swisscom

L'attacco mirato

Cyber Security Report 2019

Swisscom (Svizzera) SA
Group Security
Alte Tiefenaustrasse 6
3048 Worblaufen
www.swisscom.ch

Indice

Introduzione

Il Cyber Security Report di Swisscom 2019 è stato pubblicato. Sulla base dello stato attuale delle minacce, che abbiamo aggiornato anche quest'anno, affronteremo in dettaglio un tema particolarmente sentito all'interno della Security Community di Swisscom, tra i nostri partner e clienti, ma anche a livello internazionale: le APT.

Le Advanced Persistent Threat (APT) si caratterizzano per il fatto che gli hacker attaccano un bersaglio ben definito utilizzando un'enorme quantità di risorse allo scopo di ottenere informazioni specifiche o arrecare danni permanenti. Per poter classificare questa minaccia in modo ancora più chiaro, la inseriamo nel contesto di altre minacce quali, per esempio, criminali, terroristi e attivisti hacker. Cosa rende dunque le APT così speciali?

Mentre i criminali percorrono la strada che richiede il minor sforzo per conseguire il massimo guadagno possibile, e rispetto ai terroristi e agli attivisti hacker che invece da una parte utilizzano gli attacchi per finalità di visibilità e, dall'altra, dispongono di risorse e know-how relativamente limitati, le APT ricorrono a tecniche molto più sofisticate. Il bersaglio viene selezionato e monitorato attentamente per mesi o anni. Vengono mobilitate risorse pressoché illimitate per creare know-how e sviluppare gli strumenti adeguati. Inoltre, durante e dopo l'attacco viene prestata attenzione alla massima segretezza affinché né l'hacker, né il bersaglio vengano individuati troppo precocemente.

Il report descrive la motivazione e i mezzi degli hacker. Sulla base dei dati raccolti e analizzati da Swisscom, mostra quali metodi e strumenti vengono utilizzati con maggior frequenza dagli hacker. Indica inoltre quali contromisure sono particolarmente efficaci per individuare al meglio un attacco.

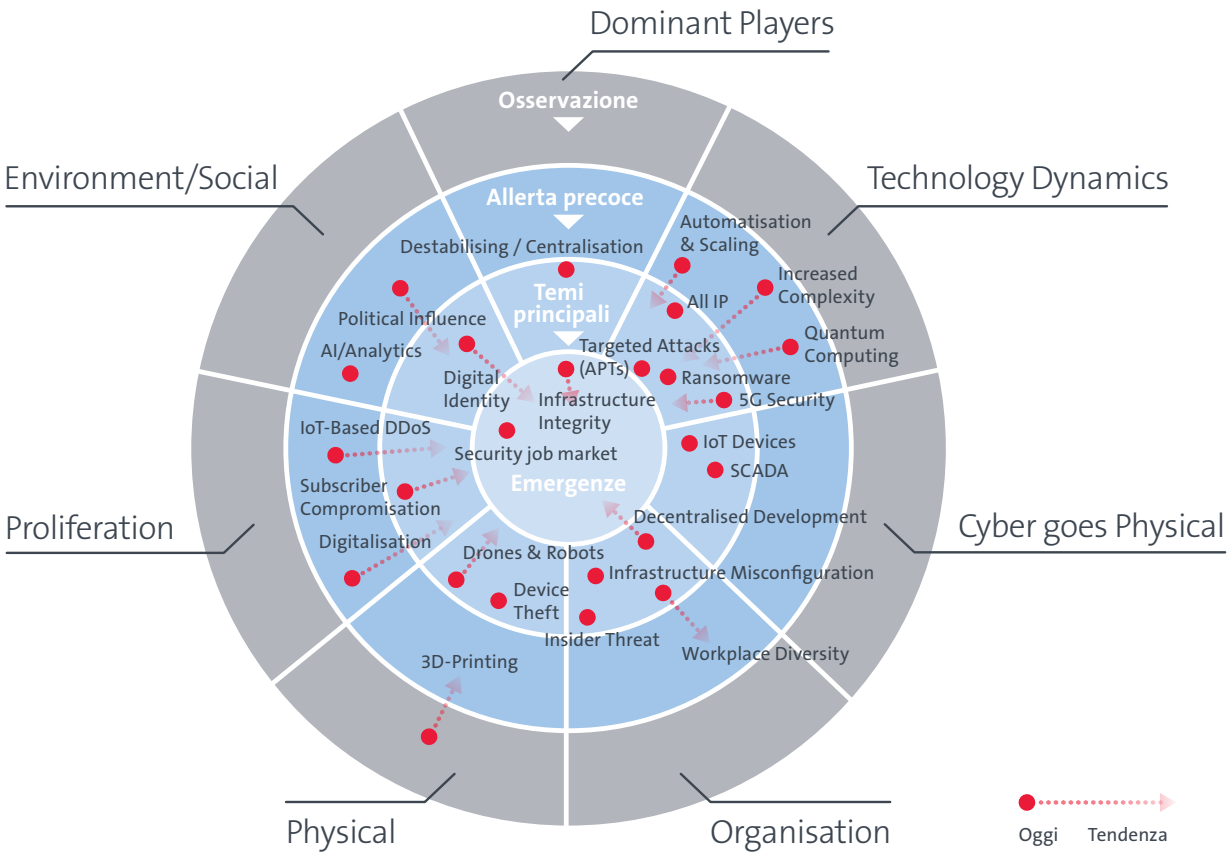
L'introduzione a questo tema è per noi motivo di particolare soddisfazione: siamo infatti riusciti a ottenere un'intervista da Costin Raiu di Kaspersky GReAT. Costin è un esperto di fama internazionale in questo ambito e si è reso disponibile a condividere con noi le sue conoscenze.

Il presente report è il risultato della collaborazione tra diversi dipartimenti in seno a Swisscom.

Quadro della situazione – Radar delle minacce

Le minacce hanno origine proprio nel continuo sviluppo di nuove tecnologie, oltre che nel loro uso e nella loro diffusione all'interno della società.

Pertanto occorre individuare quanto prima e rilevare sistematicamente le minacce potenziali. Per descrivere lo stato attuale delle minacce e la relativa evoluzione ci serviremo dello stesso radar già utilizzato nelle precedenti pubblicazioni del Cyber Security Report di Swisscom.



Radar delle minacce

Metodologia

Il radar delle minacce è diviso in sette segmenti che delimitano i diversi domini delle minacce. In ogni segmento le relative minacce possono essere assegnate a uno dei quattro cerchi concentrici. I cerchi indicano l'attualità della minaccia e quindi anche l'approssimazione della valutazione della minaccia. Più la minaccia è vicina al centro del cerchio, più è concreta e tanto più importanti sono le contromisure necessarie.

Definiamo i cerchi come

- **emergenze** per minacce già reali e controllate con un impiego relativamente importante di risorse;
- **temi principali** per minacce che sono già comparse occasionalmente e vengono controllate con un impiego normale di risorse. Spesso sussistono processi regolati per contrastare in modo efficiente queste minacce;
- **allerta precoce** per minacce non ancora comparse o che attualmente mostrano solo un'azione ridotta. Sono stati avviati dei progetti per contrastare tempestivamente una futura crescente importanza di tali minacce;
- **osservazione** per minacce che compariranno solo tra qualche anno. Non vi sono misure concrete per gestire queste minacce.

Inoltre, le minacce contrassegnate dai punti citati mostrano una tendenza. Questa può essere in aumento, in diminuzione o stabile nella propria criticità. La lunghezza del raggio della tendenza indica la velocità di trasformazione attesa della criticità della minaccia.

Minacce

Di seguito vengono spiegati brevemente i sette segmenti del radar delle minacce.

Dominant Players

In questo segmento vengono raccolte le minacce derivanti da interdipendenze di produttori, servizi o protocolli dominanti.

Emergenze	*Infrastructure Integrity:* all'interno di componenti fondamentali di infrastrutture critiche possono essere state integrate per negligenza o volutamente delle falle che mettono in pericolo la sicurezza del sistema.
Temi principali	*Destabilising Centralisation:* la forte centralizzazione nella struttura di internet comporta un rischio di accumulazione. L'interruzione di un servizio può avere effetti a livello mondiale, come ad esempio l'interruzione di Amazon Web Services (AWS).

