel cyberspazio grazie a un aumento nei propri standard di sicurezza operativa, intraprendendo inoltre una campagna globale di spionaggio informatico che punta a obiettivi strategici, politici ed economici.

Secondo quanto osservato e descritto dal Cyberpeace Institute[2], gli attacchi contro la Russia sono stati portati avanti soprattutto da gruppi di cyber hacktivisti (Anonymous, NB65, etc.) mentre - verso l'Ucraina - la Russia sta utilizzando capacità cyber "ibride" su larga scala (i dettagli sono disponibili nel comunicato pubblicato dal Computer Emergency Response Team ucraino[3]).
Nel corso del conflitto, a livello statale, i russi hanno effettuato attacchi cyber

[2] https://cyberconflicts.cyberpeaceinstitute.org/

[3] https://cert.gov.ua/

coordinati ad azioni militari sul campo.

Almeno sei gruppi Advanced Persistent Threat (APT)[4] russi e altri su cui non è stato possibile effettuare l'*attribution* hanno condotto attacchi distruttivi, operazioni di spionaggio o entrambi, mentre le forze militari russe attaccavano il Paese via terra, aria e mare.

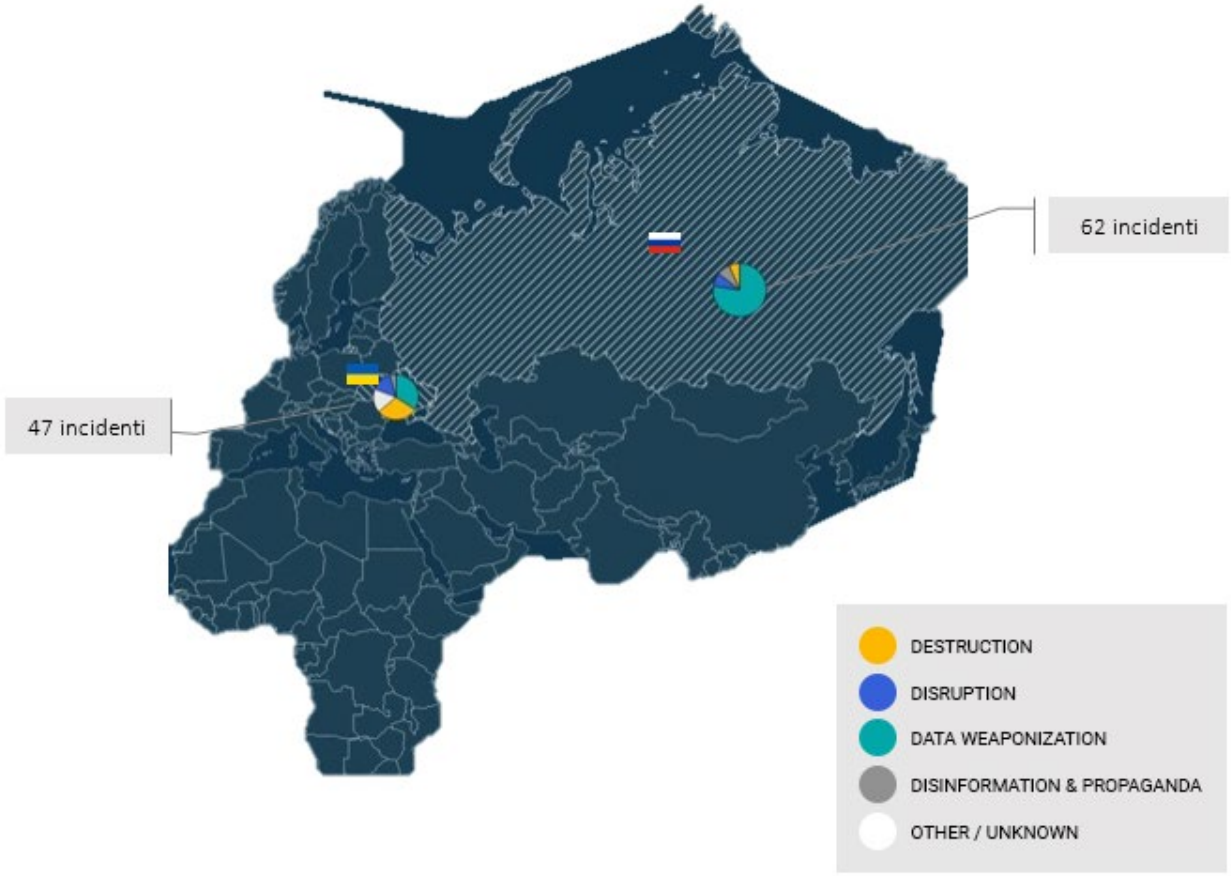


Fig.1 - Incidenti informatici durante il conflitto riportati dal Cyberpeace Institute

[4]-Microsoft, *"Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine"*.

Il grafico seguente mostra i gruppi APT dell'*intelligence* russa che hanno colpito l'Ucraina nel corso del conflitto, tra cui APT29 (SRV), APT28, Sandworm e DEV-0586 (GRU), Gamaredon e Dragonfly (FSB)[5]:

attivamente. Ad ogni modo, le azioni cibernetiche e cinetiche puntano a interrompere o compromettere le funzioni governative e militari ucraine nonché a minare la fiducia dei cittadini nelle istituzioni.

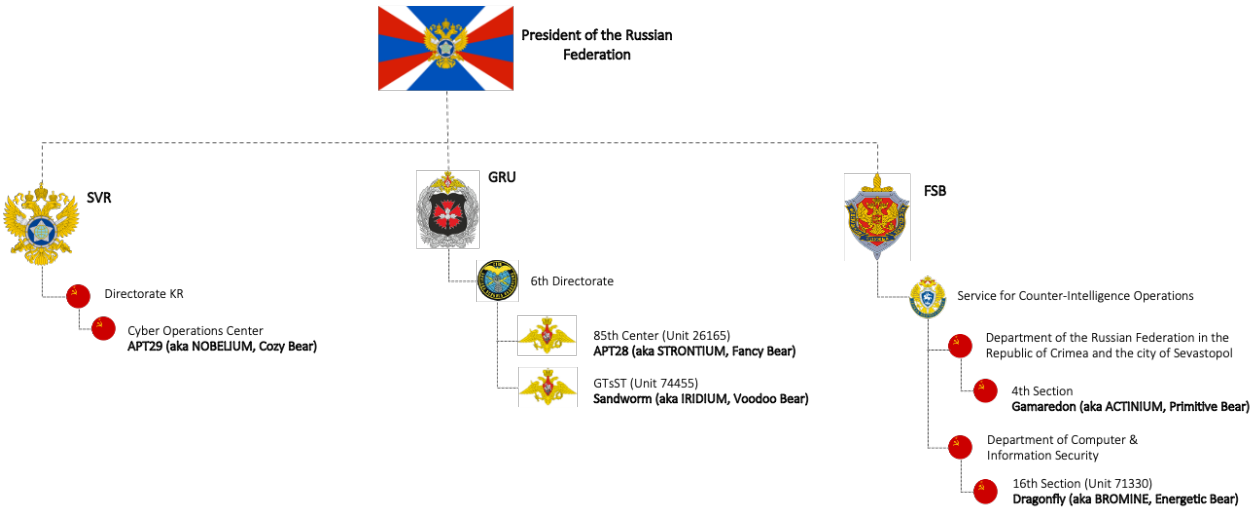


Fig. 2 – I gruppi russi APT attivi nel conflitto Russia-Ucraina

Non è chiaro se questi gruppi e le forze militari stiano solo perseguendo in modo indipendente una serie di obiettivi comuni o se si stiano coordinando

Gli attacchi distruttivi sono stati prevalenti nelle operazioni cyber russe durante questa guerra. A titolo esemplificativo, un giorno prima dell'invasione

[5] As new identified group that Mandiant calls UNC3524 has TTPs that overlap with APT28 and APT29 - https://www.mandiant.com/resources/unc3524-eye-spy-email.

militare alcuni operatori associati alla GRU, il servizio di *intelligence* militare russo[6], hanno lanciato attacchi *wiper* distruttivi su centinaia di sistemi di organizzazioni governative, informatiche, energetiche e finanziarie ucraine.

Le famiglie di malware che sono state rintracciate in questi attacchi sono:

- WhisperGate / WhisperKill
- FoxBlade, aka Hermetic Wiper
- SonicVote, aka HermeticRansom
- CaddyWiper
- DesertBlade
- Industroyer2
- Lasainraw, aka IssacWiper
- FiberLake, aka DoubleZero

WhisperGate, FoxBlade, DesertBlade e CaddyWiper sono tutte famiglie di malware che sovrascrivono i dati e rendono impossibile riavviare i computer colpiti. FiberLake è una funzionalità .NET utilizzata per cancellare dati. SonicVote cripta i file e talvolta viene utilizzato insieme a FoxBlade, mentre Industroyer2 colpisce specificamente la tecnologia operativa per ottenere effetti fisici nella produzione e nei processi industriali.

L'analisi relativa a Sandworm è stata confermata anche dal UK National Cyber Security Centre (NCSC), dalla Cybersecurity and Infrastructure Security Agency (CISA), dalla National Security Agency (NSA) e dall'FBI.
Inoltre, queste agenzie hanno identificato un nuovo malware utilizzato da Sandworm, qui denominato Cyclops Blink. Cyclops Blink appare come un framework sostitutivo per il malware VPNFilter, scoperto nel 2018, che sfruttava i dispositivi di rete, principalmente i router di piccoli uffici/uffici domestici (SOHO) e i dispositivi NAS (Network Attached Storage)[7].
Da allora l'attività del malware ha incluso tentativi di distruzione, danneggiamento e infiltrazione nelle reti di agenzie governative e in un'ampia gamma di

[6] The Trellix paper "Growling Bears Make Thunderous Noise" reports an overview of groups involved in the conflict, but also the wiper families and their attribution.

[7] https://www.cisa.gov/uscert/ncas/alerts/aa22-054a.

infrastrutture critiche, colpite in alcuni casi anche con attacchi di terra e missili da parte delle forze militari russe.

Queste operazioni cibernetiche non solo hanno danneggiato le funzionalità delle organizzazioni prese di mira ma, in molti casi, hanno impedito ai cittadini l'accesso a fonti di informazione affidabili e a servizi di vitale importanza, nel tentativo di far vacillare la loro fiducia nelle istituzioni.

Non c'è dubbio che questa guerra stia mostrando come i conflitti moderni vengano ormai combattuti usando allo stesso tempo armi tradizionali (cd. *kinetic weapon*) e digitali.
Uno tra i numerosi esempi è stato rilevato dal Microsoft Threat Intelligence Center (MSTIC)[8], che ha identificato un gruppo di hacker russi che si muoveva nella rete informatica di una società di energia nucleare. Il giorno successivo, l'esercito russo ha attaccato e occu-

Fig. 3 – Il coordinamento delle operazioni cibernetiche e militari russe in Ucraina

[8] Microsoft report *"Defending Ukraine- Early Lessons from the Cyber War"*.

pato la più grande centrale nucleare ucraina.
La stessa settimana il gruppo militare russo APT28 ha compromesso una rete governativa in Vinnytsia e due giorni dopo ha lanciato otto missili cruise contro l'aeroporto della città. Analogamente, l'11 marzo le forze russe hanno preso di mira un'agenzia governativa di Dnipro con un attacco cyber distruttivo, utilizzando contemporaneamente armi convenzionali contro gli edifici governativi.

Per completezza di informazione, nel grafico seguente sono riportate le organizzazioni governative della Federazione Russa[9], [10]:

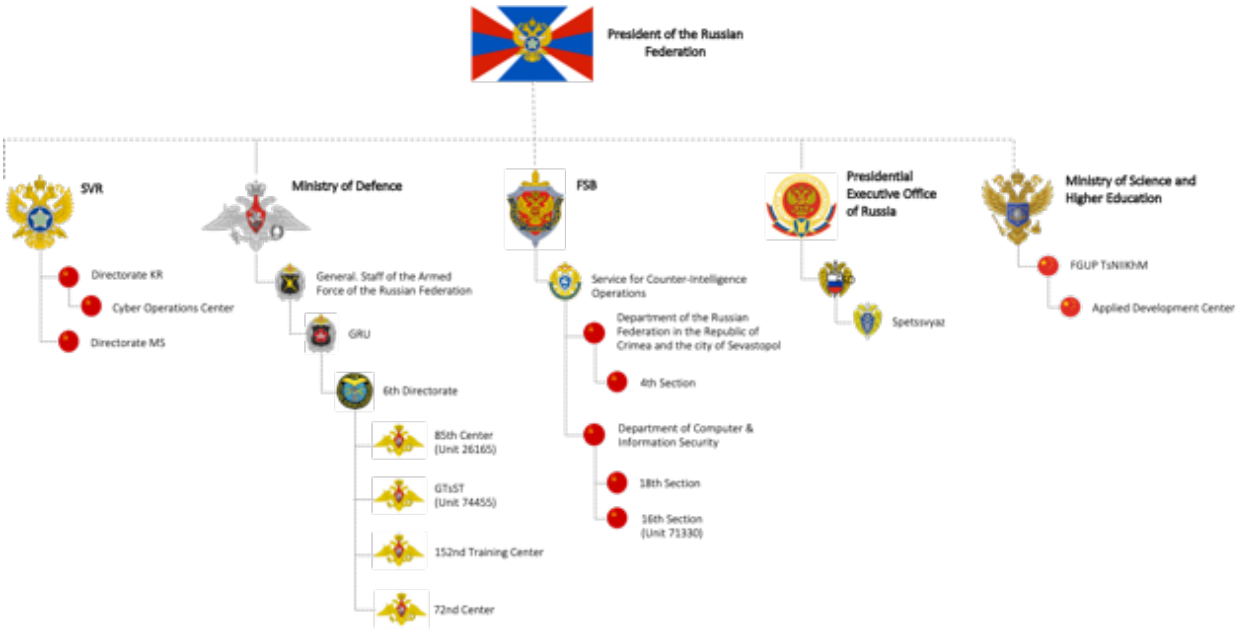


Fig. 4 – Gruppi cyber russi

[9] https://xorl.wordpress.com/2021/04/16/russias-cyber-operations-groups.

[10] https://itcsecure.com/threat-horizon/russian-intelligence-service/.

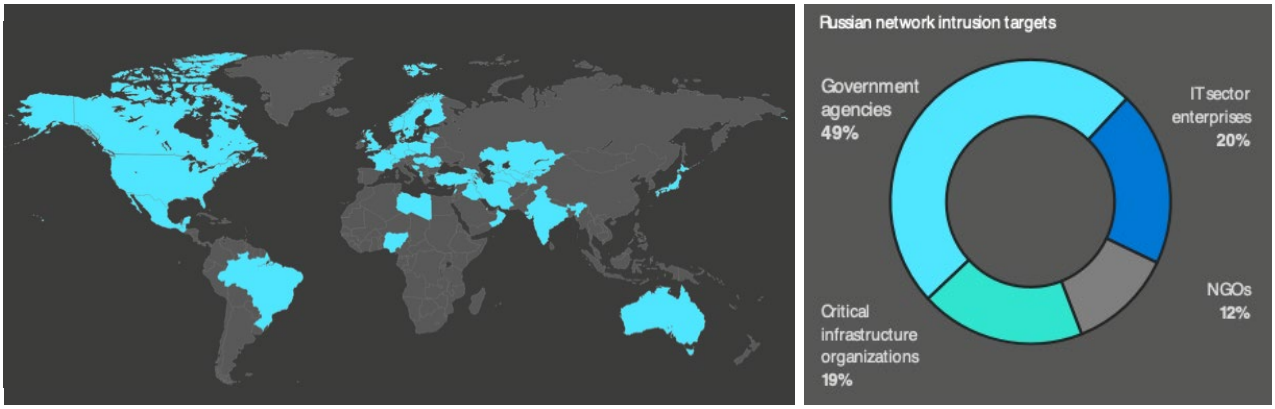


Fig. 5 – Recenti operazioni russe di infiltrazione e di spionaggio informatico al di fuori dell'Ucraina

Sono diversi gli aspetti di questo conflitto che andrebbero analizzati nel dettaglio per capire come gestire future crisi. Tra tutti, spiccano il ruolo e il supporto in termini di capacità informatiche offerto da eventuali alleati.

Anche se non sarà trattato in questo articolo, il ruolo che la NATO (in particolare gli Stati Uniti) ha avuto nel conflitto fino ad oggi rappresenta un argomento rilevante che dovrebbe essere approfondito, insieme a:

- gli impatti (in termini di mitigazione degli attacchi informatici) derivanti dall'adeguamento complessivo delle infrastrutture di sicurezza di rete prima del conflitto;
- gli effetti sul conflitto dovuti alle azioni degli stati alleati con l'Ucraina.

Proprio su questo punto, il Gen. Paul Nakasone (a capo del Cyber Command statunitense) ha dichiarato: "*Abbiamo condotto una serie di operazioni a tutto campo*: *offensive, difensive e informative*".

Ovviamente anche la Russia ha mantenuto o lanciato nuove campagne cyber contro gli stati alleati con l'Ucraina. Dall'inizio della guerra, l'MSTIC ha rilevato 128 intrusioni russe in 42 stati, Ucraina esclusa. Tra le vittime il 49% è rappresentato da agenzie governative, prese di mira molto probabilmente per il sostegno diretto o indiretto dato all'Ucraina. Un altro 12% include organizzazioni non governative, nella maggior parte dei casi centri di ricerca su po-

litica estera o gruppi umanitari impegnati nel portare aiuti alla popolazione colpita o a fornire supporto ai rifugiati. La percentuale rimanente comprende aziende informatiche o del settore energetico, insieme ad altre coinvolte in settori critici della difesa o dell'economia.

Dall'altro lato, è interessante osservare anche le attività effettuate dalla Cina nel corso di questo conflitto. Come illustrato nell'immagine che segue, sono state rilevate campagne di cyber spionaggio dalla Cina verso l'Ucraina, ma anche nei confronti della Russia.

Le operazioni di cyber spionaggio verso le due nazioni sono state condotte da differenti attori. Nello specifico, il 22 marzo 2022, il CERT-UA ha pubblicato l'avviso #4244, condividendo un rapido riepilogo e gli elementi che hanno portato ad attribuire un recente tentativo di infiltrazione a *UAC-0026*, noto anche come *Scarab*. Si tratta del primo *threat actor* cinese ad aver colpito pubblicamente l'Ucraina dall'inizio dell'invasione, utilizzando, a quanto risulta, la *backdoor* conosciuta come *Scieron*.

Sicuramente la parte più interessante delle operazioni di spionaggio cine-

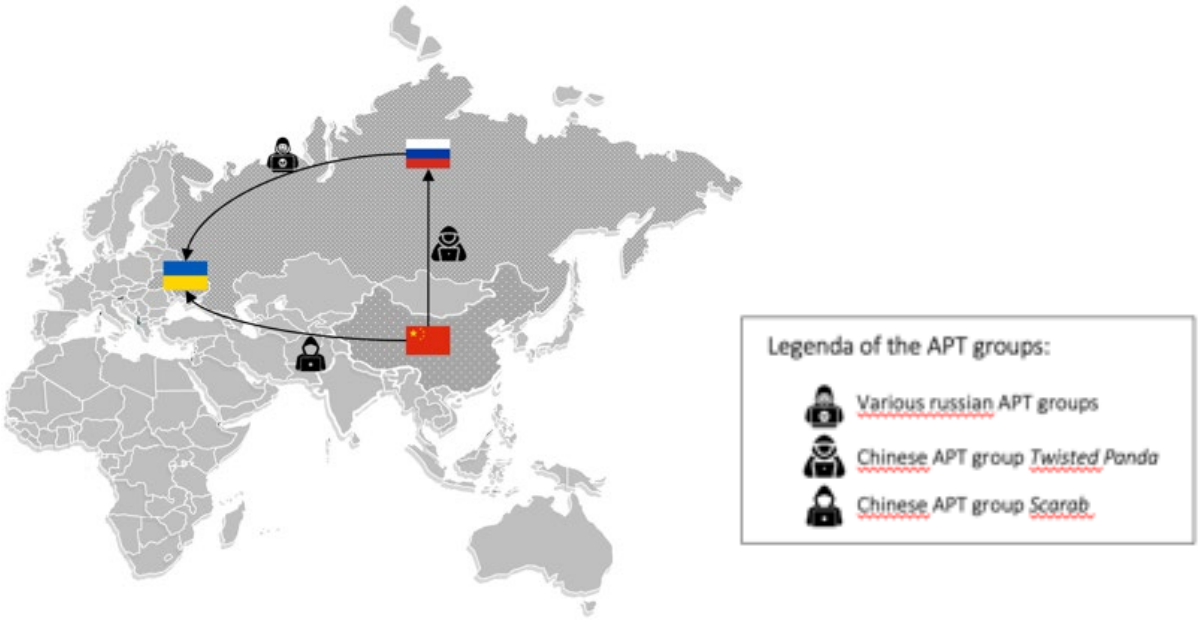


Fig. 6 – Gruppi APT attivi nel conflitto russo-ucraino

se è quella che riguarda la Russia. Il 19 maggio 2022 i ricercatori di Check Point hanno pubblicato un report[11] sulle operazioni di un gruppo ATP affiliato alla Cina - noto come *Twisted Panda* - che ha attaccato due istituti di ricerca difensiva, inclusa la Rostec Corporation russa, oltre a un'entità con sede a Minsk, in Bielorussia, la cui identità non è stata resa pubblica.

