SOPHOS
Cybersecurity delivered.

Active Adversary Playbook 2022

I comportamenti, le tattiche e gli strumenti utilizzati dai cybercriminali nel 2021 e analizzati dagli esperti di Incident Response di Sophos

Autore: **John Shier**, Senior Security Advisor, CTO Office

Whitepaper Sophos giugno 2022

Introduzione

Difendere un'organizzazione contro minacce informatiche sempre più complesse e in costante evoluzione può essere un compito arduo. I cybercriminali continuano ad adattare le proprie strategie, con comportamenti e strumenti sempre più sofisticati. Sfruttano nuove vulnerabilità e programmi informatici legittimi per eludere il rilevamento e battere sul tempo i team di sicurezza informatica.

Per i responsabili IT e i team SecOps di un'organizzazione può essere difficile tenere il passo con i nuovi approcci di questi hacker. E lo è ancora di più quando si trovano ad affrontare attacchi mirati e attivi, sferrati da più di un autore, come quando un broker di accesso iniziale (initial access broker, IAB) riesce a infiltrarsi nei sistemi di una vittima e vende quell'accesso a una gang di ransomware, che intende usarlo nel proprio attacco.

L'Active Adversary Playbook 2022 segnala chi sono i principali antagonisti da cui occorre difendersi e offre una descrizione dettagliata degli strumenti e dei comportamenti utilizzati in attacchi reali e studiati dagli esperti di Incident Response di Sophos nel corso del 2021. Fa seguito all'Active Adversary Playbook 2021 e mostra l'evoluzione del panorama delle minacce.

Lo scopo di questo documento è aiutare i team di sicurezza a capire come agiscono gli active adversary durante gli attacchi e come riconoscere e proteggersi quando riescono a infiltrarsi nella rete.

I risultati si basano sui dati relativi alle indagini sugli incidenti svolte dal team Sophos Rapid Response nel 2021. Ovunque possibile, i dati vengono messi a confronto con i risultati di incident response forniti nell'Active Adversary Playbook 2021.

Dati Demografici Di Incident Response Per Il 2021

Il report si basa su 144 incidenti che hanno colpito organizzazioni di ogni dimensione e vari settori, situate in: Stati Uniti, Canada, Regno Unito, Germania, Italia, Spagna, Francia, Svizzera, Belgio, Paesi Bassi, Austria, Emirati Arabi Uniti, Arabia Saudita, Filippine, Bahamas, Angola e Giappone.

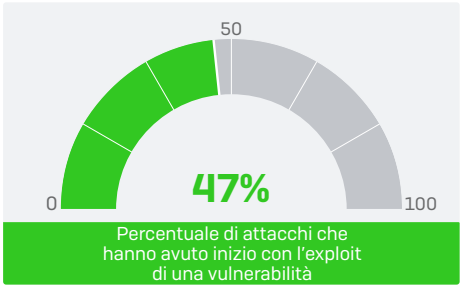
I settori più rappresentati nel sondaggio sono: industria manifatturiera (il 17% dei casi di incident response segnalati appartengono a questo settore), retail (14%), sanità (13%), IT (9%), edilizia (8%) e istruzione (6%). Per maggiori informazioni sui profili delle vittime, consulta le tabelle di dati nelle ultime pagine di questo report.

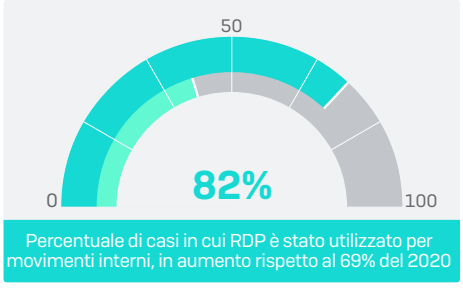
Dashboard: Anatomia Degli Attacchi Attivi Nel 2021

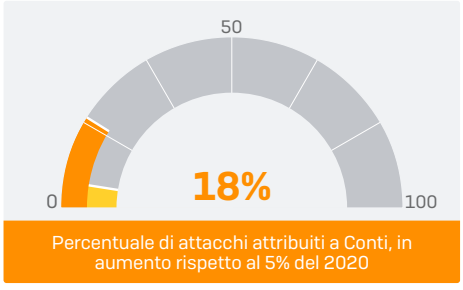
L'anno scorso, due dei principali sviluppi delle minacce informatiche si sono verificati a marzo e agosto 2021, con la segnalazione delle vulnerabilità ProxyLogon e ProxyShell nei server Microsoft Exchange. Come indicato recentemente dalla CISA e da altri enti governativi di sicurezza informatica, i bug ProxyLogon/ProxyShell sono stati ampiamente utilizzati dai cybercriminali. Non sorprende quindi che siano stati riscontrati in una quantità significativa degli incidenti su cui ha indagato Sophos nel 2021.

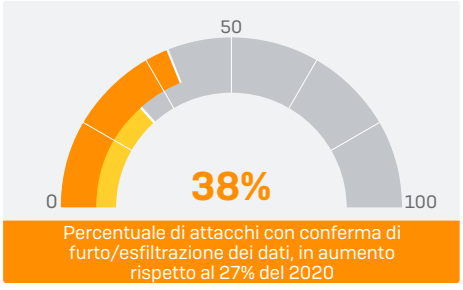
Dashboard: Anatomia Degli Attacchi Attivi Nel 2021

I risultati più salienti delle indagini di incident response









Con molta probabilità ci sono state molte più violazioni ProxyLogon/ProxyShell di quelle attualmente conosciute: è infatti possibile che gli hacker abbiano collocato web shell e backdoor sui sistemi delle vittime per mantenere la persistenza di accesso e che cerchino ora di rimanere inosservati, attendendo pazientemente l'opportunità di usare o vendere quell'accesso.

Questo ci porta a un altro sviluppo importante, che ha segnato il panorama delle minacce informatiche nel 2021: la sempre maggiore influenza e il potere dei broker di accesso iniziale (IAB).

