SOPHOS
Cybersecurity evolved.

SOPHOS THREAT REPORT 2021

Come orientarsi nella cybersecurity in un mondo pieno di incertezze

A cura di **SophosLabs**, **Sophos Managed Threat Response**, **Sophos Rapid Response**, **Sophos AI**, **Cloud Security**

INDICE DEI CONTENUTI

IL POTERE DELLA CONDIVISIONE

Joe Levy, Chief Technology Officer, Sophos

"Se vuoi andare veloce, vai da solo, se vuoi andare lontano, vai insieme."

Questo proverbio africano è particolarmente appropriato per il settore della cybersecurity. Lavorando insieme, uniti da un forte spirito di squadra, possiamo ottenere risultati migliori rispetto a quando combattiamo il cybercrimine come vendor individuali.

Tuttavia, è solamente migliorando il nostro approccio e condividendo dati di intelligence sulle minacce in maniera più completa, nonché includendo un maggior numero di partecipanti per contribuire a queste iniziative di condivisione e collaborazione (e trarne beneficio), che i vendor di soluzioni di cybersecurity possono aumentare le spese per i cybercriminali, distogliendoli dai propri intenti e lasciando un segno profondo e duraturo.

Animata da questo spirito di collaborazione, nel 2017 Sophos si è unita alla ***Cyber Threat Alliance***, un'organizzazione che si dedica ad abbattere le barriere che per anni hanno ostacolato la collaborazione tra competitor nel settore della sicurezza informatica. La CTA ha raggiunto e superato il suo obiettivo iniziale di svolgere il ruolo di archivio di dati di intelligence sulle minacce condivisi, diventando un luogo virtuale dove appianare le divergenze, paragonabile a una specie di ONU per il settore della cybersecurity.

La partnership con la CTA consente a Sophos di offrire ai clienti una protezione migliore, grazie al sistema di allerta tempestiva e allo scambio di informazioni tra i vendor, che viene reso possibile da questa alleanza. Sophos contribuisce anche alla protezione dei clienti di altri vendor, mettendo a disposizione i propri dati di intelligence sulle minacce.

Nel mese di marzo del 2020, mentre in tutto il mondo venivano istituiti lockdown per limitare la diffusione del COVID-19, Joshua Saxe, Chief Scientist presso Sophos, ha lanciato un appello su Twitter. Inorridito dal fatto che diversi cybercriminali stavano cominciando a includere nelle proprie campagne anche riferimenti al COVID-19, un gruppo di analisti di sicurezza informatica (composto da più di 4.000 esperti) ha unito le forze in segno di sfida, formando la COVID-19 Cyber Threat Coalition (CCTC) in un canale Slack creato il giorno stesso. Questo canale rappresenta una risorsa da cui la community può attingere nei momenti di crisi ed è in procinto di ottenere lo stato di organizzazione non profit sotto il patrocinio della CTA.

Fondamentalmente, queste storie sulla condivisione di dati di intelligence sulle minacce non offrono solo informazioni sulle singole organizzazioni, ma sono ben più eloquenti. Come ci insegna un altro racconto, quello dei ciechi e dell'elefante, nessun vendor da solo può conoscere la verità assoluta basandosi esclusivamente sulle proprie esperienze. La capacità di affrontare anche le questioni più complicate emerge solamente grazie all'unione di tutte le nostre esperienze. Queste iniziative di collaborazione hanno protetto milioni di persone, impedendo che diventassero vittime del cybercrimine. Tuttavia questo fatto, da solo, non spiega il ***perché*** dei loro risultati. Il loro successo è dovuto al fatto che la motivazione principale dei membri e dei fondatori era in primo luogo proteggere dai pericoli chiunque fosse a rischio. Lo scopo non era il lucro, bensì un desiderio genuino di difendere chi ne avesse bisogno, proprio quando i lupi erano in agguato.

Questo dimostra l'efficacia del modello e la sua capacità di risolvere problemi dovuti a lacune critiche che nessun vendor, da solo, era in grado di colmare. Tuttavia, può portare anche altri benefici. Il settore della sicurezza potrebbe, in futuro, considerare la possibilità di condividere modelli di machine learning o training dataset, analogamente a come oggi condividiamo block list o regole di Yara. Si potrebbero anche consolidare e sviluppare standard emergenti, come i framework STIX e ATT&CK, oppure si potrebbe partecipare a ISAC e ISAO per il settore della cybersecurity.

Il futuro sarà più connesso e questo garantirà a tutti un ulteriore vantaggio, nonché una protezione superiore.

RIEPILOGO

Il Sophos Threat Report per il 2021 esamina gli argomenti approfonditi da Sophos nel corso degli ultimi 12 mesi grazie al lavoro svolto dai SophosLabs in ambito di analisi del malware e dello spam, e dai team Sophos Rapid Response, Cloud Security e Data Science. Questi aspetti delle nostre regolari attività di protezione dei clienti forniscono ulteriori approfondimenti sul panorama delle minacce e offrono agli esperti di incident response e ai professionisti dell'IT security ottime indicazioni relativamente agli ambiti su cui è consigliabile focalizzare la propria attenzione, per garantire la protezione delle reti e degli endpoint il prossimo anno.

Il rapporto è suddiviso in quattro parti principali: una discussione sull'evoluzione del ransomware e sulla direzione che sta prendendo questa minaccia; un'analisi dei più comuni tipi di attacchi affrontati dalle organizzazioni di grandi dimensioni e dei motivi per cui questi metaforici "canarini nelle miniere" ovvero i dettagli anche più insignificanti, continuano a rappresentare un serio pericolo; l'impatto della pandemia globale sulla sicurezza informatica nel 2020; e infine un sondaggio sull'ambito di azione degli attacchi rivolti a piattaforme che non vengono tradizionalmente considerate come parte della superficie di attacco nelle reti aziendali.

Riassumendo, i punti principali del rapporto sono i seguenti:

Ransomware

- I pirati informatici che utilizzano il ransomware continuano a reinventarsi rapidamente sia nelle tecnologie utilizzate, sia nella propria modalità operativa
- I criminali che diffondo attacchi ransomware ricorrono sempre più frequentemente al furto dei dati, per poter estorcere denaro alle vittime, minacciandole di pubblicare dati riservati di natura sensibile
- Man mano che questi gruppi criminali investono più risorse nei propri attacchi contro le organizzazioni più grandi, aumentano anche i riscatti da loro richiesti
- Inoltre, le gang di cybercriminali coinvolte negli attacchi ransomware sembrano ora agire a stretto contatto con altri criminali che operano negli ambienti clandestini, con un comportamento sempre più simile a quello di vere e proprie associazioni del cybercrimine, piuttosto che gang isolate
- Attacchi ransomware che un tempo richiedevano giorni oppure settimane possono ora colpire entro poche ore

Le minacce "quotidiane"

- Uno dei principali bersagli degli attacchi sono le piattaforme server (sia Windows che Linux), che vengono anche sfruttate per colpire le organizzazioni dall'interno
- Servizi comuni come RDP e concentratori VPN continuano a essere tra gli obiettivi di attacco più sfruttati per colpire il perimetro di rete delle organizzazioni; inoltre, gli hacker utilizzano RDP per muoversi lateralmente all'interno delle reti violate
- Anche il malware "commerciale" più semplice può causare violazioni gravi, in quanto numerose famiglie di malware possono diventare "reti di distribuzione dei contenuti" per altro malware
- La scarsa attenzione verso uno o più aspetti fondamentali della sicurezza si è rivelata la causa principale della maggior parte degli attacchi più devastanti che abbiamo analizzato

Il COVID-19

- Lo smart working ha introdotto nuove sfide, in quanto estende il perimetro di sicurezza delle organizzazioni a migliaia di reti domestiche, dotate di livelli variabili di protezione
- Sebbene il cloud computing abbia attutito l'impatto delle nuove necessità di protezione degli ambienti informatici, presenta sfide diverse da quelle delle tradizionali reti aziendali
- I cybercriminali hanno cercato di migliorare la propria reputazione promettendo di non attaccare organizzazioni impegnate in attività mediche essenziali per salvare la vita delle persone; tuttavia, si sono rimangiati la parola in un secondo momento
- Le aziende criminali si sono evolute in un'economia basata sui servizi, che aiuta nuovi criminali a entrare in questo universo
- I professionisti della cybersecurity di tutto il mondo hanno unito le forze nel 2020 per formare un gruppo operativo di risposta rapida agli incidenti di sicurezza, con lo scopo di contrastare le minacce che sfruttano il potenziale di social engineering degli argomenti correlati al nuovo coronavirus

Piattaforme non convenzionali

- Gli hacker ora sfruttano regolarmente vari strumenti e utilità rivolte ai "red team", sviluppati da esperti di penetration testing in attacchi attivi e in tempo reale
- Nonostante l'impegno delle piattaforme di telefonia mobile nel monitoraggio delle app per rilevare la presenza di codice dannoso, i cybercriminali continuano ad escogitare nuovi metodi per aggirare gli ostacoli, sviluppando tecniche in grado di eludere le analisi del codice
- Il software un tempo classificato come "potenzialmente indesiderato" a causa dei costanti annunci fastidiosi (ma non dannosi) utilizza ora tattiche sempre più difficili da distinguere da quelle dei veri e propri malware
- Per colmare le lacune nei rilevamenti, gli esperti di data science hanno utilizzato approcci agli attacchi di spam e ai payload di malware normalmente associati al mondo dell'epidemiologia biologica

IL FUTURO DEL RANSOMWARE

Gli attacchi ransomware sferrati nel corso del 2020 hanno intensificato i problemi di una popolazione già in difficoltà. Mentre la pandemia imperversava, mettendo in pericolo vite umane e mezzi di sussistenza, si scatenavano anche nuove famiglie di ransomware che continuavano imperterrite ad attaccare i settori della sanità e dell'istruzione, nonostante gli ospedali fossero diventati il campo di battaglia per combattere il COVID-19 e nonostante le scuole cercassero in tutti i modi di trovare nuove strategie per garantire agli alunni l'accesso alle lezioni sia a marzo che nei mesi successivi.

Durante una pandemia, nessuna attività di raccolta fondi è sufficiente per pagare un riscatto, tuttavia alcune istituzioni scolastiche sono riuscite a riprendersi dagli attacchi mirati del primo giorno di scuola, grazie ai propri backup sicuri.

I cybercriminali che utilizzano il ransomware hanno escogitato nuovi stratagemmi per eludere i prodotti di sicurezza endpoint e per diffondersi rapidamente, trovando persino una soluzione al "problema" (che è tale dal loro punto di vista) dei backup individuali e aziendali conservati in luoghi sicuri e fuori dalla portata del ransomware.

Tuttavia, la varietà del ransomware è più limitata di quanto non possa sembrare. Con il passare del tempo, dopo aver indagato su una vasta quantità di attacchi, gli analisti di Sophos hanno scoperto che alcune famiglie di ransomware avevano lo stesso codice. Inoltre, alcuni gruppi di criminali che sferravano attacchi ransomware sembravano avere un rapporto di reciproca collaborazione, piuttosto che di competizione.

Sulla base di questi fatti, è difficile prevedere accuratamente quale sarà la prossima mossa degli hacker del ransomware. Gli autori e i pirati informatici che utilizzano il ransomware hanno investito molto tempo nel cercare di difendersi dai prodotti di protezione endpoint. Noi dobbiamo rispondere alle loro contromisure. Loro mostrano creatività e versatilità nell'escogitare nuove tattiche, noi rispondiamo con tenacia analizzando le loro mosse e trovando modi innovativi per contrastarle.

Il furto dei dati dà origine a un mercato secondario di estorsione

Fino a quest'anno, l'opinione diffusa tra i vendor di soluzioni di sicurezza che si erano trovati alle prese con il ransomware su come affrontare gli attacchi era piuttosto uniforme: bloccare i punti di ingresso più esposti (ad es. le porte RDP connesse a Internet), conservare backup off-line e risolvere rapidamente le infezioni di malware minori e innocui (come Dridex o Emotet), prima che potessero diffondere il loro payload letale.