Technology Dynamics

Questo termine indica minacce che derivano dalla rapidissima innovazione tecnologica e che, da un lato, forniscono nuove opportunità agli hacker mentre, dall'altro, creano nuove minacce dovute allo sviluppo stesso.

Temi principali	*Targeted Attacks:* attacchi mirati e complessi che perseguono un obiettivo concreto. Questa minaccia verrà illustrata nel dettaglio nei capitoli successivi di questo report. *All IP:* durante l'introduzione capillare di All IP aumentano i rischi in relazione alla tecnologia VoIP. *5G Security:* 5G è una tecnologia di comunicazione mobile ancora giovane; la sua introduzione porterà con sé, oltre a numerose opportunità, anche minacce ancora sconosciute. *Ransomware:* i dati critici vengono cifrati su vasta scala e decifrati (eventualmente) in cambio di un riscatto.
Allerta precoce	*Automatisation & Scaling:* una maggiore automazione dei processi operativi tecnici avrà un impatto più importante in caso di attacchi compiuti con successo o configurazioni errate. *Increased Complexity:* è in continua crescita la complessità dei sistemi, in particolare oltre i confini tecnologici e aziendali. Aumenta di conseguenza l'esposizione al rischio e la ricerca dell'errore diventa sempre più difficile. *Quantum Computing:* i computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti, poiché riescono a decifrarle in pochissimo tempo.

Cyber goes Physical

Questo termine indica gli attacchi tramite le infrastrutture nel cyberspazio che provocheranno sempre più danni nel mondo fisico.

Temi principali

IoT Devices: i dispositivi con una protezione debole possono essere compromessi e sabotati. Potranno così essere limitati nella propria funzione, ad esempio in fatto di disponibilità o integrità dei dati.
SCADA: esistono ancora molti sistemi di controllo protetti male o non protetti per gli impianti delle infrastrutture critiche.

Organisation

Con il termine «organizzazione» vengono indicate le minacce che si basano sulle modifiche nelle organizzazioni o che sfruttano i punti deboli nelle organizzazioni.

Temi principali

Infrastructure Misconfiguration: sfruttamento di componenti mal configurati delle infrastrutture e/o falle identificate ed eliminate tardivamente.
Workplace Diversity: oltre alle numerose opportunità che i nuovi modelli di lavoro portano con sé, l'impiego incontrollato di tali modelli, come ad es. «Bring your own Device» (BYOD) oppure il maggiore impiego di postazioni di lavoro remote comporta un'accresciuta esposizione al rischio.
Insider Threat: partner o collaboratori manipolano, usano in modo illecito o vendono per negligenza o intenzionalmente informazioni.
Decentralised Development: i classici settori di sviluppo sono in via d'estinzione, lo sviluppo di applicazioni si avvicina alle Business Unit e al contempo si riducono i cicli delle release.

Physical

Minacce derivanti da un ambiente fisico e di regola orientate verso obiettivi fisici.

Temi principali

Device Theft: il furto, in particolare di componenti dell'infrastruttura critica o in futuro sempre più di apparecchi IoT, può comportare la perdita di dati o compromettere la disponibilità dei servizi.
Drones and Robots: lo spionaggio o gli attacchi da grande distanza diventano più semplici ed economici.

Osservazione

3D-Printing: la produzione ad esempio di chiavi o di altri dispositivi fisici diventa più economica e semplice con la migliore qualità delle stampanti 3D.

Proliferation

Nel segmento Proliferation sono comprese le minacce che sfruttano la sempre più semplice ed economica disponibilità di media IT e know-how. Questo perché, da un lato, la diffusione comporta un maggior numero di aree di attacco e, dall'altro, perché incrementa la disponibilità di strumenti di attacco.

Temi principali	*Subscriber Compromisation:* il software dannoso attacca i dati privati degli utenti della rete mobile o viene utilizzato per attacchi all'infrastruttura IT o di telecomunicazione.
Allerta precoce	*IoT-Based DDoS:* Starkes la grande diffusione di dispositivi IoT con una scarsa protezione porta a un maggior numero di «candidati alla presa di controllo» per botnet. *Digitalisation:* una crescente messa in rete del mondo reale e virtuale e della vita privata e commerciale comporta un maggior numero di vie di attacco.

Environmental/ Social

In questo segmento rientrano le minacce che originano da cambiamenti socio-politici o che diventano più semplici o vantaggiose per gli hacker a causa di tali cambiamenti.

Emergenza	*Security job market:* la richiesta di professionisti di Security viene soddisfatta con molta difficoltà, comportando un minore know-how nell'attività contro attacchi sempre più complessi e intelligenti.
Temi principali	*Digital Identity:* identità digitali personali autenticate possono essere oggetto di furto o abuso, ad esempio per stipulare contratti a nome di terzi.
Allerta precoce	*AI / Analytics:* un numero maggiore di dati e migliori modelli di analisi mediante AI possono essere oggetto di abuso allo scopo di influenzare il comportamento delle persone. Le decisioni sono lasciate sempre di più a sistemi autonomi. *Political Influence:* le correnti politiche possono influire sulle decisioni tecnologiche o economiche, per esempio attraverso la scelta di determinati fornitori di tecnologie. Ne possono pertanto scaturire nuovi rischi.

Conclusione

Lo stato attuale delle minacce rimane complesso. Gli hacker traggono vantaggio dal crescente valore delle risorse virtuali, cosa che accresce la motivazione per un attacco mirato. Inoltre, le innovazioni tecnologiche e la convergenza del mondo fisico con quello virtuale creano nuove opportunità di attacco. Appare chiaro inoltre che non esiste una minaccia particolare in fase di consolidamento, ma siamo confrontati con una situazione dominata da oscillazioni e trend.

Rispetto al quadro della situazione dell'anno scorso possiamo constatare che lo stato delle minacce è rimasto complessivamente stabile. Sebbene quest'anno alcune minacce siano diventate meno critiche, come per esempio Infrastructure Misconfiguration e Workplace Diversity, la maggior parte di esse permane e mostra solo variazioni minime.

Riguardo alle due minacce diventate meno critiche, riteniamo che questo «allentamento» non sia dovuto a un minor interesse da parte di potenziali hacker, bensì alla maggiore maturità delle infrastrutture colpite. La Workplace Diversity, per esempio, viene gestita attivamente da un numero sempre maggiore di aziende, vengono utilizzati Mobile Device Management (MDM) Tool e vengono elaborate e implementate direttive per l'utilizzo di modelli Bring Your Own Device (BYOD).

Le minacce tramite i sistemi SCADA (sistemi di controllo industriali) e gli apparecchi IoT (Internet of Things) rimangono al centro dell'attenzione, tuttavia non individuiamo variazioni a breve termine. La penetrazione degli IoT non è ancora sufficiente per produrre un ulteriore inasprimento dello stato delle minacce.

Per contro, i droni hanno raggiunto attualmente una maggiore diffusione, con conseguenze talvolta negative che vengono affrontate anche nei media. Pertanto, attualmente in questo ambito individuiamo un forte trend verso un inasprimento dello stato delle minacce.

Lo stato attuale delle minacce rimane complesso. Gli hacker traggono vantaggio dal crescente valore delle risorse virtuali, cosa che accresce la motivazione per un attacco mirato

Intervista a Costin Raiu (Kaspersky GReAT)

Abbiamo avuto l'opportunità di porre sei domande sulle APT a Costin Raiu e di approfondire questo tema grazie alle esperienze e alle osservazioni che l'esperto ci ha svelato nelle sue risposte.

1. Costin Raiu, quali sono le caratteristiche principali di una Advanced Persistent Threat (APT)?

Secondo noi, a rendere avanzati un malware o un attacco sono le caratteristiche seguenti:

- l'*utilizzo di uno zero-day exploit* come accaduto con Sofacy, anche noto come APT28, Pawn Storm o FancyBear. Si tratta probabilmente del gruppo hacker che ha scoperto il maggior numero di zero-day in assoluto;
- una *piattaforma modulare altamente complessa* per l'esecuzione di varie funzioni come Regin e ProjectSauron;
- l'*utilizzo di tecniche sofisticate per infezione, persistenza o esfiltrazione.* Per esempio, RedOctober utilizzava un meccanismo di persistenza molto intelligente sotto forma di un plugin di Office e Adobe Reader in grado di eseguire codice nascosto in documenti specificamente costruiti; questo comprende anche diverse tecniche bootkit.