Il successo degli IAB dipende dalla loro capacità di essere i primi a violare i sistemi di una vittima e a ottenere un accesso che possono rivendere. Di conseguenza, gli IAB sono anche i primi a fare la loro comparsa non appena emergono nuovi bug, nella speranza di riuscire a compromettere i sistemi della vittima prima che le patch vengano applicate in maniera estensiva. Il loro obiettivo è infiltrarsi nella rete della vittima e possibilmente svolgere attività di perlustrazione iniziali per capirne il valore patrimoniale, per poi rivendere l'accesso ad altri cybercriminali (ad esempio gli autori di attacchi ransomware), che potrebbero sferrare un attacco persino vari mesi dopo l'intrusione iniziale.

Come emerge dal Sophos 2022 Threat Report, l'aumento degli IAB riflette la maggiore "professionalizzazione" degli attacchi in un mercato delle minacce informatiche che include un numero in costante incremento di fornitori di servizi specializzati. Il successo del Ransomware as-a-Service (RaaS) è un ulteriore esempio di questa tendenza.

Le prove delle analisi forense emerse durante le indagini di incident response nel 2021 hanno rivelato casi in cui le organizzazioni stavano subendo attacchi per mano di più cybercriminali contemporaneamente, inclusi IAB, gang di ransomware, cryptominer e a volte persino più autori di attacchi ransomware allo stesso momento. Questo è uno sviluppo che continuerà a plasmare il panorama delle minacce informatiche nel 2022 e negli anni a seguire.

Come conseguenza di queste attività, sta aumentando anche il periodo di tempo di permanenza degli hacker nei sistemi delle vittime. Altri cybercriminali che adottano strategie a lungo termine e che pertanto possono trovarsi (a volte contemporaneamente) nelle reti delle vittime per un periodo esteso includono gli autori di botnet e gli hacker che utilizzano piattaforme di distribuzione del malware e dropper.

Questi sviluppi vengono discussi in maniera più approfondita di seguito.

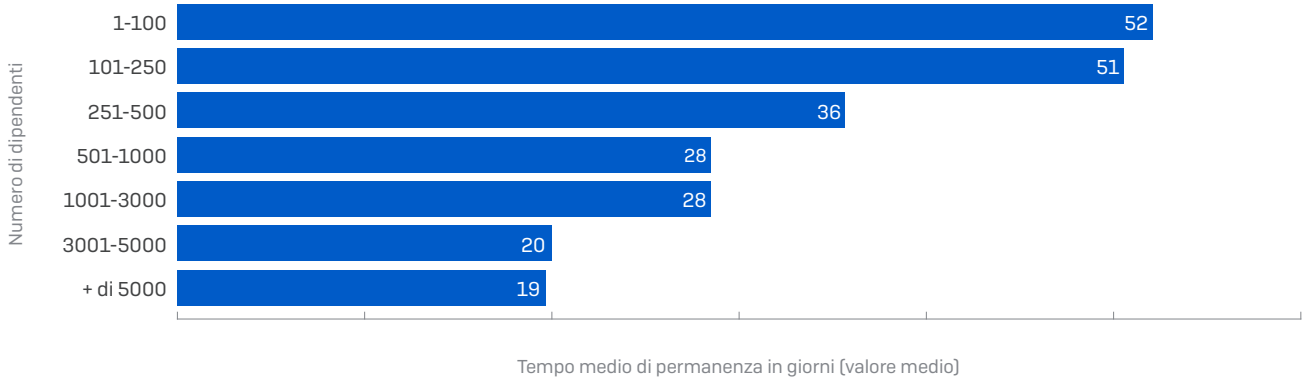
Gli Intrusi Invisibili

Le statistiche sugli incidenti mostrano che il valore mediano del tempo di permanenza sui sistemi è aumentato di un terzo tra il 2020 e il 2021, passando da 11 a 15 giorni. È stata riscontrata una variazione significativa nei dati dei vari attacchi, soprattutto per quanto riguarda il ransomware, che mostra una permanenza minore (11 giorni, in calo rispetto ai 18 del 2020), mentre per altri tipi di intrusione i tempi sono molto più estesi, con un valore mediano di permanenza pari a 34 giorni.

Variazione Nei Tempi Medi di Permanenza Degli Intrusi (Valore Mediano)

Come già ipotizzato, la durata più estesa dei tempi di permanenza potrebbe riflettere la presenza di uno IAB. Per imprese o settori di dimensioni minori, come quello dell'istruzione (tempo medio di permanenza degli intrusi: 34 giorni), i tempi di permanenza più estesi potrebbero anche riflettere quanto è difficile per i team IT interni poter individuare proattivamente le minacce, svolgere indagini e rispondere ad avvisi e potenziali incidenti.

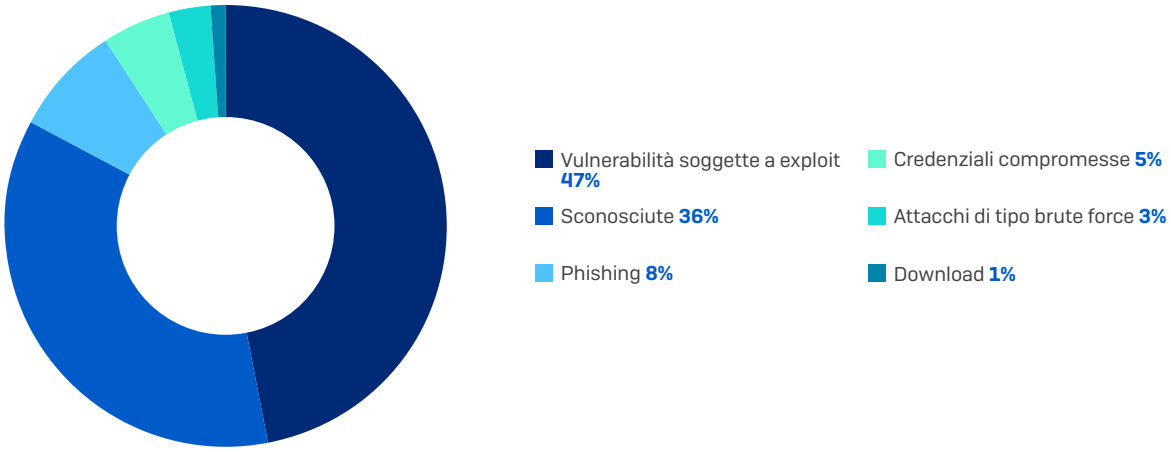
Tempo Medio Di Permanenza Degli Intrusi Per Dimensioni Dell'Azienda (Valore Mediano)