Molti attacchi sferrati contro organizzazioni di alto profilo (ad es. distretti scolastici negli Stati Uniti) non sono andati a segno, principalmente grazie ai responsabili IT, che hanno conservato backup di dati critici.

Per contrastare la prontezza delle proprie vittime, diverse famiglie di ransomware hanno cominciato a utilizzare un'ulteriore strategia di estorsione per aumentare la pressione sulle organizzazioni e indurle a pagare il riscatto, anche se erano presenti backup dei dati essenziali. Non si limitavano a tenere in ostaggio i computer, ma ne prelevavano i dati, minacciandone la pubblicazione qualora la vittima si fosse rifiutata di pagare la somma richiesta.

Negli ultimi sei mesi, gli analisti di Sophos hanno osservato che i cybercriminali che lanciano attacchi ransomware tendono ora a utilizzare un set di strumenti comuni (e in lento aumento), con i quali esfiltrano dati dalla rete di una vittima. Questo set di strumenti contiene risorse comuni che sono legittime, alla portata di tutti e impossibili da rilevare per i tradizionali prodotti di sicurezza endpoint. L'elenco di famiglie di ransomware che agiscono in questo modo continua ad aumentare e al momento include: Doppelpaymer, REvil, Clop, DarkSide, Netwalker, Ragnar Locker, Conti e molti altri. Gli hacker gestiscono siti di "pubblicazione delle informazioni", dove comunicano i dati che hanno prelevato illecitamente; REvil mette in vendita i dati sul proprio sito web.

I cybercriminali si servono di questo set di strumenti per copiare informazioni interne di natura sensibile, comprimendole in un archivio e trasferendole fuori dalla rete e dalla portata della vittima. Ecco alcuni esempi degli strumenti utilizzati a tale scopo, che abbiamo osservato finora:

- Total Commander (gestore file con client FTP incorporato)
- 7zip (software per la creazione di archivi)
- WinRAR (software per la creazione di archivi)
- psftp (client SFTP PuTTY)
- cURL per Windows

Per il furto dei dati, gli hacker sono molto meno selettivi e tendono ad impossessarsi di cartelle intere, indipendentemente dai tipi di file che contengono (di solito per la cifratura il ransomware preferisce dare la priorità a tipi di file strategici, escludendone molti altri).

Le dimensioni non contano. Ai cybercriminali non interessa la quantità di dati da rubare. Le strutture delle directory variano da azienda ad azienda e alcuni tipi di file sono più facili da comprimere rispetto ad altri. Abbiamo osservato furti di quantità variabili (da 5 GB a 400 GB) di dati compressi, prima della distribuzione del ransomware sui sistemi della vittima.

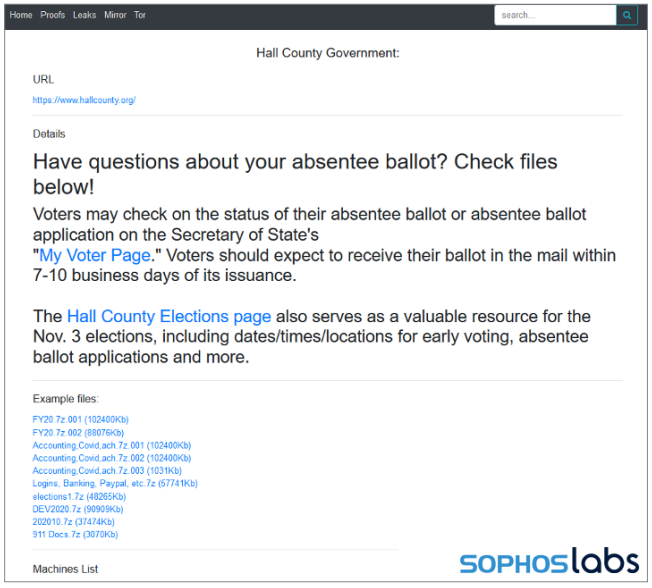


Fig.1. A ottobre del 2020, la pagina di pubblicazione delle informazioni del ransomware Doppelpaymer ha rivelato che gli hacker avevano colpito le reti della contea di Hall in Georgia, USA. Le informazioni pubblicate illecitamente includevano un riferimento a un file chiamato "elections" (elezioni), che conteneva documenti elettorali per le elezioni primarie statali del 2020 e un elenco degli scrutatori delle elezioni del 2018, oltre ad altri file di natura sensibile. Secondo l'agenzia di stampa Associated Press, il ransomware avrebbe cifrato il database di verifica delle firme utilizzato dalla contea per convalidare le schede elettorali. Fonte: SophosLabs.

Solitamente i criminali inviano i dati esfiltrati a servizi cloud legittimi, una strategia che rende più difficile l'individuazione di questo tipo di attività, visto che si tratta di destinazioni normali e comuni per il traffico di rete. Quelli che seguono sono i principali servizi di cloud storage utilizzati dagli hacker per conservare i dati esfiltrati:

- Google Drive
- Amazon S3 (Simple Storage Service)
- Mega.nz
- Server FTP privati

Per concludere la loro attività devastante, i cybercriminali del ransomware cercano di colpire sempre più frequentemente i server locali che contengono backup dei dati critici. Quando individuano tali server, eliminano (o cifrano) i backup poco prima di sferrare un attacco di cifratura non autorizzata sull'intera rete.

Conservare un backup dei dati critici off-line non è mai stato così importante. Se riescono a trovare il backup, i cybercriminali, con il loro attacco ransomware, lo distruggeranno.

Le somme richieste come riscatto salgono, parallelamente all'aumento degli attacchi

È difficile pensare che solamente due anni fa gli analisti di Sophos si erano stupiti del bottino da 6 milioni di dollari che i pirati informatici che avevano lanciato l'attacco con il ransomware SamSam erano riusciti ad accaparrarsi. In un attacco contrastato da Sophos nel 2020, la somma iniziale richiesta dai cybercriminali era pari a più del doppio della cifra guadagnata attraverso SamSam in 32 mesi di attività.

Come per il pugilato, il ransomware è suddiviso in tre categorie: i pesi massimi che attaccano le reti delle grandi imprese, i pesi welter che colpiscono le organizzazioni della società civile (enti di sicurezza pubblica e pubblica amministrazione) e i pesi piuma che prendono di mira singoli computer e utenti privati. Sebbene rientrare tra i principali pesi massimi possa essere un traguardo di discutibile prestigio, un paragone tra le elevate richieste di riscatto di questa categoria e quelle rivolte alle categorie inferiori non sarebbe adeguato.

Sophos dispone di un team dedicato che svolge indagini sugli attacchi ransomware, spesso in stretta collaborazione con le organizzazioni e le persone scelte come bersaglio da questi attacchi. Il team è in grado di ricostruire dal punto di vista forense gli eventi di un attacco dopo la sua conclusione, e a volte di bloccarlo mentre è ancora in corso. Il team Sophos Rapid Response entra in azione nei casi in cui è presente una possibilità di fermare o limitare i danni. Tuttavia, a volte gli attacchi avvengono in maniera talmente rapida che non è possibile intraprendere alcuna azione. La vittima deve pertanto decidere se pagare o meno il riscatto e a questo punto Sophos non è più coinvolta.

Questo è il momento in cui intervengono aziende come Coveware, che rappresenta le vittime di attacchi ransomware in qualità di negoziatore nelle trattative con i cybercriminali. Alex Holdtman, CTO di Coveware, ha confermato i nostri sospetti: i "pesi massimi" del ransomware sono il fattore primario nella determinazione di somme vertiginose per le richieste di riscatto.

Pagamenti riscossi su base trimestrale relativi ad attacchi ransomware

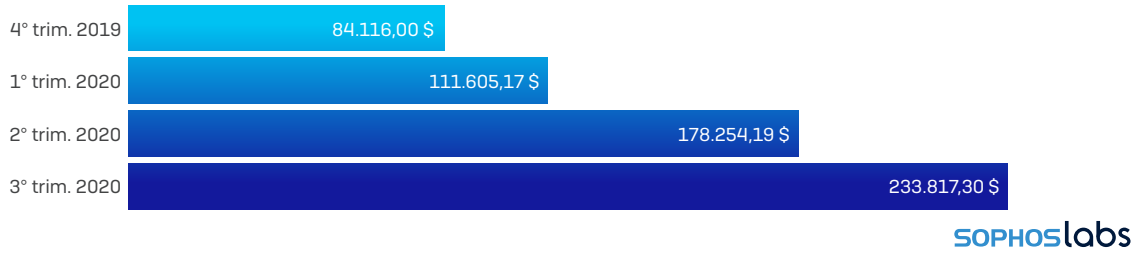


Fig.2. La media delle richieste di riscatto ha subito un incremento del 21% nell'ultimo trimestre ed è triplicata negli ultimi 12 mesi. Fonte: Coveware.

Negli ultimi tre mesi, i riscatti riscossi hanno subito un incremento del 21%, anche se Coveware ritiene che questa media possa essere deviata anche solo da uno o due attacchi con riscatti particolarmente elevati. La somma media dei pagamenti di riscatti effettuati nel trimestre che si è appena concluso è ora pari all'equivalente in criptovaluta di 233.817,30 $. Un anno fa, il pagamento medio era di 84.116 $.

I cybercriminali che utilizzano il ransomware sono consci delle perdite di denaro causate dai tempi di inattività e hanno sondato il terreno per scoprire il limite massimo della somma che possono richiedere durante un attacco ransomware.

Molte famiglie di ransomware hanno cominciato ad adottare tentativi di estorsione come ulteriore strategia che si affianca alla semplice richiesta di riscatto, con lo scopo di aiutare i cybercriminali in azione a concludere le trattative con un esito a loro favorevole. Come già accennato nel nostro rapporto, questa tattica viene utilizzata da gruppi quali Netwalker e altri. Agendo in questo modo, anche se la vittima dell'attacco dovesse avere backup dei dati ripristinabili, potrebbe essere comunque costretta a pagare il riscatto, nella speranza che i cybercriminali non divulghino al pubblico le informazioni interne.

Per quanto riguarda i riscatti di ransomware meno elevati, le richieste sono in aumento, anche se Holdtman sostiene che non siano paragonabili a quelle dei "pezzi grossi". Molte piccole imprese e singoli individui vengono colpiti, ma per loro le richieste di riscatto rimangono per lo più invariate.

Una delle giornate tipiche di un esperto che opera nel team Sophos Rapid Response, di risposta rapida al ransomware

Un'organizzazione colpita dal ransomware Maze (al tempo ancora attivo) si è rivolta al team Sophos Rapid Response. Abbiamo svolto indagini e contrastato attivamente l'attacco mentre era ancora in corso. Quello che segue è un riepilogo giornaliero dell'attacco durante il suo svolgimento.

Prima del Giorno 1
A un certo punto, prima che l'attacco diventi attivo, i pirati informatici compromettono un computer situato nella rete della vittima.

Questo computer viene quindi utilizzato come "appiglio strategico" all'interno della rete. In diverse occasioni, l'hacker lo utilizzerà per connettersi ad altri computer mediante Remote Desktop Protocol (RDP).

Giorno 1
Il primo segno di attività malevola affiora quando un beacon SMB di Cobalt Strike viene installato come servizio su un controller di dominio (Domain Controller, DC) non protetto. Gli hacker sono ora in grado di controllare il DC dal computer precedentemente violato, sfruttando un account di Amministratore di dominio con una password debole.

Giorno 2
Gli hacker creano, eseguono ed eliminano una serie di operazioni pianificate e script batch. Dalle prove raccolte dagli investigatori emerge che queste operazioni sono simili a una tecnica che sarebbe poi stata utilizzata in un secondo momento per la distribuzione degli attacchi ransomware. È possibile che i cybercriminali abbiano testato il metodo che avevano intenzione di utilizzare.

Servendosi dell'account dell'Amministratore di dominio e dell'accesso tramite RDP, gli hacker si spostano lateralmente all'interno della rete per attaccare altri server critici.