In base ai dati telemetrici di Check Point, questa sarebbe solamente l'ultima fase di un'operazione di cyber spionaggio cinese contro entità filorusse che dura almeno dal giugno 2021. La minaccia più recente relativa a questa campagna è stata scoperta nell'aprile 2022.

L'operazione è stata attribuita ad attori affiliati al governo cinese con possibili legami con APT10 (conosciuto anche come Stone Panda) e Mustang Panda. Gli attacchi sono partiti da e-mail di *phishing* contenenti un link che sembrava falsamente provenire dal Ministero della Salute russo. Come riportato sopra, Twisted Panda si è infiltrato in tre nuove organizzazioni a marzo 2020. Le vittime hanno tutte sede negli Stati Uniti e comprendono una multinazionale di assicurazioni, un'azienda di produzione di apparecchiature e un'organizzazione di servizi professionali e di consulenza per soluzioni tecnologiche.

Basandosi sulle connessioni tra gli autori delle minacce, crediamo sia plausibile collegare Twisted Panda al Ministero della Sicurezza di Stato Cinese (MSS). Il grafico che segue illustra i gruppi di operazioni cyber cinesi[12].

La Cina aveva già effettuato in passato operazioni di spionaggio nei confronti della Russia, ma in questo caso risaltano gli obiettivi scelti e la possibilità che le informazioni ricercate dall'*intelligence* cinese possano essere collegate a questo specifico momento del conflitto.

[11] https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

[12] https://xorl.wordpress.com/2021/04/20/chinese-cyber-operations-groups/

Innanzitutto, è indubbio che Rostec - holding statale operante nel settore aerospaziale e della difesa - assuma un valore strategico. Non a caso l'11 marzo 2022 è stata colpita da un attacco DDoS (*Distributed denial-of-service*) che ha portato alla chiusura del suo sito. Rostec ha affermato di aver subito continui attacchi a partire dal febbraio 2022, quando la Russia ha invaso l'Ucraina.

Il sito di Rostec è stato chiuso per implementare le contromisure necessarie a fermare l'attacco, attribuito all'Ucraina. Molti domini e risorse di Rostec erano infatti nella lista degli obiettivi di attacchi DDos presentata dall'IT Army of Ukraine, un gruppo di volontari provenienti da tutto il mondo creato per sostenere l'Ucraina sul fronte cyber.

Fig. 7 – Gruppi cyber cinesi

Non disponendo di informazioni specifiche riguardanti gli obiettivi della campagna di spionaggio cinese nei confronti dei russi, possiamo solamente fare supposizioni su quali possano esserne gli obiettivi reali. Una questione che ci è sembrata rilevante e su cui l'intelligence cinese potrebbe avere mire è legata al livello di produzione di armi e strumenti comunicativi utilizzati dalla Russia nel conflitto.

Come vedremo più avanti nel dettaglio, la Russia sta gestendo un grave problema di produzione causato dalle sanzioni[13] imposte dalla NATO e applicate da molti Stati[14], in particolare dal non poter importare tutti i prodotti *dual-use*[15], ossia gli strumenti che possono essere utilizzati a fini sia civili e sia militari.

È importante capire e tenere conto di queste limitazioni, poiché possono fornire indicazioni sulla durata del conflitto, oltre a delineare le strategie militari ed economiche che la Russia potrebbe adottare[16].

Lo sforzo produttivo dei sistemi offensivi russi nel corso della guerra è molto elevato, in quanto esiste un limite alla percentuale di scorte che la Russia può utilizzare contro l'Ucraina senza rischiare poi di non riuscire a difendersi eventualmente da NATO, Cina o altri Paesi ritenuti nemici[17].
Senza una catena di approvvigionamento affidabile che possa aumentarne la produzione i russi sono costretti a trattenere gran parte delle scorte, limitando la loro capacità di colpire

[13] https://rostec.ru/en/news/4513317/.

[14] https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/.

[15] https://www.engadget.com/us-sanctions-russia-technology-105132550.html

[16] https://www.globaldefensecorp.com/2022/04/06/sanctions-hit-rostec-china-quietly-replaced-russia-as-arms-exporter/.

[17] https://www.reuters.com/world/us-imposes-additional-russia-related-sanctions-treasury-website-2022-03-31/.

l'Ucraina nei prossimi mesi. Questo è il problema principale dell'apparato militare russo, dal momento che le armi più moderne dipendono fortemente da componenti specialistiche prodotte all'estero[18].

Nel corso della guerra, i russi hanno utilizzato ampiamente missili da crociera e balistici per colpire obiettivi militari, politici ed economici ucraini[19]. Questo tipo di armi sono fondamentali, soprattutto date le scarse prestazioni dell'aviazione russa. Non si conosce precisamente di quante scorte dispongano i russi ma, con l'avanzare della guerra, gli ufficiali ucraini hanno notato un ridimensionamento dei sistemi di armamento per diverse missioni, addirittura con un ritorno ai sistemi Grad-1 su obiettivi secondari.

Fig. 8 – Sede principale del Rostec Institute

[18] "*Operation Z - The Death Throes of an Imperial Delusion*", Jack Watling and Nick Reynolds for Royal United Services Institute for Defence and Security Studies.

[19] https://graphics.reuters.com/UKRAINE-CRISIS/WEAPONS/lbvgnzdnlpq/.

Secondo le valutazioni degli Stati Uniti, l'esercito russo sarebbe attualmente a corto di armi di precisione.

Sarà fondamentale per la Russia potersi procurare componenti da altri Paesi per produrre armi da usare nel conflitto. Di seguito alcuni esempi.

I missili da crociera 9M727 (lanciati dall'Iskander-K) sono dotati di un computer con elevate caratteristiche di robustezza, ottenute grazie a materiali e componenti altamente specializzati. Dei sette punti di attacco di questi computer, che consentono di trasmettere dati attraverso lo scudo termico, solamente uno è di progettazione sovietica e viene prodotto in Russia; gli altri sei sono tutti sviluppati da aziende statunitensi. Le guide che collegano i circuiti stampati e il corpo del computer (e che devono mantenere l'allineamento dei componenti anche sotto immensa pressione) sono anch'esse di produzione statunitense, così come gli stessi circuiti stampati.
I 9M727 non sono l'unico esempio di dipendenza da componenti stranieri: la stessa problematica si riscontra su tutte le armi russe rinvenute sul campo di battaglia. Il missile teleguidato 9M949 da 300 mm, che costituisce la parte principale dell'artiglieria di precisione russa come munizione per il sistema di lancio multiplo di razzi Tornado-S, utilizza un giroscopio a fibre ottiche di produzione statunitense per la navigazione inerziale.
Il sistema di difesa aerea TOR-M2 si basa su un oscillatore di progettazione britannica presente nel computer che controlla il radar della piattaforma, l'Iskander-M, il missile da crociera Kalibr, il missile da crociera terra-aria Kh-101 e molti altri ancora.
Il laboratorio tecnico dell'*intelligence* ucraina ha condotto dei test sulle radio militari russe di tipo Aqueduct (R-168-5UN-2, R-168-5UN-1 e R-168-5UT-2), utilizzati per le comunicazioni tattiche dell'esercito russo, scoprendo che molte componenti elettroniche fondamentali sono prodotte negli Stati Uniti, in Germania, nei Paesi Bassi, nella Corea del Sud e in Giappone. Questo schema si ripete ovunque: quasi tutto l'hardware militare moderno della Russia dipende da sistemi elettronici complessi importati da Stati Uniti, Regno Unito, Germania, Pa-

esi Bassi, Giappone, Israele, Cina e altri ancora.

Lo spettro di una guerra a lungo raggio mette la Russia dinanzi a una serie di sfide molto maggiori rispetto a quelle previste per una guerra lampo.

Per districarsi tra il problema di dipendenza dalle componenti estere per gli armamenti e le sanzioni sempre più pesanti, l'amministrazione presidenziale russa ha istituito a metà marzo un comitato interdipartimentale che esaminasse gli strumenti di difesa russi, al fine di stabilire cosa possa essere prodotto internamente o rifornito da Paesi "amici" (ovvero quelli che non rispettano o non applicano così rigidamente le sanzioni statunitensi) e di trovare canali non ufficiali per reperire componenti critici. Questo comitato è presieduto dal deputato del Ministero della Difesa russo Aleksey Krivoruchko, che ha decretato una serie di provvedimenti legali per raggiungere questi obiettivi. Il 17 marzo, il Ministro della Difesa russo Sergei Shoigu e il Ministro del Commercio e dell'Industria Denis Manturov hanno firmato un regolamento che velocizza le procedure di accettazione dei materiali nella produzione militare, spostando l'onere del rischio sugli appaltatori che forniscono le componenti. Il 30 marzo il Primo Ministro russo Mikhail Mishustin ha annunciato che la Russia accetterà le importazioni parallele, consentendo l'ingresso nel Paese di materiali senza l'autorizzazione di chi possiede la relativa proprietà intellettuale. In base a quanto riportato dai media occidentali, le richieste russe di equipaggiamento militare cinese hanno riguardato essenzialmente due aspetti: le munizioni e, soprattutto, i componenti microelettronici necessari per continuare a produrre armi complesse.
Inoltre, anche se rimane possibile costruire alcune componenti in Russia - a un costo maggiore e con un'affidabilità ridotta - molte componenti degli armamenti complessi russi non possono essere sostituite. Ad esempio, l'Istituto russo di Radio Ingegneria ed Elettronica dell'Accademia delle Scienze ha condotto un esame delle architetture di comunicazione dei veicoli militari russi, compreso l'aereo da trasporto Il. L'analisi della sola cabina di comunicazione di questo aereo ha rilevato 80 componenti

che non potevano essere sostituite con parti prodotte in Russia.

Infine, oltre alle sanzioni attuali, va considerato che altre potrebbero essere implementate a breve, impattando fortemente la possibilità da parte della Russia di ottenere armi prodotte in Stati alleati[20].

Come sopra indicato, il fatto che la Cina stia ricorrendo a tecniche di spionaggio informatico per ottenere informazioni sulla disponibilità di armi russe nel conflitto rimane solamente un'ipotesi. A prescindere dalla sua validità, l'obiettivo di quest'analisi è mostrare come uno Stato possa utilizzare le tecniche di cyber warfare e quanto sia complesso analizzare tali operazioni.

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

[20] https://www.australiannews.net/news/270771417/which-countries-produce-russian-weapons.

BIOGRAFIA

Francesco Schifilliti

Esperto in sicurezza delle informazioni, digital forensic e cyber threat intelligence per grandi aziende. È stato il Practice Manager di Forensic 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 e docente in corsi e master in digital forensics e malware forensics.

Cognitive Security (COGSEC)

La disinformazione è una delle questioni più critiche del nostro tempo: riguarda l'influenza online e offline su scala globale, colpendo sia i singoli individui sia le masse. Le operazioni nell'ambiente dell'informazione sono condotte nell'ambito della sicurezza cognitiva (COGSEC).
Attraverso Internet e i social media la manipolazione della nostra percezione del mondo avviene su scale di tempo, spazio e intenzionalità prima inimmaginabili: questa è la fonte di una delle più grandi vulnerabilità che dobbiamo imparare a gestire.

La COGSEC è la disciplina che si occupa dello studio dei pericoli sociologici e politici legati all'esposizione di massivi flussi di informazioni dissonanti, che possono contribuire all'aumento di atteggiamenti ostili nelle popolazioni, al declino della coesione sociale, della fiducia istituzionale, a ridurre l'efficacia della produzione della ricerca scientifica e l'affidabilità delle fonti in generale; a tale scopo studia il comportamento degli utenti e i modelli di diffusione o interazione con i contenuti ingannevoli.

Sebbene emerga dall'ingegneria sociale e dalle discussioni sull'inganno sociale nello spazio della sicurezza informatica, se ne distingue sotto diversi aspetti. La COGSEC non va confusa con la *Cognitive Cyber Security*, che invece si occupa dell'applicazione delle tecnologie e dei metodi delle scienze cognitive - tra le quali il *cognitive computing* - per la protezione dello spazio cibernetico, attraverso l'applicazione di tecnologie di Intelligenza Artificiale modellate sui processi del pensiero umano al fine di rilevare le minacce alla sicurezza dei sistemi informatici.

Mentre l'attenzione della sicurezza informatica è rivolta all'influenza di pochi individui, focalizzandosi sull'inganno come mezzo per compromettere i sistemi informatici, la COGSEC si concentra sullo sfruttamento dei pregiudizi cognitivi in grandi gruppi pubblici, quindi sull'influenza sociale come fine.

LO SCENARIO GENERALE

"*L'obiettività è un mito che ci viene proposto e imposto*", affermava qualche anno fa Dmitry Konstantinovich Kiselyov, presentatore televisivo e propagandista russo, noto come "il portavoce di Putin" nonché a capo di Rossiya Segodnya, un gruppo mediatico controllato dallo Stato.

La Russia, come altri Stati-nazione, sfrutta queste vulnerabilità per la produzione e la diffusione dell'informazione, per sviluppare quella che è stata definita "guerra cognitiva".

Contenuti ingannevoli, fuorvianti, falsificati o fabbricati ad arte vengono regolarmente creati e diffusi online con l'intento di creare confusione e ampliare le divisioni politiche-sociali, o di commettere crimini.
L'elaborazione delle informazioni, con l'evolversi della tecnologia, è diventata sempre più sofisticata: abbiamo già assistito al passaggio dal predominio del testo a quello delle immagini e dei video e, negli ultimi tempi, stiamo assistendo all'arrivo di un'informazione multimediale "sintetica" grazie all'utilizzo di tecnologie come quella dei *deepfake*. Nell'ambito della COGSEC, gli attacchi basati su *deepfake* sono diventati tra le principali e più pericolose minacce da affrontare nell'attuale contesto storico e ancor più nel prossimo futuro.
Il risvolto psicologico è proprio il mancato riconoscimento tra ciò che è vero e ciò che è falso; i *deepfake* si possono definire come "*true lies*" ("bugie vere"), in grado di mettere in crisi la fiducia verso l'Altro e contestualmente aumentare la frammentarietà del Sé.

Allo stesso tempo il costo della tecnologia è in costante calo, il che consente a più attori di entrare in scena. La capacità di influenzare le menti è stata "democratizzata", poiché qualsiasi individuo o gruppo può comunicare e influenzare un gran numero di persone online (si pensi ad es. agli "*influencer*" sui social media).

L'associazione tra tecnologie della comunicazione ed elaborazione dell'informazione ci sta rendendo più connessi, più orientati ai dati e più curiosi, de-

terminando una nuova era nella storia dell'interazione umana.

Un altro aspetto chiave di questo fenomeno è la capacità di elaborazione della nostra mente attraverso queste tecnologie, che è sempre più bidirezionale. Mentre le persone ricevono informazioni allo stesso tempo trasmettono, spesso inconsapevolmente, dati: quali informazioni leggiamo, quanto tempo dedichiamo a un post, il nostro livello di interazione, tutte informazioni che permettono ad algoritmi software di identificare e descrivere gran parte della nostra personalità, abitudini, relazioni, amicizie, religione, cultura e vizi.
La guerra cognitiva non colpisce corpi fisici ma le menti esposte a queste tipologie di attacco, cercando di distruggere i nemici dall'interno verso l'esterno oltre che di costringere il nemico a fare la volontà dell'attaccante, renderlo incapace di resistere, scoraggiarlo o sviarlo dai suoi reali obiettivi.

La Guerra cognitiva odierna è in parte l'evoluzione delle operazioni psicologiche (PsyOps) della Guerra Fredda.
Come nelle attività di PsyOps "classica", si identificano tre tipologie principali di informazioni:

- **Informazioni bianche** (*White Product*): informazioni ufficiali identificabili in termini di provenienza e fonte certa (ad es. un documento pubblicato da un ente governativo su canali ufficiali);
- **Informazioni grigie** (*Gray Product*): informazioni di provenienza ambigua (ad es. un documento apparentemente ufficiale ma pubblicato da fonti non ufficiali);
- **Informazioni nere** (*Black Product*): informazioni ufficiali o che devono sembrare provenire da fonti ostili, nemiche.

Rispetto però alle operazioni di guerra psicologica che utilizzano tutte e tre le tipologie di informazioni, la guerra cognitiva utilizza quasi esclusivamente informazioni grigie, in quanto l'ambiguità permette un'estrema efficienza, mentre le informazioni di tipo bianco e nero sono troppo trasparenti e rischiose per influenzare l'opinione pubblica.
Inoltre le PsyOps raramente hanno avuto a che fare con ampie fasce di

pubblico, essendo piuttosto mirate a aspecifici target.

Se infine confrontiamo la guerra cognitiva con le altre tipologie di combattimento, non cinetiche, che utilizzano le informazioni, possiamo notare un'elevata interazione della guerra cognitiva in tutti gli ambiti operativi [1] (Tab. 1).

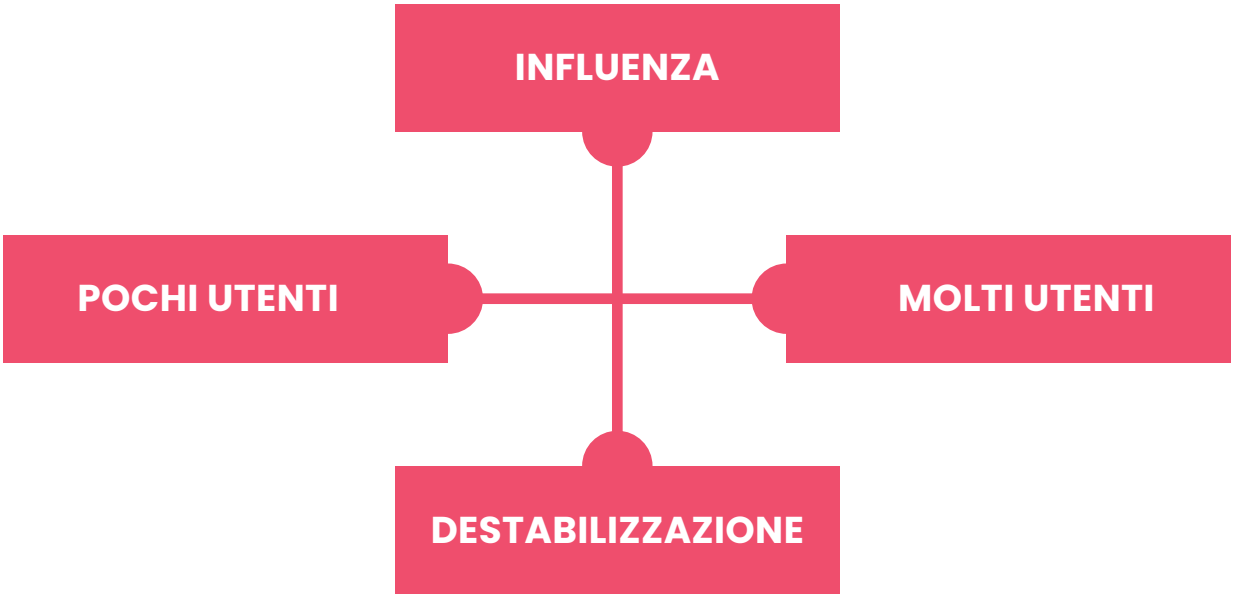
CLASSIFICAZIONE DEGLI ATTACCHI

Uno dei primi aspetti che la *Cognitive Security* deve gestire, per poter avviare strategie e tattiche di difesa, è la classificazione degli attacchi. In particolare si deve tener conto degli eventi e collocarli in specifici ambiti di

CARATTERISTICA	PSYOPS WARFARE	ELECTRONIC WARFARE	CYBER WARFARE	INFORMATION WARFARE	COGNITIVE WARFARE
Utilizzo di sistemi massivi Trend e trasmissione informazioni/dati			✓	✓	✓
Sviluppare forme di pensiero e comportamentali	✓				✓
Capacità estrema di raggiungere il pubblico target			✓		✓
Interessato alla circolazione/ascolto di informazione	✓	✓		✓	✓

Tab. 1

accadimento, in modo da disporre non solo della tipologia di evento ma anche dell'impatto in grado di generare. In Fig. 1 si riporta un grafico formato da una coppia di assi in base ai quali gli attacchi possono essere classificati.



Tab. 1

Il primo obiettivo di una guerra cognitiva è destabilizzare le popolazioni bersaglio. La destabilizzazione avviene interrompendo il corretto funzionamento dell'organizzazione del governo del Paese, ad es. rimarcando preesistenti divisioni all'interno di gruppi nella popolazione, delegittimando il governo o la *leadership* politica, rallentando la produttività chiave della nazione, confondendo una popolazione su cosa sia giusto e di chi possa fidarsi, facendola così concentrare sui problemi interni anziché su obiettivi comuni/esteri.