Le Cause All'Origine Degli Attacchi

Non è sempre possibile, o semplice, identificare la causa all'origine di un attacco. A volte, quando gli incident responder entrano in azione, i cybercriminali hanno già eliminato ogni traccia delle proprie attività; in altri casi, i team di IT security hanno già formattato o eseguito un re-imaging dei computer compromessi. Nonostante questo, i dati dimostrano che, di tutti gli incidenti analizzati da Sophos, gli exploit di vulnerabilità per le quali non sono state applicate patch (ad es. ProxyLogon o ProxyShell) sono stati la causa all'origine di quasi la metà (47%) degli incidenti informatici osservati nel 2021.

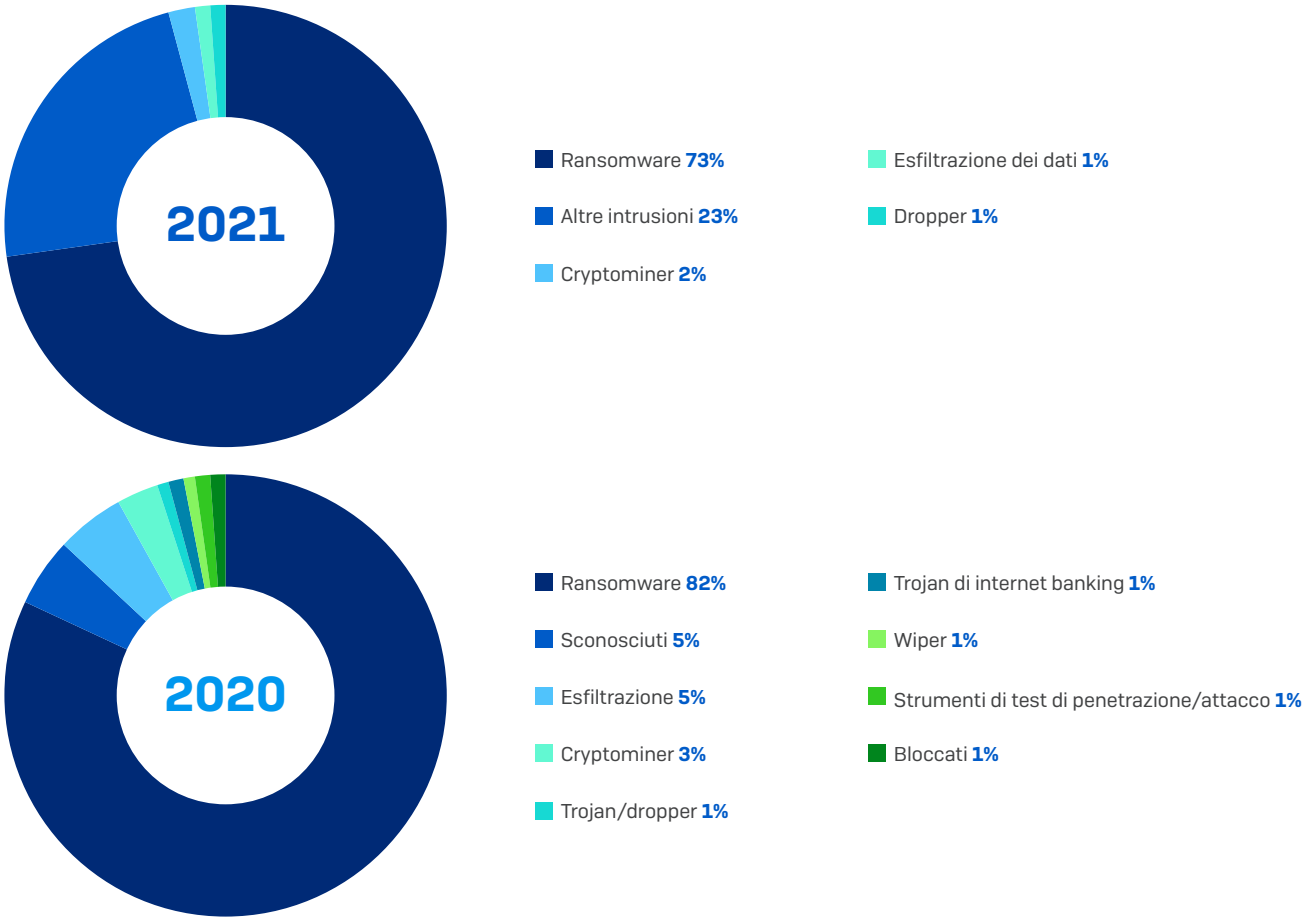
Cause All'Origine Degli Attacchi



I Principali Tipi Di Attacco

La detonazione del ransomware è quasi sempre il punto in cui un attacco diventa visibile per il team di IT security. Pertanto, non sorprende affatto che il ransomware sia stato il protagonista del 73% degli incidenti per i quali Sophos ha intrapreso azioni di risposta nel 2021. Il ransomware è stato il tipo di attacco prevalente anche nel 2020, con l'82% dei casi (probabilmente la percentuale elevata riflette il minore set di dati). Per quanto riguarda l'esfiltrazione dei dati, riscontrata solo nell'1% degli incidenti, gli esperti di incident response ritengono che probabilmente queste minacce si sarebbero evolute in attacchi ransomware, ma che sono state identificate e neutralizzate in tempo.

Tipi di attacco



Il secondo tipo di attacco in ordine di prevalenza, identificato durante le indagini di incident response, è stata la categoria "altri tipi di intrusione", con il 23% degli incidenti. In questo report, il termine "altri tipi di intrusione" definisce le intrusioni che non hanno implicato ransomware o altri tipi di attacco.