Utilizzano Advanced IP Scanner, uno strumento legittimo di scansione della rete, per cominciare a mappare la rete e compilare un elenco di indirizzi IP sui quali sarebbe poi stato distribuito il ransomware. I cybercriminali creano un elenco a parte di indirizzi IP appartenenti ai computer utilizzati dagli amministratori IT dell'organizzazione selezionata come bersaglio.

Successivamente, gli hacker sfruttano lo strumento Microsoft ntdsutil per eseguire il dump del database di credenziali di Active Directory con hash.

I pirati informatici proseguono quindi eseguendo vari comandi WMI per raccogliere informazioni sui computer compromessi e tornano a occuparsi dell'esfiltrazione dei dati: identificano un file server e, servendosi dell'account dell'Amministratore di dominio compromesso, effettuano l'accesso da remoto tramite RDP. Cominciano a comprimere le cartelle situate in questo file server.

Gli hacker trasferiscono gli archivi sul controller di dominio e successivamente cercano di installare l'applicazione di cloud storage Mega sul DC. Questa operazione viene bloccata dal team di sicurezza, per cui gli hacker passano alla versione web e caricano i file compressi.

Giorno 3
L'esfiltrazione dei dati su Mega prosegue nel corso della giornata.

Giorni 4 e 5
Durante questo periodo di tempo non viene osservata alcuna attività malevola. In incidenti analizzati in passato, abbiamo osservato che, per sferrare l'attacco, i pirati informatici attendono un fine settimana o una giornata festiva, quando il team di IT security non è operativo o non si occupa delle attività della rete. .

Giorno 6
Una domenica. Viene avviato il primo attacco ransomware Maze, grazie all'utilizzo di un account di Amministratore di dominio compromesso e dell'elenco degli indirizzi IP identificati. L'attacco colpisce più di 700 computer e viene bloccato dal team di sicurezza. Gli hacker non si rendono conto che l'attacco è stato sventato, oppure sperano che basti essere in possesso dei dati rubati per minacciare la vittima, perché a questo punto effettuano una richiesta di riscatto pari a 15 milioni di $.

Giorno 7
Il team di sicurezza installa sistemi di protezione aggiuntiva e avvia il monitoraggio 24/7 delle minacce. Hanno inizio le indagini di incident response e viene rapidamente identificato l'account di amministrazione compromesso. Vengono anche scoperti diversi file dannosi e ogni comunicazione tra gli hacker e i computer infettati viene bloccata.

Giorno 8
Vengono scoperti altri strumenti e tecniche utilizzati dai cybercriminali, nonché ulteriori prove relative all'esfiltrazione dei dati. Vengono bloccati altri file e account.

Giorno 9
Nonostante le attività difensive, gli hacker mantengono l'accesso alla rete e utilizzano un altro account compromesso per sferrare un secondo attacco. Questo attacco è simile al primo: esegue comandi su un DC, elaborando tutti gli indirizzi IP elencati in file txt.

L'attacco viene identificato rapidamente. Il ransomware viene rilevato automaticamente e sia l'account compromesso che il payload del malware vengono disattivati ed eliminati. Nessun file viene cifrato.

I cybercriminali non demordono ed effettuano un altro tentativo. Il terzo tentativo si verifica poche ore dopo il secondo attacco.

A questo punto i pirati informatici sembrano essere sempre più disperati, poiché questo attacco colpisce un solo computer. Si tratta del file server principale da cui erano stati prelevati i dati esfiltrati.

I cybercriminali di Maze adottano un approccio diverso, implementando una copia completa di una virtual machine (VM) e un programma di installazione dell'hypervisor VirtualBox, in un attacco documentato su SophosLabs Uncut a settembre 2020.

Il risultato del terzo tentativo è stato identico a quelli precedenti: il team Sophos Rapid Response ha rilevato e sventato l'attacco e nessun file è stato cifrato. Il team ha aiutato il cliente a espellere i cybercriminali dalla rete, rimuovendo così qualsiasi loro capacità di proseguire con gli attacchi.

LE MINACCE QUOTIDIANE AFFRONTATE DALLE IMPRESE: COME I "CANARINI NELLE MINIERE", ATTENZIONE AI DETTAGLI

Se si dovesse valutare la situazione degli attacchi informatici in base alle notizie riportate dalle testate giornalistiche, si potrebbe pensare che il disastro sia imminente. Le organizzazioni di grandi dimensioni subiscono attacchi ogni giorno, ma non sono tutti eventi inaspettati (come ad esempio casi gravi di violazioni dei dati) in grado di rovinare le sorti (e le quote di mercato) di un'azienda, distruggendone la reputazione. Molti attacchi sono molto più banali e includono malware che il team dei SophosLabs monitora in un elenco di "Soliti sospetti" tra i "Più ricercati".

Tuttavia, sebbene questi attacchi (e alcuni dei tipi di malware che utilizzano) siano noti e semplici da contenere, ogni attacco ha il potenziale di diventare incontrollabile, se non viene gestito in maniera tempestiva ed efficace. Per utilizzare una metafora ornitologica, questi attacchi comuni che si verificano ogni giorno sono un po' come i canarini nelle miniere: un indicatore precoce di una presenza tossica che potrebbe precipitare fuori controllo.

Attacchi che prendono di mira server Windows e Linux

Sebbene la maggior parte degli incidenti di sicurezza che abbiamo rilevato nel 2020 abbia colpito desktop o laptop con sistemi Windows, si è osservato un incremento costante degli attacchi contro server Windows e non Windows. Generalmente, da tempo i server rappresentano un bersaglio allettante per gli attacchi e i motivi sono molteplici: vengono frequentemente eseguiti per lunghi periodi di tempo senza essere monitorati o sorvegliati, i server sono spesso dotati di capacità di memoria e CPU superiori rispetto a quelle dei singoli laptop, e infine i server possono svolgere un ruolo privilegiato all'interno della rete, magari con possibilità di accesso ai dati più sensibili e importanti di un'organizzazione. Questi tratti distintivi li rendono un potenziale punto di accesso molto allettante per gli hacker più persistenti. Nel 2021 queste caratteristiche rimarranno invariate e Sophos prevede un aumento costante del volume degli attacchi rivolti ai server.

La maggior parte degli attacchi che colpiscono i server sono classificabili in tre tipi di profilo (ransomware, cryptomining ed esfiltrazione dei dati), ciascuno dei quali presenta un set corrispondente e ben definito di tattiche e tecniche utilizzate dagli hacker. Una delle best practice per gli amministratori è evitare di eseguire sui server le tradizionali app per desktop, come ad es. client di posta o browser web, per tutelare i sistemi dalle infezioni. Di conseguenza, gli attacchi rivolti ai server hanno dovuto modificare le proprie tattiche.

I server Windows connessi a Internet ricevono una quantità infinita di tentativi di brute force tramite RDP, una tattica di attacco che da tre anni è associata al ransomware e ne indica la presenza. Il team Sophos Rapid Response ha notato che spesso la causa originaria degli attacchi ransomware esaminati era correlata a un accesso iniziale alla rete della vittima tramite RDP. Successivamente, i computer compromessi venivano sfruttati per mantenere l'accesso alla rete e assumere il controllo dei server di DC, dai quali potevano poi proseguire con le rimanenti fasi dell'attacco.

Gli attacchi di cryptojacking tendono invece a colpire una gamma più ampia di funzionalità di Windows, all'interno di applicazioni che vengono solitamente eseguite sull'hardware dei server, come ad es. software di database.

Per esempio, un metodo utilizzato dal cryptominer Lemon_Duck sfrutta un attacco brute force contro server connessi a Windows che eseguono Microsoft SQL Server. Una volta dedotta la giusta password del database, gli hacker possono quindi utilizzare il database in questione per riassemblare il payload del cryptojacker, scriverlo sul file system del server ed eseguirlo. Il computer infetto effettuerà quindi un tentativo di exploit delle vulnerabilità per mezzo di EternalBlue e/o SMBGhost, nel tentativo di diffondere il cryptojacker.

Per gli attacchi Lemon_Duck non fa alcuna discriminazione, in quanto può infettare anche i server Linux. Il malware cerca di sferrare attacchi brute force per ottenere password SSH prelevate da un elenco relativamente ristretto. Se il tentativo ha esito positivo, gli hacker caricano shellcode dannoso che stabilisce la persistenza approfittando delle falle di un servizio che si chiama Redis. Il cryptojacker può anche nascondersi eseguendo i propri comandi di avvio dall'interno di un cluster di Hadoop.

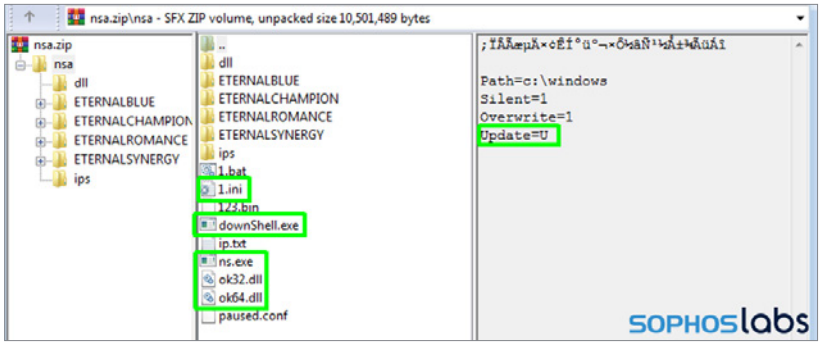


Fig.3. Uno dei cryptojacker più prolifici, MyKings, distribuiva i componenti di installazione della botnet (evidenziati in verde) all'interno di un archivio Zip, insieme a molti altri exploit ottenuti dalla NSA grazie a The Shadow Brokers. Fonte: SophosLabs.

Talvolta gli hacker prendono di mira i server perché, invece di un pagamento rapido o di un flusso costante di criptovalute, puntano a prelevare dati di valore, memorizzati su questi server. Nel 2020, Sophos ha scoperto un attacco rivolto ai server Linux che sfruttava un tipo di malware che abbiamo denominato Cloud Snooper. Questi server erano ospitati in un cluster di cloud computing e i cybercriminali erano riusciti a eludere il rilevamento escogitando un sistema intelligente di relay dei messaggi, aggregando i propri messaggi di comando e controllo a comunissime connessioni HTTP.

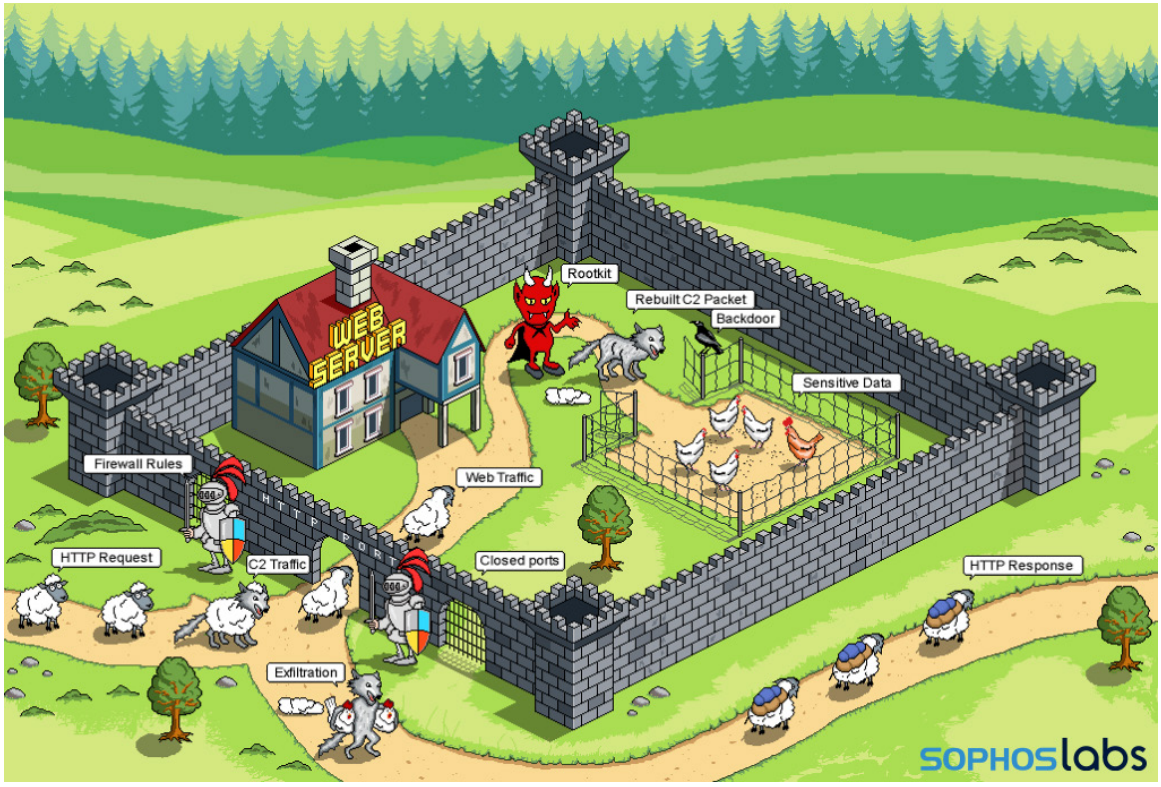


Fig.4. Illustrazione metaforica di un "lupo travestito da pecora" che mostra come il malware APT Cloud Snooper è riuscito a nascondere i propri comandi e a prelevare i dati camuffando le proprie attività per farle sembrare normali richieste e risposte HTTP, con l'aiuto di uno strumento che monitorava il traffico di rete e riscriveva i pacchetti TCP/IP in tempo reale. Fonte: SophosLabs.