Il secondo obiettivo fondamentale è influenzare le popolazioni bersaglio, manipolando l'interpretazione e la comprensione di fatti ed eventi al fine di guidare le azioni del bersaglio nel

modo desiderato dall'autore dell'attacco. L'obiettivo di influenzare è diverso dall'obiettivo di destabilizzare: l'intento finale, in questo caso, è che un target abbia la stessa mentalità e opinione su un determinato pensiero, fatto o evento. Non esistono limiti a questa capacità di influenza: gli attaccanti possono spingersi fino al cambiamento radicale di pensiero di una popolazione, o di parte di essa, anche verso idee radicate e fondamentali con cui è cresciuta.
Per raggiungere un pubblico più vasto l'attaccante può utilizzare come vettori personaggi famosi, politici o accademici, promuovendo ideologie estremiste, dissenso, delegittimando elezioni, governi, etc.

Se la guerra cognitiva, nella sua attuale forma, è già di per sé pericolosa, nel prossimo futuro le sue capacità offensive saranno sempre maggiori e il suo potenziale crescerà in maniera esponenziale con le tecnologie; si pensi ad es. alla guerra cognitiva nel metaverso, sublimazione virtuale del pensiero e della vita reale delle persone.
Altre discipline - come la psicologia, la sociologia e le neuroscienze - sono agli albori di fronte a questa nuova problematica da comprendere e gestire. La velocità della tecnologia e la sua rapida evoluzione applicativa dimostrano capacità di adattamento e mutazione estremamente rapide. La massiccia presenza di dati comportamentali resi disponibili dall'avvento dei social media ha consentito ai ricercatori di fare progressi significativi nella comprensione delle dinamiche delle grandi masse di popolazione online.
Tuttavia, man mano che gli scienziati approfondiscono la conoscenza dell'evoluzione umana nelle sue interazioni, comportamenti e capacità di pensiero, paradossalmente diventiamo sempre più vulnerabili a coloro che cercano di sfruttare queste intuizioni e conoscenze per sviluppare nuove azioni di attacco.

Una delle maggiori differenze tra la guerra cognitiva e le altre forme di guerra non cinetica è che, mentre gli altri attacchi richiedono un'azione pro-attiva verso un nemico (pensiamo a un attacco cyber di tipo DDOS oppure all'invio di un'email di *phishing*), la guerra cognitiva può elaborare attacchi in cui le vittime si imbattono anche

casualmente nelle minacce, ad es. tramite innocui post o tweet casuali, che attirano l'utente spingendolo a cercare attivamente informazioni che affermano le convinzioni che si vogliono trasmettere, in maniera molto simile alle tecniche di marketing *push* e *pull*. Con l'avvento dell'Intelligenza Artificiale vengono utilizzati algoritmi in grado di catturare la nostra attenzione e guidarci verso l'obiettivo desiderato dal nemico, che è in grado di creare narrazioni e storie utilizzando i dati forniti dagli stessi utenti a loro insaputa.

COGNITIVE SECURITY VS CYBER CRIME

La natura sempre più organizzata e "professionale" del crimine informatico vede la *cognitive security* in prima linea nel contrasto agli attacchi cognitivi dei cyber criminali.

Da sempre il raggiro e l'inganno sono alla base di truffe e reati economici nel cyber spazio; negli ultimi anni l'utilizzo avanzato della disinformazione ne ha aumentato esponenzialmente l'impatto.

Il *Framing Bias*, che sfrutta i *bias* cognitivi (meccanismi spesso inconsci della mente umana, attraverso i quali creiamo distorsioni nelle valutazioni di fatti e avvenimenti), è uno dei vettori più comunemente sfruttati ad es. nelle truffe BEC (*Business Email Compromise*). Esso si riscontra laddove un individuo prende una decisione a causa del modo in cui le informazioni vengono presentate, piuttosto che esaminare i fatti o attenersi a procedure e processi noti: ad esempio la pressione psicologica di ricevere un'email dall'amministratore della propria azienda, nella quale si viene esortati a svolgere un "compito urgente", a causa della paura di disattendere la richiesta ed eventualmente ricevere una nota di demerito o addirittura il licenziamento, potrebbe sostituire il pensiero analitico e by-passare i processi di sicurezza di gestione dei flussi aziendali.

La *Cognitive Security* deve così sviluppare difese per attacchi basati anche su strumenti legati alla psicologia e alle neuroscienze. È necessario comprendere i pregiudizi cognitivi e utilizzare la consapevolezza della sicurezza per

coltivare una cultura della fiducia: non lasciare che i preconcetti - o quello che si vorrebbe accadesse - offuschino il giudizio del momento, la riflessione e l'analisi obiettiva è la principale linea di difesa contro i cyber criminali.

Da anni si parla infatti di "*Human Firewall*", cioè degli utenti come miglior strumento di difesa. Fornire ai dipendenti di un'organizzazione la formazione continua e la conoscenza degli strumenti e degli ambienti informatici in cui sono quotidianamente "immersi" rappresenta la baseline di sicurezza primaria. Dare alle persone l'istruzione necessaria a comprendere e combattere i propri pregiudizi significa proteggere le organizzazioni, ridurre significativamente i rischi e promuovere una cultura della fiducia nei rapporti e nei processi operativi.

La diffusione della disinformazione, delle *fake news* e il fenomeno dell'illetteratismo - meglio conosciuto come analfabetismo funzionale - sono vettori di attacco cognitivi estremamente potenti, soprattutto nell'ambito digitale. Sempre più spesso si riscontrano attacchi di ingegneria sociale personalizzati che sfruttano i pregiudizi cognitivi delle vittime. Negli ultimi attacchi di s*ocial engineering* registrati e nello specifico nel *phishing* (mirati a rubare credenziali, esfiltrare dati, installare *ransomware* etc.) si nota appunto un'elevata personalizzazione e qualità del vettore di attacco cognitivo, di solito tesa a sfruttare specifici *bias* fondati su alcune "scorciatoie mentali" che gli esseri umani eseguono inconsciamente quando interpretano le informazioni: semplificare l'elaborazione delle informazioni per accelerare il processo decisionale. I criminali informatici manipolano i pensieri e le azioni di un destinatario per convincere quella persona ad avere comportamenti rischiosi, come ad esempio fare click su un link che in condizioni normali non aprirebbero, o inserire informazioni riservate su un sito Web per velocizzare una "pressante" richiesta da parte di un superiore.

Un aspetto interessante da evidenziare negli attacchi cognitivi è che nella maggior parte dei casi è proprio l'utente che li innesca: quindi, sebbene siano sempre più disponibili sul mercato

tecnologie (soprattutto basate sull'A.I.) per individuare attacchi cognitivi, attualmente l'unica difesa che la cognitive security può adottare efficacemente per questo tipo di attacco è la formazione continua, fino al "*nagging*" degli utenti.

Va infine evidenziato che la formazione alla sicurezza su questa tipologia di minacce deve essere specifica: i tradizionali programmi di formazione, infatti, raramente tengono conto del ruolo svolto dai pregiudizi cognitivi in queste situazioni e, soprattutto, in genere non considerano i ruoli delle persone e il loro comportamento passato. Un recente studio[1] commissionato da Elevate Security sui tradizionali corsi di sensibilizzazione ai rischi informatici ha addirittura evidenziato come, se sulla tematica specifica si svolgono quasi esclusivamente attività di *phishing simulator*, all'aumentare delle simulazioni e delle mere verifiche la formazione possa addirittura risultare controproducente, facendo sì che le persone facciano click sui collegamenti malevoli più spesso rispetto a persone con poca o nessuna formazione.

LA COGNITIVE SECURITY E IL CICLO DELL'INTELLIGENCE

Tra tutte le metodologie di difesa in ambito cyber la *Cognitive Security* è sicuramente la più affine all'utilizzo del trattamento delle informazioni attraverso il cosiddetto "ciclo dell'*intelligence*", un processo di analisi in varie fasi finalizzato a rappresentare e trasformare i dati "grezzi" raccolti in un contesto analitico e/o scenario con possibili svolgimenti e accadimenti.

Le principali macro-fasi del ciclo dell'intelligence sono:

- **Pianificazione** – rappresenta l'indice dell'intera attività: obiettivi dell'analisi, identificazione dei dati necessari, metodologie e strumenti di raccolta, risorse da impiegare per l'analisi, consumatore finale dell'elaborazione. È di fatto un aspetto che riguarda l'i-

[1] https://elevatesecurity.com/resource/cyentia-elevating-human-attack-surface-management.

nizio e la fine del ciclo: l'inizio perché comporta l'elaborazione di specifici requisiti di raccolta e la fine perché l'intelligenza finita, l'elaborato che supporta le decisioni, può generare a sua volta nuovi requisiti.

- **Raccolta** – indica appunto la raccolta delle informazioni grezze (OSINT, CLOSINT ecc.) necessarie per produrre l'elaborato finale.
- **Elaborazione** – racchiude le attività di scrematura, riduzione e conversione della grande quantità di informazioni raccolte in moduli di base utilizzabili dagli analisti.
- **Analisi e produzione** – converte le informazioni di base elaborate in informazioni complete realizzate attraverso l'integrazione, la valutazione e l'analisi di tutti i dati disponibili.
- **Diffusione** – l'ultimo passaggio, che può ri-alimentare il primo, è la distribuzione dell'intelligence finita ai consumatori finali, ovvero i decisori i cui bisogni hanno reso l'analisi necessaria.

La *Cognitive Security* opera attraverso queste fasi: la sua policy d'azione viene implementata sulla **pianificazione** delle necessità di sicurezza dell'organizzazione, è in grado di acquisire e **raccogliere** informazioni potenzialmente pericolose, **elabora** queste informazioni sulla base delle vulnerabilità note e le minacce individuate, **analizza e produce** regole e processi di sicurezza per la difesa, **diffondendo** e mettendo a disposizione dell'utente finale la conoscenza e gli strumenti necessari per poter prendere una decisione: ad esempio, banalmente, se cliccare o meno su un link.

Negli ultimi anni si sta sviluppando, all'interno del modello di *Cognitive Security*, un ulteriore modulo di contro-*intelligence*, cioè un processo pro-attivo rivolto al contrasto dello spionaggio, della criminalità organizzata e del terrorismo in ambito cyber: un processo di raccolta e analisi dei dati basato sulla *deception technology*. Utilizzando questa tecnologia si cerca di attirare la potenziale minaccia in un ambiente artefatto, simile a un ambiente reale, dove poter studiare i vettori di attacco, stimolare l'agente ostile a esporsi ed eventualmente testare il potenziale di minaccia senza provocare alcun danno

reale. I risultati vanno a integrare gli altri dati acquisiti nella fase di **raccolta**. Inoltre questo modulo, attirando gli agenti ostili in mondi artefatti e controllati, ne rallenta le attività sui target reali, impegnandone le risorse su obiettivi fittizi e a volte riuscendo addirittura ad annullare un attacco.

IMPLEMENTAZIONE DELLA COGNITIVE SECURITY

Di fatto la COGSEC è quindi l'insieme delle tecniche e delle metodologie di difesa dagli attacchi di ingegneria sociale, dalle manipolazioni - intenzionali e non - della cognizione e capacità sensoriale degli utenti. Tecniche e tecnologie di sicurezza cognitiva mirano a rafforzare gli individui e le popolazioni contro queste influenze nocive e a rendere inefficaci gli *influencer* dannosi.

Tentare di influenzare il pubblico non è certo una novità. Politici, *lobbies*, *leader* di mercato e altri soggetti hanno da sempre usato retorica, propaganda e messaggi per manipolare l'opinione pubblica. Ciò che è nuovo sono gli strumenti oggi a loro disposizione: la capacità di diffusione e la trasmissione h24 di notizie consentono flussi costanti di informazioni, che a loro volta rendono più facile che mai influenzare la mente umana.

Le democrazie occidentali risultano più esposte a questo tipo di attacchi; grazie infatti alla libertà di informazione gli attacchi cognitivi vengono effettuati più facilmente, a differenza di quanto avviene in Stati autoritari (come Cina, Russia e, molto più drasticamente, Corea del Nord) in cui si applicano restrizioni, divieti e censura generale nei confronti di Internet e delle piattaforme social. Inoltre le democrazie occidentali sono carenti nella loro comprensione della guerra cognitiva e, spesso, anche meno preparate ad affrontare tale minaccia in rapida evoluzione.

In termini generali, sviluppare una difesa basata sulla sicurezza cognitiva prevede tre elementi fondamentali:

1. aumentare la resilienza cognitiva contro l'influenza dannosa, che include la coltivazione del pensiero critico e dell'alfabetizzazione mediatica at-

traverso l'istruzione, nonché lo sviluppo di strumenti in grado di fornire identificazione e difesa in tempo reale per le persone e le organizzazioni che incontrano sforzi di influenza sofisticati. Queste tecnologie devono funzionare sulla medesima scala e alla stessa velocità di Internet, ad esempio consentendo l'identificazione automatizzata di *deepfake* e altri media manipolati;

2. raggiungere un'ampia consapevolezza della situazione, che include il rapido rilevamento e caratterizzazione delle campagne di influenza dannosa nonché la previsione di assistenti personali virtuali che aiutino gli individui e le organizzazioni a identificare le fonti e gli obiettivi dei contenuti ingannevoli;
3. creare capacità di coinvolgimento cognitivo accurate e solide per contrastare l'influenza dannosa, come quella diffusa online da agenti o *bot* basati su software.

Contrariamente alla sicurezza informatica che enfatizza la protezione di dispositivi, computer, reti e altre macchine, la sicurezza cognitiva si concentra sulla protezione dell'essere umano: obiettivo che richiede un approccio socio-tecnico capace di integrare una serie di discipline tra cui scienze sociali/comportamentali, Intelligenza Artificiale, scienza dei dati e informatica avanzata. Questo approccio implica non solo l'integrazione olistica di strumenti, modelli e set di dati ma anche la traduzione delle esigenze di sicurezza cognitiva in problemi che possano essere affrontati in collaborazione da governi, industrie e mondo accademico. Rispondere a questa esigenza è un importante banco di prova per la sicurezza cognitiva, soprattutto in termini di sicurezza nazionale.

Per cambiare le sorti di una guerra cognitiva è necessario, quindi, lavorare a vari livelli per definire e misurare le minacce, valutare le vulnerabilità e svolgere attività di formazione volta alla mitigazione e alla risposta verso campagne di attacco cognitivo.

La sicurezza cognitiva deve poter affrontare domande chiave, quali: "Come proteggiamo le popolazioni da campagne di disinformazione e disinformazione su larga scala?", "Come misuriamo

l'efficacia delle tecniche e delle tecnologie di sicurezza cognitiva?". Affrontare le questioni etiche, legali e sociali è fondamentale per lo sviluppo di tecniche e tecnologie di sicurezza cognitiva. Le linee di difesa della sicurezza cognitiva devono fornire la ragionevole certezza che eventi, fatti e pensieri delle persone non siano influenzati da agenti esterni con intenzioni dannose comunicate online e/o offline.

Francesco Arruzzoli, *Sr. Cyber Security Threat Intelligence Analyst*

Riferimenti

Backes, Oliver and Andrew Swab. **"Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States."** Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019.

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.

Il potenziamento della cooperazione internazionale in materia di cybercrime e prove elettroniche

INTRODUZIONE

Evento centrale del semestre di Presidenza Italiana del Consiglio d'Europa, il 13 maggio 2022 si è tenuta a Strasburgo, alla presenza del Ministro della Giustizia Marta Cartabia, la cerimonia di apertura per la firma del Secondo Protocollo Addizionale alla Convenzione di Budapest.

La Convenzione - trattato internazionale di riferimento per l'azione di autorità giudiziarie e forze dell'ordine in materia di *cybercrime* - si è quindi arricchita di ulteriori, importanti strumenti operativi per ottenere accesso a prove elettroniche in differenti giurisdizioni in modo rapido ed efficiente, anche tramite la cooperazione diretta con i *service provider* stranieri o la trasmissione di dati e informazioni in situazioni di emergenza.

Allo stesso tempo, il Secondo Protocollo garantisce un forte sistema di salvaguardie e condizioni che tutelano i diritti fondamentali degli individui eventualmente coinvolti nelle attività investigative, inclusa la protezione dei dati personali nel momento in cui questi, per esigenze investigative, debbano essere trasferiti da un Paese all'altro.

Il Protocollo è il risultato di oltre 4 anni di negoziazioni coordinate dal Consiglio d'Europa, che hanno coinvolto 75 nazioni per un totale di oltre 600 contributi. Nella stessa giornata in cui è stato dichiarato aperto, oltre 20 Paesi hanno proceduto alla sottoscrizione del Protocollo, primo tra i quali l'Italia.

Nel presente contributo è inquadrato il contesto di questo nuovo strumento legale internazionale e i suoi elementi qualificanti per una cooperazione internazionale più efficiente in materia di *cybercrime* e prove elettroniche. Viene poi analizzato un caso di studio relativo all'accesso alle informazioni di registrazione di un nome di dominio (ex WHOIS).

LA CONVENZIONE DI BUDAPEST E I PROTOCOLLI ADDIZIONALI

La Convenzione sul Cybercrime (ETS N. 185) venne aperta per la firma e la ratifica nel 2001 a Budapest. Da allora ha rappresentato il primo - e unico, ad oggi - trattato internazionale su criminalità informatica e prove elettroniche.

La Convenzione fornisce strumenti di diritto sostanziale, diritto procedurale e cooperazione giudiziaria internazionale per indirizzare il fenomeno del *cybercrime* secondo schemi operativi condivisi, con il triplice obiettivo di:

1. definire un gruppo di condotte illecite comuni da criminalizzare come reati;
2. identificare le procedure per la cooperazione tra forze dell'ordine e settore privato;
3. istituire dei meccanismi di accesso transfrontaliero a prove elettroniche da parte delle autorità giudiziarie, che preservi i diritti fondamentali delle persone e garantisca l'applicazione delle norme dello Stato di diritto.

Ad oggi sono 66 i Paesi membri della Convenzione di Budapest, mentre altri 13 si trovano all'ultimo step prima della ratifica. Secondo recenti studi, sono comunque più di 120 i Paesi che utilizzano la Convenzione come standard di riferimento per le norme di diritto sostanziale e procedurale applicate nel contesto del *cybercrime* e della prova elettronica. Numeri cresciuti sensibilmente nell'ultimo quinquennio, anche grazie all'intensa attività di *capacity building* condotta dal Consiglio d'Europa e supportata dall'Unione Europea.

Quello aperto per la firma il 12 maggio è il Secondo Protocollo Addizionale, che si aggiunge quindi al Primo, concernente la criminalizzazione di atti di razzismo e xenofobia online, redatto e aperto per la firma in parallelo con la Convenzione (nel 2001).

I Protocolli Addizionali costituiscono delle estensioni della Convenzione, con un numero di previsioni addizionali che vanno a giustapporsi agli articoli della Convenzione e che quindi non ne alterano né la sostanza, né la validità operativa. Vanno pertanto intesi come

strumenti supplementari che si aggiungono a quelli stabiliti dalla Convenzione di Budapest.

IL SECONDO PROTOCOLLO ADDIZIONALE PER IL RAFFORZAMENTO DELLA COOPERAZIONE INTERNAZIONALE IN MATERIA DI CYBERCRIME E PROVE ELETTRONICHE

Il Secondo Protocollo Addizionale prende le mosse da due considerazioni di scenario:

- in prima battuta, come riscontrato anche da studi condotti dalla Commissione Europea, le prove della quasi totalità dei crimini commessi – non solo di natura cyber, ma anche di tipo fisico – è incrementalmente prodotta e archiviata in forma elettronica, su sistemi che si trovano in giurisdizioni straniere o in località non identificabili, come avviene sempre più spesso nel caso dei sistemi cloud;
- risulta poi necessario rendere più efficiente la cooperazione internazionale tra Stati e settore privato, in particolar modo garantendo un quadro più chiaro sulla certezza del diritto per i fornitori di servizi su Internet, nel caso in cui debbano decidere se e come rispondere a richieste dirette di accesso a prove elettroniche provenienti da forze dell'ordine di altre giurisdizioni.

In considerazione di quanto sopra il Comitato della Convenzione di Budapest (T-CY), in cui siedono tutti i Paesi membri, ha avviato già nel 2015 un gruppo di studio sull'efficacia delle procedure di cooperazione internazionale previste nella Convenzione e, sulla base delle evidenze riscontrate, ha deliberato nel 2017 circa l'opportunità di non emendare la Convenzione ma di introdurre misure addizionali, avviando contestualmente le negoziazioni per il Secondo Protocollo Addizionale, conclusesi nel 2021 con il testo adottato dal Consiglio d'Europa, aperto per la firma e la ratifica nel mese di maggio 2022.