Altre caratteristiche sono una *replicazione lenta* associata a *persistenza a livello di rete, infezione dell'hardware di rete di livello professionale* come core router e *attacchi alla catena di fornitura.*

Alcuni esempi significativi delle modalità di esecuzione di questi attacchi sono Duqu2, SYNful Knock o Shadowpad e CCleaner compromise.

Questo elenco non è esaustivo. Altri esempi sono attacchi a caratteristiche hardware, infezione del BIOS, attacchi distruttivi contro l'hardware (un esempio sopra tutti, l'attacco con Stuxnet) o malware multi-piattaforma.

2. Quali sono i cambiamenti più significativi dell'attività APT che sta osservando e quali ambiti sono maggiormente interessati da questi cambiamenti?

Attualmente stiamo monitorando oltre 100 gruppi e operazioni APT. Abbiamo iniziato a monitorare i gruppi APT in modo regolare nel 2010, dopo la vicenda di Stuxnet, e quando è stato chiaro che si trattava di una vera e propria tendenza abbiamo deciso di continuare. Nel 2015, arrivati a quasi 100 gruppi e operazioni APT noti, abbiamo lanciato il nostro servizio di reporting APT privato.

Osserviamo inoltre che sempre più gruppi APT stanno passando agli attacchi fileless. Questi attacchi rendono più difficile individuare le infezioni, poiché nel sistema non sono presenti file infetti. Inoltre, vediamo che un numero crescente di gruppi sta facendo ricorso a tool pubblici come Empire Powershell, Metasploit, Cobalt Strike o Mimikatz. È difficile distinguerli l'uno dall'altro.

3. Qual è stata l'APT più interessante che ha analizzato?

Probabilmente Duqu2. Innanzitutto abbiamo pensato che Duqu2 fosse speciale perché è stato utilizzato per colpire Kaspersky Lab. L'idea di una APT concepita per colpire una società di sicurezza è piuttosto ardita, dato che è impossibile sperare che l'intrusione non venga scoperta. In secondo luogo, Duqu2 era fuori dal comune nel senso che si trattava di una minaccia solo in memoria, vale a dire che, durante l'esecuzione, esisteva solo nella memoria di diversi sistemi informatici, senza artefatti sui dischi. Questo ha complicato enormemente il rilevamento. Infine, l'utilizzo di una vulnerabilità zero-day in Windows per bypassare i prodotti Kaspersky è apparso piuttosto interessante e ha permesso di elaborare diverse migliorie dei prodotti per rilevare questo comportamento in futuro.

4. Quali sono gli errori tipici che le organizzazioni commettono nel prepararsi a un attacco APT e in che modo rispondono a una ATP?

Nella maggior parte dei casi, le organizzazioni concentrano i propri sforzi nell'impedire che un hacker esterno possa accedere alle risorse interne, ma poche adottano misure per individuare un hacker una volta che quest'ultimo è entrato nella rete interna. In base ai risultati della nostra attività di ricerca sappiamo che gli hacker passano gran parte del loro tempo nel movimento laterale e nell'esfiltrazione. Pertanto, le organizzazioni dovrebbero concentrarsi su queste fasi. Inoltre sono carenti nell'implementazione delle misure di mitigazione TOP35 dell'Australian DSD[1] contro le APT.

[1] https://acsc.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

5. Quali sono gli errori tipici che gli hacker commettono durante le loro operazioni? In quali casi le organizzazioni possono avere un vantaggio sui loro avversari?

Spesso riscontriamo errori di Opsec come falle nella VPN, percorsi PDB dimenticati in file binari o timestamp di compilazione che aprono un varco per identificare gli hacker.

6. Quali sono le capacità più importanti che bisogna avere per essere preparati a intrusioni APT su vasta scala?

Per le società è fondamentale avere accesso a una threat intelligence privata, disporre di un Security Operation Center perfettamente operativo, implementare i filtri di rete e rilevare il meccanismo di movimento laterale ed esfiltrazione. Inoltre, le organizzazioni dovrebbero conoscere in modo approfondito le modalità di lavoro degli hacker. Per esempio, quali tool utilizzano e come operano durante le fasi dell'attacco. La maggior parte di essi utilizza Mimikatz, Powershell e Webshells.

Costin Raiu

Costin Raiu è specializzato nell'analisi delle Advanced Persistent Threat (APT) e di attacchi malware complessi. È a capo del Global Research and Analysis Team (GReAT) di Kaspersky che ha analizzato, tra le altre, le operazioni Stuxnet, Duqu, Flame ed EquationGroup. Costin vanta oltre 19 anni di esperienza nel campo delle tecnologie antivirus e della ricerca sulla sicurezza. È membro del Virus Bulletin Technical Advisory Board, membro della Computer AntiVirus Researchers' Organisation (CARO) e reporter per la Wildlist Organisation International. Prima di approdare a Kaspersky Lab, Costin ha lavorato per GeCad in qualità di Chief Researcher e come Data Security Expert nel gruppo di sviluppatori di RAV Antivirus.

Componenti dell’attacco mirato

La missione, ossia l'obiettivo strategico, ha finalità completamente diverse a seconda dell'attore; inoltre, gli attori hanno capacità diversissime gli uni dagli altri per perseguire tali finalità

Nei media vengono spesso riportate notizie di aziende colpite da un determinato malware o di determinati malware utilizzati per rubare i dati di un'azienda che possono essere convertiti in denaro. Per comprendere gli attacchi mirati dobbiamo avere ben chiaro che non è il malware che esegue l'attacco, ma è l'azienda ad essere attaccata da persone. In ambito informatico, queste persone vengono spesso chiamate «attori» (Threat Actors / Cyber Operators) e rappresentano i componenti principali alla base di un attacco. Gli attori che si celano dietro gli attacchi mirati eseguono questi attacchi non casualmente, ma con un obiettivo strategico, sono mossi dalle motivazioni più disparate e utilizzano modi operandi diversificati che fungono da ulteriori componenti di un attacco mirato e che verranno presentati nelle pagine seguenti.

Threat Actor Landscape

La missione, ossia l'obiettivo strategico, ha finalità completamente diverse a seconda dell'attore; inoltre, gli attori hanno capacità diversissime gli uni dagli altri per perseguire tali finalità. Per un migliore orientamento e per favorire la valutazione del potenziale e della motivazione dei diversi attori, li suddividiamo nei gruppi seguenti:

Le Advanced Persistent Threat e l'attacco mirato

L'Advanced Persistent Threat (APT) rappresenta il livello più alto degli attori informatici. Gli attacchi mirati di un'APT vengono eseguiti sulla base di una missione concepita per conseguire un vantaggio strategico, raggiungere obiettivi politici o influenzare positivamente gli sviluppi tecnologici. A questo riguardo, un'APT è presumibilmente orchestrata da un governo o da suoi incaricati. La particolarità dell'APT consiste nel fatto che gli attacchi ad essa correlati vengono considerati come «state-sponsored», vale a dire che gli attori sono tollerati dallo Stato e rappresentano quindi hacker «legali» (o, perlomeno, protetti dallo Stato). La legalità statale, la difficile tracciabilità e l'esecuzione quasi esente da rischi hanno fatto sì che sempre più Stati abbiano potenziato le proprie capacità informatiche e gli attacchi APT.[2]

[2] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

Oltre alle APT «legali», esiste un altro gruppo marginale che si può considerare una sorta di apripista degli Stati o dei governi che ad oggi non hanno ancora creato capacità tali da poter eseguire autonomamente attacchi avanzati come quelli di un'APT. Al più tardi dalle rivelazioni su Hacking Team carpite dall'attivista hacker Phineas Phisher è risultato chiaro che questo gruppo marginale persegue chiari obiettivi finanziari e strategici.[3]

I criminali informatici e l'attacco mirato

I criminali informatici agiscono secondo una logica perlopiù opportunistica e utilizzano qualunque mezzo d'attacco a loro disposizione (per es. un exploit contro Microsoft Office che è stato pubblicato) contro un ampio spettro di obiettivi. Se entrano in possesso di un nuovo mezzo d'attacco, utilizzano anche quest'ultimo per trarre vantaggio dal maggior numero possibile di attacchi. Oltre agli attacchi opportunistici, esistono anche attacchi mirati e ben organizzati che perseguono lo scopo di rubare, attaccando un bersaglio dedicato, un'elevata quantità di dati o altri valori. Per farlo, gli hacker hanno bisogno di rimanere all'interno del sistema della vittima per un periodo di tempo piuttosto lungo («Dwell Time»). Questi criminali organizzati presentano spesso caratteristiche tecniche che non hanno nulla da invidiare a molte APT. La differenza decisiva risiede tuttavia negli obiettivi strategici di questi attori.