Gli amministratori dei server di solito non installano prodotti di protezione endpoint sui server; tuttavia, con l'avvento di questi tipi di attacchi, questa convinzione comune è cambiata.

Chi sottovaluta il malware "commerciale" lo fa a suo rischio e pericolo

Non tutte le vittime vengono colpite da vulnerabilità zero-day sfruttate da un'Advanced Persistent Threat (APT) progettata per colpire sistemi governativi. La maggior parte degli attacchi utilizza malware ordinario, distribuito con mezzi comuni, tipicamente un'e-mail di spam o un allegato o un link dall'aspetto innocuo, accompagnato da varie esortazioni ad aprirlo. Sophos riceve ogni mese migliaia di corrispondenze di telemetria che riguardano questi tipi comuni di malware. Di solito i dati indicano che un computer protetto da uno dei nostri prodotti ha bloccato l'attacco.

Nei computer sprovvisti di protezione, nei quali può eseguirsi liberamente, il malware traccia il profilo del computer della vittima, estrae tutte le credenziali di accesso e le password salvate per i siti web che controllano informazioni di valore (di solito conti bancari o servizi finanziari, ma anche altro), invia le informazioni raccolte ai cybercriminali che l'hanno distribuito e rimane in attesa di ulteriori istruzioni, che possono arrivare entro pochi secondi... Oppure dopo diversi giorni.

Ma non bisogna lasciarsi ingannare dalle apparenze di queste famiglie di malware che sembrano *comuni e ordinarie*. Questi semplici strumenti sono pericolosi e possono causare seri problemi, se non ne viene eliminata la persistenza. Come accennato in precedenza in questo rapporto, il team dei SophosLabs gestisce un elenco dei malware "Più ricercati"; sono analisti che si dedicano quasi esclusivamente a studiare le famiglie di malware più persistenti. Di seguito ne riportiamo un breve riepilogo.

Dridex e Zloader

Uno dei più comuni tipi di malware è il *loader*. Le funzionalità dei loader hanno lo scopo di consegnare payload di altri malware per conto dei cybercriminali che li usano direttamente o indirettamente. Le famiglie di malware Dridex e Zloader sono entrambe piattaforme loader consolidate, in circolazione da diverso tempo. Gli hacker sfruttano sia Dridex che Zloader per raccogliere informazioni sul sistema della vittima e inviarle ai cybercriminali, che possono quindi decidere tranquillamente quali componenti o payload distribuire, a seconda delle informazioni ricevute dal bot.

La funzione principale del loader Dridex è quella di contattare il proprio server di comando e controllo (C2), recuperare uno o più payload cifrati e distribuirli. Intercettare questi payload è estremamente difficile per gli analisti, in quanto i cybercriminali li distribuiscono secondo necessità, utilizzando ad esempio applicazioni VNC nascoste (per il controllo remoto) o proxy SOCKS. Questi payload permettono agli hacker di agire nel contesto del dispositivo dell'utente e di accedere alle risorse del sistema della vittima che non possono raggiungere direttamente.

Sebbene non sia possibile definire con certezza la logica lato server che determina le azioni svolte durante un'infezione, possiamo comunque dedurre alcune regole, visto che i bot cercano di non infettare i computer utilizzati dagli analisti. Il bot invia agli hacker un elenco di programmi installati. Se questi programmi includono strumenti di analisi o componenti di virtual machine, i bot non distribuiranno payload su quel computer. Nel caso di Zloader, gli hacker di questo bot diffondono malware con un messaggio di spam. Se il processo di infezione del computer richiede troppo tempo, da 8 a 12 ore dopo l'invio dello spam, i payload smettono di essere inviati.

Inoltre, il bersaglio ideale deve essere un computer pulito, ma non troppo. Un'installazione Windows troppo semplice non attiva la distribuzione del payload, ma lo stesso vale per un computer con una quantità elevata di strumenti.

Agent Tesla e RATicate, infostealer e RAT

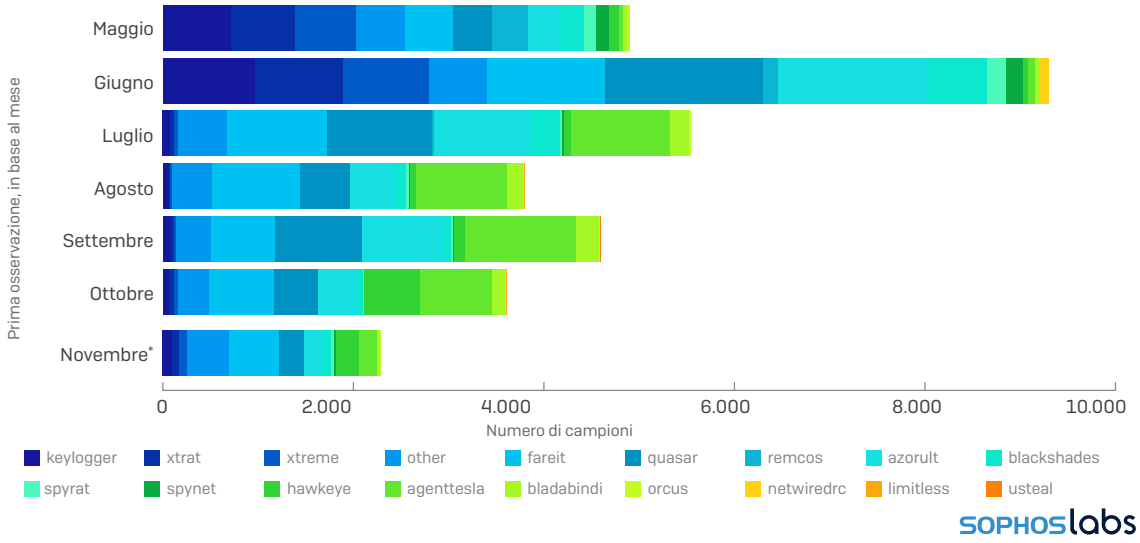


Fig.5. Tutti i nuovi campioni di malware di tipo Remote Access Trojan (RAT) vengono eseguiti nel nostro sistema sandbox interno. Questa tabella indica quanti nuovi campioni univoci abbiamo rilevato in un periodo di sette mesi. Questi campioni sono poi stati classificati nelle 18 famiglie di RAT più comuni, raggruppate per nome. * Dati relativi solo alla prima parte del mese. Fonte: SophosLabs.

Remote Access Trojan (RAT) e infostealer sono due delle forme di malware più longeve. Come suggerisce il nome stesso, i RAT offrono agli hacker la capacità di controllare il computer infettato da remoto. Anche gli infostealer sono fedeli al proprio nome, in quanto puntano a prelevare illecitamente ed esfiltrare credenziali, certificati e altre informazioni di natura sensibile. Due delle famiglie dei malware "Più ricercati" con cui abbiamo avuto a che fare negli ultimi 12 mesi sono Agent Tesla (un infostealer) e RATicate (un RAT).

Proprio come i loader, anche i RAT presentano un meccanismo che utilizzano per consegnare payload aggiuntivi, incluse versioni aggiornate di se stessi. Abbiamo osservato che RATicate distribuisce altri malware, incluso Agent Tesla. Abbiamo anche notato che queste famiglie di RAT vengono inviate o comunicano tramite gli stessi indirizzi IP o server. Questo indica un elemento comune tra gruppi che non hanno nessun'altra correlazione reciproca.

La sconfitta di Trickbot

Per almeno quattro anni, Trickbot è stato un malware particolarmente persistente e fastidioso. La sua famigerata botnet ha aperto la strada per quelli che ormai sono diventati comportamenti e caratteristiche comuni, ad esempio la comunicazione con l'infrastruttura C2 tramite TLS. Questo bot è implicato in diversi attacchi ransomware di alto profilo ed è anche noto per aver portato a termine vari tentativi di furto di credenziali.

Fig.6. Trickbot è stato sconfitto con una singola riga di codice. Fonte: SophosLabs.

A ottobre 2020, mentre stavamo preparando questo rapporto, Microsoft e il Dipartimento di Giustizia degli Stati Uniti hanno annunciato di aver sequestrato diversi server e di aver utilizzato il sistema di comando e controllo della botnet per inviare un comando che ha interrotto le comunicazioni tra il 90% della botnet e la rispettiva infrastruttura di comando e controllo.

Gli inquirenti sono riusciti a caricare sull'infrastruttura di Trickbot una configurazione intenzionalmente dannosa, che è stata scaricata da tutti i bot. Questa configurazione induceva la botnet a credere che il proprio server di comando e controllo fosse il computer infettato su cui veniva eseguita. La botnet ha quindi interrotto i contatti con i suoi server C2 e non è più stata in grado di recuperare payload o istruzioni.

L'operazione ha avuto un impatto radicale sugli hacker di Trickbot, ma prevediamo che questo malware riprenderà, in futuro, le proprie attività criminali.

Meccanismi di distribuzione

I metodi applicati dalla maggior parte degli attacchi malware seguono un percorso ben definito, che include l'utilizzo di e-mail contenenti link a file dannosi o allegati altrettanto pericolosi. In alternativa, gli hacker possono assumere un ruolo più attivo, sfruttando RDP o altri servizi vulnerabili ospitati al limite del perimetro di rete e connessi pubblicamente a Internet.

RDP: il vettore di attacco nº1 per il ransomware

Windows Remote Desktop Protocol, o RDP, è un servizio standard disponibile su tutte le versioni correnti di Windows. RDP offre agli amministratori IT o agli utenti dei computer un modo estremamente semplice per accedere a un computer quando non si trovano nel luogo fisico dove è situato il computer in questione. Questa opzione può essere molto utile nel caso di una pandemia che costringe improvvisamente le persone a lavorare da casa. Purtroppo negli ultimi tre anni i cybercriminali che agiscono sferrando attacchi ransomware si sono sempre più frequentemente serviti di questa piattaforma di accesso remoto per infiltrarsi nei sistemi e causare danni su vasta scala alle imprese, ottenendo pagamenti sostanziali dalle loro vittime.