Spesso un'intrusione è il risultato di una vulnerabilità soggetta a exploit per la quale non sono state applicate patch (come ProxyLogon e ProxyShell), ma può anche derivare dall'utilizzo improprio di servizi di accesso

remoto o VPN non protette, da credenziali rubate o da sviste di sicurezza (ad es. quando vengono lasciati punti di ingresso esposti a Internet).

Il punto è che le intrusioni sono state rilevate e neutralizzate prima che un payload devastante potesse essere distribuito sui sistemi della vittima. È ragionevole supporre che alcune di queste intrusioni, se non persino tutte, siano state parte dell'inventario degli IAB: accessi "messi da parte" in attesa di essere venduti a un altro cybercriminale. Se le intrusioni non fossero state rilevate, è probabile che molte si sarebbero evolute in veri e propri attacchi ransomware.

I cryptominer sono stati il principale tipo di attacco nel 2% degli incidenti analizzati. Spesso la presenza di cryptominer pericolosi viene rilevata per via dell'impatto che hanno sulla performance del sistema, in quanto le attività illecite di mining di criptovalute sottraggono capacità di elaborazione ai computer. Potrebbe sembrare più facile ignorare i cryptominer, considerandoli una minaccia meno pericolosa, che genera solamente seccature trascurabili. Tuttavia, il fatto che siano presenti nella rete dimostra che esiste un punto di ingresso vulnerabile e questo potrebbe essere foriero di problemi informatici molto più seri in futuro.

Lo stesso vale per i dropper e i sistemi di distribuzione del malware in senso lato, che sono progettati per distribuire, caricare o installare altri payload pericolosi sul sistema di una vittima. Sono elementi che spianano la strada a un attacco e forniscono una piattaforma per altri componenti pericolosi, come le backdoor e i ransomware. I team di sicurezza informatica devono pertanto considerare la presenza di dropper e sistemi di distribuzione del malware (inclusi Trickbot, Emotet e altri) altrettanto seria quanto quella delle più pericolose gang di ransomware, poiché spesso questi elementi sono precursori di attacchi più gravi.

Uno Spazio Molto Affollato

I tipi di attacco non si escludono a vicenda. Come abbiamo già accennato, è possibile trovare contemporaneamente più di un cybercriminale (inclusi IAB, gang di ransomware e cryptominer) nella rete di una singola vittima.

Ad esempio, sebbene i cryptominer fossero il principale tipo di attacco solo nel 2% dei casi di incident response osservati, sono stati riscontrati anche nel 7% degli incidenti di ransomware. Spesso i cryptominer analizzano i sistemi per individuare e rimuovere altri miner nelle reti infettate, ma possono tranquillamente coesistere con altre minacce, come appunto il ransomware.

Gli attacchi simultanei rilevati da Sophos nel 2021 includono un incidente con ransomware Atom Silo e due cryptominer e un incidente con doppio attacco ransomware di Netwalker e REvil. Questa tendenza continuerà anche nel 2022.

La Toolbox Dei Cybercriminali

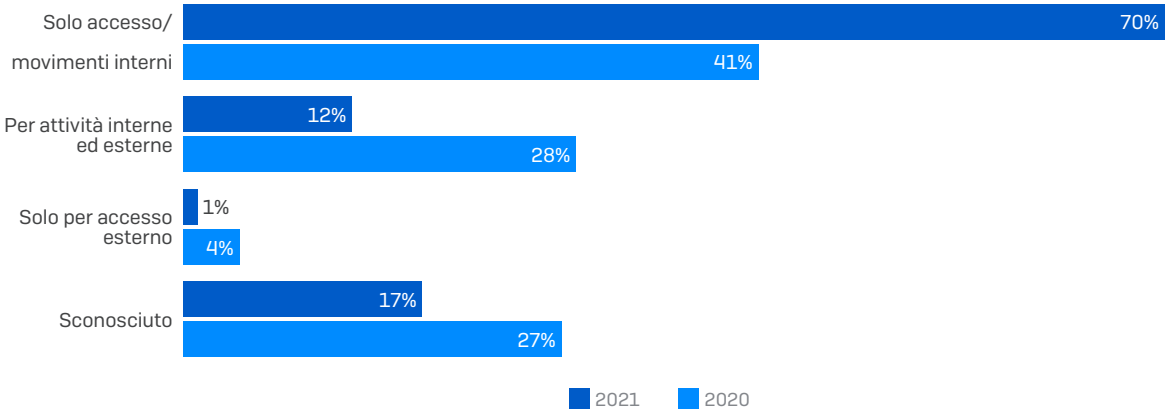
Il Remote Desktop Protocol (RDP) E' Una Delle Principali Minacce Interne

Il Remote Desktop Protocol (RDP) ha svolto un ruolo importante in almeno 83% degli attacchi, una tendenza in aumento rispetto al 73% del 2020. Nell'82% dei casi ne è stato osservato un uso interno, mentre il suo uso esterno è stato riscontrato nel 13% degli incidenti. Queste statistiche possono essere confrontate con i dati del 2020, quando ammontavano rispettivamente al 69% e al 32%.

Tuttavia, è interessante considerare il modo in cui i cybercriminali utilizzano l'RDP. In meno di tre quarti (70%) degli incidenti causati da RDP, questo strumento è stato utilizzato *esclusivamente* per l'accesso interno e per i movimenti laterali, con un incremento significativo rispetto al 41% del 2020.

L' RDP è stato impiegato per l'accesso esterno *solo* in appena l'1% dei casi, in calo rispetto al 4% del 2020; inoltre, solo nel 12% degli attacchi i cybercriminali hanno utilizzato l'RDP sia per l'accesso esterno che per i movimenti interni, con una percentuale più che dimezzata rispetto al 2020 (quando era pari al 28%).