Il cuore operativo del Protocollo è costituito da un numero consistente di articoli divisi in sezioni, ciascuna delle quali

focalizzata su un ambito specifico:

- procedure per il potenziamento della collaborazione diretta con fornitori di servizio e ulteriori entità di altri Paesi, nello specifico l'acquisizione di informazioni sulla registrazione di nomi di dominio e l'accesso alle informazioni di registrazione degli utenti;
- procedure per il potenziamento della cooperazione internazionale tra autorità competenti per l'accesso a dati in altre giurisdizioni, nello specifico le condizioni di obbligatorietà a dare seguito alle richieste di perquisizione e confisca dei dati provenienti da altri Paesi nonché le procedure per la collaborazione sull'accesso ai dati in caso di emergenza;
- procedure per l'assistenza mutua tra autorità competenti in situazioni di emergenza;
- procedure per la cooperazione internazionale in assenza di un quadro di accordi internazionali tra Stati che sia applicabile, in cui sono incluse le previsioni per la raccolta di testimonianze in videoconferenza e, di fondamentale rilevanza, le norme per costituire i gruppi congiunti di investigazione (JIT - *Joint Investigation Team*) e per la conduzione delle investigazioni congiunte;
- norme per garantire la protezione dei dati personali nel corso di investigazioni transfrontaliere sul *cybercrime*, o che comunque includono l'utilizzo di prove elettroniche.

Non è negli scopi di questo articolo approfondire nel dettaglio ciascuna previsione ma, con l'obiettivo di illustrare la portata di questo nuovo strumento legislativo, si enucleeranno le caratteristiche principali di uno di essi: quello relativo all'accesso alle informazioni di registrazione dei nomi di dominio (Art. 6).

CASO DI STUDIO: LE INFORMAZIONI DI REGISTRAZIONE DEI NOMI DI DOMINIO NELLE INVESTIGAZIONI IN MATERIA DI CYBERCRIME

Il contesto operativo entro cui si collocano le previsioni dell'art. 6 del Secondo Protocollo Addizionale alla Convenzione di Budapest è quello dell'accesso, da

parte di forze dell'ordine e autorità giudiziarie, alle informazioni che permettono l'identificazione del titolare di un nome di dominio Internet.

È questa un'informazione essenziale in particolare nella fase iniziale di un'investigazione in materia di criminalità informatica, quando le prime risultanze a disposizione sono spesso relative a nomi e indirizzi di siti Internet che siano stati usati – ad esempio – per condurre un attacco informatico (e.g. uso di *botnet, phishing, ransomware*, etc.).

Al momento della registrazione del nome di dominio presso il prestatore di servizi designato, ciascun titolare è obbligato a fornire un certo numero di informazioni che includono anche dati personali, quali il nome, l'indirizzo, l'indirizzo di posta elettronica e il numero di telefono. Tali informazioni sono conservate in un archivio digitale mantenuto dal prestatore di servizi.

Fino all'entrata in vigore del Regolamento Europeo in materia di Protezione dei Dati Personali (GDPR, 25 maggio 2018), tali informazioni erano rese disponibili dai prestatori di servizi di registrazione a chiunque ne facesse richiesta attraverso un servizio gratuito denominato WHOIS. In termini investigativi i casi d'uso per tale tipo di informazione sono molteplici, come ad esempio:

- l'identificazione di un punto di contatto per uno specifico dominio;
- la raccolta di informazioni preliminari sul possessore di un dominio;
- l'identificazione di correlazioni e collegamenti con altri dominii che sono stati registrati con le stesse informazioni (e.g. lo stesso indirizzo email);
- la determinazione delle azioni di cooperazione internazionale da attivare;
- l'identificazione delle eventuali controparti da citare in giudizio;
- l'utilizzo per supportare le richieste di mandati di perquisizione;
- l'utilizzo come prova elettronica.

Tale pubblicazione su fonti aperte di dati personali, però, è stata considerata in molti Paesi in potenziale conflitto con i principi di protezione dei dati personali e per questo più volte criticata dalla comunità internazionale[1]. L'entrata in

vigore del GDPR poi, riconfermando il ruolo cardine di questi principi, ha introdotto un significativo regime sanzionatorio[2] e accentuato i requisiti relativi al consenso.

In considerazione di questi elementi, l'ICANN ha emesso delle "Specifiche Temporanee" con le quali ha sospeso, nel maggio 2018, l'obbligatorietà per i prestatori di servizi di registrazione di rendere disponibili i dati personali dei titolari dei nomi di dominio tramite fonti aperte (e pertanto della loro disponibilità tramite servizio WHOIS) e ha avviato un percorso all'interno della propria comunità *multi-stakeholder* per la definizione di una nuova policy per il trattamento di dette informazioni da parte dei soggetti legittimati al loro utilizzo (incluse forze dell'ordine e autorità giudiziarie) con le relative soluzioni tecniche e organizzative.

Ad oggi, il percorso intrapreso da ICANN non si è ancora concluso e ogni richiesta di accesso alle informazioni di registrazione di un dominio è gestita dal singolo prestatore di servizi sulla base di considerazioni di opportunità e circostanza.
L'impatto della redazione delle informazioni reperibili tramite WHOIS su forze dell'ordine e altri utenti è tutt'oggi molto rilevante, sia in termini di informazioni effettivamente disponibili e sia dei tempi necessari per evadere una singola richiesta[3].

A prescindere dagli sviluppi dell'azione di ICANN sotto il profilo procedurale e tecnico, risulta comunque evidente

[1] Si veda, ad esempio, l'opinione dell'Article 29 Working Party, *Opinion on The Use of Public Directories for Reverse or Multi-criteria Searching Services* (https://ec.europa.eu/newsroom/article29/items), già pubblicata nel 2000.

[2] L'art. 83, par. 5 del GDPR prevede che in caso di inosservanza dei principi base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 sono previste sanzioni fino 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

[1] Si veda, ad esempio, il report dell'AntiPhishing Working Group: *ICANN, GDPR, and the WHOIS: A Users Survey – Three Years Later* (https://docs.apwg.org/reports/M3AAWG_APWG_WHOIS_User_Survey_Report_2021.pdf), giugno 2021

la necessità di poter disporre di nuovi strumenti legislativi che consentano alle FDO di accedere a questo tipo di prove elettroniche (che spesso si trovano in giurisdizioni diverse da quella di appartenenza) e agli erogatori di servizi che le custodiscono di fornirle senza incorrere in violazioni della normativa vigente in materia di protezione dei dati personali.

L'ARTICOLO 6 DEL SECONDO PROTOCOLLO ADDIZIONALE ALLA CONVENZIONE DI BUDAPEST

L'art. 6 rientra nelle misure di cooperazione rafforzata introdotte dal Secondo Protocollo Addizionale e pertanto, come specificato nei principi generali (art. 5), tali procedure si applicano indipendentemente dall'esistenza o meno di un trattato di assistenza giudiziaria o di un accordo fondato su normative uniformi o reciproche fra le Parti interessate.

L'obiettivo è definire le basi legali e le procedure da adottare per la cooperazione diretta tra le autorità competenti di una Parte e un prestatore di servizi di registrazione di nomi di dominio nel territorio di un'altra Parte; e si pone in complementarità con le policy e le buone pratiche in corso di definizione nel contesto del governo di Internet.

Il primo paragrafo dell'articolo richiede a ciascuna Parte di adottare le necessarie misure per autorizzare le proprie autorità competenti a inviare una richiesta relativa a informazioni di registrazione dei nomi di dominio per identificazione o contatto del titolare.

Si noti, inoltre, che non si richiede che il fornitore di servizi sia fisicamente presente nella giurisdizione verso la quale si effettua la richiesta ma solamente che esso fornisca i propri servizi su quel territorio.

La richiesta è inviata direttamente dalle autorità competenti al fornitore di servizi, senza pertanto passare attraverso l'autorizzazione o l'intermediazione delle autorità giudiziarie della giurisdizione di destinazione. L'esecuzione della richiesta – che può includere anche un'ingiunzione, se la normativa domestica lo consente – avviene però sempre solo

su base volontaria e non viene fornito alcun meccanismo di vigilanza sulla sua applicazione.

Specularmente a quanto previsto nel primo paragrafo, nel secondo si prevede che ciascuna Parte adotti le misure necessarie per consentire ai fornitori di servizi di registrazione dei nomi di dominio presenti sul suo territorio di rispondere a richieste a norma del paragrafo 1. Tale misura non è da intendersi come impositiva di un obbligo a fornire una risposta, che altresì può essere prodotta alle "condizioni ragionevoli previste dal diritto nazionale"; inclusa, ma non limitatamente a, la normativa sulla protezione dei dati personali.

Il Secondo Protocollo Addizionale pone un forte accento sul tema delle salvaguardie e del bilanciamento necessario tra protezione dei diritti umani e libertà fondamentali, imponendo condizioni che limitano sia lo scopo di applicazione sia la quantità di dati che possono essere trasmessi, perimetrando le condizioni di applicazione del potere procedurale secondo principi di necessità e proporzionalità.

RILEVANZA DELL'ARTICOLO 6 E PROSPETTIVE DI UTILIZZO

L'art. 6 del Secondo Protocollo Addizionale alla Convenzione risponde all'esigenza pressante di predisporre strumenti efficaci di cooperazione internazionale tra autorità inquirenti e settore privato, in un contesto di rilevante utilità e attualità per le indagini informatiche.

L'esistenza di un quadro legislativo di riferimento che abiliti le autorità competenti a richiedere le informazioni di registrazione dei nomi di dominio - nello scenario attuale, in cui tali informazioni non sono più disponibili su fonti aperte - è un fattore che si prevede possa incrementare sensibilmente l'efficacia delle investigazioni e della cooperazione tra le Parti che ratificheranno il Secondo Protocollo Addizionale alla Convenzione di Budapest.

La disposizione preserva, comunque, l'elemento di volontarietà della cooperazione tra autorità competenti e fornitori di servizi in un'altra giurisdizione, così riaffermando un principio base che

questi 20 anni di vita della Convenzione hanno dimostrato in numerosissime occasioni: un'azione di contrasto realmente efficace ad un fenomeno in continua evoluzione e per sua natura cross-nazionale, come quello del cybercrime, può svilupparsi solo sulla base di una cooperazione forte e convinta tra le Parti, nonché tra autorità pubbliche ed entità private.

Matteo Lucchetti, *Direttore Operativo di Cyber 4.0, il Centro di Competenza nazionale ad alta specializzazione sulla cybersecurity*

BIOGRAFIA

Matteo Lucchetti

Matteo Lucchetti è Direttore Operativo di Cyber 4.0, il Centro di Competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e co-finanziato dal Ministero dello Sviluppo Economico. Fino ad Aprile 2021 è stato Programme Manager Cybercrime al Consiglio d'Europa, responsabile del programma Global Action on Cybercrime Extended (GLACY+), iniziativa globale di capacity building su criminalità informatica a supporto di entità governative, autorità giudiziarie e forze dell'ordine in Africa, America Latina, Asia-Pacifico. Precedentemente ha lavorato presso l'Agenzia della Commissione Europea sui Diritti Fondamentali, su temi di protezione dei dati personali nei programmi di surveillance, dopo una carriera di oltre dieci anni nel settore bancario italiano come esperto di cyber security e cybercrime. Matteo Lucchetti è membro dell'Advisory Board del Global Forum for Cyber Expertise (GFCE) e collabora con l'Unione Europea e altre organizzazioni internazionali come esperto in ambito cyber security e cybercrime.

Cybercrime-as-a-Service (CaaS). Il ruolo delle transazioni in criptovalute nel Darknet

«The potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes»

David L. Carter (1995:22)

INTRODUZIONE

Fin dal giorno della sua caduta, a causa di un furto provocato mediante una ben congegnata tecnica di ingegneria sociale (**social engineering**), l'essere umano si è trovato costantemente immerso nelle attività criminose compiute dai suoi simili e nei connessi tentativi di occultare tali attività.
Queste attività si connotano per essere il più elusive possibili, inafferrabili quanto basta, tanto da aver dato vita, spesse volte, a processi e giudizi sommari al fine di poter ristabilire l'ordine economico, politico e sociale messo costantemente in pericolo da singoli e gruppi umani.

Del resto, una scia di conseguenze dirette e indirette fa seguito a ogni atto criminoso e non stupisce che tutti i gruppi umani abbiano cercato di limitare la loro perniciosa diffusione; per non dire poi che tali atti sono all'opposto del perseguimento di uno sviluppo ottimale, il quale costituisce l'obiettivo precipuo di ogni collettività organizzata.

Ciò premesso, il processo di digitalizzazione - le cui fondamenta sono da rinvenirsi a seguito del secondo conflitto mondiale, con la messa a punto della teoria dell'informazione e dei primi modelli di computer - si è vieppiù accompagnato al correlato sviluppo

della criminalità informatica (*cybercrimes, e-crimes, electronic crimes, internet crimes, netcrimes, computer-related crimes*[1]).
A questo riguardo, già l'utilizzo di un'estesa terminologia mostra assai bene che in questo campo non vi è ancora una rigorosa concettualizzazione; ma ciò vale anche, in generale, per tutti i termini correlati alla *cybersecurity* e alla *cyber intelligence* (Paliotta 2022a).

Si comprende, del resto, come una definizione rigorosa di tale campo di studi sarebbe di vitale importanza non solo per l'investigazione scientifica del fenomeno ma anche perché piccole variazioni nella concettualizzazione del *cybercrime* potrebbero influenzarne la misurazione e lo stesso contrasto da parte delle forze dell'ordine (Carter 1995; Brenner 2004; Broadhurst 2006; Barn & Barn 2016; Phillips *et alii* 2022; Paliotta 2022b).

Uno dei principali fattori insiti nella difficoltosa stima della criminalità informatica è, difatti, proprio la mancanza di definizioni rigorose, di tassonomie e sistemi di classificazione in grado di tenere conto dell'ampia gamma dei reati informatici. A questa situazione si sta ponendo rimedio in alcuni paesi, quali gli Stati Uniti, mediante un atto legislativo *ad hoc*, il "*Better Cybercrime Act*" (Paliotta 2022b). Il problema della carente concettualizzazione è ulteriormente aggravato dalla considerazione che la legislazione in materia di *cybercrime*, nelle varie giurisdizioni statuali, non è né sistematica né uniforme; e che a tale mancanza di unità corrispondono altrettanti sforzi internazionali frammentati e non continuativi, anche se la recente firma del "*Second Additional Protocol*" della Convenzione

[1] Senza entrare in maggiori dettagli, il concetto di *computer crime* può essere distinto da quello di *computer-related crimes* in quanto il primo è connotato da un significato più ristretto rispetto al secondo termine. «*Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network*» (Gercke 2012:11).

di Budapest[2] sembra andare nell'auspicata direzione di un maggiore coordinamento fra Stati.

Il *cybercrime* si può definire, per i fini che qui interessano, come lo svolgimento di un'attività criminale in cui un artefatto digitale (hardware e software) può essere sia lo strumento utilizzato per l'attacco malevolo sia l'obiettivo dello stesso, oppure ambedue, che sia o meno collegato a Internet, escludendo al contempo i reati tradizionali che sono solo facilitati dall'uso dell'hardware. Quest'ampia definizione permette di superare diverse difficoltà terminologiche perché, ad esempio, essa non coprirebbe i crimini tradizionali come l'omicidio se, in ipotesi, l'aggressore usasse una tastiera per colpire e uccidere la propria vittima. Vi verrebbe ricompreso, invece, il caso di un agente malevolo che introducesse dispositivi USB contenenti software dannoso ai fini della distruzione, deterioramento, alterazione, danneggiamento dei dati contenuti su un computer anche quando questi non fosse collegato a un *network*.

Il primo criminale condannato per crimini elettronici sembra sia stato, nel 1981, Ian Murphy - **alias** "Captain Zap" - per aver penetrato e alterato il dispositivo orario della fatturazione dell'American Telephone & Telegraphs (AT&T) al fine di ottenere tariffe scontate durante il normale orario di attività commerciale[3].

Riguardo alla tipologia dei reati, la Convenzione sul *cybercrime*[4] distingue

[2] https://www.coe.int/en/web/cybercrime/the-budapest-convention. Il 12 maggio 2022 Austria, Belgio, Bulgaria, Cile, Colombia, Estonia, Finlandia, Islanda, Italia, Giappone, Lituania, Lussemburgo, Montenegro, Marocco, Pesi Bassi, Nord Macedonia, Portogallo, Romania, Serbia, Spagna, Svezia e Stati Uniti hanno firmato il "*Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*" (CETS No. 224). I dettagli del nuovo Trattato possono essere reperiti al seguente indirizzo: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=224. La consultazione dello stesso all'indirizzo: https://rm.coe.int/1680a49dab.

[3] https://robertherjavec.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present.

[4] Council of Europe Convention on Cybercrime (CETS No. 185): https://rm.coe.int/1680081561.

quattro diversi tipi di condotte:

1. offese contro la confidenzialità, integrità e disponibilità (CIA) di computer, dati e sistemi [art. 2, accesso illegale; art. 3, intercettazione illegale; art. 4, interferenze sui dati; art. 5, interferenze sui sistemi; art. 6, uso improprio dei dispositivi];
2. offese relative ai computer [art. 7, contraffazione dei computer; art. 8, frodi relative ai computer];
3. offese relative al contenuto [art. 9, offese relative alla pedopornografia];
4. offese relative al copyright [art. 10, offese relative alla violazione del copyright].

Senza scendere in maggiori dettagli, in questa sede si può mettere in evidenza che la deterrenza contro il *cybercrime* è una componente integrale di una strategia nazionale di *cybersecurity* e di protezione delle infrastrutture critiche, come si può evincere anche dalla recente divulgazione di quella italiana (ACN 2022)[5].

L'oggetto precipuo del *cybercrime* è un artefatto digitale e, dunque, il luogo di elezione di tali attività criminose non può che essere la rete, nella sua componente *clearnet* ma, ancor di più, in quella *darknet*.
Così come nella rete sono diffusi i negozi on-line, dove gli utenti possono vendere e comprare ciò che vogliono, sono altrettanti diffusi dei luoghi virtuali dove possono essere venduti ed offerti beni e servizi illegali. Si tratta dei cosiddetti *Black Markets*, i quali adottano funzionalità assai comuni sulla rete (quali la reputazione, che varia in base ai *feedback* rilasciati dai clienti) ma soprattutto una modalità definita "*central escrow service*" che rassicura la domanda e l'offerta che gli scambi vengono effettuati in maniera consona a quanto convenuto tra i due contraenti. A solo titolo esemplificativo, qualora un prodotto/servizio acquistato non venisse consegnato, l'acquirente può contattare il "*central escrow service*" e chiedere il blocco del pagamento al venditore.

[5] https://www.acn.gov.it/strategia-nazionale-cybersicurezza.

Cybercrime-as-a-Service (CaaS). Il ruolo delle transazioni in criptovalute nel Darknet

Anche nel caso di tali mercati, il presupposto principale si basa sulla mutua fiducia che quanto pattuito sia effettivamente consegnato e pagato; nondimeno possono verificarsi casi di truffa. In tali mercati digitali sono viepiù diffusi i servizi di messaggistica basati su tecniche crittografiche, quali Pretty Good Privacy (PGP) in modo da permettere la cifratura dei messaggi tra le parti e aumentare così il livello di sicurezza e anonimato degli stessi[6].

Una delle peculiarità del *darknet* che si vuole qui mettere in evidenza è la fornitura dei servizi e beni secondo il modello *Anything as-a-Service* (XaaS): i potenziali clienti si interfacciano con delle console web caratterizzate da un'elevata facilità di utilizzo le quali sottintendono, tuttavia, una notevole complessità dell'architettura basata su un grado di automazione interna che generalmente fornisce livelli variabili di tolleranza e resilienza ai guasti e un'alta scalabilità, ovvero la capacità di aumentare/diminuire i carichi di lavoro relativi alla fornitura di beni e servizi. I servizi XaaS permettono anche un notevole risparmio sui costi di gestione rispetto alle infrastrutture tradizionali, oltre a una *user experience* facilitata: per tali ragioni sono ampiamente presenti in quasi tutte le aree di business.

In questo testo si ipotizza che la diffusione attuale del *cybercrime*, principalmente basato sui forum e sui mercati digitali, venga spiegata almeno in parte dalla fornitura XaaS delle attività criminose; e che tali caratteristiche facilitino l'approccio al crimine informatico anche da parte di un'ampia frangia di neofiti i quali sono messi nelle migliori condizioni per poter iniziare una soddisfacente carriera in questo settore economico, emergente sia in termini di costi benefici sia di profitti realizzabili in brevissimo tempo.

Tale tendenza è da ricollegarsi a un processo crescente di servitizzazione dell'economia e di commodificazione delle minacce informatiche (*malwa-*

[6] Per un approfondimento delle vicende che hanno portato alla realizzazione del software PGP e delle motivazioni ideali dei loro fautori, cfr. Paliotta 2021.

re, ransomware, exploit) le quali trovano un mercato sempre più fiorente, atto ad accoglierle e utilizzarle su una superficie di attacco che si è estesa oramai a tutte le imprese - anche le piccole e piccolissime - e ai singoli consumatori. Si tratta, in un certo modo, di una globalizzazione e volgarizzazione delle *cyber threats*, nel senso che esse possono colpire qualsiasi segmento del corpo sociale, a cui deve necessariamente fare da contraltare, per la loro difesa, un'altrettanta diffusa *cyber awareness*[7].

Un esempio di tal genere, nonché una delle ragioni del perché non sia consigliabile condividere informazioni personali in rete, è trattato in questo stesso Quaderno, nel capitolo "*Il furto di identità e come non facilitarlo - il luogo comune "non ho nulla da nascondere"*" (D'Amore 2022).