Tentativi di accesso tramite RDP in base agli honeypot

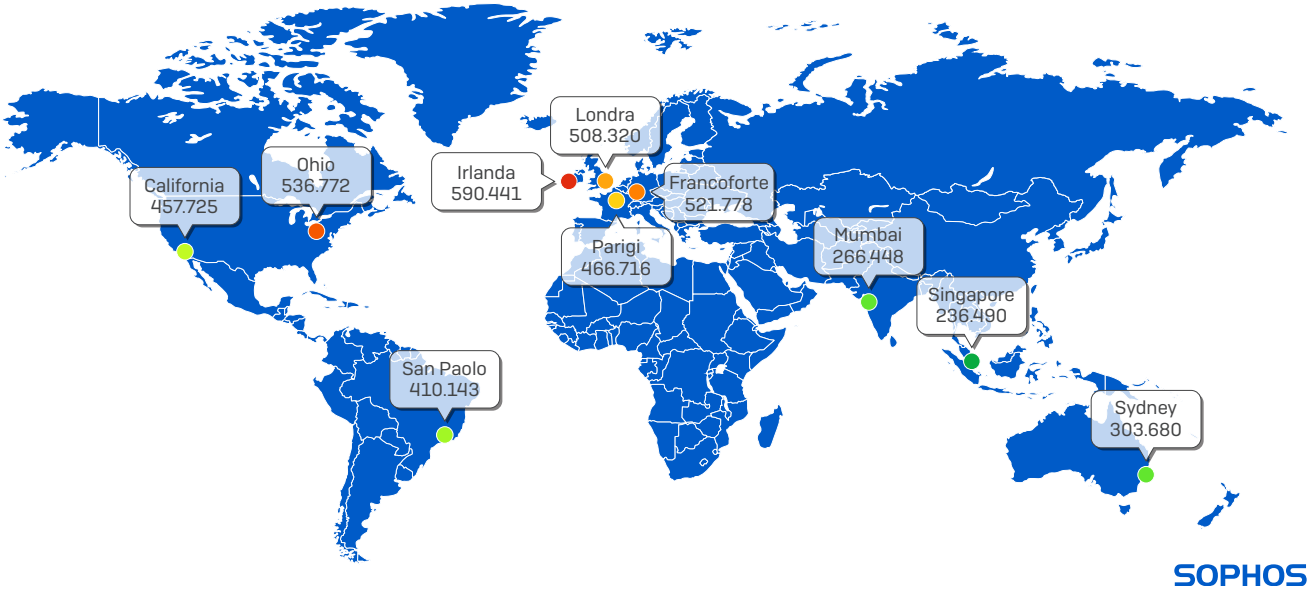


Fig.7. Abbiamo distribuito honeypot in datacenter situati in varie parti del mondo e abbiamo permesso agli hacker di accedervi con attacchi brute force. I computer honeypot sono stati individuati "naturalmente", senza che venissero annunciati in alcun modo. La mappa indica quanti attacchi sono stati osservati in ogni honeypot durante il mese in cui abbiamo condotto i nostri test.

L'impatto dell'era del lockdown da COVID-19 non ha fatto altro che aggravare il problema, in quanto un numero sempre maggiore di organizzazioni e dipendenti sono stati costretti dalle circostanze a utilizzare RDP per rimanere operativi. Il rischio principale dell'RDP è che questa risorsa non era stata progettata per resistere al tipo di attacchi presenti sull'internet pubblico. Se la password dell'RDP è debole, facile da dedurre o se viene sottoposta ad attacchi brute force con tentativi di accesso automatizzati, l'hacker può infiltrarsi nella rete e muoversi come desidera.

Il team Sophos che gestisce la risposta agli incidenti più gravi segnala che l'RDP rimane una delle principali "cause originarie" degli attacchi ransomware osservati. Il consiglio per i responsabili IT delle organizzazioni rimane lo stesso di sempre: RDP non dovrebbe mai essere connesso all'Internet pubblico. Deve essere piuttosto collocato dietro a un firewall che costringe gli utenti a connettersi tramite VPN o altri sistemi zero-trust. Inoltre, gli amministratori devono ottimizzare le policy per le password di Windows, in modo che prevedano l'utilizzo di password più lunghe e dell'autenticazione a fattori multipli mediante token o app.

In una ricerca svolta prima del lockdown, Sophos ha configurato honeypot in 10 datacenter situati in varie parti del mondo, al fine di comprendere meglio la gravità del problema. In un periodo di 30 giorni, gli honeypot hanno ricevuto in media 467.000 tentativi di accesso tramite RDP, equivalenti a circa 600 tentativi all'ora in ciascun datacenter. Dalla ricerca è emerso che ciascun honeypot riceveva un flusso di tentativi di accesso sempre più frequenti e aggressivi, fino a quando non abbiamo concluso l'esperimento.

I 5 principali nomi utente utilizzati in tutti i tentativi di accesso non riusciti

NOME UTENTE	TENTATIVI DI ACCESSO NON RIUSCITI
administrator	2.647.428
admin	376.206
user	79.384
ssm-user	53.447
test	42.117

Fig.8. I tentativi brute force tramite Remote Desktop Protocol utilizzano i più comuni nomi utente Windows, incluso l'account predefinito "administrator". Fonte: SophosLabs.

Business Email Compromise e Business Email Spoofing

Business Email Compromise (BEC) è il nome ufficiale di un tipo di spam specifico che cerca di ottenere un pagamento in maniera fraudolenta. In un attacco BEC, gli spammer inviano messaggi camuffati da comunicazioni ufficiali provenienti da un dirigente di alto livello di un'azienda. I messaggi sono rivolti a dipendenti di livello inferiore e richiedono il trasferimento di fondi o acquisti per conto di quel dirigente. Gli hacker possono falsificare l'aspetto dei messaggi di posta interni (una strategia talvolta denominata Business Email Spoofing) o in alternativa possono assumere controllo degli account del server di posta dell'organizzazione, per poi utilizzarli per inviare la richiesta fraudolenta.

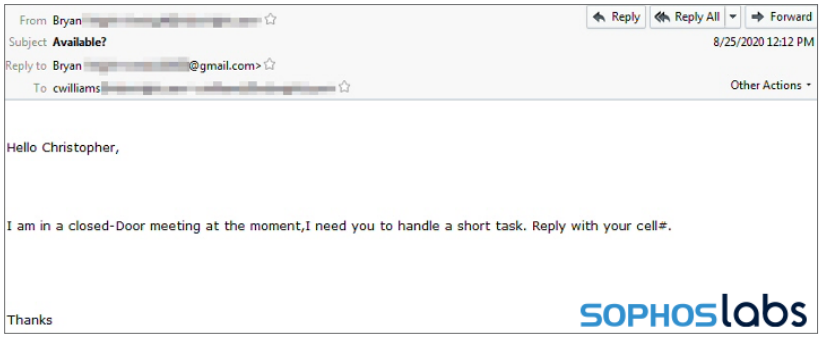


Fig.9. In questo esempio di Business Email Compromise tratto da un caso vero, il truffatore finge di essere un dirigente che chiede a un dipendente di rispondere a una richiesta urgente. L'e-mail ha un indirizzo di risposta diverso (un account Gmail) da quello del mittente nell'intestazione: una prova inconfutabile che c'è qualcosa che non va, sempre che la vittima faccia attenzione alle intestazioni dei messaggi e-mail. Fonte: SophosLabs.

Gli hacker di BEC, che cercano di assumere l'identità di un dirigente, potrebbero chiedere al dipendente di acquistare costose carte regalo o di concludere transazioni finanziarie di vario genere. Di solito gli attacchi sono rivolti a individui e organizzazioni specifici. I messaggi e-mail di BEC hanno un aspetto completamente diverso da quelli di spam, perché non seguono i modelli tipici dello spam: spesso non contengono allegati o link malevoli e sembrano essere comunicazioni interne dell'organizzazione. A volte includono "firme" tipiche dell'organizzazione o altri elementi riconoscibili dai dipendenti, allo scopo di assumere un'apparenza più convincente per le vittime, a differenza delle e-mail di spam.

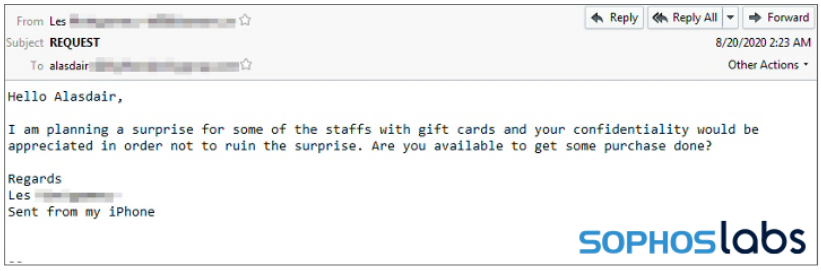


Fig.10. Una volta che la vittima ha preso atto della richiesta iniziale, il truffatore procede con la "vera" richiesta, accompagnata da un pretesto plausibile. Fonte: SophosLabs.

Le truffe di tipo BEC puntano sulla distanza fisica tra la vittima della truffa (il dipendente) e il presunto mittente del messaggio (il dirigente). Inoltre, dipendono dalla rapidità di azione della vittima, in quanto la richiesta deve essere completata prima che qualcuno possa rendersi conto di quello che sta accadendo e impedisca al dipendente di acquistare carte regalo o effettuare bonifici bancari. I truffatori di BEC possono inviare il messaggio quando sanno che il dirigente non è reperibile per via di un viaggio d'affari.

Questi tipi di richieste fraudolente spesso implicano lo scambio di vari messaggi tra cybercriminali e vittime. La conversazione potrebbe iniziare con una semplice richiesta di risposta all'e-mail dell'hacker, per poi trasformarsi in una serie di messaggi che portano alla "vera" richiesta di acquisto, sulla base di un pretesto plausibile.

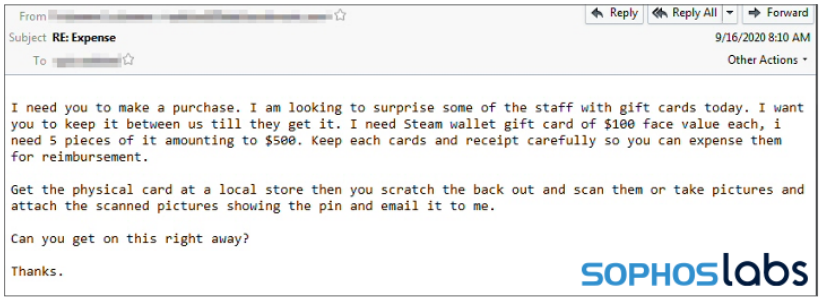


Fig.11. A un certo punto dell'attacco il truffatore di BEC farà una richiesta che va contro ogni regola di buon senso, come ad esempio il bonifico di un'ingente somma di denaro a favore di un conto che la vittima della truffa non riconosce. Questo presenta un'ottima occasione per qualsiasi dipendente avveduto di mettere in discussione la legittimità della richiesta: perché il dirigente chiede di grattare il PIN della carta regalo e ne vuole una fotografia, se si tratta di regali per altre persone? Fonte: SophosLabs.

Quando la maggior parte di noi lavorava in ufficio, la vicinanza fisica tra vittima e presunto mittente del messaggio avrebbe subito rivelato la truffa. Tuttavia, il nostro ambiente di lavoro distribuito, nel quale è raro che dirigenti e dipendenti si trovino nello stesso luogo fisico, rende impossibile recarsi personalmente alla scrivania di un'altra persona per chiedere di confermare la richiesta.

Le truffe BEC esistevano anche prima dell'era del COVID-19, ma ora che le persone lavorano da remoto, questi truffatori sono a caccia di vittime. Poiché questo attacco sfrutta la tendenza naturale di molte persone a volere essere di aiuto, si tratta di un tipo di truffa particolarmente efficace. Se si dovesse ricevere un'e-mail come questa, la nostra raccomandazione è quella di fidarsi del proprio istinto e parlare direttamente con il mittente, se possibile, o in alternativa di chiedere consiglio a un'altra persona. Più sono i dipendenti effettivi coinvolti nella gestione di queste richieste, maggiore sarà la probabilità di smascherare la truffa prima che possa causare qualsiasi danno.