L'uso Del Remote Desktop Protocol (RDP) da parte dei cybercriminali



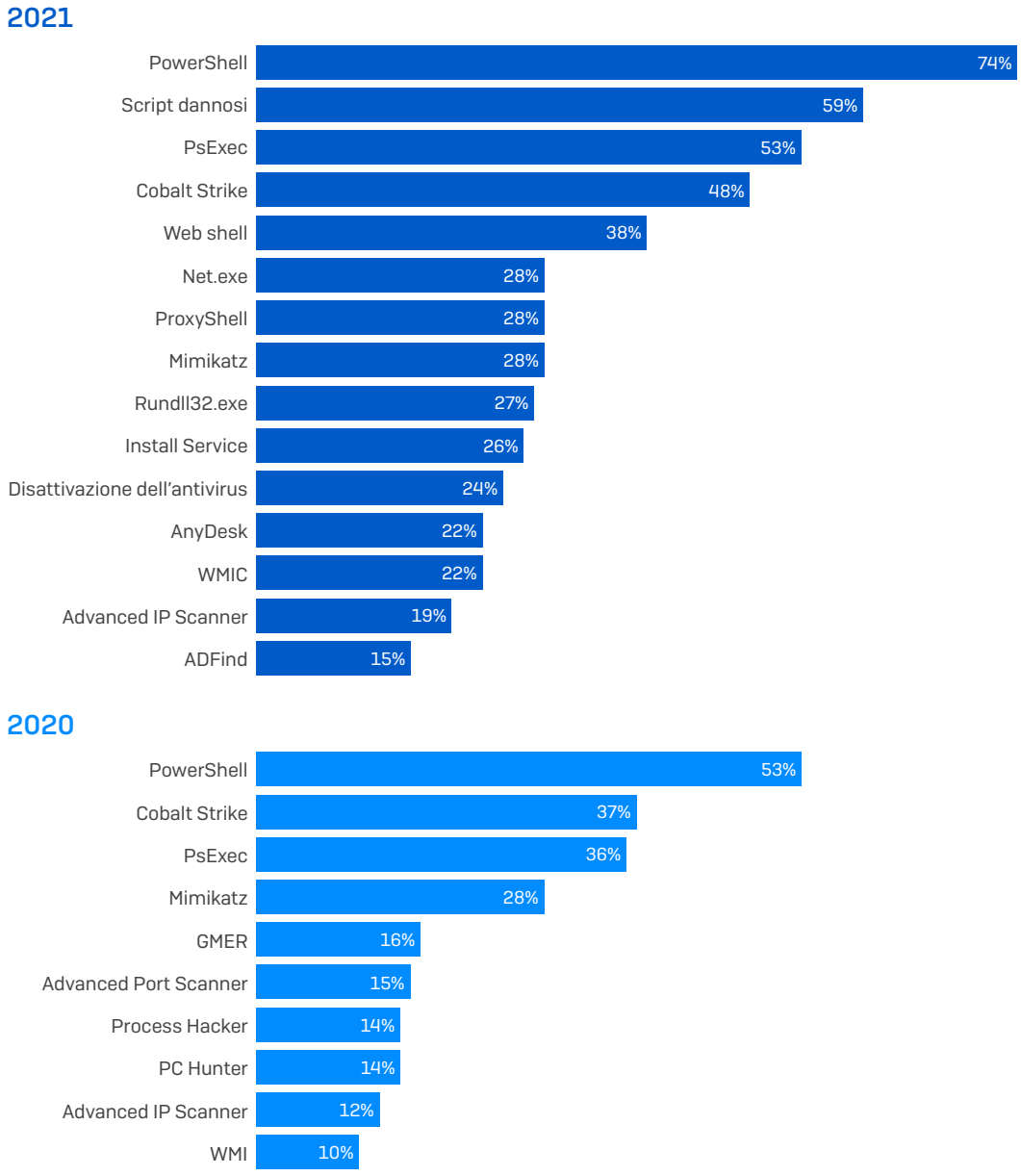
La diminuzione dell'uso di RDP per l'accesso esterno è probabilmente una conseguenza diretta del potenziamento delle misure di sicurezza, che includono appunto la disattivazione di questo servizio. L' RDP rimane tuttavia accessibile all'interno del perimetro di rete e difendere questo accesso con una protezione di livello avanzato deve essere uno degli obiettivi principali dei team di sicurezza.

Il Toolset Di Attacco Nel 2021

Il grafico riportato di seguito mostra gli "artefatti" (inclusi strumenti, tecniche e servizi) individuati più frequentemente nei toolset dei cybercriminali nel 2021. Molti sono strumenti legittimi, che possono essere utilizzati dai professionisti dell'IT per scopi perfettamente innocui. Sono molto ricercati tra i cybercriminali, perché permettono di mimetizzare le loro azioni tra le regolari operazioni informatiche della vittima e di svolgere attività come furto di credenziali, individuazione delle risorse, movimenti laterali, esecuzione del malware e altro.

La quantità e la natura di questi artefatti sottolinea maggiormente quanto sia difficile per i team di sicurezza identificare le attività di rete dannose tra quelle legittime.

Gli Artefatti Utilizzati Più Frequentemente Negli Attacchi



Un'analisi più approfondita degli elementi utilizzati durante gli attacchi rivela il tipico playbook per gli attacchi informatici nel 2021.

Gli Artefatti Che Compongono I Toolset

Gli artefatti identificati durante le indagini di incident response possono essere suddivisi in tre categorie: strumenti legittimi e di hacking, file binari di Microsoft e altri artefatti (script, tecniche, servizi e altro).

Le indagini di incident response hanno individuato 525 artefatti diversi, un dato molto più alto rispetto ai 132 rilevati nel 2020 (sebbene anche i campioni analizzati fossero di più), inclusi 209 strumenti legittimi e di hacking, 107 file binari di Microsoft e altri 209 artefatti.

Strumenti Legittimi E Di Hacking

Questi strumenti includono software utilizzati per assistere gli attacchi. Cobalt Strike (48%) e Mimikatz (28%) si trovano ai primi due posti, come nel 2020; seguono AnyDesk (22%), Advanced IP Scanner (19%) e ADFind (15%). Confrontando le statistiche con quelle del 2020, la diffusione di Cobalt Strike è aumentata (rispetto al 37% dell'anno precedente), Mimikatz è rimasto stabile (mantenendosi al 28%) e tre nuovi strumenti sono entrati nella top 5.