I terroristi e l'attacco mirato

Nonostante la società tema fortemente che i terroristi possano eseguire attacchi a sistemi di importanza critica, finora non sono noti casi in cui i terroristi abbiano perseguito e raggiunto i propri obiettivi strategici attraverso attacchi informatici mirati. Al contrario: relativamente ai timori attuali, il Cambridge Centre for Risk Studies non ha finora osservato alcun gruppo non statale di stampo terroristico che abbia acquisito la capacità di eseguire attacchi informatici mirati e avanzati in grado di arrecare danni fisici.[4] Al contempo, il World Wide Threat Assessment of the US Intelligence Community 2018 indica che il cyberspazio viene utilizzato dai terroristi principalmente per scopi mediatici.[5]

Continuiamo a ritenere che il terrorismo informatico rappresenti un pericolo e che in futuro assumerà un ruolo più preminente.

Gli attivisti hacker e l'attacco mirato

Gli attivisti hacker eseguono attacchi mirati generalmente sulla base di motivazioni politiche allo scopo di dare voce alla loro protesta. Questi attori si ritrovano spesso a livello globale in gruppi di omologhi per coordinare ed eseguire gli attacchi oppure mettono a segno gli attacchi in solitaria. Le abilità degli attivisti hacker variano molto da un soggetto all'altro. Lo scopo è raggiungere un obiettivo strategico decisivo nel minor tempo possibile e suscitare una grande attenzione mediatica. Finora si è osservato che questi attori eseguono principalmente operazioni Smash and Grab per rendere note le loro attività il più rapidamente possibile.

[3] https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/
[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf
[5] https://www.wilsoncenter.org/article/world-wide-threat-assessment

Targeting

I bersagli (target) degli attacchi mirati non vengono scelti in modo casuale, ma secondo una relazione specifica che collega il bersaglio dell'attacco con l'hacker.

Target of Interest

Tanto più il bersaglio dell'attacco soddisfa l'esigenza di un hacker, quanto più l'importanza del bersaglio aumenta e diventa un Target of Interest (TOI) per gli attori. Gli aspetti principali che descrivono questa esigenza sono la caratteristica esclusiva del bersaglio, il dispendio di risorse necessario e i costi ad esso correlati per eseguire l'attacco, nonché i rischi che possono derivare per gli hacker.

Target of Opportunity

Un'importanza inferiore è quella rivestita dal Target of Opportunity (TOO). Questi bersagli soddisfano un'esigenza secondaria degli attori e vengono compromessi per essere successivamente utilizzati per esempio come trampolini e giungere così al vero e proprio Target of Interest. Tuttavia, può anche essere che il bersaglio fosse vulnerabile per una capability in un determinato momento e sia stato compromesso. Questo può far sì, tra le altre cose, che il Target of Opportunity diventi un Target of Interest se, in un momento successivo, gli attori si rendono conto che la vittima ha un valore più elevato di quanto inizialmente ipotizzato.[6]

Tanto più il bersaglio dell'attacco soddisfa l'esigenza di un hacker, quanto più l'importanza del bersaglio aumenta e diventa un Target of Interest (TOI) per gli attori.

[6] www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Esecuzione dell’attacco

Esistono molti metodi per descrivere l'esecuzione di un attacco informatico. Noi abbiamo scelto il framework MITRE ATT&CK, i cui dati si basano su attacchi che sono stati messi a segno nel mondo reale. ATT&CK è un metodo analogo a quello della Cyber Kill Chain[7] per la descrizione degli attacchi informatici[8]. Mentre la Cyber Kill Chain rappresenta più che altro una descrizione dall'alto, il framework ATT&CK descrive in dettaglio le attività di oltre 80 Threat Actors (Groups). ATT&CK contiene principalmente i modi operandi delle Advanced Persistent Threat nelle diverse fasi dell'attacco, descritti sulla base delle Tactics, Techniques and Procedures (TTPs)[9] di questi attori.

La nostra valutazione dei dati è stata eseguita su un periodo di diverse settimane utilizzando ATT&CK Enterprise[10] (di seguito ATT&CK), con ultimo accesso a gennaio 2019. ATT&CK viene continuamente ampliato e aggiornato. I dati del framework, insieme alle esperienze del team GReAT di Costin Raiu, permettono tuttavia di ottenere valutazioni molto precise in termini sia qualitativi che quantitativi.

A gennaio 2019 ATT&CK conteneva

Abbiamo raccolto nei capitoli seguenti le informazioni high-level a nostro avviso più importanti del framework ATT&CK, prestando particolare attenzione all'Advanced Persistent Threat.

[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[8] https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
[9] https://apps.dtic.mil/dtic/tr/fulltext/u2/1004650.pdf
[10] https://attack.mitre.org/matrices/enterprise/

Le fasi dell'attacco

Con il termine «Tactics», ATT&CK indica le diverse fasi dell'attacco che un Threat Actor deve superare per raggiungere il proprio obiettivo strategico. A questo riguardo si parla anche di «obiettivi tattici». ATT&CK definisce le seguenti Tactics:

Initial Access	La fase di Initial Access costituisce la situazione di partenza per tutte le successive fasi dell'attacco. Comprende il contatto iniziale con l'obiettivo dell'attacco e la compromissione del Patient Zero.
Persistence	I punti di persistenza all'interno della rete target assicurano l'accesso continuo alla rete. Tanto più significativo è l'obiettivo (Target of Interest), quante più risorse vengono impiegate per la persistenza nel corso di un'intrusione a lungo termine.
Privilege Escalation	L'escalation dei privilegi serve spesso per poter installare software dannoso o punti di persistenza. Livelli di autorizzazione superiori servono, tra le altre cose, anche per potersi espandere ad altri sistemi o ottenere accesso agli obiettivi strategici (per es. i dati).
Discovery	L'attività di ricognizione all'interno della rete target serve a individuare sistemi, utenti e dati rilevanti per la missione.
Lateral Movement	Con questo termine viene indicata l'espansione all'interno della rete ai dati rilevanti per la missione. Spesso, a questo si accompagna la fase di esecuzione e installazione di altri punti di persistenza.
Collection	Durante questa fase vengono raccolti i dati rilevanti per la missione.
Exfiltration	Si tratta della fase finale per concludere con successo la missione e consiste nell'esfiltrazione dei dati rilevanti.

Parallelamente a queste fasi si svolgono le fasi seguenti, che dipendono dal successo nel raggiungimento dell'obiettivo delle rispettive fasi:

Execution

L'esecuzione di codici dannosi su un sistema locale o remoto si verifica principalmente nelle fasi di Initial Access e Lateral Movement. Senza l'esecuzione di un codice controllato dall'hacker non sarebbe possibile passare alla fase successiva. Per questo, l'Execution è uno dei presupposti fondamentali per permettere la prosecuzione dell'attacco e la diffusione all'interno della rete target.

Defense Evasion

L'elusione dei meccanismi di difesa e riconoscimento (per es. la disattivazione del firewall sull'endpoint o la cancellazione di dati di log) è uno degli obiettivi tattici che l'autore dell'attacco utilizza in ognuna delle altre fasi della sua missione per dissimulare la sua presenza o eludere i meccanismi di riconoscimento.