Le stranezze della scienza: un glitch retrò di Office colpisce ancora

Quando si tratta di documenti di Office dannosi (maldoc) e degli exploit che cercano di distribuire, le vecchie strategie continuano a riproporsi, svaniscono dopo un aggiornamento di Microsoft che risolve il problema e infine (a volte) ritornano. Da diversi anni i SophosLabs monitorano le strategie utilizzate dagli hacker per incorporare nei maldoc un'ampia varietà di exploit cambiati frequentemente. Spesso i cybrecriminali che utilizzano i maldoc come punto di partenza per i loro attacchi prediligono le nuove vulnerabilità, in quanto non tutti gli utenti installano subito le patch. Inoltre, a volte i vendor di sicurezza impiegano del tempo prima di implementare una difesa protettiva basata sul comportamento o altre caratteristiche del nuovo vettore.

La maggior parte dei maldoc osservati negli ultimi 12 mesi è stata creata con strumenti detti "generatori", che offrono agli hacker un sistema di menu di tipo "punta e clicca", che consente loro di decidere quale o quali exploit includere nel documento dannoso. Siccome gli strumenti di protezione endpoint si sono migliorati nelle capacità di identificazione di questi exploit più moderni, che solitamente prevedono l'utilizzo di script incorporati nel documento, gli autori dei maldoc sembrano aver ripescato un bug di vecchia data che aiuta a nascondere le macro o altri contenuti dannosi in un documento.

Questo bug viene comunemente detto exploit **VelvetSweatshop**, sebbene non si tratti affatto di un exploit. VelvetSweatshop fu introdotto da Microsoft in Microsoft Office 2003, anche se ha cominciato a essere utilizzato in maniera impropria solamente dal 2013, quando le cartelle di lavoro di Excel che sfruttavano la vulnerabilità CVE-2012-0158 sono state mascherate con l'aiuto di questo glitch. Un foglio di calcolo di Excel o file .doc di Word veniva contrassegnato come file "di sola lettura" ed era semplicemente un documento protetto con password contenente una password predefinita di... Esatto: VelvetSweatshop.

Quest'anno abbiamo osservato l'utilizzo di molti fogli di calcolo di Excel che sfruttavano questa tecnica come stratagemma per eludere il rilevamento avanzato delle minacce. Poiché il file è cifrato, il vero contenuto malevolo viene nascosto dietro un potente sistema di crittografia e risulta inaccessibile agli antivirus, che non riescono a eseguire la scansione, a meno che non supportino l'ultimo algoritmo impiegato dagli hacker. Siccome viene utilizzata la password predefinita, Excel apre il contenuto cifrato senza richiedere la password, per cui per l'esecuzione la cifratura è trasparente. I programmi di protezione endpoint hanno aggiunto supporto per la cifratura e la password predefinita, ma i cybercriminali continuano a trovare nuovi algoritmi crittografici, che presentano le stesse caratteristiche ma non sono stati (ancora) inclusi nelle scansioni AV.

Siamo rimasti alquanto sorpresi dalla scoperta di un bug talmente longevo che, se fosse un essere umano, frequenterebbe l'ultimo anno di scuola. Tuttavia, non sorprende che gli autori di builder di documenti da utilizzare con intento malevolo abbiano cercato di servirsene.

Sicurezza informatica: una retrospettiva di 20 anni

Sebbene un rapporto annuale offra la possibilità di passare in rassegna gli eventi significativi degli ultimi 12 mesi, riteniamo che un viaggio indietro nel tempo (analizzando gli ultimi due decenni) possa fornire un contesto pertinente per l'attuale panorama delle minacce. L'inizio del nuovo millennio è stato un punto di svolta per la sicurezza informatica, che è diventata una disciplina professionale, nonché una vera e propria industria. Questa cronologia di minacce ed eventi scandisce i momenti significativi nell'evoluzione del comportamento delle minacce.

Man mano che l'utilizzo di internet sia per scopi professionali che di intrattenimento si diffondeva tra imprese e singoli individui, le reti diventavano bersagli ideali per worm emergenti ed estremamente prolifici: il malware autopropagante. I worm hanno infettato complessivamente decine di milioni di sistemi in tutto il mondo, con danni e costi di riparazione pari a più di 100 miliardi di $.

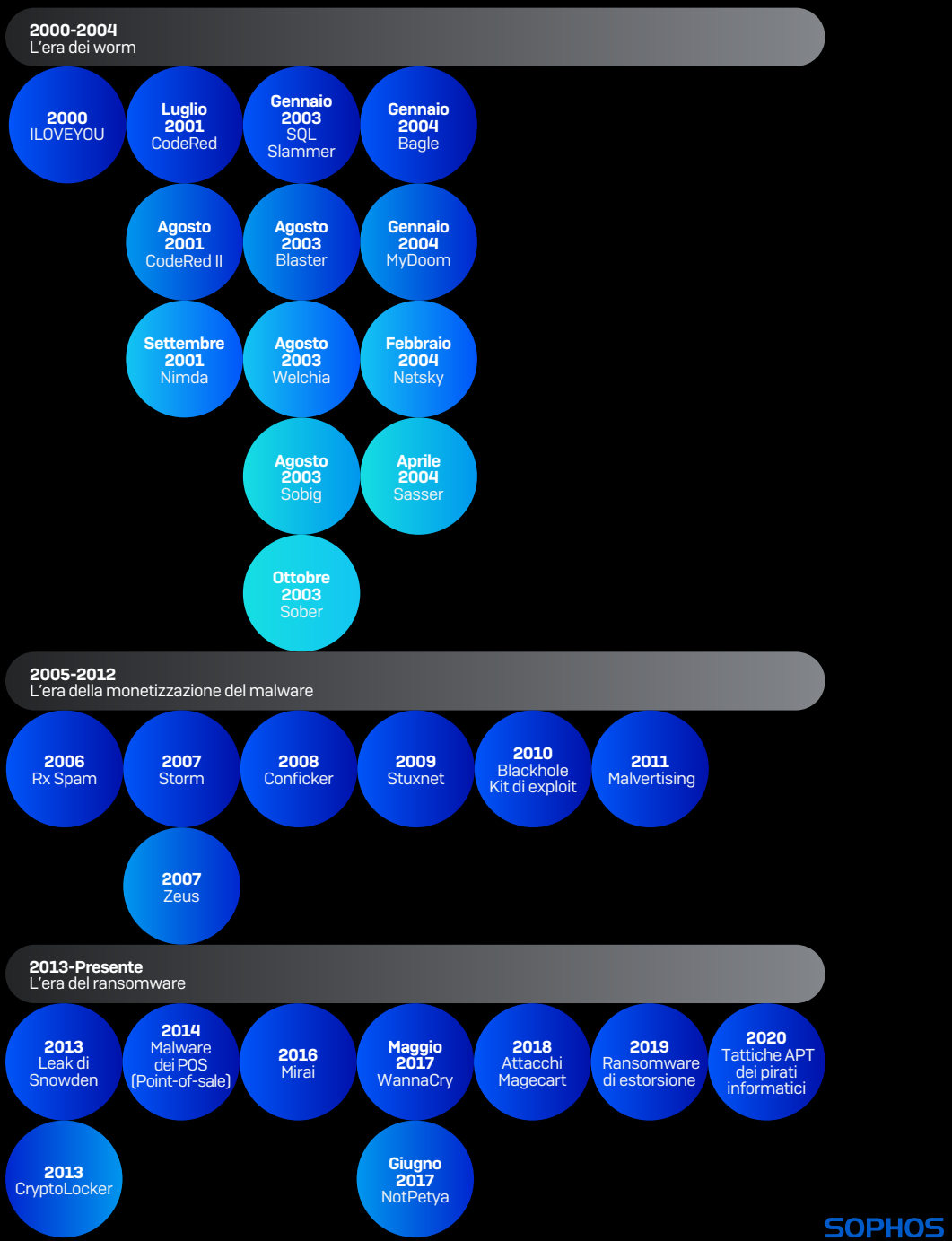


Fig.12. Fonte: Sophos

2000-2004 - L'era dei worm

2000 - ILOVEYOU
Il worm ILOVEYOU sfruttava uno stratagemma di social engineering che persiste ancora oggi: veniva inviato come allegato e-mail di spam ed è riuscito a infettare circa il 10% di tutti i computer Windows connessi a Internet.

Luglio 2001 - CodeRed
Con un nome ispirato a una varietà di Mountain Dew, al tempo la bevanda preferita degli esperti che l'hanno scoperto, CodeRed utilizzava una vulnerabilità di tipo buffer overflow in IIS per diffondersi e rovinare i siti web. Un mese dopo ne è emersa una versione aggiornata, che installava una backdoor sui computer connessi alla rete.

Agosto 2001 - CodeRed II

Settembre 2001 - Nimda

Gennaio 2003 - SQL Slammer
Con soli 376 byte, Slammer sfruttava un buffer overflow nelle applicazioni database di Microsoft. Raddoppiando il tasso di infezione ogni 8,5 secondi, Slammer è riuscito a disattivare porzioni significative di Internet in soli 15 minuti.

Agosto 2003 - Blaster
Blaster è stato creato tramite il reverse engineering di una patch Microsoft, precedendo di pochi mesi il primo Patch Tuesday. Sfruttava una vulnerabilità buffer overflow nel servizio RPC dei sistemi Windows XP e 2000 e sferrava un attacco DDoS contro windowsupdate.com se nella data corrente il giorno del mese era successivo al 15 o se il mese era successivo a settembre.

Agosto 2003 - Welchia

Agosto 2003 - Sobig

Ottobre 2003 - Sober

Gennaio 2004 - Bagle

Gennaio 2004 - MyDoom
Si ritiene che il 25% di tutte le e-mail inviate nel 2004 abbia avuto origine dal worm MyDoom, che proliferava inviandosi tramite e-mail a nuove vittime e sferrando attacchi Denial-of-Service (DDoS).

Febbraio 2004 - Netsky

Aprile 2004 - Sasser

2005-2012 - L'era della monetizzazione del malware
Fino al 2005 circa, le cause degli incidenti di malware potevano essere attribuite a una particolare curiosità o all'intenzione di causare disagi. Il malware prevalente era quello delle botnet, progettato a scopo di invisibilità e profitto. Questa era ha visto anche l'inizio del cosiddetto spam farmaceutico. Gli exploit che sfruttavano le vulnerabilità dei software sono diventati elementi essenziali del malware, dando vita al malvertising. Ovunque ci fosse un'opportunità di guadagno, i cybercriminali la sfruttavano.

2006 – Rx Spam
Quella che in passato era stata una semplice seccatura (o un metodo per propagare worm) diventava ora un'attività a scopo di lucro che prevedeva la vendita di farmaci disponibili su prescrizione medica, solitamente contraffatti, e promossi tramite spam. Si ritiene che gli "spammer farmaceutici" abbiano ricavato miliardi di dollari dalla vendita di farmaci che sarebbe stato possibile ottenere semplicemente rivolgendosi al proprio medico.

2007 - Storm

2007 - Zeus

2008 - Conficker
Conficker ha infettato rapidamente milioni di computer in tutto il mondo, ma non ha causato gravi danni. Lo scopo effettivo di questo worm non è conosciuto, ma migliaia di host rimangono a tutt'oggi infettati, e il traffico di scansione di Conficker viene regolarmente rilevato come parte della "radiazione di fondo" di Internet.

2009 - Stuxnet
Stuxnet è stata una delle prime armi digitali a colpire un sistema fisico: le centrifughe nucleari utilizzate dallo stato dell'Iran per arricchire l'uranio. A tutt'oggi, molte minacce seguono le orme di Stuxnet, in quanto ha aperto permanentemente la via all'utilizzo del malware come strumento di guerra tra i governi.

2010 - Kit di exploit Blackhole
I kit di exploit (ovvero kit di strumenti creati per sfruttare le vulnerabilità dei software) hanno connesso diversi ambiti dell'ecosistema del cybercrimine. La nascita del Crimeware-as-a-Service può essere datata alla comparsa dei servizi offerti dagli autori del kit di exploit Blackhole.