La versione più diffusa di tale modello di affari, qui definibile come *Cybercrime-as-a-Service* (CaaS), è senz'altro quella del *Ransomware-as-a-Service* (RaaS), divenuta tristemente nota anche in Italia a seguito della crisi pandemica e dei relativi attacchi effettuati da molteplici gruppi, alcuni composte da giovanissimi cyber criminali, quali Lapsus$ Team (Paliotta & Guzzo 2022a) e Killnet Legion.

Ciò premesso, nelle pagine seguenti viene affrontato il tema di come si stia sempre più sviluppando un mercato delle attività cyber criminose che adotta vieppiù modalità commerciali, connotandosi sempre più come un vero e proprio comparto economico specializzato.

Di conseguenza, come era facile attendersi, l'emersione di tali mercati digitali sta provocando una forte reazione da parte delle forze di polizia, in uno sforzo congiunto a livello internazionale con l'obiettivo del loro contrasto e chiusura; così come mostrato nella Fig. 1, relativa

[7] Per tali ragioni si sono proposti interventi formativi già a partire dalla scuola di base e una sorta di formazione obbligatoria per tutte le imprese, in parte finanziata anche con fondi pubblici (Paliotta & Guzzo 2022b).

a uno degli ultimi casi in ordine di tempo (Hydra), che verrà qui brevemente esaminato.

in grado di assicurare al meglio l'anonimità delle transazioni economiche in rete. Si tratta ovviamente delle cripto-

Fig.1 Screenshot del sito Hydra, chiuso dalle forze dell'ordine statunitensi e di altri Paesi. Fonte: https://bit.ly/3txi7SB.

Un ulteriore aspetto preso in esame, strettamente connaturato al fenomeno oggetto di studio, è relativo alla moneta utilizzata per gli scambi su tali mercati criminali, che non può che essere quella

valute e, sempre più in questi ultimissimi anni, della *Decentralized Finance* (DeFi)[8]. Quest'ultima è una tecnologia finanziaria (*fintech*) emergente, basata su registri distribuiti sicuri simili

a quelli utilizzati dalle criptovalute. Le caratteristiche principali che ne hanno determinato il successo, anche all'interno del *darknet*, sono la mancanza di un controllo preventivo da parte delle banche e delle istituzioni finanziarie nonché la relativa sicurezza dei protocolli di scambio utilizzati, l'utilizzo di un *wallet* digitale entro cui conservare le criptovalute e la possibilità di effettuare transazioni in tempo reale sulla rete.
Nel resto dell'articolo verrà preso in esame il caso di Hydra, una piattaforma da collegarsi alla Federazione Russa: il quale servirà a illustrare, con un certo grado di dettaglio, le caratteristiche precipue di un CaaS al fine di formulare ipotesi circa i motivi della loro costante adozione presso un così ampio numero di cyber criminali.

IL RUOLO DEI MARKETPLACE: IL CASO HYDRA

Il 5 aprile 2022, il Dipartimento del Tesoro degli Stati Uniti[9] (U.S. Department of the Treasury's Office of Foreign Assets Control - OFAC) ha sanzionato il mercato darknet più grande e importante del mondo, l'Hydra Market, operante in lingua russa con 19.000 account di venditori e oltre 17 milioni di profili clienti[10], al fine di interrompere la proliferazione delle attività di criminalità informatica, vendita di droghe e altri servizi illegali disponibili attraverso il sito con sede nella Federazione Russa. All'operazione congiunta hanno collaborato il Dipartimento di Giustizia degli Stati Uniti, l'FBI, la Drug Enforcement Administration, l'IRS-CI e l'Homeland Security Investi-

[8] «*DeFi is an open and global financial system built for the internet age - an alternative to a system that's opaque, tightly controlled, and held together by decades-old infrastructure and processes. It gives you control and visibility over your money. It gives you exposure to global markets and alternatives to your local currency or banking options. DeFi products open up financial services to anyone with an internet connection and they're largely owned and maintained by their users. So far tens of billions of dollars worth of crypto has flowed through DeFi applications and it's growing every day*», https://ethereum.org/en/defi.

[9] https://home.treasury.gov/news/press-releases/jy0701.

[10] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html.

gations. L'azione statunitense è stata rafforzata dalla cooperazione internazionale con la polizia criminale federale tedesca (Bundeskriminalamt - BKA) la quale ha spento i server Hydra localizzati in Germania e sequestrato bitcoin per un valore di 25 milioni di dollari. Il fatturato della piattaforma era stato stimato in almeno 1,23 miliardi di euro nel solo 2020. In particolare, il "Bitcoin Bank Mixer" (Fig. 2), un servizio utilizzato per l'offuscamento delle transazioni digitali, aveva reso le indagini delle forze dell'ordine molto difficili, come afferma-

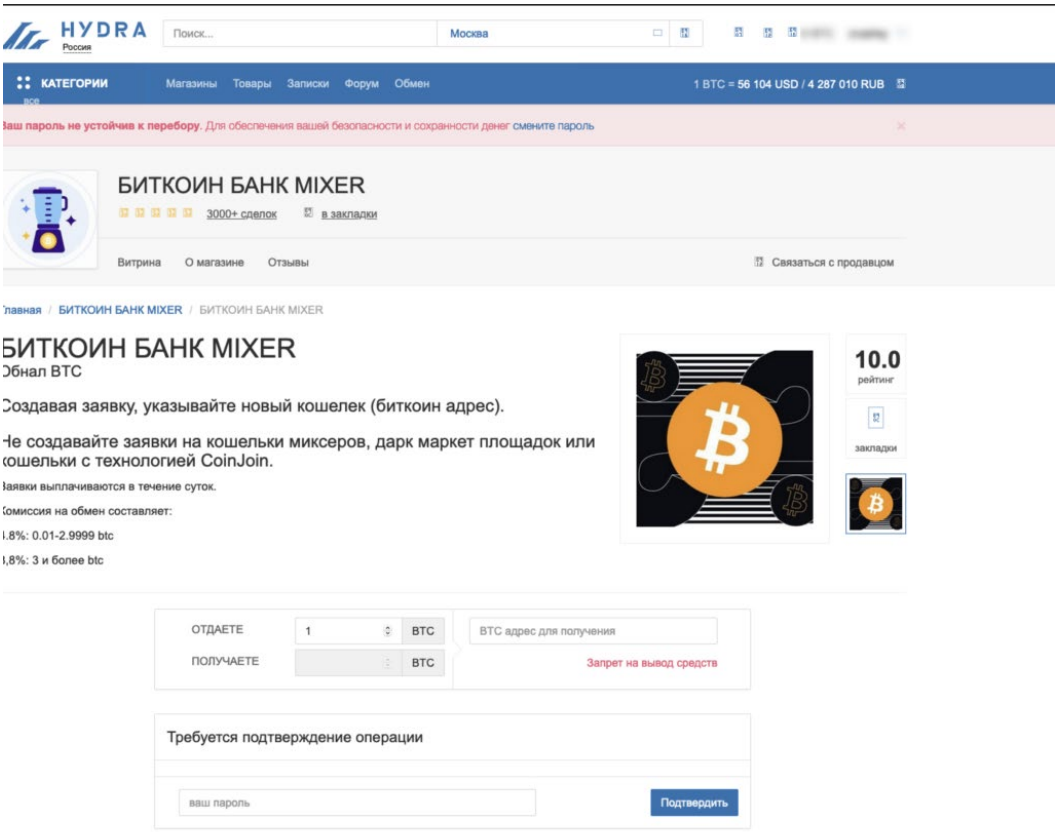


Fig.2 Screenshot di presentazione del servizio "Bitcoin Bank Mixer" su Hydra.
Fonte: https://blog.chainalysis.com/reports/hydra-garantex-ofac-sanctions-russia.

to dalla polizia stessa. La necessità di far uso di un "Bitcoin Bank Mixer" si spiega colla considerazione che, sebbene gli indirizzi bitcoin siano pseudoanonimizzati, l'intera storia finanziaria di un account viene meticolosamente registrata sulla blockchain. Le tracce create sono pubbliche e tracciabili, il che contrasta con la promessa di anonimità. I mixer o tumbler Bitcoin rispondono a questa esigenza, non sempre per motivi illegali, in quanto sono dei software o servizi che mescolano le criptovalute di diversa provenienza in modo da offuscarne completamente gli account di provenienza originali.

Nel giorno della presentazione alla stampa della chiusura di Hydra, la segretaria del Tesoro statunitense Janet L. Yellen aveva affermato che gli attori malevoli che hanno fatto uso di *ransomware* e coloro che sono coinvolti in altri crimini informatici devono essere considerati come una potenziale minaccia per gli interessi degli Stati Uniti e ciò costituisce uno dei fattori alla base della decisione di chiudere i server di Hydra. Un secondo fattore determinante è stata la volontà di interrompere l'infrastruttura finanziaria degli attori malevoli che fanno uso di *ransomware* richiedendo pagamenti in valuta virtuale a causa della loro natura anonima e dei mezzi di scambio non facilmente rintracciabili: «*Our actions send a message today to criminals that you cannot hide on the darknet or their forums, and you cannot hide in Russia or anywhere else in the world. In coordination with allies and partners, like Germany and Estonia, we will continue to disrupt these networks*»[11].

Il vice procuratore generale Lisa O. Monaco aveva dichiarato: «*The Department of Justice will not allow darknet markets and cryptocurrency to be a safe haven for money laundering and the sale of hacking tools and services. Our message should be clear: we will continue to go after darknet markets and those who exploit them. Together with our partners in Germany and around the world, we will continue our work to disrupt the*

[11] https://home.treasury.gov/news/press-releases/jy0701.

ecosystem that allows these criminal actors to operate»[12].

La lotta contro il riciclaggio di denaro da un lato e il cybercrime dall'altro, ben esemplificato dalle minacce estorsive legate al *ransomware*, sono divenute una priorità assoluta dell'Amministrazione Biden anche a seguito degli attacchi alle infrastrutture critiche, tra cui quella relativa alla Colonial Pipeline avvenuta il 7 maggio 2021 e a cui aveva fatto seguito l'*Executive Order* presidenziale del 15 aprile 2021 in tema di attività cybercriminali[13].
Anche lo «sviluppo responsabile delle risorse digitali» rappresenta una priorità delle amministrazioni d'oltreoceano, come si può evincere dall'*Executive Order* 14067 del 9 marzo 2022, "*Ensuring Responsible Development of Digital Assets*"[14] in cui si dà priorità agli sforzi per identificare e mitigare i rischi di finanziamento illecito nell'ecosistema delle risorse digitali.
Le transazioni su Hydra venivano condotte in criptovaluta e gli operatori della piattaforma addebitavano una commissione per ogni transazione. L'indagine svolta dall'OFAC ha anche evidenziato che oltre 8 milioni di dollari erano da collegarsi ai proventi del *ransomware* ed erano stati trasferiti attraverso la criptovaluta di Hydra, comprese le transazioni con i gruppi cybercriminali Ryuk, Sodinokibi e Conti, tra gli altri. Citando un rapporto di Chainalysis, l'OFAC ha riportato che circa l'86% di tutti i bitcoin illeciti ricevuti dagli scambi di valuta virtuale russi nel 2019 provenivano da Hydra[15].

Inizialmente disponibile solo attraverso la rete TOR, Hydra era nota per la ven-

[12] https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

[13] https://home.treasury.gov/system/files/126/14024.pdf.
Cfr. anche il precedente Executive Order 13757 of December 28 2016, https://home.treasury.gov/system/files/126/E.O.%2013694%2C%20as%20amended%2C.pdf.

[14] https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[15] https://home.treasury.gov/news/press-releases/jy0701.

dita di narcotici ma con il passare del tempo aveva allargato il suo raggio di azione commerciale includendovi, tra altre offerte, carte di credito rubate, documenti contraffatti (inclusi quelli di identità), banconote false e tools di attacco informatico[16]. Grazie a quest'ampia offerta di beni e servizi, anno dopo anno i volumi di transazioni annuali avevano fatto registrare un cospicuo incremento, passando da una stima di 9,4 milioni di dollari nel 2016 ad almeno 1,37 miliardi di dollari nel 2020 (Fig. 3) con un tasso di crescita del 624% nei suoi tre

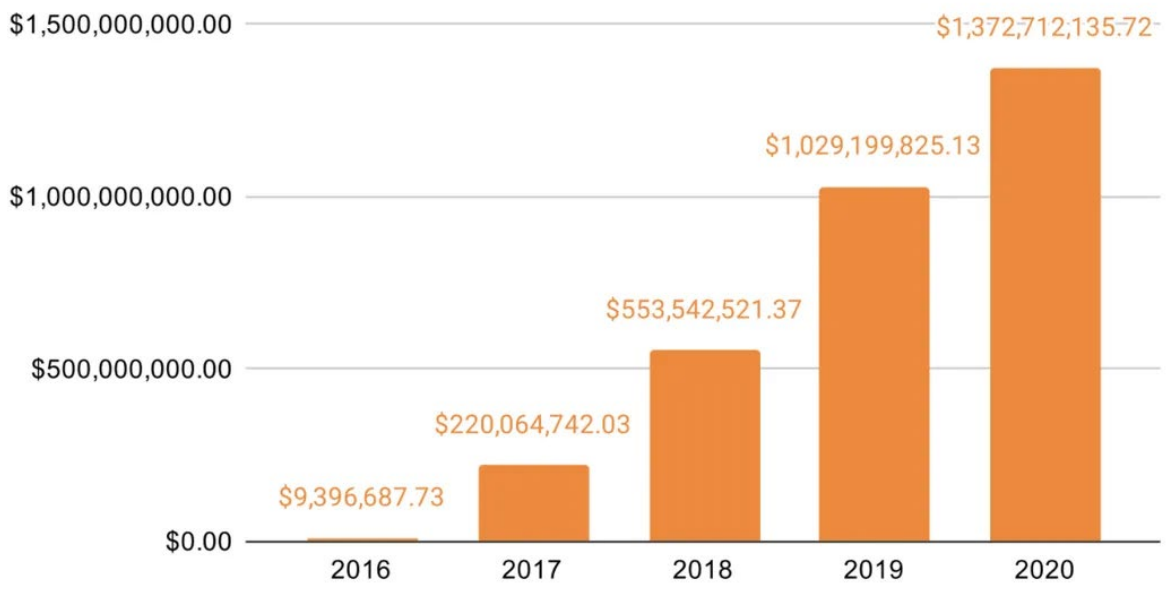


Fig.3 Volumi di transazioni annuali svolte sul darknet Hydra, dal 2016 al 2020

Fonte: https://flashpoint.io/blog/chainalysis-hydra-cryptocurrency-research.

[16]-«*Hydra's admins have learned from previous dark web drug markets and know that trust is key, so the marketplace has a sophisticated quality assurance set up. Hydra has its own team of chemists and human guinea pigs to test each product and medics on standby to give safety advice. There is a subforum where these test results are posted, complete with graphs, analysis, and photos. If the gear's not up to scratch, the administration hands out penalties. Anyone trying to pass oregano as high-grade chronic will get kicked off the site. No fentanyl is allowed, and neither are weapons, hitmen, viruses or porn, although drugs, fake passports, dodgy SIM cards, and counterfeit cash are sold*», https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web.

anni più recenti, dal 2018 al 2020[17].

In un recente rapporto (Chainalysis-Flashpoint 2021) viene messo in risalto come una caratteristica del successo di Hydra dipendesse dal richiedere ai potenziali fornitori di beni e servizi illeciti requisiti rigorosi. A partire almeno da luglio 2018, gli amministratori di Hydra (identificabili almeno in una dozzina di operatori) avevano fissato, difatti, la regola di almeno 50 vendite effettuate con successo prima che venissero consentiti i prelievi e che un account *eWallet* dovesse contenere almeno 10.000 dollari prima di poter operare sulla piattaforma.
A seguito di una transazione i venditori di Hydra, reclutati sulla piattaforma stessa (Fig. 4) distribuivano le merci

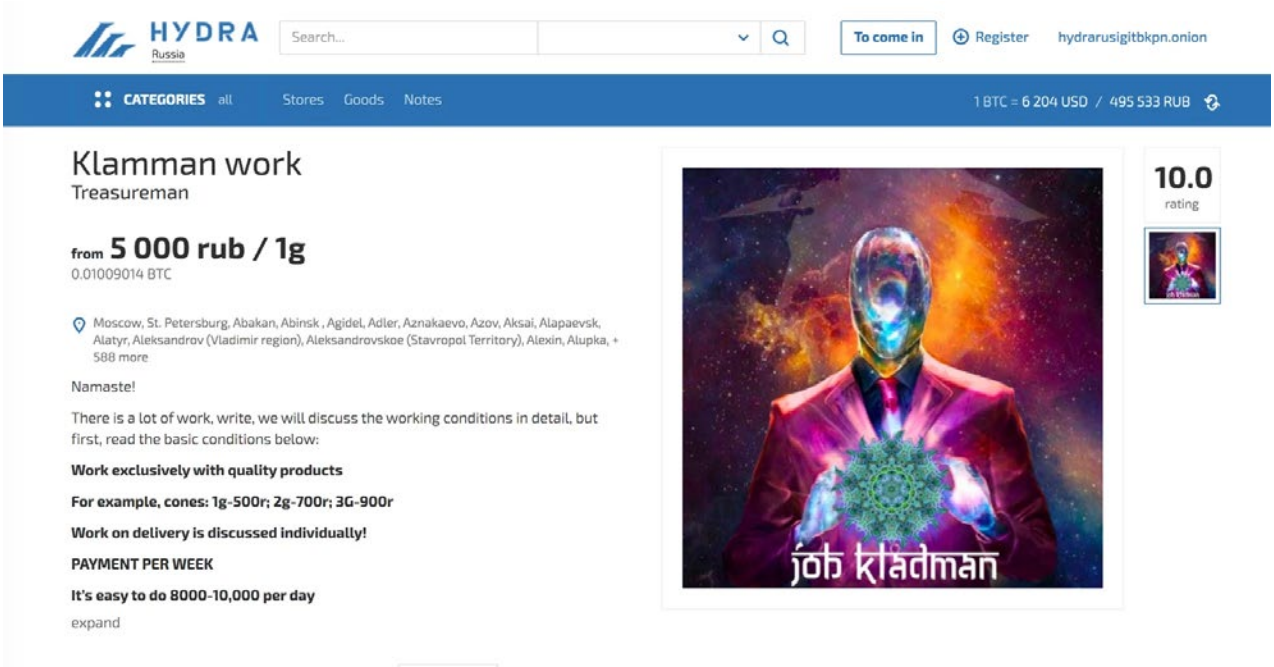


Fig.4 Messaggio pubblicato su Hydra al fine del reclutamento per lo svolgimento di un Klamman work. Fonte: https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web.

[17] https://flashpoint.io/blog/chainalysis-hydra-cryptocurrency-research.

illecite in determinati luoghi fisici, occultandoli in forma anonima, a volte sepolti o nascosti in un luogo poco appariscenti. Gli acquirenti ricevevano la posizione solo dopo l'acquisto - spesso utilizzando valuta virtuale - e potevano così recuperare la merce illecita. «*With the help of an invisible army of young couriers, Hydra is monopolising Russia's traditional street drug trade. Like a real-life videogame, the online stores on Hydra employ drug dealers known as kladmen ("treasuremen" or "droppers"), whose job is to stash drugs in GPS-tagged hiding spots ready for pick up by online buyers. It's a street-tech workaround in a country where the postal system is slow and unreliable and regular street drug dealing is highly risky. It's basically Pokémon Go for drugs*»[18].