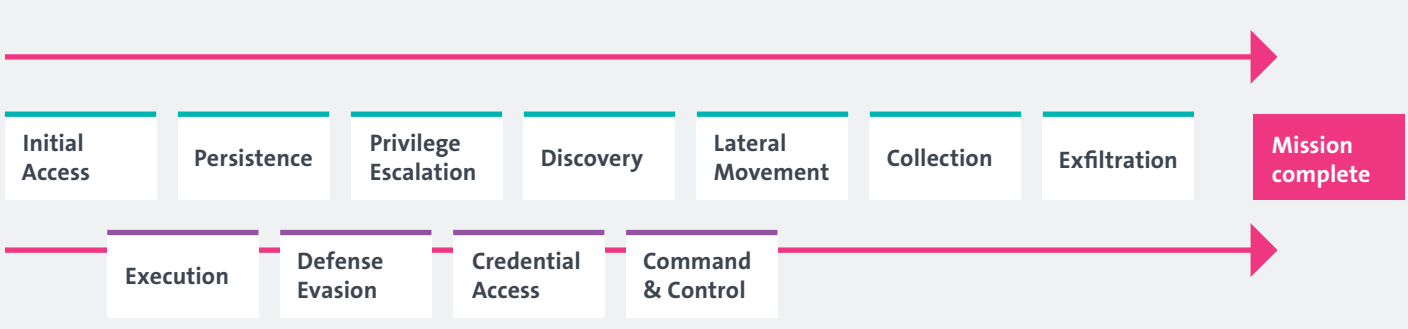
Credential Access

I dati di accesso rappresentano una delle funzioni chiave per gli hacker. Da una parte, consentono di penetrare e muoversi all'interno della rete target senza destare sospetto. Dall'altra permettono di accedere ai dati di cui gli hacker vogliono impossessarsi. Inoltre, la possibilità di riutilizzare i dati di accesso permette agli hacker di eseguire il loro attacco con un dispendio di risorse minimo, non essendo necessario scrivere, acquistare né utilizzare altrimenti alcun exploit.

Command & Control

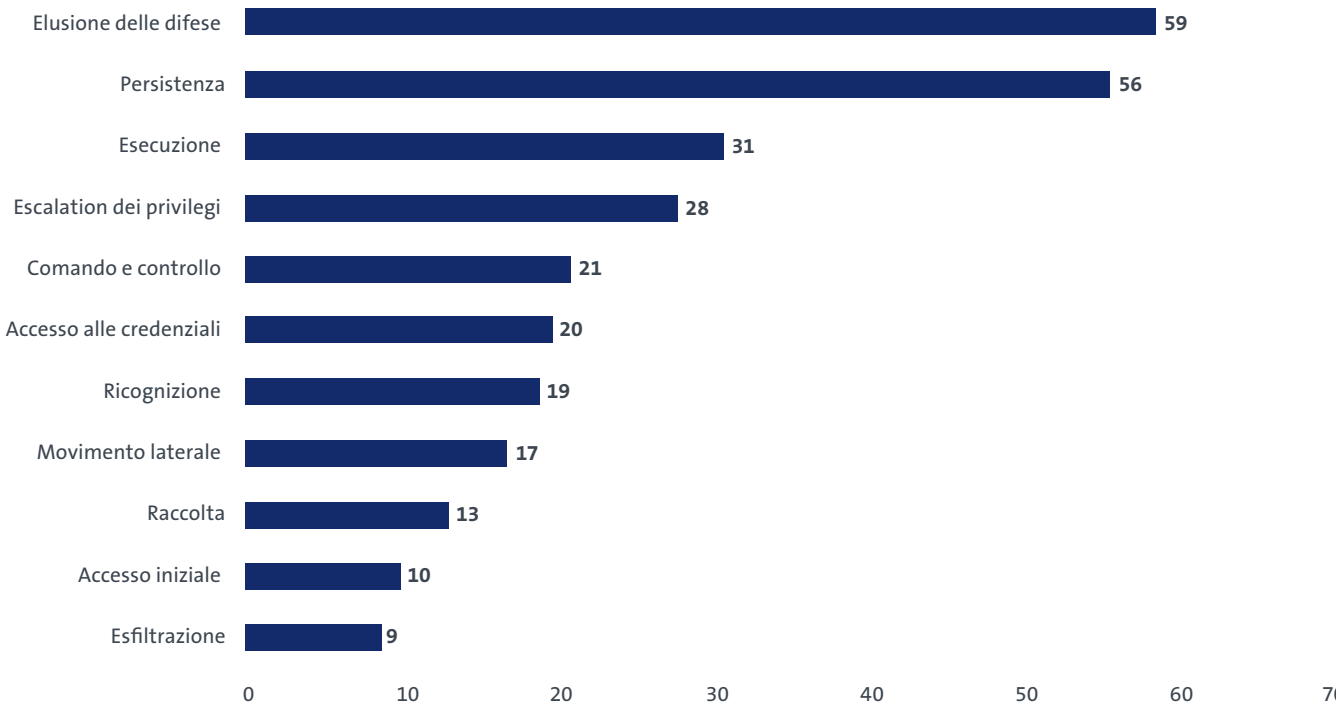
Il canale Command & Control è il mezzo di comunicazione che permette all'hacker di tenere sotto controllo l'infrastruttura target compromessa. Se l'hacker perdesse questo canale, l'attacco verrebbe immediatamente sospeso. Gli hacker mirati stabiliscono spesso più canali Command & Control.

La figura seguente chiarisce le interdipendenze:



Modi operandi degli attori

Per raggiungere o superare una determinata fase, gli attori utilizzando nel framework ATT&CK[11] i più svariati modi operandi, denominati anche Techniques. Ciascuna fase può contenere più modi operandi; a loro volta, gli stessi modi operandi possono presentarsi in più fasi. ATT&CK contiene 224 di questi modi operandi, che si ripartiscono tra le diverse fasi nel modo seguente:



Il diagramma a barre fornisce indicazioni significative sui modi operandi degli attori e mostra chiaramente in quali fasi gli attori mostrano di possedere maggiori e minori capacità. Se, dunque, si analizzano le fasi considerando quelle con il maggior numero di modi operandi, si deduce che gli attori possono attingere a un ampio spettro di modi operandi per eludere i meccanismi di difesa nelle varie fasi dell'attacco mediante Defence Evasion e hanno a disposizione un numero quasi equivalente di modi operandi per garantire l'accesso a lungo termine nella fase Persistence.

Estratto dall'intervista a Costin Raiu, che spiega questa affermazione:

Quali sono le capacità più importanti che bisogna avere per essere preparati a intrusioni APT su vasta scala?

Le organizzazioni dovrebbero conoscere in modo approfondito le modalità di lavoro degli hacker. Per esempio, quali tool utilizzano e come operano durante le fasi dell'attacco. La maggior parte di essi utilizza Mimikatz, Powershell e Webshells.