2011 - Malvertising

2013-presente - L'era del ransomware
Il ransomware è la minaccia che ha avuto l'impatto più significativo su questa era. Sebbene worm, trojan di internet banking, malvertising e spam continuino a persistere, niente si avvicina alla forza distruttiva del ransomware. Si stima che i danni causati dagli attacchi ransomware negli ultimi 7 anni ammontino a migliaia di miliardi di dollari. Il ransomware è probabilmente anche la prima forma di malware ad aver svolto un ruolo nella morte di una persona. Inoltre, molte delle minacce odierne esistono fondamentalmente per consegnare malware e, proprio come per i kit di exploit, il ransomware ha dato un'ulteriore spinta a un ecosistema di cybercrimine già ben avviato.

2013 - I leak di Snowden

2013 - CryptoLocker
Nel corso della sua breve esistenza, CryptoLocker ha fornito ai cybercriminali una formula vincente, grazie alla combinazione di due tecnologie già esistenti: la cifratura e le criptovalute. CryptoLocker ha trasformato il panorama delle minacce in modo permanente, con conseguenze che persistono a tutt'oggi. A tre mesi dal suo rilascio, il portafoglio di Bitcoin utilizzato da CryptoLocker conteneva quasi 30 milioni di $.

2014 - Malware dei POS (Point-of-sale)

2016 - Mirai

Maggio 2017 - WannaCry
WannaCry, l'ibrido ransomware-worm più diffuso, ha dimostrato (ancora una volta) quanto possano essere gravi le conseguenze della mancata applicazione delle patch. Approfittava degli exploit prelevati illecitamente dall'NSA e rilasciati pubblicamente da The Shadow Brokers. Gli attacchi hanno costretto Microsoft a rilasciare aggiornamenti fuori banda per prodotti non supportati.

Giugno 2017 - NotPetya
NotPetya ha messo in ginocchio alcune delle più importanti aziende globali di spedizione e logistica, causando, a quanto si dice, danni che superano i 10 miliardi di $. Alcune delle imprese colpite non si sono ancora riprese completamente dal colpo.

2018 - Attacchi Magecart

2019 - Ransomware di estorsione
In un attacco sferrato contro il consiglio comunale di Johannesburg, in Sud Africa, i cybercriminali che utilizzano ransomware Maze hanno affiancato agli attacchi sferrati anche l'utilizzo dell'estorsione. Questi criminali non si sono solamente limitati a cifrare e prelevare illecitamente i dati, ma hanno anche minacciato di pubblicare le informazioni rubate, a meno che non venisse effettuato un pagamento. Questa tattica è stata imitata da molti altri gruppi di cybercriminali, che la utilizzano come piano di riserva contro le vittime che posseggono backup validi.

2020 - Tattiche APT dei pirati informatici
L'impiego di strumenti e tattiche di livello governativo, che ha avuto inizio negli ultimi anni, è diventata una tendenza dominante nel 2020. Le gang di professionisti del cybercrimine sfruttano strumenti sofisticati del calibro di Cobalt Strike per provocare danni devastanti, mentre altri attacchi (Dharma) li includono all'interno di toolkit di facile utilizzo per gli hacker alle prime armi.

IL RUOLO DEL COVID-19 COME MOLTIPLICATORE DELLA FORZA DEGLI ATTACCHI

Il nuovo coronavirus, COVID-19, ha avuto un impatto enorme su tutti gli aspetti della cybersecurity. I pirati informatici sono diventati più spavaldi e hanno cominciato a prendere di mira il personale, anche dirigente, che lavora in smart working. Le paure e le preoccupazioni che si sono diffuse tra le persone in generale sono state aggravate dalle ondate di campagne di spam e ransomware realizzate per attaccare istituzioni già indebolite o allo stremo, oltre a organizzazioni della società civile che già si trovavano ad affrontare una forte pressione finanziaria. Per non parlare dei vari tipi di truffe alla ricerca di rendita e delle speculazioni su qualsiasi oggetto difficile da reperire, dai DPI alla carta igienica.

La casa come nuovo perimetro di rete

La vita normale è cambiata nel mese di marzo del 2020, quando i lavoratori che potevano lavorare da remoto e gli studenti di qualsiasi età sono stati costretti a rimanere a casa nel disperato tentativo di arrestare la diffusione del COVID-19 e limitare la pressione su ospedali già sovraffollati. Improvvisamente ci siamo trovati non tanto a lavorare da casa, bensì a vivere al lavoro.

Molte persone hanno fatto fatica ad adattarsi a una nuova normalità che non prevedeva il tragitto da casa a ufficio. La richiesta di soluzioni di accesso tramite VPN e servizi di autenticazione a fattori multipli ha subito un'impennata. I Chromebook sono diventati difficili da trovare. In soli due mesi Zoom ha subito una crescita evolutiva che normalmente avrebbe richiesto dieci anni. Inoltre, mentre avveniva tutto questo, Microsoft, Adobe, Apple e Google effettuavano aggiornamenti e rilasci di manutenzione con varie patch per diverse piattaforme.

Truffe via e-mail a tema COVID-19 e Coronavirus in forte aumento

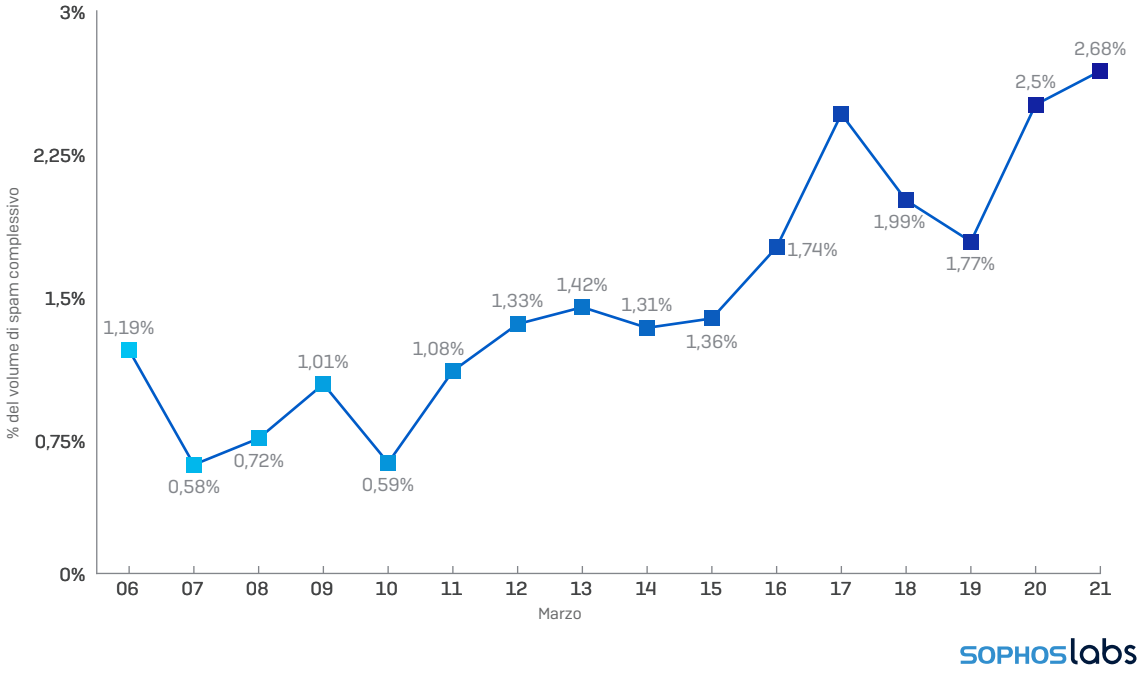


Fig.13. Dopo il primo lockdown è stato rilevato a livello mondiale un numero significativo di e-mail di spam che citano i termini COVID-19 o Coronavirus. Fonte: SophosLabs.

Il COVID-19 ci ha fatto diventare tutti esperti informatici: abbiamo infatti dovuto gestire patch, scaricare aggiornamenti di sicurezza e risolvere problemi di connettività che ci avrebbero altrimenti impedito di partecipare a meeting di lavoro o di permettere ai nostri figli di frequentare una lezione virtuale. È aumentata la richiesta di cuffie, microfoni, sistemi di illuminazione e soluzioni di protezione per rete ed endpoint. Inoltre, abbiamo dovuto sottoporre i ragazzi più giovani a un corso intensivo su phishing, spam, troll, cyberbullismo e malware camuffato da copia gratuita di un gioco pronto per essere avviato.

Non è stato un periodo facile e a tutt'oggi non lavoriamo allo stesso ritmo del mese di febbraio 2020, ma per molti la nuova normalità potrebbe essere, sotto certi aspetti, un'evoluzione positiva. Molti uffici hanno preso la decisione di autorizzare lo smart working anche al termine del lockdown e del divieto di presenza fisica dei dipendenti sul posto di lavoro, con notevoli potenziali vantaggi sia per l'ambiente che per la qualità della vita delle persone.

Con l'espansione dei perimetri dei posti di lavoro, in modo da includere tutti i dipendenti in smart working, le circostanze hanno messo in luce la gravità della situazione in termini di come viene considerato il ruolo delle reti domestiche quali ultima linea di difesa. Il modem nel mobiletto all'ingresso è diventato il perimetro di rete. Dobbiamo reinventare il modo con cui viene garantita una difesa che agisce in profondità.

Crimeware as-a-Service

Può essere utile considerare i creatori di malware come una sorta di startup tecnologica. All'inizio i loro tentativi sembrano goffi, ma presto acquisiscono un seguito. Inoltre, i software dannosi possono avere un business model, proprio come i software legittimi.

Il termine "crimeware" è intenzionalmente inclusivo: alcuni autori di malware (o di strumenti che ne semplificano la distribuzione o l'ottimizzazione con nuove funzionalità) non vendono direttamente i propri prodotti, bensì li concedono in licenza per un anno come avviene per Adobe Creative Suite. Abbiamo denominato questa categoria di business model "Crimeware-as-a-Service," (CaaS), e prevediamo che sarà tipica della nuova normalità.

Uno degli esempi più tristemente noti di malware CaaS è Emotet. Questo trojan distribuito tramite spam è in circolazione da diversi anni e sembra essere progettato per garantire agli aspiranti criminali un'esperienza semplice e priva di problemi. Emotet appartiene a una classe di malware collettivamente nota ai ricercatori con il nome di "loader". La funzione principale di Emotet è consegnare altro malware sul computer di una vittima. Agisce sfruttando una complicata rete progettata per distribuire e-mail di spam utilizzate con intento malevolo per infettare un numero elevato di vittime.

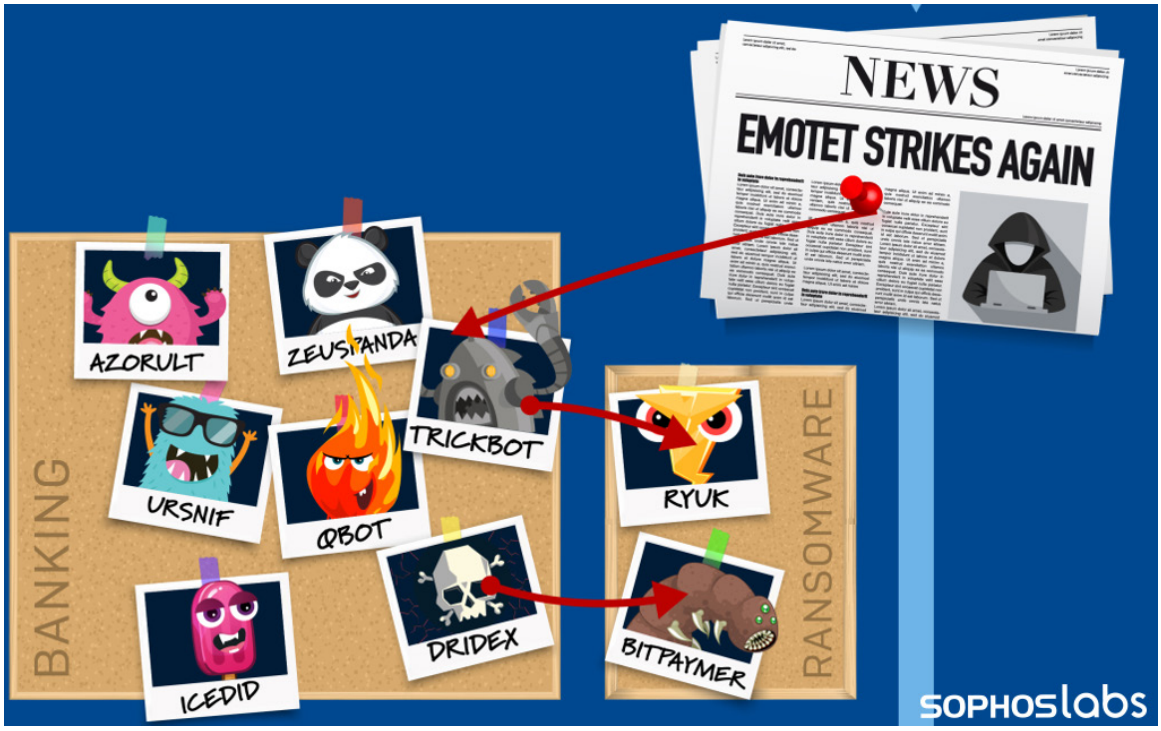


Fig.14. Fonte: SophosLabs.