Un'altra restrizione attuata era relativa ai principali Paesi di destinazione dei fondi in criptovalute. Le visualizzazioni dei dati geospaziali, riferiti ai flussi transazionali di Hydra, confermano queste restrizioni vedendo nella Federazione Russa di gran lunga la principale destinazione dei fondi provenienti da tutti i conti Hydra (sia acquirenti che venditori). I venditori di Hydra dovevano anche obbligatoriamente convertire i loro guadagni in rubli, la valuta fiat russa, per cui non sorprende che gli scambi siano basati esclusivamente o principalmente nella Federazione Russa e nei paesi un tempo appartenenti all'Unione sovietica (Azerbaijan, Moldova, Tajikistan, Ucraina, Kazakistan, Bielorussia, Uzbekistan, Armenia, Kyrgyzstan). Infine, Hydra conduceva gli affari in un modo rigoroso e secondo un codice di condotta supervisionato da un hub centralizzato, tanto da imporsi su tutti i concorrenti. «*While in other markets vendors pay once to open an account, on Hydra every one of its estimated 5,000 shops has to pay a monthly rent. This starts at $100 a month and rises to $1,000 a month for an enhanced account, known as a Trusted Seller, whose ads appear on the top banner. Trusted Sellers must have racked up at least 1,000 transactions and customer disputes should not exce-*

[18] https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web.

ed seven percent of the total number of orders per month»[19].
Da evidenziare, infine, che l'unico periodo di inattività degno di nota della piattaforma si era verificato durante un breve periodo di tempo, alla fine di marzo 2020, coincidente con l'inizio della pandemia di Covid-19[20].
In Fig. 5 viene mostrata una lista pubblicata su Hydra relativa un servizio di prelievo bitcoin in *cash out*. A questo riguardo, è stato frequentemente mes-

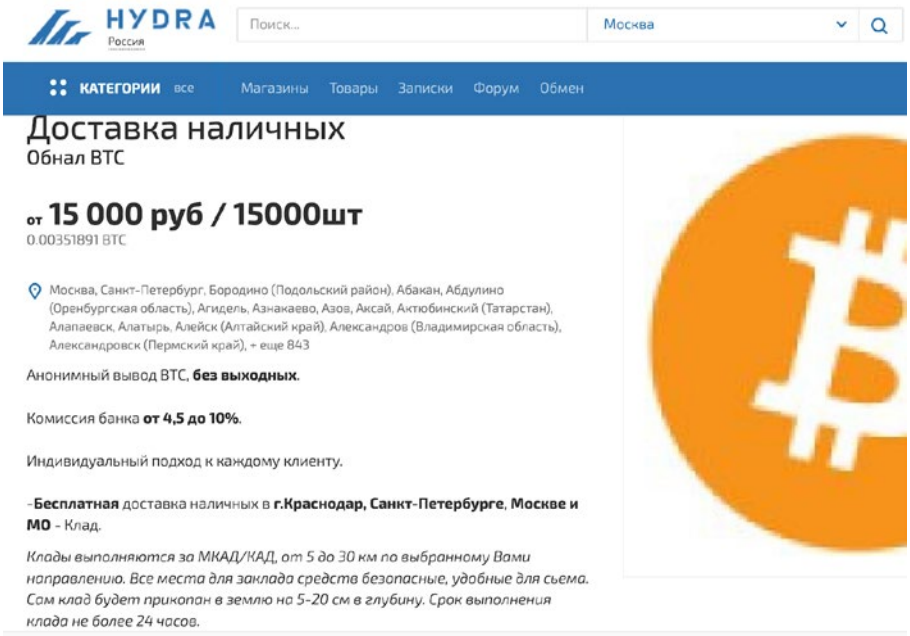


Fig.5 Una lista pubblicata su Hydra per un servizio di prelievo bitcoin in cash out.

Fonte: https://www.elliptic.co/blog/buried-treasure-criminals-to-go-to-extreme-lengths-to-cash-out-crypto.

[19] https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web.

[20] Un messaggio postato il 31 marzo 2020 conteneva la seguente affermazione: «*Dear shops. Due to the imposed restrictions in a number of areas, you need to temporarily remove your products from the online displays, to which access will be limited in the near future. Do not create additional difficulties for yourself, our customers, and the moderators. After restrictions are removed, you can put them back*» - HYDRA Administration (Flashpoint - Chainalysis 2021:4).

so in risalto il ruolo della piattaforma: «*However, to say Hydra is just a darknet market is misleading - Hydra also offers sophisticated cash-out services that are designed to let users move large volumes of illicit cryptocurrency covertly, and as such could also function as a money laundering service for sanctioned Russian entities*»[21].
Le attività illecite svolte sulla *darknet* Hydra avevano un collegamento con l'*exchange* di valute virtuali Garantex, fondato nel 2019, la cui maggioranza delle operazioni vengono svolte a Mosca e San Pietroburgo, originalmente con sede nella Repubblica d'Estonia. Nel febbraio 2022, a Garantex era stata ritirata l'autorizzazione a fornire servizi di valuta virtuale perché erano state rilevate carenze significative in materia di riciclaggio AML/CFT [*Countering the Financing of Terrorism*] oltre a diverse connessioni tra Garantex e i *wallets* utilizzati per svolgere attività criminali. Anche in questo caso un'operazione congiunta, svolta tra le forze dell'ordine statunitensi e le loro controparti estoni, ha permesso di scoprire che Garantex ha facilitato oltre 100 milioni di dollari in transazioni associate ad attori illeciti e mercati *darknet*[22]. Questa somma includeva quasi 6 milioni di dollari provenienti dal gruppo russo di *Ransomware-as-a-Service* (RaaS) Conti e altri 2,6 milioni di dollari da Hydra. A Garantex è stato applicato l'Executive Order presidenziale 14024 per aver operato nel settore dei servizi finanziari della Federazione Russa, anche a seguito delle sanzioni economiche applicate a quest'ultima per l'invasione militare dell'Ucraina e le potenziali elusioni messe in essere per aggirarle.

[21] https://blog.chainalysis.com/reports/cryptocurrency-ukraine-russia-sanctions.

[22] «*Treasury is committed to taking action against actors that, like Hydra and Garantex, willfully disregard anti-money laundering and countering the financing of terrorism (AML/CFT) obligations and allow their systems to be abused by illicit actors. Wanton disregard for regulations and compliance by persons that run virtual currency exchanges will be rigorously investigated, and where appropriate, perpetrators will be held accountable. Additionally, the United States urges the international community to effectively implement international standards on AML/CFT in the virtual currency area, particularly regarding virtual currency exchanges. The virtual currency industry has a critical role to play in implementing appropriate AML/CFT and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currencies to undermine the national security of the United States and our partners*», https://home.treasury.gov/news/press-releases/jy0701.

CONCLUSIONI

Il *darknet* si può definire come uno spazio virtuale popolato da una tipologia ben determinata di singoli e di gruppi umani intrinsecamente connessi tra loro, con una serie di attività che per loro natura si collocano entro uno spazio non regolato dalle leggi comuni. È uno spazio digitale che ha tra le sue caratteristiche precipue il ricollocamento delle tradizionali attività di carattere criminoso in un nuovo contesto digitale. È facilmente accessibile grazie alla tecnologia di anonimizzazione TOR (ma sempre più presente anche nel *clearnet*) ed è il luogo dove si svolge, a tutti gli effetti, un'economia su scala globale grazie alle moderne criptovalute, bitcoin *in primis*.

Seppur digitale, il *darknet* esiste in uno spazio sociale, economico e politico molto reale, creato da una ben determinata comunità virtuale che opera in un mondo apparentemente senza confini, che sfrutta l'anonimato ai suoi fini e riesce a colmare il divario digitale, nell'interazione socioeconomica, tra parti interessate alla compravendita di beni e servizi illeciti. È questo il caso della piattaforma Hydra, illustrata brevemente nelle pagine precedenti.

In base alla disamina di questo caso, possono essere tratte alcune considerazioni di carattere generale. Innanzitutto, il *cybercrime* stava già cambiando in modo significativo, in linea con una tendenza di accentuata digitalizzazione presente nella società intera, ma si deve evidenziare che esso ha fatto segnare uno sviluppo ancora maggiore a seguito della crisi pandemica da Covid-19 (D'Amore 2021) e dell'invasione dell'Ucraina da parte della Federazione Russa, per l'incremento delle attività malevole da parte degli attori *nation-state*. Ambedue le crisi hanno cambiato il quadro generale della società globale, soprattutto nel mondo occidentale, tanto che attualmente le statistiche mostrano che i crimini informatici hanno superato i reati "tradizionali".

Tale incremento è da mettere in stretta correlazione con un modello di servizio XaaS che qui si è definito come *Crime-as-a-Service* (CaaS). Numerosi fornitori hanno ovviamente venduto strumenti e servizi di *hacking* tramite il

darknet Hydra, per esempio. Ma su tali piattaforme è possibile anche richiedere una sorta di *hacking* "a noleggio", con servizi altamente personalizzati forniti da professionisti, quali l'accesso illegale agli account online di obiettivi ben determinati, scelti dell'acquirente. Il caso che si è qui illustrato con maggior dettaglio è quello relativo a Hydra; non solo perché esso era il più grande ed esteso al mondo ma anche perché, fino al momento della chiusura, poteva essere considerato davvero un caso di successo. Alcune caratteristiche strutturali gli avevano permesso di operare e prosperare in un ambiente fortemente competitivo come il mercato *darknet*. Come è stato sinteticamente osservato, «*Hydra opened as a less-antagonistic option to its now-defunct competitor, Russian Anonymous Marketplace (aka "RAMP"), which was notorious for eliminating its competition via DDoS attacks and operator doxxing. Following the takedown of RAMP, Hydra built networks across Russia's regions and helped to vertically integrate some aspects of drug production and trade*»[23].

Un tale modello di CaaS di successo rappresenta pertanto un caso paradigmatico: grazie alla standardizzazione e diffusione della tecnologia attuale, alla globalizzazione economica e alle recenti tendenze geopolitiche, esso sembra essere il più rispondente a una sorta di democratizzazione e volgarizzazione delle attività cyber criminali, rendendole più comuni, più lucrative, più facili da commettere e più difficili da individuare. In questo senso anche l'usuale distinzione tra la criminalità "organizzata" e quella commessa dai "colletti bianchi" va sfumando sempre più, in quanto gli stessi gruppi criminali tradizionali diventano più sofisticati e mettono a frutto i loro capitali illeciti e le loro competenze tecnologiche per ricavarsi una nicchia, altamente profittevole, nel processo di digitalizzazione attuale. Per questa ragione possiamo aspettarci dei cambiamenti nelle pratiche e nei metodi di commissione dei crimini a scopo di lucro, così come dei diversi autori di

[23] https://flashpoint.io/blog/hydra-marketplace-servers-seized-by-germany.

reati, forse provenienti da uno spettro più ampio della società. La tecnologia porterà cambiamenti anche nelle tecniche di prevenzione, individuazione e investigazione nonché in quelle di attacco, grazie alle nuove tecnologie - intelligenza artificiale *in primis* - come mostrato nel contributo "*Cognitive Security*" presente in questo stesso Quaderno (Arruzzoli 2022).

Tra tutti i servizi offerti sui mercati *darknet* quello attualmente di maggior successo, oltre alla vendita di stupefacenti, è indubbiamente il RaaS, il quale viene offerto come modello di *franchising* perché consente anche ai neofiti, anche senza competenze pregresse di programmazione (*script kiddies*), di divenire degli attaccanti attivi e prendere così parte all'economia del CaaS. Da questo punto di vista, si tratta di un processo incipiente di "democratizzazione" del crimine informatico, in grado di offrire alle persone comuni e ai *player* più piccoli una sorta di *entry level* in tale mercato riducendo, al contempo, il rischio di esposizione per coloro che si trovano in cima alla catena del valore. Ad esempio, in una tipica ipotesi di *insider threat*, un dipendente insoddisfatto potrebbe decidere di collaborare con uno sviluppatore RaaS per infettare la propria organizzazione dall'interno al fine di condividere il risultante profitto criminoso. Del resto, tale eventualità si appresta a divenire sempre più comune anche grazie a dei veri e propri spot pubblicati sui canali dei social networks, tra i quali Telegram, tanto da rappresentare un aspetto assai rilevante nel caso di alcuni gruppi, ad esempio Lapsus$ Team (Paliotta & Guzzo 2022).

In base alla breve disamina svolta in questo articolo si può infine concludere che, essendo la criminalità informatica connaturata a una dimensione internazionale, la lotta alla stessa richieda un approccio globale e uno sforzo congiunto di diverse entità statali. Le sfide giuridiche, tecniche e istituzionali poste dal *cybercrime*, difatti, sono globali e di vasta portata; e possono essere affrontate solo attraverso una strategia coerente che tenga conto, in un quadro di cooperazione internazionale del ruolo delle diverse entità e delle iniziative già esistenti.

La chiusura di Hydra, che fa seguito a quelle di simili altre piattaforme, mostra anche un aspetto di *cyber intelligence*, propedeutico a tali chiusure, svolto dalle entità statali, dalle forze dell'ordi-

ne e finanche dai *vendor* commerciali. L'attività di ricognizione delle *darknet* (seppur onerosa, non solo in termini di tempo, per la numerosità dei siti e delle conversazioni da monitorare) è senz'altro strategica dal punto di vista dei risultati che si riescono a raggiungere. Come è stato opportunamente messo in risalto, «l'*intelligence sul Dark Web può garantire l'accesso a informazioni strategiche e tattiche sulle intenzioni avverse dei cyber criminali. Ciò consente di calcolare il rischio imminente o quello potenziale ed il suo tempo di accadimento*»[24]. È chiaro che tale attività pone una serie di sfide non semplici da affrontare in quanto vi sono forti tendenze al mimetismo, all'inganno, all'utilizzo di codici di linguaggio o di peculiari espressioni linguistiche che hanno l'obiettivo di "offuscare" l'intenzionalità criminosa alla base di tali interazioni. Per ovviare a tali problematiche sono state messe a punto molteplici tecniche (a solo titolo esemplificativo, il *darknet spidering* e l'a*uthorship analysis*) le quali costituiscono le basi di una moderna *pre-reconnaissance cyber threat intelligence*. Tra le entità istituzionali esistenti in Italia è indubbio che una tale attività dovrebbe essere svolta dalla neocostituita Agenzia per la Cybersicurezza Nazionale (ACN), rafforzando le capacità di proattività della stessa in linea con la sua missione di favorire la cyber resilienza, poiché aiuterebbe l'individuazione e la classificazione delle minacce desumibili dalle interazioni delle comunità criminali del *darknet*, da condividere successivamente con i singoli *Security Operations Center* (SOC) delle infrastrutture critiche, collegate in rete in una sorta di HyperSOC.

Un ultimo aspetto riguarda, infine, il ruolo delle valute virtuali; come si è visto il metodo di pagamento preferito sui mercati *darknet*, nell'erronea convinzione che esse siano un mezzo di scambio anonimo e non tracciabile. Le tecniche adottate da Hydra avevano permesso uno scambio crescente di fondi illeciti attraverso i *wallets* associati e, nello stesso tempo, la piattaforma aveva adottato «*increasingly strict KYC [Know Your Customer*[25]*] and AML [Anti-Money*

[24] https://blog.cerbeyra.com/threat-intelligence/come-fare-intelligence-dark-web-per-difendere-azienda.

Laundering[26]*] roles on cryptocurrency exchanges by sellers offering various cashout services ranging from transfers using compromised P2P exchange accounts, to "hidden treasure" cashout, where cash is hidden at a specific location, often underground*»[27]. Del resto, i pagamenti collegati all'attività estorsiva dei *ransomware* sono spesso richiesti in valuta virtuale per simili motivi. Le chiusure delle piattaforme darknet degli ultimissimi anni mostrano, tuttavia, che lo scambio pseudoanonimo di criptovalute non è sempre etichettabile come prono al crimine: in più occasioni, i servizi illeciti che riguardavano le criptovalute si sono mostrati tracciabili all'ispezione delle forze dell'ordine e moltissimi mercati sono stati chiusi, in gran parte a causa della trasparenza intrinseca della blockchain. Tutto ciò può forse far realisticamente pensare che l'epoca d'oro del *darknet* sia giunta finalmente all'epilogo e che una larga porzione del *cybercrime* abbia perso la sua Tortuga digitale. Alcune autorità di settore sembrano esserne convinte, o almeno così sembrerebbe stando a un comunicato emesso dall'Europol a seguito dell'Operation DisrupTOR del settembre 2020: «*The golden age of dark web marketplace is over. Operations such as these highlight the capability of law enforcement to counter encryption and anonymity of dark web market places. Police no longer only takes down such illegal marketplaces - they also chase down the criminals buying and selling illegal goods through such sites. The dark web is not a fairy tale - vendors and buyers are no longer hidden in the shadow*»[28].

[25] KYC è una procedura tecnica e si riferisce principalmente alle procedure di verifica dell'identità utilizzate per garantire che i clienti siano chi dicono di essere.

[26] AML è un framework generico utilizzato per indicare un'intera serie di meccanismi implementati per proteggere dal riciclaggio di denaro e dalla criminalità finanziaria. KYC è uno dei meccanismi che ne fanno parte.

[27] https://flashpoint.io/blog/hydra-marketplace-servers-seized-by-germany.

[28] https://www.zdnet.com/article/the-dark-web-wont-hide-you-anymore-police-warn-crooks.

Effettivamente, però, si possono nutrire molti dubbi al riguardo in quanto ad una chiusura corrispondono altrettante aperture di nuove piattaforme. Si è altresì consapevoli che gli antichi mestieri del criminale e del poliziotto continueranno a esistere, seppure in modalità ampiamente digitalizzate.

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

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale (ACN) (2022), **"Strategia Nazionale di Cybersicurezza"**, Roma, ACN, pp. 32;

Arruzzoli Francesco (2022), **"Cognitive security"**, Quaderni di Cyber Intelligence n. 2, ICT Security Magazine Press;

Barn Ravinder, Balbir Barn (2016), **"An ontological representation of a taxonomy for cybercrime"**, Twenty-Fourth European Conference on Information Systems (ECIS), Istanbul (TR), pp. 15;

Brenner Susan W. (2004), **"Cybercrime Metrics. Old Wine, New Bottles?"**, Virginia Journal of Law and Technology, v. 9, n. 13, Fall, pp. 54;

Broadhurst Roderic G. (2006), **"Development in the global law enforcement of cyber-crime"**, Policing. An International Journal of Police Strategies and Management, v. 29, n. 2, pp. 408-433;

Carter David L. (1995), **"Computer Crime Categories. How Techno-Criminals Operate"**, FBI Law Enforcement Bulletin, v. 64, n. 7, July, pp. 21-26;

D'Amore Fabrizio (2021), "La cybersecurity ai tempi del Covid19: stato dell'arte e nuovi scenari di attacco", Agenda digitale", 23 luglio, https://bit.ly/3rpuAHr;

D'Amore Fabrizio (2022), "Il furto di identità e come non facilitarlo - il luogo comune "non ho nulla da nascondere"", Quaderni di Cyber Intelligence n. 2, ICT Security Magazine Press;

Flashpoint - Chainalysis (2021), "Hydra. Where The Crypto Money Laundering Trail Goes Dark. Sequencing Cryptocurrency Flows on the Russian Cybercrime Market "Hydra"", Report, pp. 16;

Gercke Marco (2012), "Understanding cybercrime. Phenomena, challenges and legal response", ITU Telecommunication Development Bureau, Geneva (CH);

Paganini Pieluigi (2021), "Ransomware: una nuova evoluzione delle pratiche estorsive", CyberSecurity 360, 14 maggio, https://bit.ly/34a6ck9;

Paliotta Achille Pierre (2021), "La crittologia moderna. Dalla società dell'informazione all'informazione quantistica", Tesi di Master SIIS discussa il 21 giugno, pp. 54;

Paliotta Achille Pierre (2022a), "Una riflessione preliminare sul processo di Istituzionalizzazione della Cyber Intelligence (CYBINT)", Quaderni di Cyber Intelligence n. 1, ICT Security Magazine Press;

Paliotta Achille Pierre (2022b), "Dagli Usa la legge "benchmark" che può essere utile anche in Italia", Il Sussidiario, 20 aprile, pp. 2, https://bit.ly/3rQOBGv;

Paliotta Achille Pierre, Antonio Guzzo (2022a), "Il modello di business della cybergang Lapsus$ Team - L'importanza della leva comunicativa e del fattore umano", ICT Security Magazine, 28 marzo, pp. 4, https://bit.ly/3Dj18Hm;

Paliotta Achille Pierre, Antonio Guzzo (2022b), "Attacchi cyber, Italia fragile: serve una nuova istruzione di base", Agenda digitale, 31 marzo, pp. 2, https://bit.ly/36EjlxQ;

Phillips Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, Mary P. Aiken (2022), "Conceptualizing Cybercrime. Definitions, Typologies and Taxonomies", Forensic Science, n. 2, pp. 379-398;

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.

Insider Threat o Minaccia Interna

«Se non vuoi far sapere il tuo segreto ad un nemico, non dirlo ad un amico»

Benjamin Franklin

Nell'analizzare il tema delle minacce interne, voglio prendere in prestito un'espressione latina: "*Nosce te ipsum*", che riprende il più antico "γνῶθι σαυτόν - *Gnothi sauthon*" greco, entrambe traducibili nell'esortazione "*conosci te stesso*". Le aziende più virtuose spendono ingenti somme per proteggere i propri perimetri dalle minacce esterne.

Ma se il pericolo fosse dentro le proprie mura?

Le organizzazioni che vogliono acquisire un'elevata postura di sicurezza devono *in primis* conoscere sé stesse, i propri limiti e le eventuali insidie interne, per contrastarle e acquisire una maturità più elevata.
Basta ad esempio andare, durante la pausa pranzo, in un ristorante nelle vicinanze di una *big company* per ascoltare le conversazioni dei lavoratori dell'impresa, acquisendo informazioni sensibili e di grande valore per i *competitor*.

La minaccia interna (o "*insider threat*") è ancora un fattore fin troppo sottovalutato: sebbene le aziende siano consce del problema, infatti, raramente gli dedicano le risorse o l'attenzione esecutiva necessaria a risolverlo.

Ma cosa si intende per *Insider Threat*?

Il termine racchiude ogni possibile minaccia proveniente da persone interne all'organizzazione: ad esempio dipendenti, ex dipendenti, appaltatori o soci in affari, che dispongono di informazioni relative ai dati, ai sistemi informatici e alle pratiche di sicurezza aziendali.
Le minacce interne presentano un rischio complesso e dinamico che colpisce i domini pubblici e privati di tutti i settori, incluse le infrastrutture critiche.