Cobalt Strike è una suite commerciale di strumenti di exploit, realizzata per aiutare i team di sicurezza a ricreare vari scenari di attacco. I cybercriminali provano a utilizzare un "beacon" di Cobalt Strike per creare una backdoor su un computer infettato. I beacon possono essere configurati per eseguire comandi, scaricare file e avviare altri software, nonché per inoltrare comandi ad altri beacon installati nella rete della vittima e instaurare una comunicazione con il server di Cobalt Strike. Se Cobalt Strike viene rilevato sulla rete, occorre indagare subito.

Anche il secondo strumento in ordine di diffusione, **Mimikatz**, era stato originariamente progettato come strumento di sicurezza offensivo; può essere utilizzato per prelevare password e altre credenziali degli account, al fine di sfruttarle in un attacco.

Gli hacker si servono di scanner di rete legittimi, come **Advanced Port Scanner** e **IP Scanner**, per generare un elenco di IP e nomi dei dispositivi, che consente loro di colpire in maniera mirata le infrastrutture e i computer più importanti della vittima.

L'utilizzo improprio dello strumento di gestione IT legittimo **AnyDesk** sta diventando molto più comune, poiché offre ai cybercriminali accesso diretto a un computer, con la possibilità di controllare mouse e tastiera e la capacità di vedere lo schermo. Tra i software più diffusi del 2021 si trovano anche servizi di accesso remoto quali **TeamViewer**, **Screen Connect**, **Atera RMM** e **Splashtop**.

Process Hacker, **PCHunter** e **GMER** sono tutti strumenti legittimi che includono driver del kernel. Se un cybercriminale riesce a installare il kernel giusto, spesso può disattivare i prodotti di sicurezza.

File Binari Di Microsoft

La separazione tra strumenti Microsoft e strumenti generici dimostra come gli hacker abbiano sviluppato tattiche di tipo "living off the land". Questi strumenti sono firmati digitalmente da Microsoft. Come prevedibile, **PowerShell** (74%) si trova in cima alla classifica, seguito da **PsExec** (53%), "**net.ex**e" (28%), "**rundll32.exe**" (27%) e lo strumento da **riga di comando WMI** (WMIC) (22%). Confrontando i dati con quelli del 2020, l'uso di PowerShell, PsExec e WMIC è aumentato nel 2021.

Lo strumento "net.exe" è stato osservato in diverse fasi di attacco, principalmente in quella di individuazione, mentre "rundll32.exe" è stato utilizzato ampiamente per l'esecuzione e per eludere i sistemi di difesa.

Altri strumenti Microsoft che potrebbero indicare la presenza di un hacker in agguato all'interno della rete sono "**whoami.exe**", **Task Scheduler** (per mantenere la persistenza) e "**schtasks.exe**" (per eseguire codice dannoso). L'uso di questi strumenti va monitorato attentamente.

Altri Artefatti

Questa categoria include sia strumenti che tecniche, ad esempio: tentativi di disattivare la protezione, vulnerabilità come ProxyShell, uso di servizi cloud quali **Mega.io**, altri tipi di malware, infezioni secondarie e l'uso di protocolli di trasporto.

Nel 59% degli incidenti analizzati, sono stati rilevati **script dannosi** (diversi da PowerShell). Gli script dannosi sono codici software che permettono agli hacker di svolgere attività pericolose. Alcuni esempi di script

utilizzati in maniera impropria dai cybercriminali includono gli script batch e da riga di comando DOS/CMD, gli script Python (una raccolta di comandi inseriti in un file, da eseguire come programma) e VBScript (script Visual Basic che possono essere eseguiti su Windows o Windows Explorer).

Le web shell sono state il secondo tipo di minaccia in ordine di diffusione (rilevate nel 38% degli incidenti), ma anche la presenza di ProxyShell (28%) e ProxyLogon (11%) è degna di nota. A completare la top 10 troviamo: l'installazione di servizi, la disattivazione della protezione, il dump di LSASS, la creazione di account non autorizzati, la modifica del registro e la cancellazione dei log.

Esfiltrazione Dei Dati

Nel 2021 **Rclone** è comparso nell'elenco dei principali artefatti utilizzati per l'esfiltrazione. Rclone è uno strumento da riga di comando che si connette a un'ampia selezione di provider di archiviazione nel cloud (ad es. Mega) e nel 2021 è stato il programma più utilizzato per l'esfiltrazione dei dati. Altri provider di archiviazione nel cloud osservati nelle statistiche di quest'anno sono stati: **Dropbox**, **DropMeFiles**, **M247**, **pCloud** e **Sendspace**.

Oltre a Rclone, altri strumenti di esfiltrazione dei dati rilevati nelle indagini sugli incidenti sono: **Megasync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP** e **Ngrok**.

La comparsa di strumenti di esfiltrazione nelle toolbox del 2021 non sorprende, visto che il 38% di tutti gli incidenti rilevati prevedeva l'esfiltrazione dei dati, con un aumento rispetto al 27% del 2020. Altri incidenti (8% in totale) hanno mostrato segni di attività di raccolta dei dati e preparazione per una loro potenziale rimozione. Nei casi di avvenuta esfiltrazione, i dati suggeriscono che le informazioni prelevate illecitamente sono poi state divulgate nel 46% degli incidenti.

Generalmente, i cybercriminali rimuovono le informazioni nell'ultima fase di attacco prima della distribuzione del ransomware. Le analisi sugli incidenti condotte da Sophos mostrano che nel 2021 il valore mediano dell'intervallo tra l'esfiltrazione dei dati e la distribuzione del ransomware era di circa 44 ore. L'intervallo medio era di poco più di quattro giorni (4,28), mentre il valore mediano dell'intervallo era appena sotto i due giorni (1,84).

Indipendentemente da come viene calcolata la media, il punto è che dopo l'esfiltrazione i team di sicurezza hanno potenzialmente un certo lasso di tempo per impedire che venga attuata la fase finale e più distruttiva dell'attacco. Di conseguenza, è fondamentale attribuire la massima priorità di indagine a qualsiasi rilevamento di strumenti noti per essere utilizzati per esfiltrare dati.