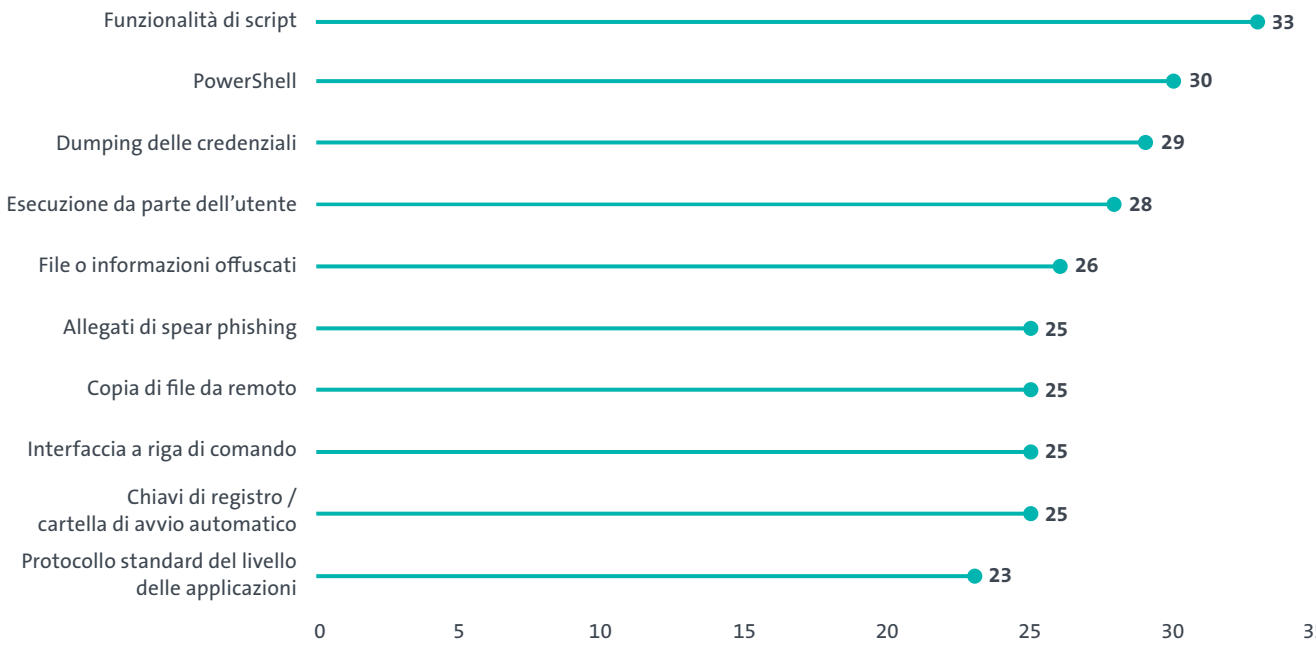
[11] https://attack.mitre.org/

Modi operandi più utilizzati in base agli attori
Un'analisi dei gruppi APT e dei relativi modi operandi mostra un chiaro trend verso attacchi fileless, confermato anche da Costin Raiu.

La figura seguente mostra la top 10 dei modi operandi più utilizzati dagli 80 attori contenuti in ATT&CK:

Quali sono i cambiamenti più significativi dell'attività APT che sta osservando e quali ambiti sono maggiormente interessati da questi cambiamenti?

Osserviamo inoltre che sempre più gruppi APT stanno passando agli attacchi fileless. Questi attacchi rendono più difficile individuare le infezioni, poiché nel sistema non sono presenti file infetti.



La top 10 dei modi operandi è riassumibile nei due temi «Living off the Land» e «Metodi di efficacia comprovata».

Living off the Land

Sempre più gruppi APT ricorrono a script che ad oggi sono integrati in modo standard nei sistemi operativi Windows, per esempio Powershell e Command-Line Interfaces, per eseguire il loro codice dannoso. Questo senza essere riconosciuti dalle soluzioni di Application Whitelisting e senza lasciare tracce significative sul sistema.

Come meccanismo di persistenza, i modi operandi più apprezzati dagli attori rimangono le Registry Run Keys e l'inserimento di voci nella Windows Startup Folder.

I metodi di efficacia comprovata conducono all'obiettivo

Non tutti gli attori hanno le risorse per sviluppare Zero Day Exploit. La maggior parte degli attori ricorre ancora a Spear Phishing Attachment e User Execution per l'esecuzione del codice dannoso da parte dell'utente.

Gli attori APT utilizzano vie semplici per arrivare al loro obiettivo. Con il Credential Dumping vengono ottenuti e poi utilizzati dati di accesso validi per muoversi all'interno dell'infrastruttura e rendere possibile l'accesso.

Per l'esfiltrazione dei dati, l'ulteriore caricamento e salvataggio di codici sotto il controllo dell'hacker, i modi operandi più amati continuano ad essere la semplice copia di file (Remote File Copy) attraverso protocolli legittimi (Standard Application Layer Protocol) e l'utilizzo di codifiche e cifrature (Obfuscated Files or Information).

Software degli attori

Il software utilizzato dagli attori implementa i modi operandi necessari per una fase dell'attacco. A questo riguardo, gli attori ricorrono alle più diverse categorie di software che, all'interno di ATT&CK, rappresentano un Tool, una Utility o un Malware.[12]

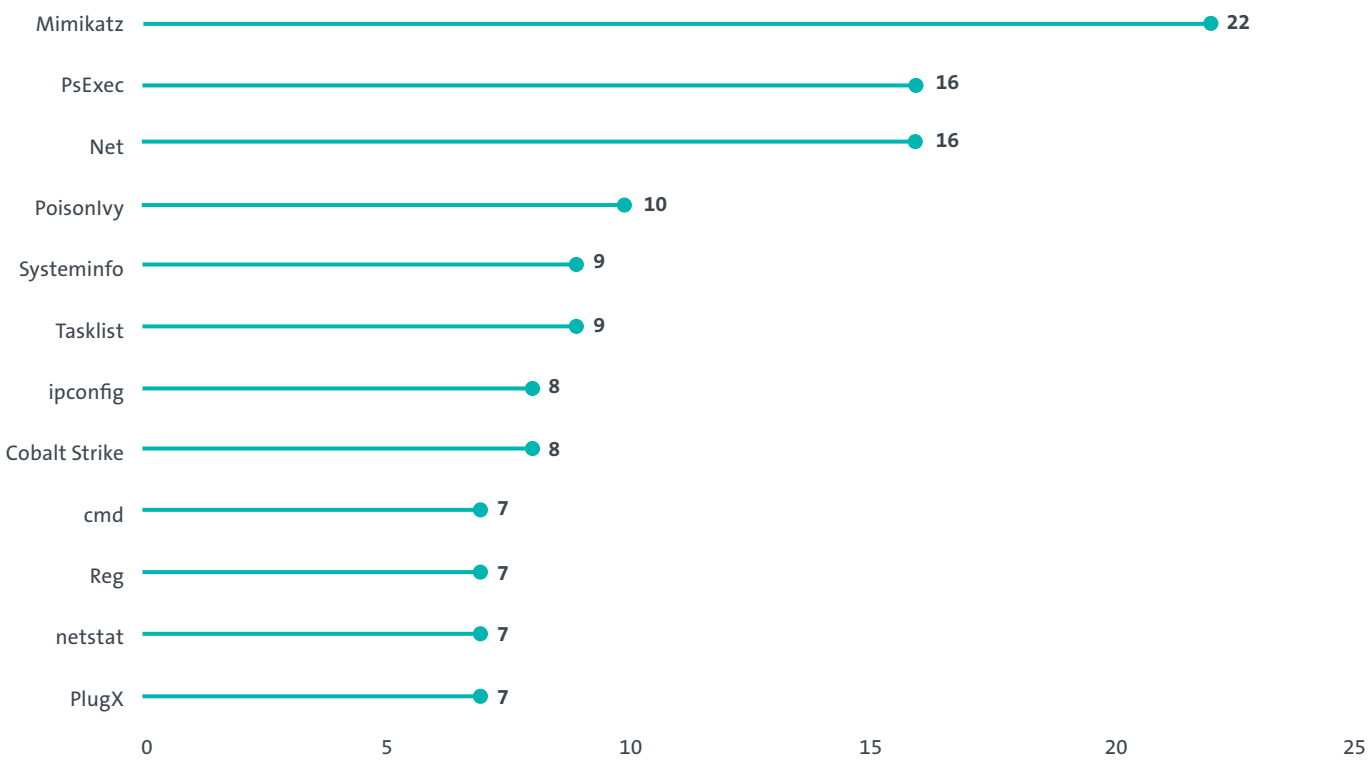
[12] https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Software più utilizzati in base agli attori
Da un'analisi dei gruppi APT e dei software da essi utilizzati emerge che i tool e i software Off-the-Shelf già integrati nel sistema operativo sono quelli utilizzati più di frequente. Questa osservazione è in linea con le esperienze di Costin Raiu.

La figura seguente mostra la top 10 dei software più utilizzati dagli 80 attori contenuti in ATT&CK.

Quali sono i cambiamenti più significativi dell'attività APT che sta osservando e quali ambiti sono maggiormente interessati da questi cambiamenti?

Vediamo che un numero crescente di gruppi sta facendo ricorso a tool pubblici come Empire Powershell, Metasploit, Cobalt Strike o Mimikatz. È difficile distinguerli l'uno dall'altro.