La definizione di queste minacce è un passaggio fondamentale per comprendere e stabilire un programma di mitigazione. Per esempio, gli *Insider* possono includere:

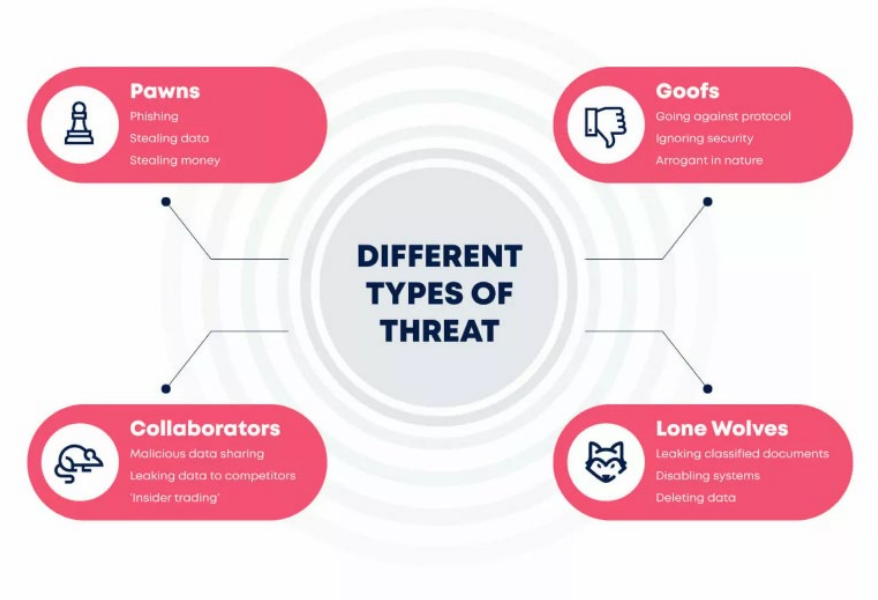
- un soggetto di cui l'organizzazione si fida, inclusi dipendenti, membri dell'organizzazione o coloro a cui la stessa abbia fornito accesso e informazioni sensibili;
- un soggetto a cui è stato assegnato un badge o altro dispositivo di accesso che lo identifica come qualcuno che effettua accessi regolari o continui;
- un soggetto a cui l'organizzazione ha fornito un computer e/o l'accesso alla rete;
- un soggetto che sviluppa i prodotti e i servizi dell'organizzazione (questo gruppo include coloro che conoscono i segreti dei prodotti che danno valore all'organizzazione);
- un soggetto che conosce i fondamenti dell'organizzazione, inclusi prezzi, costi e punti di forza e debolezza;
- un soggetto a conoscenza della strategia e degli obiettivi aziendali, a cui sono affidati i piani futuri o i mezzi per sostenere l'organizzazione;
- nell'ambito istituzionale l'insider può essere una persona avente accesso a informazioni protette che, se compromesse, potrebbero causare danni alla sicurezza nazionale o all'incolumità pubblica.

La finalità perseguita può essere il furto (di proprietà intellettuale, di informazioni riservate o di valore commerciale), il sabotaggio di sistemi informatici oppure una frode. L'utilizzo e/o la vendita di informazioni privilegiate da parte dei propri dipendenti o fornitori rappresenta tuttora uno dei problemi irrisolti in materia di sicurezza informatica.

A seconda dell'identità dell'attore e dal suo intento, l'Insider può essere ricompreso in quattro categorie[1]:

1. **Pedine** (o *Pawns*): un **dipendente o collaboratore che viene ingannato o costretto a eseguire un attacco permettendo agli aggressori l'accesso ai dati**. Spesso le pedine vengono identificate e manipolate tramite schemi di *social engineering* o *spear phishing*, progettati *ad hoc* per ottenere delle informazioni sensibili. Ad esempio, gli utenti possono scaricare inconsapevolmente un malware o fornire credenziali tramite siti contraffatti o comunicazioni ingannevoli.
2. **Personale incompetente** (o *Goofs*): alcuni *insider* sono **addetti ai lavori negligenti o che eseguono deliberatamente azioni potenzialmente dannose per l'azienda**. Solitamente questi soggetti peccano di superbia, ritenendo che le politiche di sicurezza non si applichino a loro ovvero di sapere, meglio di altri, come mantenere protetti loro stessi e i sistemi aziendali.
   Si stima che **il 95% delle aziende abbia al suo interno utenti che tentano di aggirare i controlli di sicurezza previsti**, come ad esempio la disattivazione dei blocchi popup, la sospensione dei programmi antivirus o l'archiviazione di dati sensibili in un archivio cloud non approvato.
3. **Collaboratori** (o *Collaborators*): un collaboratore è **un *insider* che sceglie di lavorare con aggressori esterni, come società concorrenti o altri Stati nazionali**. Questi utenti abusano dei propri privilegi, legittimati dalla loro posizione in azienda, per fornire informazioni e/o accesso

[1] M. Siciliano, "*Insider Threat: tipologie di cyber minacce e contromisure*" https://www.ictsecuritymagazine.com/articoli/insider-threat-tipologie-di-minacce-e-contromisure.



a terze parti, in genere in cambio di vantaggi economici o personali.

4. **Lupi solitari** (o *Lone Wolves*): un lupo solitario è **un *insider* che lavora in modo indipendente per un proprio vantaggio o scopo**. Questi utenti hanno spesso una conoscenza approfondita dell'organizzazione in cui operano e sanno come sfruttare i loro privilegi interni.

Se l'*insider threat* può recare danno all'interno di un'organizzazione privata, occorre pensare anche alle realtà considerate strategiche per il sistema Paese.

Infatti, in caso di "next level" della minaccia interna, possono configurarsi alcune gravi condotte. In particolare:

- **Spionaggio** - attività clandestina tesa a raccogliere, a vantaggio di un'altra organizzazione (o Stato) informazioni utili dal punto di vista industriale, scientifico, economico o politico.
- **Terrorismo** - intesa come minaccia interna che ha l'obiettivo di promuovere l'uso della violenza illegittima, finalizzata a incutere terrore nei membri di una collettività organizzata e a destabilizzarne l'ordine mediante azioni violente.

- **Divulgazione non autorizzata di informazioni sensibili**.
- **Corruzione** - comprende la partecipazione alla criminalità organizzata transnazionale.
- **Furto di proprietà intellettuale** - riguarda la sottrazione di segreti commerciali o prodotti proprietari.
- **Sabotaggio** - descrive azioni deliberate volte a danneggiare l'infrastruttura fisica o virtuale di un'organizzazione, inclusa la non conformità con la manutenzione o le procedure IT oppure l'eliminazione di codice per impedire operazioni regolari.
- **Violenza** - include tutti i comportamenti minacciosi che creano un ambiente intimidatorio, offensivo e ostile all'interno dell'organizzazione.
- **Perdita o degrado** (intenzionale o meno) di risorse.

Lo **spionaggio aziendale** merita un breve approfondimento a sé stante. Non c'è dubbio che sia un tema poco considerato dalla classe dirigente italiana; eppure si tratta di un problema rilevante per la salvaguardia della nostra economia nazionale.

Un paio di anni fa, il rapporto annuale al Parlamento del Dipartimento di Informazione per la Sicurezza della Repubblica (DIS) sottolineava chiaramente "*la persistente esposizione ad iniziative di spionaggio industriale, specie con modalità cyber agevolate dalla digitalizzazione pressoché integrale dei processi produttivi e più pervasive nei confronti delle piccole e medie imprese*"[2].

Purtroppo esistono moltissime realtà, sia governative sia private, che nemmeno accennano a tali problematiche nelle mappe di rischio dei propri modelli di compliance.
Per dirla in termini più semplici, nella gran parte dei casi lo spionaggio industriale è fuori dai radar di chi è deputato alla sicurezza organizzativa, ivi compreso il *top management*.

Al riguardo preme condividere alcuni spunti ritenuti particolarmente attuali,

[2] A. Vaccaro, https://www.ilsole24ore.com/art/perche-spionaggio-aziendale-continua-ad-essere-ignorato-ADjB8CX

che però richiederebbero ulteriori riflessioni e approfondimenti:

1. l'importanza – ormai consolidata – della *cybersecurity* all'interno delle organizzazioni, a tutela e protezione delle informazioni;
2. lo sviluppo della *Supply Chain Security* e la gestione dei rischi delle terze parti, ossia le attività a tutela della propria catena di fornitura (sul punto è intervenuta la recente normativa sul Perimetro di Sicurezza nazionale cibernetica a tutela degli asset strategici per il Paese);
3. l'incremento delle c.d. "*internal investigations*", strumento di origine anglosassone ormai diffuso anche in Italia, con il quale le aziende portano avanti indagini finalizzate ad accertare eventuali comportamenti illeciti commessi dai propri dipendenti a danno dell'azienda medesima.

In un sistema economico globalizzato e altamente concorrenziale, le informazioni costituiscono una risorsa fondamentale per le aziende che intendono competere efficacemente sui mercati nazionali ed esteri. Il segreto industriale, infatti, tutela tanto gli aspetti organizzativi quanto i processi e i prodotti; deve quindi essere adeguatamente implementato e salvaguardato, nel rispetto delle norme esistenti e delle *best practice* internazionali.

Per tutelare questo patrimonio informativo le organizzazioni devono investire su soggetti specializzati, con competenze verticali su tecniche investigative e di *intelligence*: dal più tradizionale HUMINT a quelle di natura più cyber, che sfruttano tecnologie di AI e ML per l'acquisizione e l'analisi dei dati.

Oggi più che mai, il *Security Manager* assume un ruolo di fondamentale importanza nell'organigramma aziendale.

I crimini informatici e le relative tecniche, utilizzate al fine di compromettere i sistemi per acquisirne i dati, sono in continua evoluzione e richiedono una formazione costantemente aggiornata.

Diventa quindi necessario, per un'azienda, poter contare su esperti in grado di controllare e garantire la sicurezza (fisica e logica) dell'organizzazione; e, soprattutto, nell'organizzazione.

Alcuni consigli su come difendersi:

- servirsi di programmi di *security* contro le minacce interne basati su monitoraggi continui dell'ambiente di sicurezza, che consentono un tempestivo rilevamento di attività pericolose;
- investire sulla formazione e sensibilizzazione dei dipendenti, tramite campagne di *awareness* sulla sicurezza delle informazioni;
- predisporre policy mirate e specifiche contromisure per le minacce interne;
- utilizzare la microsegmentazione, ossia la creazione di ambienti separati che isolano i carichi di lavoro e li proteggono tramite accessi privilegiati;
- implementare soluzioni di *Identity Access Management*.

"Nessuna tipologia di rete, firewall o software di sicurezza può far fronte a un utente che clicca su un link all'interno di una mail o che lascia gli accessi dello smartphone a qualcuno che finge di appartenere al dipartimento IT" (Australian Computer Society Report).

In altre parole: possiamo chiudere la porta di casa a chiave con tutte le mandate, ma se la minaccia è già all'interno non saremo mai veramente al sicuro.

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

BIOGRAFIA

Giuseppe Maio

Giuseppe Maio è Security Advisor in ambito Governance, Risk and Compliance (GRC) per un importante società di Consulenza strategica. Dopo aver conseguito una laurea in Giurisprudenza presso l'Università Mediterranea di Reggio Calabria, ha frequentato un master di II Livello presso l'Università LUISS Guido Carli in "Cybersecurity: Politiche Pubbliche, Normative e Gestione". Attualmente è membro della Commissione Cyber Threat Intelligence & Warfare presso la Società Italiana di Intelligence.

Il furto di identità e come non facilitarlo – il luogo comune “non ho nulla da nascondere”

In questo articolo analizzeremo cosa significhi proteggere la nostra privacy, prendendo in considerazione alcuni possibili comportamenti perpetrati da soggetti definiti, qui, semplicemente “attaccanti.” Cercheremo di capire quali dati possano costituire un rischio e come fare per non divulgarli. Inoltre guarderemo la questione “lato attaccante”, per capire cosa farà dei nostri dati e perché potrebbe essere nocivo.
Le basi tecniche cui faremo riferimento sono il *world wide web* - ipertesto consultabile attraverso un browser - e il fatto che certe pagine web non siano accessibili a chiunque ma richiedano un’autenticazione (spesso: username e password).

1 - QUALI DATI PRIVATI È POSSIBILE REPERIRE IN RETE?

Di ogni tipo: per rendercene conto, basta inserire in un moderno motore di ricerca (Google, Bing, ecc.) alcune semplici parole chiave come “carta d’identità”, “documento”, “passaporto” o “denuncia”, selezionando i risultati di tipo “immagine”. Oltre a immagini di volti, possiamo facilmente reperire nomi, indirizzi, numeri di telefono, codici fiscali… il che, in un mondo onesto, non costituirebbe un problema. Ma il mondo pullula di disonesti.
Si potrà dire: i proprietari li hanno messi in rete e nella maggioranza dei casi sapevano quello che facevano. Non sono del tutto d’accordo, soprattutto relativamente alle conseguenze indirette, di cui discuteremo.
Inoltre, la pubblicazione sul web non è l’unica sorgente di dati personali; questi possono essere condivisi in molti modi, per esempio usando una rete sociale (Instagram, Facebook, TikTok ecc.) che a sua volta si poggia sul web, con una differenza che deriva da quella esistente fra *surface web* e *deep web*.
Appartengono al *surface web* tutti i

siti che possono essere consultati da un motore di ricerca; appartengono al *deep web* (da non confondere con il *dark web*) i siti che non possono essere raggiunti da un motore di ricerca per vari motivi, uno dei quali è la necessità di sapersi autenticare. Per completezza, aggiungiamo che appartengono al *dark web* tutti i siti che offrono pagine web attraverso una "*overlay network*" (rete sovrapposta) come la rete Tor e che possono essere consultati esclusivamente tramite il Tor browser; non essendo questi raggiungibili da un normale motore di ricerca, tecnicamente appartengono al *deep web* (che naturalmente non si esaurisce nel *dark web*).

Precisata la differenza, c'è da dire che un enorme quantitativo di dati personali è affidato al *deep web* e, almeno in linea di principio, non disponibile alla visione di chiunque. Si tratta spesso di foto e video che appartengono alla sfera più privata, incluso il fatto che spesso includono volti di minori (cosa che in teoria dovrebbe essere soggetta ad autorizzazione). Dati protetti, dunque? La risposta, purtroppo, è no. Anche assumendo che i server che realizzano la rete sociale – chiamiamola S – non siano e non saranno compromessi, rimane il fatto che gli "amici" ottenuti attraverso la rete sociale possono spesso visualizzare tali informazioni.

Facciamo chiarezza. Assumiamo che S, attenta alla privacy e moderna, divida il pubblico, rispetto a un utente X, in più fasce:

A. quella con cui si condividono contenuti soggetti a selezione;
B. quella degli amici stretti con cui si condivide tutto, con qualche possibile eccezione;
C. quella degli utenti di S (inclusi i non amici di X), con si può scegliere di condividere qualcosa;
D. il resto del mondo (che include i non iscritti a S), con cui si condivide ciò che si reputa pubblico.

Anche supponendo che un utente possa configurare e caratterizzare completamente le fasce A, B, C e D, quanti saranno disposti a farlo? In molti casi prevarranno le impostazioni di *default* scelte dall'applicazione. Anche se i comportamenti di *default* saranno *privacy preserving* (non sempre è così!) è comunque compito di X definire le

eccezioni, sia in positivo che in negativo, e non è scontato che X lo faccia. Ci sono poi reti sociali in cui la privacy è, a causa dello scopo della rete, poco attuata dagli utenti (es. LinkedIn, app di *dating*).

Inoltre, poche reti sociali consentono a X di definire i permessi di visione agli “amici degli amici”. Il che si traduce nel fatto che, per quanto attenti possiamo essere nel concedere gli accessi, dipenderemo spesso dai comportamenti dei nostri contatti. Ad esempio, supponiamo di voler tenere privato il numero di cellulare, per cui lo diamo solo a pochi contatti stretti: cosa ci garantisce rispetto alla richiesta automatica di WhatsApp, Signal o Line di accedere alla rubrica? Può darsi che gli amici stretti consegneranno a queste app la loro rubrica, per non parlare del fatto che potrebbero decidere di dare il nostro numero a qualcuno senza consultarci in proposito.

Dal lato dell’attaccante, è possibile reperire dati sia attraverso un motore di ricerca, sia diventando utente di una rete sociale e ottenendone dati che diventano così accessibili: questo può essere fatto sia di persona, sia usando una specifica applicazione. Una delle tecniche più antiche, ma ancora attuali, è prendere contatto con un uomo attraverso un profilo social che mostra la foto di una donna avvenente: pochi sapranno resistere alla tentazione di accogliere una nuova amica attraente.

2 - COME SONO CEDUTI I DATI?

In realtà ciò è stato discusso nella Sez. 1. Tuttavia, non abbiamo ancora menzionato un fatto centrale e ricorrente. Siamo tutti utenti del web, a prescindere dalle reti sociali: e i siti web vorrebbero sapere alcune informazioni di base sugli utenti, per migliorare gli avvisi pubblicitari da mostrare (ad esempio, appare un po’ goffo mostrare a un uomo avvisi destinati a un pubblico femminile). Ecco che nascono alcune domande di base, quali sesso, fascia di età, malattie croniche, vizi, bisogno di credito/mutui, composizione del nucleo familiare ecc. Tutto – o quasi – è considerato lecito al fine di acquisire queste informazioni, che nella maggior parte dei casi saranno trattate in maniera automatica.

Un meccanismo di base che spicca fra gli altri è quello dei cookies. Come noto, il protocollo per l'acquisizione dei file che caratterizzano il contenuto di un sito è http, un protocollo *stateless* (senza memoria). Per ovviare a tale limite (talvolta tecnicamente rilevante) è stato introdotto il meccanismo dei *cookies*:

- un server web, nel trasmettere informazioni a un browser, può decidere autonomamente di inviare dei frammenti di informazione (spesso dei numeri) chiamati appunto cookies. Ovviamente il server conterrà una tabella che associa a ciascun numero varie informazioni;
- il browser riceve i *cookies* e, se non espressamente istruito a fare diversamente, li conserva fino a una data di scadenza (spesso più lontana della data media di dismissione del dispositivo). Il *cookie* spesso descrive la pagina di attuale visualizzazione;
- il browser, nel mandare una richiesta qualunque a un server web, controlla se conservi *cookies* non scaduti provenienti da quel server e, se sì, li invia al server assieme alla richiesta;
- lo scambio di *cookies* fra server e browser avviene di norma silenziosamente, senza che l'utente ne abbia percezione. Il numero di cookies ricevuto da un browser in un giorno di navigazione può facilmente raggiungere diverse migliaia;
- ogni browser possiede un "contenitore" in cui depositare e da cui attingere *cookies*;
- tale contenitore è diverso da browser a browser e da utente ad utente (anche se condividono lo stesso dispositivo).

Inoltre occorre tenere presente che, se si visita il sito W, questo offrirà presumibilmente contenuti provenienti da altri siti, diciamo Y e Z. Per tale ragione W si chiama "*first party*" (prima parte) e Y e Z si chiamano "*third parties*" (terze parti). Non è difficile comprendere che i *cookies* ricevuti da siti di terze parti servono principalmente a queste ultime per ricostruire informazioni sull'attività di navigazione di un utente e, in particolare, sui contenuti consultati. Invece i *cookies* di prima parte hanno spesso una valenza tecnica, conservando informazioni su un'avvenuta autenticazione e su una preferenza di navigazione. In definitiva, è consigliabile l'approccio ba-

sato sul configurare il browser in modo che rifiuti automaticamente i *cookies* di terze parti (è possibile, anche se talvolta va cercato[1]). Il meccanismo che contempla pagine composte da contenuti provenienti da diversi siti fa sì che nascano relazioni fra siti, che possono portare alla condivisione di informazioni. La Figura 1 mostra le relazioni fra siti visitati in quasi un anno da parte dell’autore; in Figura 2 ne è mostrato un frammento. Oggi sono molti gli *add-on* (componenti aggiuntivi) disponibili per dotare un browser di una migliore capacità di controllo dei *cookies*; non approfondiremo questo dettaglio, privilegiando i concetti di base. Inoltre ci sono molti browser, ciascuno con una sensibilità diversa rispetto alla tutela della riservatezza dei dati degli utenti. Fra questi

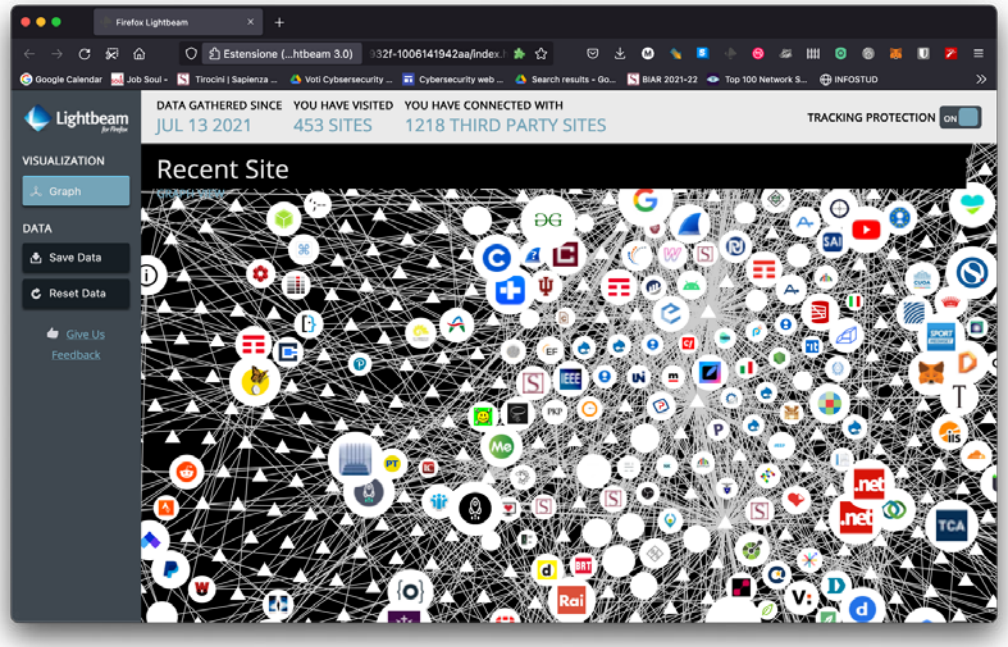


Figura 1. Illustrazione fornita dall’add-on LightBeam per la visualizzazione delle relazioni fra siti web visitati.