Combinazione Di Più Strumenti

Le indagini sugli incidenti hanno rivelato una tendenza regolare a utilizzare una combinazione di più strumenti sulle reti delle vittime, il che costituisce un potente segnale di allarme per i team di IT security (in alcuni casi sono disponibili dati comparativi del 2020):

- Nel 2021, la combinazione tra PowerShell e script non PowerShell dannosi è stata osservata nel 64% dei casi
- La combinazione tra PowerShell e Cobalt Strike è stata riscontrata nel 56% dei casi, rispetto al 58% del 2020
- PowerShell e Cobalt Strike sono stati rilevati nel 51% dei casi, rispetto al 49% del 2020
- PowerShell, script dannosi e Cobalt Strike sono stati individuati nel 42% dei casi
- PowerShell, script dannosi e PSExec sono stati osservati nel 38% dei casi
- PowerShell, Cobalt Strike e PsExec sono stati identificati nel 33% dei casi, in aumento rispetto al 12% del 2020
- Cobalt Strike e Mimikatz sono stati rilevati contemporaneamente nel 16% dei casi

Come per l'anno scorso, anche quest'anno le correlazioni di cui sopra sono di fondamentale importanza, poiché il loro rilevamento può essere un importante campanello di allarme che indica un attacco imminente o che conferma la presenza di un attacco attivo.

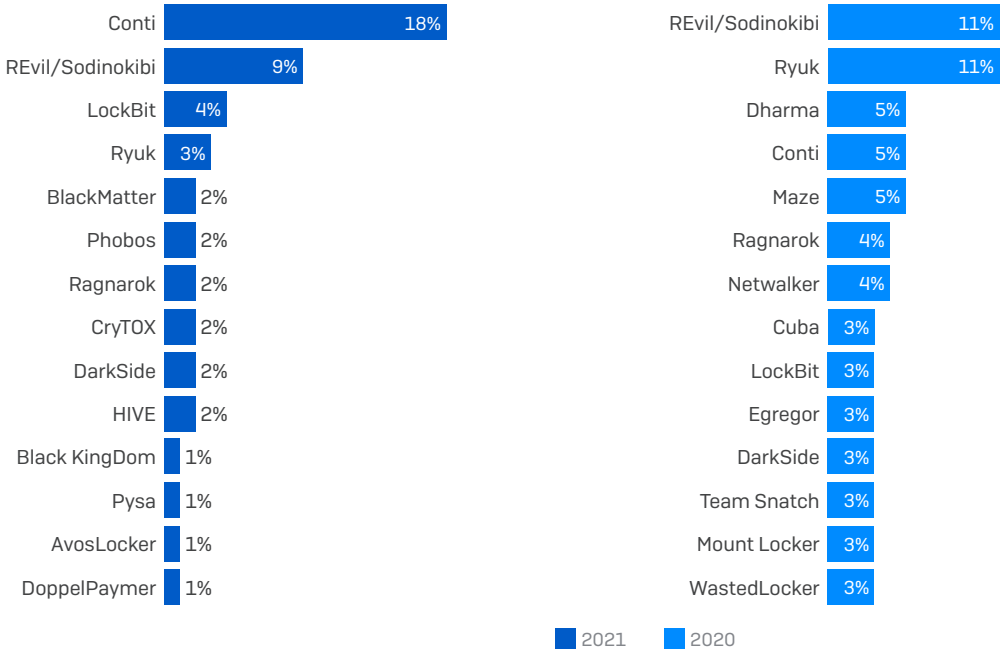
I Principali Cybercriminali Del Ransomware Del 2021

Nei 144 incidenti analizzati, sono stati identificati 41 cybercriminali del ransomware. Di questi, circa due terzi (28) sono nuove gang osservate per la prima volta nel 2021. 18 gang di ransomware emerse negli incidenti del 2020 sono scomparse dall'elenco nel 2021, il che dimostra senza ombra di dubbio quanto sia diventato affollato, dinamico e complesso il panorama delle minacce informatiche e quanto tutto ciò complichi il lavoro dei team di cybersecurity.

Sotto vari punti di vista, il 2021 è stato l'anno di Conti, un prolifico RaaS identificato in poco meno di un incidente su cinque (18%), tra quelli analizzati da Sophos. Occorre tuttavia notare che il ransomware REvil è stato individuato in 10 incidenti, nonostante abbia smesso di essere operativo a luglio del 2021 (facendo una breve ricomparsa a settembre 2021 e successivamente nel 2022).

Altre famiglie di ransomware prevalenti nel 2021 includono DarkSide, il RaaS responsabile del famoso attacco a Colonial Pipeline negli Stati Uniti, e Black KingDom, una delle "nuove" famiglie di ransomware, emersa a marzo 2021 in seguito all'individuazione della vulnerabilità ProxyLogon.

Distribuzione Dei Principali Cybercriminali Del Ransomware



Circa un quarto (24%) degli incidenti nel 2021 (e il 25% nel 2020) sono associati ad altre gang di ransomware, mentre non è stato possibile attribuire con certezza il resto degli incidenti a una gang nota specifica.

Sophos ha divulgato molte informazioni sul ransomware Conti. Per l'elenco completo degli articoli su Conti e su altre famiglie di ransomware prevalenti (inclusi LockBit, Ryuk e altri), visita il Centro di intelligence Sophos sul ransomware.

Conclusione

Tutte le organizzazioni possono essere vittime di un cyberattacco. E come abbiamo visto, sempre più spesso si ha a che fare con più di un singolo hacker. Da phishing e frode finanziaria, fino ad autori di botnet, piattaforme di distribuzione del malware, cryptominer, IAB, furto di dati, spionaggio industriale, ransomware e molto di più: se una rete ha un punto di ingresso vulnerabile, i cybercriminali lo troveranno e utilizzeranno una di queste strategie per approfittarne.

Fino a quando il punto di ingresso non verrà reso inutilizzabile e fino a quando non si eliminerà dai sistemi qualsiasi elemento residuo lasciato dagli hacker per stabilire e mantenere l'accesso, chiunque potrà sfruttare questa opportunità. E molto probabilmente lo farà.