Contromisure e relativi effetti

Le contromisure agli attacchi mirati si fondano su una protezione di base consistente in misure preventive, quali l'utilizzo di patch aggiornate, l'implementazione di un'autenticazione a 2 fattori, connessioni internet solo attraverso proxy ecc. Queste misure sono talvolta sufficienti a deviare l'interesse degli attori non statali su altri obiettivi.

Nei capitoli precedenti abbiamo trattato gli aspetti fondamentali dei Threat Actors, che possono essere espressi come Intent (obiettivi strategici), Opportunity (area di attacco) e Capability (modi operandi). Proprio questi aspetti devono essere tenuti in considerazione per sviluppare contromisure adeguate che abbiano l'effetto più efficace possibile. La difesa più efficace in assoluto sarebbe eliminare l'obiettivo strategico (Intent). I governi o le aziende che non salvano dati non diventano obiettivi di un attore statale che pratica lo spionaggio e desidera ottenere un vantaggio dal furto di dati. Questa difesa, tuttavia, è applicabile in pochissimi casi. Se prendiamo in esame l'area di attacco disponibile, vediamo che negli ultimi anni questa non si è ridotta ma, al contrario, si è estesa. L'aumento della digitalizzazione, il salvataggio di dati nel cloud e i dispositivi everything connected, always-on e IoT contribuiscono a creare un'area di attacco di dimensioni enormi per le aziende, la società e i singoli soggetti.

Dobbiamo dunque basare le contromisure a nostra disposizione sull'aspetto delle capacità e dei modi operandi dei Threat Actors, cosa che spesso sfocia in una competizione testa a testa e che, in considerazione della molteplicità dei modi operandi, appare estremamente complessa.

A uno sguardo più attento, tuttavia, ci si accorge che la maggior parte dei modi operandi e dei software utilizzati può essere scoperta con metodi di riconoscimento che monitorano le attività del sistema.

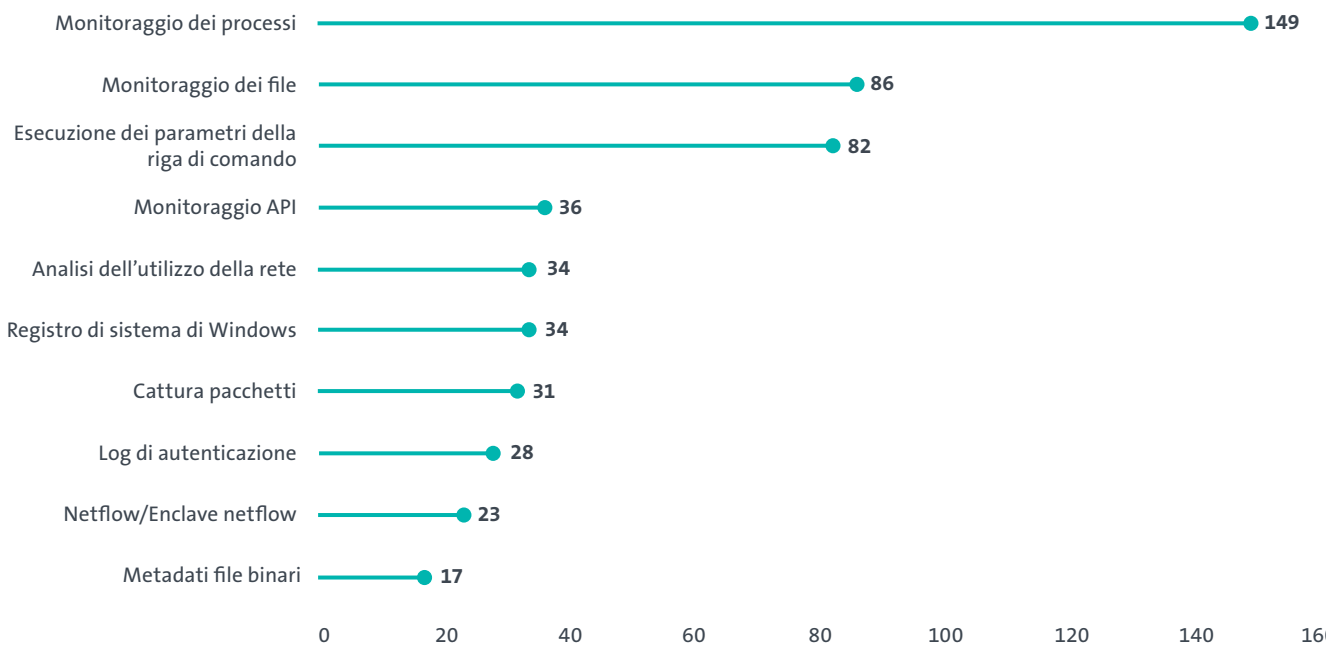
Metodi di riconoscimento con la maggiore copertura

La nostra analisi mostra che, dei modi operandi degli attori, la maggior parte può essere riconosciuta attraverso il monitoraggio delle operazioni di processo e di file. Questa constatazione implica che questi metodi di riconoscimento sono i più promettenti in quanto a possibilità di continuare a monitorare i modelli di attacco per essere in grado di seguire le attività di un aggressore dopo l'accesso iniziale.

La figura seguente con la top 10 dei metodi di riconoscimento chiarisce ulteriormente questo concetto:

Quali sono gli errori tipici che le organizzazioni commettono nel prepararsi a un attacco APT e in che modo rispondono a una ATP?

Nella maggior parte dei casi, le organizzazioni concentrano i propri sforzi nell'impedire che un hacker esterno possa accedere alle risorse interne, ma poche adottano misure per individuare un hacker una volta che quest'ultimo è entrato nella rete interna.



I metodi di riconoscimento delle attività di processo riconoscono la maggior parte dei modi operandi utilizzati dagli attori. Le attività degli utenti e delle reti forniscono ulteriore contesto.

Attività di sistema

L'esecuzione di codice controllata dagli attori è un presupposto fondamentale per raggiungere l'obiettivo strategico degli attori. Per seguire il modello di attacco degli attori, i metodi di riconoscimento più efficaci dei modi operandi sono il monitoraggio dei processi, dei file e delle modifiche nel registro di sistema di Windows. Anche se queste forme di riconoscimento sono le più efficaci, bisogna prevedere un volume di dati e un tuning molto elevati. I processi, i collegamenti di rete, le operazioni su file e registro di sistema devono essere compresi appieno.

Attività degli utenti e delle reti

Oltre al monitoraggio delle attività di sistema, i dati di rete e i log delle autenticazioni degli utenti portano alla luce la maggior parte dei modi operandi degli attori.

Cosa fa Swisscom

Gli attacchi mirati stanno diventando sempre più probabili e i mezzi tecnologici attualmente disponibili spesso non sono sufficienti per tenere testa alle capacità degli attori informatici professionisti. Per questi motivi, Swisscom utilizza un modello di sicurezza basato sul rischio, che promuove una forte cultura della sicurezza all'interno dell'azienda attraverso la formazione dei collaboratori, che coinvolge la community nella cultura della sicurezza per es. attraverso il programma Bug Bounty[13] e che presuppone misure di sicurezza preventive fondamentali come per es. le applicazioni di Whitelisting e Patching, e la limitazione del traffico di rete e degli allegati e-mail. La prevenzione è solo un aspetto parziale che, alla fine, è comunque destinato a fallire di fronte ad attori altamente motivati. È quindi necessario assumere un atteggiamento proattivo e capire le Tactics, Techniques and Procedures degli attori, facendo poi confluire le informazioni ottenute nel rilevamento delle minacce. Denominiamo questo approccio Threat Intelligence e lo poniamo alla base dell'attività di rilevamento, per esempio simulando un attacco mirato tramite Red Teaming, andando alla ricerca di rischi non ancora rilevati nella rete aziendale tramite Threat Hunting e confrontandoci regolarmente con altre aziende dello stesso settore, all'interno di Sharing Group.

Red Teaming

Gli hacker sono sempre un passo avanti; quindi, ci mettiamo noi stessi nei panni di un hacker. Nel 2015 Swisscom ha deciso di percorrere nuove strade ed è stata la prima azienda svizzera a istituire un Read Team ufficiale. Il Red Team è formato da un piccolo gruppo di collaboratori di Swisscom che eseguono attacchi quanto più possibile realistici contro l'infrastruttura e i servizi di Swisscom. Si tratta di Ethical Hackers, vale a dire di hacker bene intenzionati, che eseguono attacchi contro Swisscom ma NON contro le applicazioni e i dati degli utenti finali.