[1] Appare più difficile sui dispositivi mobili.

prevale, ai fini del controllo della privacy, quello prodotto da Mozilla[2] e noto con il nome di Firefox[3]. I web server usano anche altri meccanismi di tracciamento, talvolta molto più tecnici, che giustificano il ricorso alla modalità di navigazione chiamata *privata* o *anonima*.
Si tratta di una modalità nata nel passato per obiettivi differenti, che oggi offre ancora alcuni aspetti interessanti. La modalità privata non lo è davvero (il server web riceve ugualmente il nostro IP), tuttavia in questa modalità i browser allestiscono un nuovo contenitore per i *cookies* (e per altre informazioni) che nasce vuoto e durante la naviga-

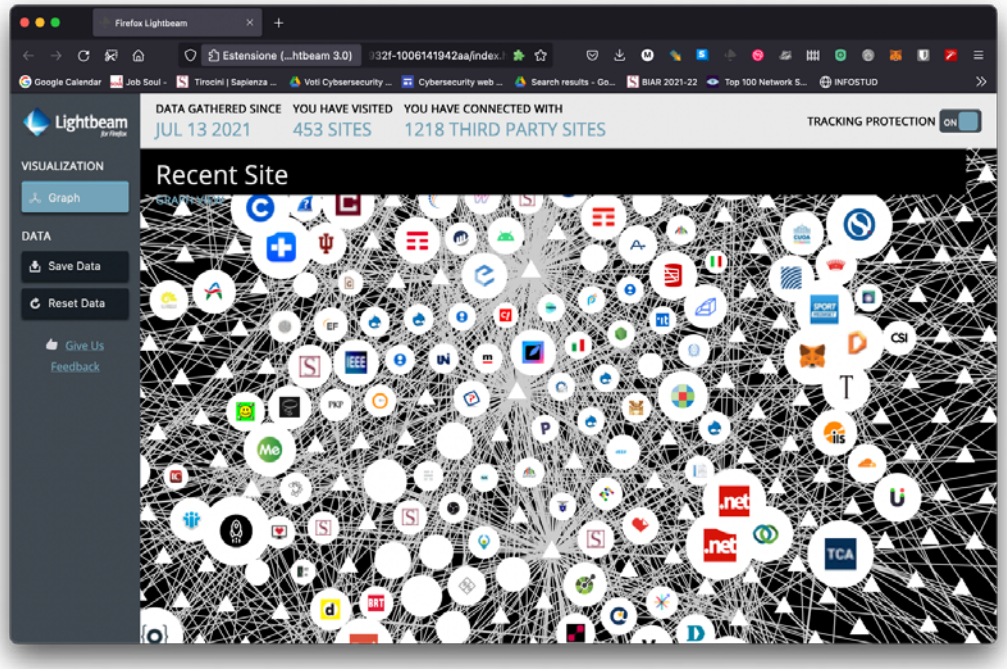


Figura 2. Dettaglio frammento di LightBeam.

[2] https://www.mozilla.org/it.

[3] https://www.mozilla.org/it/firefox/new.

zione riceve tutti i *cookies* somministrati, anche fornendoli, ma che viene distrutto alla chiusura del browser, perdendo automaticamente tutti i dati collezionati. In questo modo renderà vana la somministrazione di *cookies* di qualunque tipo, inclusi quelli "buoni" (es., autenticazione avvenuta).

3 - QUALE CESSIONE DATI È DA CONSIDERARSI RISCHIOSA E PERCHÉ?

Dalle riflessioni precedenti capiamo facilmente la molteplicità dei meccanismi che consentono all'attaccante di collezionare i nostri dati. A questi vanno aggiunti quelli di esfiltrazione, che attaccano un server per estrarne i dati contenuti: in particolare, le password. In effetti il riuso delle password, pratica prediletta da molti utenti, favorisce fortemente il furto d'identità, in cui l'attaccante può impersonare la vittima e agire passivamente o attivamente in sua vece. Esistono varie tipologie di furto di identità; ed è abbastanza pacifico che sebbene i meccanismi lesivi della privacy discussi in Sez. 2 possano essere fastidiosi, condizionando la pubblicità ricevuta, di norma non conducono a furti di identità. Tuttavia, ci sono stati casi emblematici in cui giganti del web sono incorsi in famosi scandali unendo tecniche disparate: ad esempio il caso Facebook-Cambridge Analytica[4], ove i dati di 87 milioni di utenti FB furono usati con scopi di propaganda politica.

In effetti sembrerebbe naturale domandarsi se i meccanismi illustrati in Sez. 2 non potrebbero essere sfruttati dalle forze dell'ordine a fini investigativi, o trovare addirittura applicazioni forensi. Se da un lato appare scontato che la disponibilità dei dati presso i siti che effettuano tracciamento costituisca un patrimonio di indubbio interesse che potrebbe facilitare analisi, profilazione psicologica, valutazioni ecc., dall'altro dobbiamo prendere atto che il concetto di confine nazionale, per quanto riguarda la rete, ha perso ogni significato. Così assistiamo ad aziende od organizzazioni che si trovano in uno Stato, ma che con-

[4] Si veda, ad es., https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

servano i dati su qualche server localizzato in altro Stato. Ne deriva la difficoltà, per le forze dell'ordine, di ottenere tali dati, rendendosi in genere necessarie rogatorie internazionali dai tempi lunghi (poco compatibili con quelli dell'investigazione) e dagli esiti incerti. Questo perché manca una legislazione comune di valenza internazionale, anche se la UE ha recentemente fatto significativi passi avanti in tal senso. Eppure, la magistratura dello Stato ove risiedano i dati potrebbe ordinarne sequestro ed esportazione, chiarendo che in caso di cifratura c'è l'obbligo di fornirne le chiavi.

Più significativa per i nostri scopi è invece la valenza degli atti descritti in Sez. 1, nonché dell'esfiltrazione della password.

Va premesso che in generale esistono due tipi di attacco informatico: "a pioggia" e "mirato". Nei primi si è attaccati per il semplice fatto di essere utenti di Internet; nei secondi invece l'attacco è legato al nostro ruolo, status o funzione e integra un'azione espressamente studiata per noi. Va detto che il rapporto fra questi è dell'ordine di 100 a 1: ne consegue che la somma dei danni provocati dagli attacchi a pioggia diventa considerevole sul piano quantitativo mentre, nel caso degli attacchi mirati, questi possono produrre danni ingenti in ragione della loro maggiore "qualità".

In aggiunta, gli attacchi mirati sono molto onerosi - non molti possono permettersi i costi necessari alla progettazione - e pertanto sono solitamente imputabili a gruppi motivati e ben organizzati, talvolta anche a governi nazionali. Qui ci concentreremo solamente sugli attacchi a pioggia poiché, nella situazione evocata dal titolo, le vittime sono persone "qualsiasi" che ritengono di non aver nulla da nascondere.

Mettiamoci nei panni di un attaccante che dedica tempo e sforzi per realizzare attacchi a pioggia (usando i meccanismi descritti in Sez. 1), eventualmente resi più efficaci da password o dati esfiltrati in seguito a qualche attacco a server[5]. L'attaccante colleziona dunque dati ottenuti con questi meccanismi, correlando le varie informazioni relative allo stesso soggetto: in Figura 3, l'esito di una semplice ricerca su un celebre social. Nel tempo, i dati correlati attribuiti a

uno stesso soggetto diventano corposi: quello è il momento maturo per venderli e, a tale scopo, cosa c’è di meglio di un mercato nero raggiungibile nel *dark web*[6]?

Dunque assistiamo alla messa in vendita di nomi, indirizzi, foto, e-mail ecc. relativi a uno stesso soggetto; e questo viene fatto per moltissimi soggetti. Esaminiamo, a seguire, i due principali tipi di abusi che i legittimi proprietari dei dati possono subire: il furto d’identità e la presenza in raccolte estranee di dati.

Nel primo caso, l’acquirente è spesso una persona che vuole intentare una truffa ai danni di altri individui o di istituti finanziari (bancari, assicurativi ecc.). Per organizzare tale frode, il truffatore ha bisogno di usare identità “normali” - molto meglio avere dati reali che creare identità fittizie con il pericolo di qualche dimenticanza - così rendendo la sua opera più robusta e a prova di numerose verifiche. Il risultato è che risulterà molto più credibile ed efficace nel portare la truffa a compimento. Naturalmente le forze dell’ordine conoscono bene il fenomeno; tuttavia le vittime di furti d’identità potranno rimanere all’interno di liste di potenziali sospetti, consultate ogni volta che si verifichi una frode in rete.

Il secondo caso fa riferimento al ben noto fenomeno della pedopornografia in rete[7]. È piuttosto frequente il caso in cui il criminale si sia procurato una collezione di materiali pornografici relativi a minori, concentrati su dettagli anatomici e mancanti di volti specifici o figura

[5] Gli attacchi di questo tipo sono migliaia, alcuni dei quali divenuti celebri. Ad esempio, nel 2015 il sito per adulteri Ashley Madison (https://www.ashleymadison.com) veniva attaccato per la pubblicazione di circa 60GB di dati aziendali, inclusi dati degli utenti (https://en.wikipedia.org/wiki/Ashley_Madison_data_breach). In generale esistono siti che tengono traccia delle esfiltrazioni più rilevanti e offrono una consultazione dei dati esfiltrati, come ad es. il sito https://haveibeenpwned.com.

[6] Ce ne sono a centinaia. Sul merito, l’autore sceglie di non pubblicare la URL per non favorirne la divulgazione; le varie URL possono essere minuziosamente raccolte attraverso un’attività standard di OSINT.

[7] Confermando la posizione dell’autore, si omettono le URL di siti dark web dedicati alla pedopornografia e alla coprofilia, piuttosto numerosi e comunque ricavabili da normali attività OSINT.

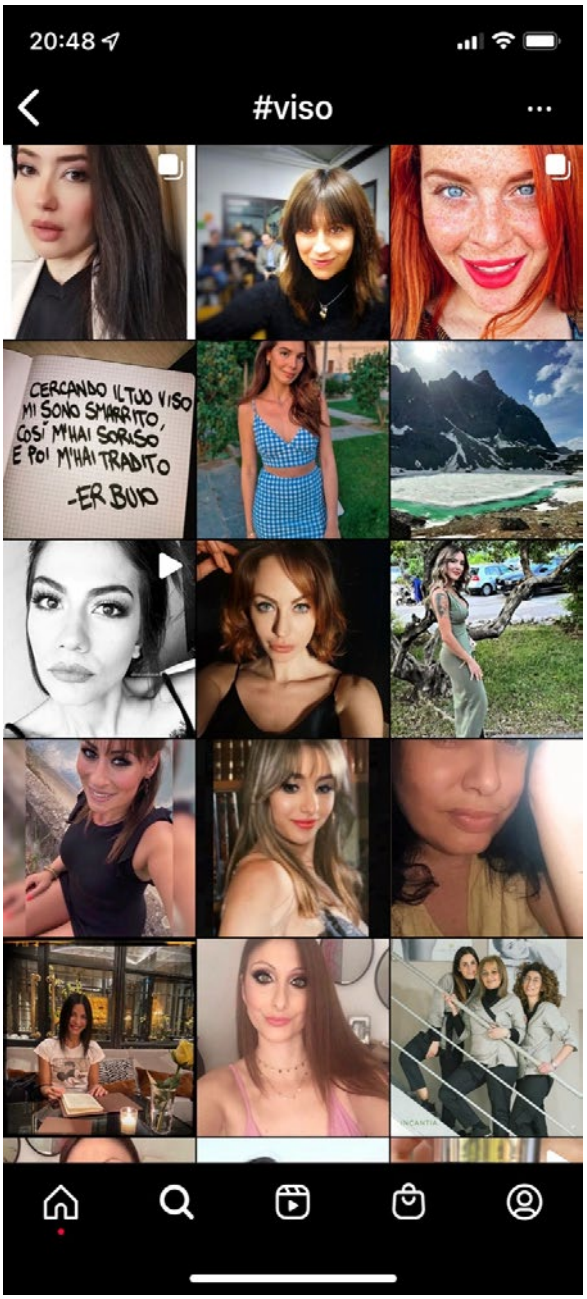


Figura 3. Ricerca dell'hashtag #viso su Instagram.

del corpo. È pratica comune ricorrere a fotomontaggi o, semplicemente, all'arricchimento della collezione mediante immagini prese da chi "non ha nulla da nascondere", per suggerire il volto o la figura del minore o di un suo parente stretto. Basta una qualche compatibilità nel colore della pelle. Anche in questo caso, ammesso il successo nel dimostrare l'estraneità, si rischia l'inclusione in liste di possibili sospetti.

4. ALTRE MINACCE

Finora ci siamo focalizzati sugli attacchi a pioggia. Nel caso di attacchi mirati, diversamente, non c'è limite alle conseguenze ottenibili; basti citare i *deepfake*[8], consistenti nell'uso di tecniche di *machine learning* (considerata parte dell'intelligenza artificiale) che mediante l'uso di *autoencoders* o reti generative avversarie (GAN) riescono, a partire da alcune immagini date, ad "addestrare" reti generative neurali all'alterazione delle immagini stesse. Il fenomeno ha

[8] Francesco Arruzzoli "Deepfake & Cyber Intelligence. Tecniche di creazione, rilevamento e prevenzione", ICT Security Magazine, https://www.ictsecuritymagazine.com/pubblicazioni/deepfake-cyber-intelligence/

acquisito notorietà nel 2017, quando queste tecniche furono usate per associare volti di attrici famose ai corpi nudi di modelle compiacenti. Tra i più celebri s’includono anche un video di Putin che annuncia la resa dell’Ucraina e uno di Obama, dove l’ex Presidente USA afferma che “*stiamo entrando in un’era in cui i nostri nemici possono far dire a chiunque qualunque cosa in ogni momento*”.

I *deepfake* accrescono fortemente la difficoltà di distinguere immagini genuine da quelle alterate: esistono anche numerose app[9] che mettono a disposizione questa possibilità, alimentando però diversi dubbi sull’opportunità di depositare dati (come immagini di volti reali) all’interno di database il cui uso è per lo meno opaco.

Fabrizio D’Amore, *Docente presso l’Università degli Studi di Roma “La Sapienza”, membro del Cyber Intelligence and Information Security Center*

[9] Ad esempio, MyHeritage o FaceApp per Android e iOS.

BIOGRAFIA

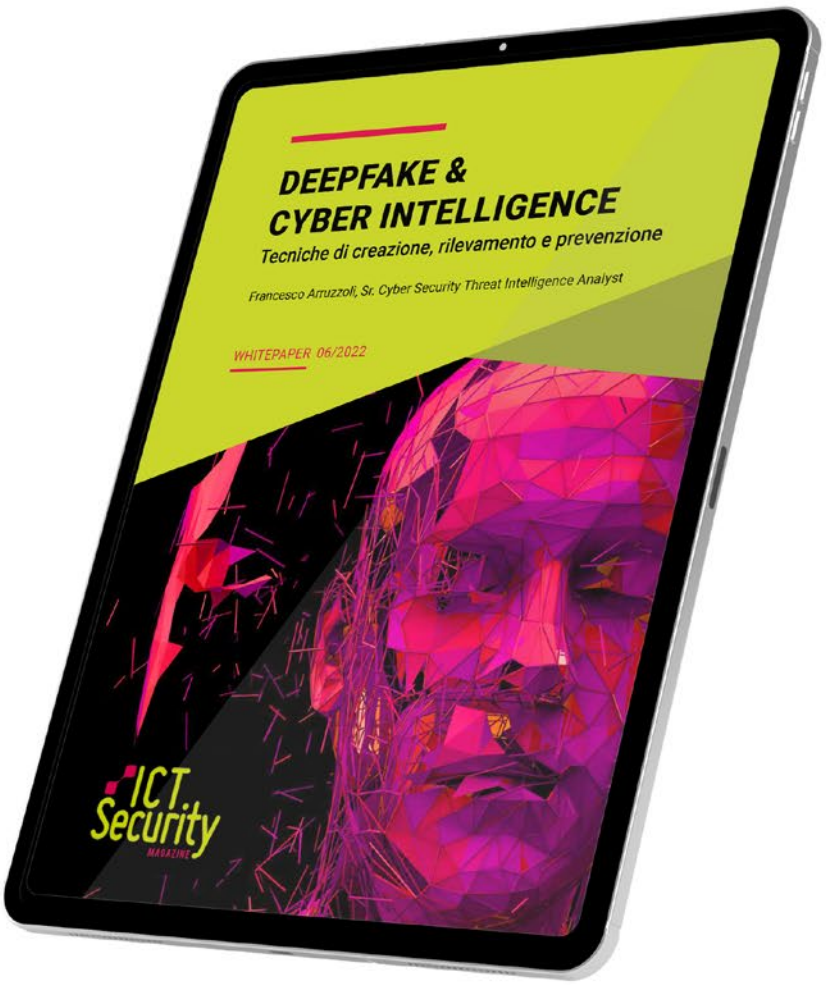
Fabrizio D'Amore

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.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

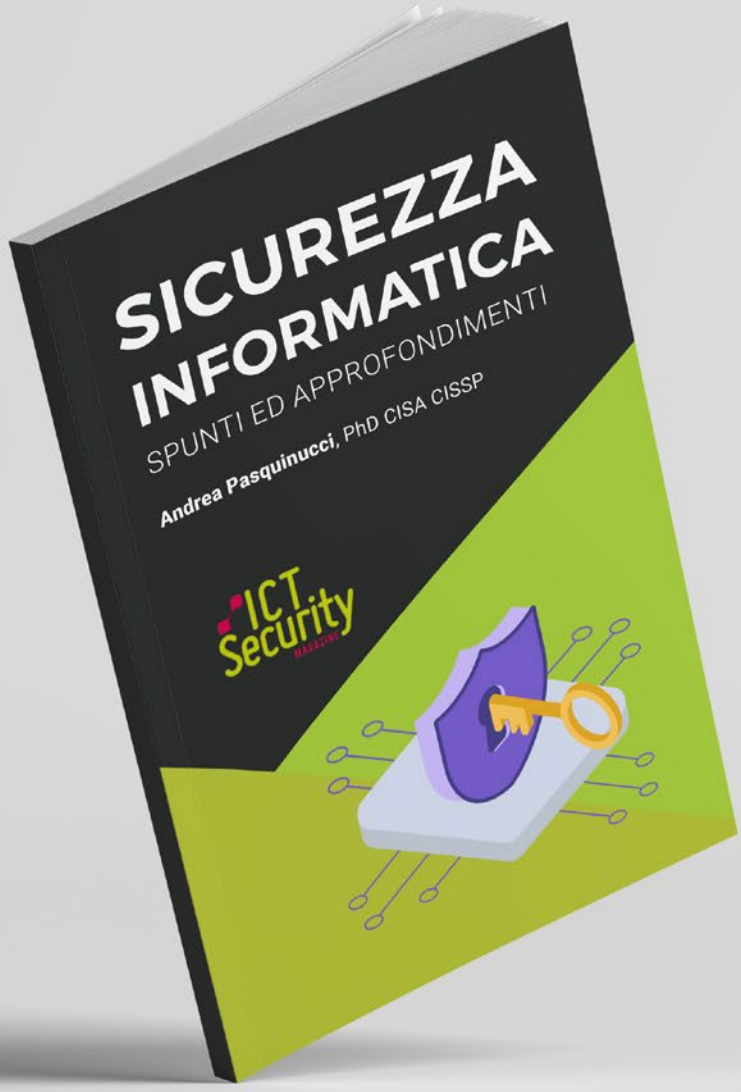
Download gratuito su www.ictsecuritymagazine.com



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

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**