I team di sicurezza possono difendere la propria organizzazione monitorando le attività sospette e svolgendo indagini. La differenza tra operazioni innocue e dannose non è sempre facile da stabilire. In qualsiasi ambiente virtuale o fisico, le tecnologie possono fare molto, ma da sole non bastano. L'esperienza e le competenze di un essere umano, unite alla capacità di risposta, sono una parte essenziale di qualsiasi soluzione di sicurezza.

In ambito di incident response, ciò che abbiamo imparato nel 2021 è quanto velocemente ed estensivamente i cybercriminali riescano ad approfittare delle vulnerabilità più diffuse e accessibili, con conseguenze che includono periodi di permanenza più lunghi e la presenza nei sistemi di più hacker contemporaneamente. Per i responsabili di cybersecurity, queste lezioni sono importantissime: indicano infatti quanto ora come non mai sia fondamentale svolgere indagini e rispondere tempestivamente ai segnali di allarme che potrebbero indicare la presenza di tecniche e toolset di cybercriminali noti.

Sophos Rapid Response

I risultati di questo report si basano sui dati provenienti da incidenti analizzati da Sophos Rapid Response, un team di esperti specializzati in incident response e neutralizzazione delle minacce. Il servizio Sophos Rapid Response è disponibile sia per i clienti Sophos che per aziende che non utilizzano prodotti e soluzioni di Sophos.

Se stai affrontando un incidente attivo e desideri parlare con il team Rapid Response, puoi chiamare uno di questi numeri in qualsiasi momento:

Italia: +39 02 873 17993

Stati Uniti: +1 4087461064

Australia: +61 272084454

Canada: +1 7785897255

Francia: +33 186539880

Germania: +49 61171186766

Regno Unito: +44 1235635329

Svezia: +46 858400610

Tabelle Di Dati Aggiuntive

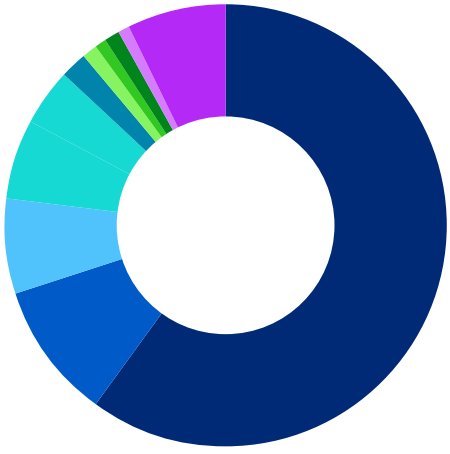
Artefatti Rilevati Dalle Indagini Sugli Incidenti E Mappati Secondo La Catena Di Attacco MITRE

Gli strumenti, le tecniche e altri artefatti osservati durante le indagini sugli incidenti sono stati mappati in base al framework MITRE ATT&CK. Ulteriori dettagli verranno pubblicati in un articolo di accompagnamento su Sophos News.

Fasi di attacco MITRE											
Accesso iniziale	Esecuzione	Persistenza	Privilege escalation	Elusione dei tentativi di difesa	Accesso con credenziali	Individua-zione	Movimenti laterali	Raccolta	Comando e controllo	Esfiltrazione	Impatto
Artefatti											
Servizi remoti	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Esplorazione della rete	Cobalt Strike	Rclone	Cifratura dei dati
Exploit	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Violazione della rete

Dati Demografici Di Incident Response Per Il 2021

Casi di incident response in base al paese

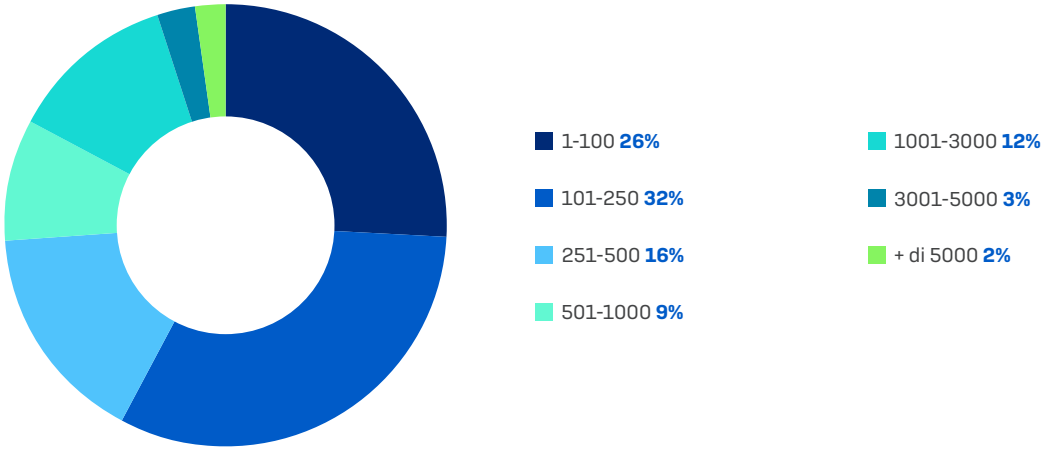


- Stati Uniti **60%**
- Germania **10%**
- Regno Unito **7%**
- Canada **6%**
- Italia **4%**
- Spagna **2%**
- Francia **1%**
- Svizzera **1%**
- Belgio **1%**
- Filippine **1%**
- Altri **7%** (Paesi Bassi, Austria, Emirati Arabi Uniti, Arabia Saudita, Bahamas, Angola, Giappone)

Casi di incident response in base al settore

- Industria manifatturiera **17%**
- Retail **14%**
- Sanità **12%**
- Information Technology **9%**
- Edilizia **8%**
- Istruzione **6%**
- Prodotti alimentari **4%**
- Logistica **4%**
- Finanza **4%**
- Intrattenimento **3%**
- Servizi **3%**
- Organi di informazione **3%**
- Altri **13%** (trasporti, industria farmaceutica, MSP/hosting, non profit, enti governativi, settore alberghiero, settore legale, agricoltura, fonti di energia, settore immobiliare)

Casi di incident response in base alle dimensioni dell'organizzazione (numero di dipendenti)



Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

2022-05-25 IT (DD)

SOPHOS