Quali sono i loro obiettivi?

- Individuare vulnerabilità e mostrarne gli effetti prima che lo faccia qualcun altro
- Testare il Blue Team e, in questo modo, aiutare l'azienda a sviluppare contromisure e a migliorare le procedure
- Apprendere dagli incidenti di altre aziende e testare se si sarebbero potuti verificare anche all'interno di Swisscom

Gli attacchi mirati stanno diventando sempre più probabili e i mezzi tecnologici attualmente disponibili spesso non sono sufficienti per tenere testa alle capacità degli attori informatici professionisti.

[13] https://www.swisscom.ch/en/about/company/portrait/network/security/bug-bounty.html

Threat Hunting

L'attività di Threat Hunting è finalizzata a individuare minacce ancora sconosciute. Non sostituisce un Security Operation Center (SOC) funzionante, ma utilizza metodi in parte automatizzati, e pure manuali, per il riconoscimento di comportamenti di attacco e modelli che non sono riconoscibili dai meccanismi di protezione esistenti. Questa procedura fornisce per esempio nuovi metodi di riconoscimento. Il CSIRT di Swisscom esegue regolarmente sessioni di Threat Hunting per individuare l'esistenza di rischi all'interno della rete Swisscom. A questo riguardo, il framework ATT&CK viene spesso utilizzato come riferimento per comprendere le Tactics e le Techniques dei singoli attori. In seguito a questa attività, il CSIRT pubblica periodicamente nuovi metodi di riconoscimento per SIGMA[14] e YARA[15] e li rende accessibili alla community. SIGMA è un formato di firma generico e aperto con il quale vengono descritti una tantum dati di log rilevanti come riconoscimento, che diventano utilizzabili per diversi sistemi SIEM e di log. SIGMA è uno dei pochi tool in grado di descrivere gli attacchi con le Tactics e le Techniques di ATT&CK e che rende il riconoscimento direttamente utilizzabile per altri soggetti. Con YARA è possibile creare firme e riconoscimenti propri che possono essere utilizzati sia per file che per Memory Scan. Il CSIRT di Swisscom emana periodicamente regole YARA per toolset di hacker e li condivide con public community fra cui, per esempio, signature base di Florian Roth[16] o altre community chiuse.

Come già menzionato nei capitoli precedenti, dobbiamo capire che gli attacchi non vengono eseguiti da macchine, bensì da persone; di conseguenza, sono necessarie persone anche per attivare una reazione. Per questo Swisscom utilizza diversi Security Operation Center (SOC) per poter monitorare sistematicamente le potenziali attività degli hacker. Gli analisti del CSIRT di Swisscom si attivano non appena viene rilevata un'attività che indica attacchi specificamente mirati all'infrastruttura IT di Swisscom.

Sharing Group e Community

Oltre a condividere informazioni sulla base di SIGMA e YARA, il CSIRT di Swisscom e i collaboratori che ne fanno parte sono membri attivi in molti Trust Group finalizzati alla collaborazione operativa quotidiana di CSIRT, SOC e Threat Intelligence Team. Obiettivo di questi Trust Group è favorire l'incontro tra persone con gli stessi problemi nella prassi quotidiana e semplificare lo scambio di esperienze. Swisscom condivide regolarmente all'interno di questi sharing group e community informazioni su osservazioni e rischi attuali, nonché su indicatori di software dannosi e attacchi.

Protezione delle aziende più completa grazie al riconoscimento precoce e a una reazione professionale in caso di cyber attacchi – disponibile come servizio

Al giorno d'oggi sono disponibili enormi quantità di informazioni aziendali e personali su diverse fonti di dati (reti, applicazioni, terminali, social media, cloud, darknet e molte altre). Al costante aumento dell'integrazione in rete e della digitalizzazione si associa una maggiore stratificazione delle minacce. Risulta pertanto essenziale riconoscere tempestivamente gli incidenti rilevanti per la sicurezza.

Un'attività professionale di Threat Detection & Response richiede processi e tool specifici, un'esperienza pluriennale e collaboratori altamente specializzati. Per un'azienda non è praticamente più possibile comprendere da sola cyber attacchi sempre nuovi e reagirvi adeguatamente. L'affiancamento di un partner competente diventa quindi

[14] https://github.com/Neo23x0/sigma/

[15] https://yara.readthedocs.org

[16] https://github.com/Neo23x0/signature-base

indispensabile. Da anni Swisscom protegge in modo efficace l'infrastruttura di rete, i dati dei clienti e dei prodotti nonché se stessa contro le minacce informatiche. L'azienda utilizza la propria esperienza per ridurre al minimo i rischi informatici in collaborazione con i propri clienti. Una buona visualizzazione dei dati favorisce il riconoscimento precoce di potenziali incidenti relativi alla sicurezza. L'analisi tempestiva e la giusta reazione in caso di security incident migliorano il livello di sicurezza e l'utilizzo delle risorse all'interno dell'azienda.
Con il servizio Threat Detection & Response, i clienti aziendali possono scegliere tra quattro versioni del servizio a seconda dell'entità del supporto che desiderano ricevere da Swisscom ai fini della cyber security. Qui di seguito indichiamo riassuntivamente le versioni disponibili:

Security Analytics as a Service: i clienti ricevono, attraverso un dashboard, una panoramica dei potenziali incidenti relativi alla sicurezza sulla base di dati di log dell'azienda definiti.

Security Operation Center (SOC) as a Service: in aggiunta a Security Analytics, i clienti ricevono analisi corredate da raccomandazioni d'intervento concrete e un accesso diretto agli specialisti del SOC di Swisscom. Da oltre 10 anni forniamo servizi di SOC per aziende svizzere sul territorio nazionale e all'estero. I nostri analisti SOC sono in grado di interpretare i Security Events & Incidents in modo rapido e competente.

Computer Security Incident Response Team (CSIRT) as a Service: per analizzare e gestire incidenti critici relativi alla sicurezza è possibile richiedere l'assistenza di esperti di Swisscom che conducono il processo di Security Incident Management. Questi esperti con comprovata esperienza forniscono supporto ai clienti nell'accertamento delle prove e nella comunicazione a clienti e partner.

Threat Intelligence as a Service: i clienti vengono informati in modo proattivo in merito alla presenza di informazioni commerciali e personali sensibili della loro azienda all'interno di reti pubbliche e chiuse (per es. darknet).[17]

Conclusione

Nella maggior parte dei casi, gli attacchi mirati, in particolare di APT con obiettivi statali e strategici, non sono evitabili. La crescente digitalizzazione del mondo attira sempre più attori nel cyberspazio. Per questo dobbiamo aspettarci di poter diventare, prima o poi, un Target of Interest o, perlomeno, un Target of Opportunity. Gli attori hanno a disposizione un'ampia gamma di modi operandi nelle diverse fasi dell'attacco per le quali ricorrono sempre più spesso a tool Off-the-Shelf e a metodi Living-off-the Land. Le APT rappresentano il livello più alto degli attori informatici, tuttavia non sviluppano Zero Day Exploit per ogni operazione, ma ricorrono a metodi sicuri nell'ambito dei quali la persona rimane un bersaglio interessante per eludere i meccanismi di sicurezza e attivare l'esecuzione di codice dannoso.

Si sente spesso dire che agli hacker basta un'unica azione riuscita per poter entrare in un sistema. Come ha dimostrato la nostra analisi, possiamo controbattere che, se strutturiamo le nostre misure di riconoscimento in modo tale che i modi operandi degli attori possano essere riconosciuti, agli hacker basta commettere un unico errore per essere riconosciuti. Concentrarsi sul riconoscimento dell'esecuzione, sulla Execution Phase, rappresenta a questo riguardo un approccio molto promettente. Tuttavia, in particolare per le APT, è necessario aver compreso l'intero intrusion pattern prima di poter fermare l'attacco.

[17] Ulteriori informazioni e contatti su questo tema: www.swisscom.ch/detection