Tuttavia, quest'anno Emotet ha attraversato due momenti particolarmente difficili. Il malware ha mantenuto la comunicazione con i propri server C2 per quasi cinque mesi, durante i quali le e-mail di spam che avrebbe dovuto consegnare per sferrare gli attacchi sono svanite nel nulla. Le e-mail di spam contenenti Emotet sono misteriosamente riapparse a luglio.

Il ransomware Dharma è un altro malware CaaS che merita di essere nominato. A differenza di altri ransomware più costosi, Dharma richiede un riscatto fisso e non troppo elevato. Questo è dovuto al business model di Dharma: è un ransomware di formazione per aspiranti criminali che devono apprendere i principi di base. I criminali che lo utilizzano pagano un abbonamento per ottenere payload dai creatori di Dharma e dividono con loro gli utili degli attacchi.

Gli hacker si stanno specializzando sempre di più e sembra che il business model utilizzato dai cybercriminali, basato sulla collaborazione con terzisti, freelancer e associati, non sia destinato a svanire nel futuro immediato.

Spam, truffe e promesse non mantenute

I lockdown in tutto il mondo sono stati seguiti da un'ondata di truffe per mezzo di e-mail di spam. In tempi di relativa tranquillità, le campagne di spam più efficaci cercano di suscitare nel destinatario un senso di urgenza ad agire come indicato nel messaggio. Si tratta di uno stratagemma psicologico noto, perché riflettendo anche solo qualche istante sui contenuti del messaggio di spam, probabilmente si capirebbe subito che si tratta di una truffa. Se lo spammer riesce a suscitare una reazione di paura, la vittima agisce prima di pensare e cade in trappola.

Il COVID-19 aveva già causato un nervosismo generale, per cui gli spammer non hanno dovuto neppure fare sforzi particolari.

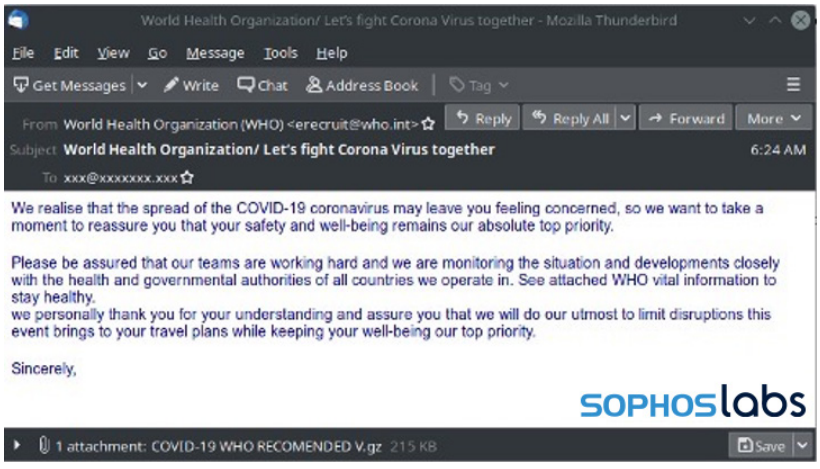


Fig.15. Fonte: SophosLabs.

Poche settimane dopo l'inizio del lockdown, abbiamo deciso di analizzare in maniera più approfondita un altro fenomeno: la registrazione di nuovi domini. Nel giro di poche settimane, erano stati registrate migliaia di nuovi domini contenenti una combinazione dei termini *COVID-19*, *Corona*, o *virus*.

Domain	First Seen	Nameserver	Ns Ip
coronavirusshaquilleoneal.com	2020-03-14 07:00:38	ns-cloud-b1.googledomains.com	216.239.32.107

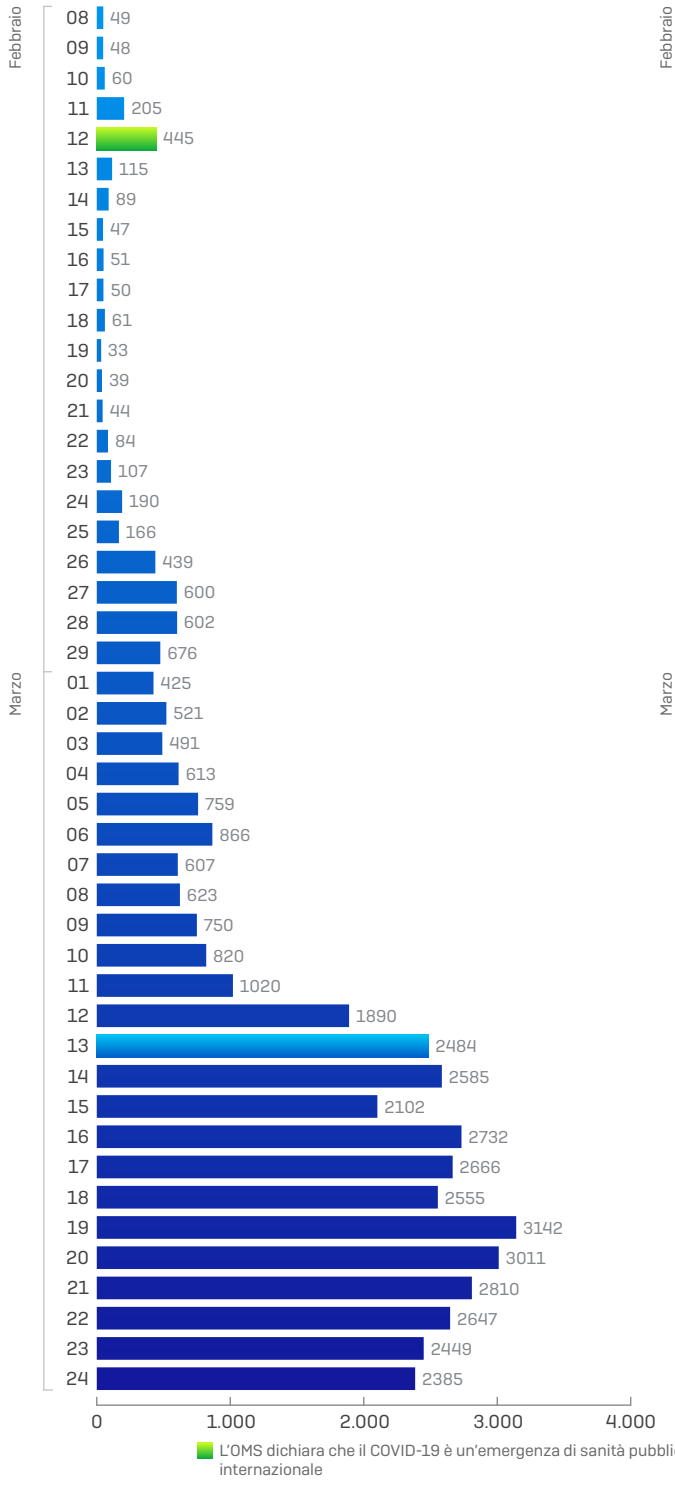
SOPHOSlabs

Fig.16. Fonte: SophosLabs.

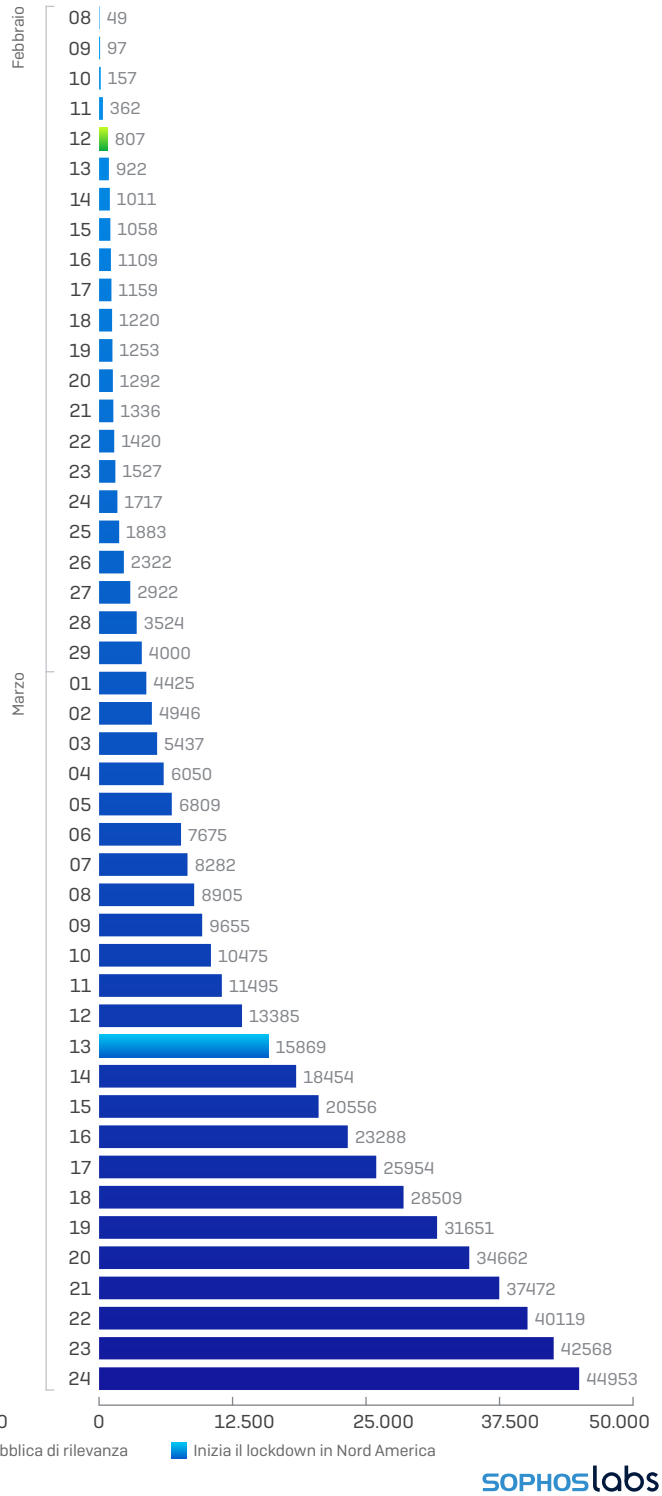
Alcuni di questi siti erano evidentemente stati creati a scopo umoristico, mentre altri presentavano nomi simili a quelli di enti sanitari legittimi, locali o nazionali.

Abbiamo anche cercato domini e sottodomini associati al COVID-19 nei log di trasparenza dei certificati TLS. I log di trasparenza dei certificati sono utili per rintracciare i sottodomini dotati di certificati TLS (un'informazione che non viene visualizzata nei dati di registrazione di nuovi domini) e nomi di dominio.

Nuovi domini COVID registrati, al giorno



Totale di nuovi domini a tema COVID, ad oggi



SOPHOSlabs

Fig.17. Nei primi mesi della crisi da COVID-19, sono state registrate migliaia di domini (e almeno altrettanti certificati) al giorno, contenenti le parole "COVID-19" o "corona". Fonte: SophosLabs.

Nuovi certificati TLS al mese con i termini “COVID-19” o “corona” nel nome host

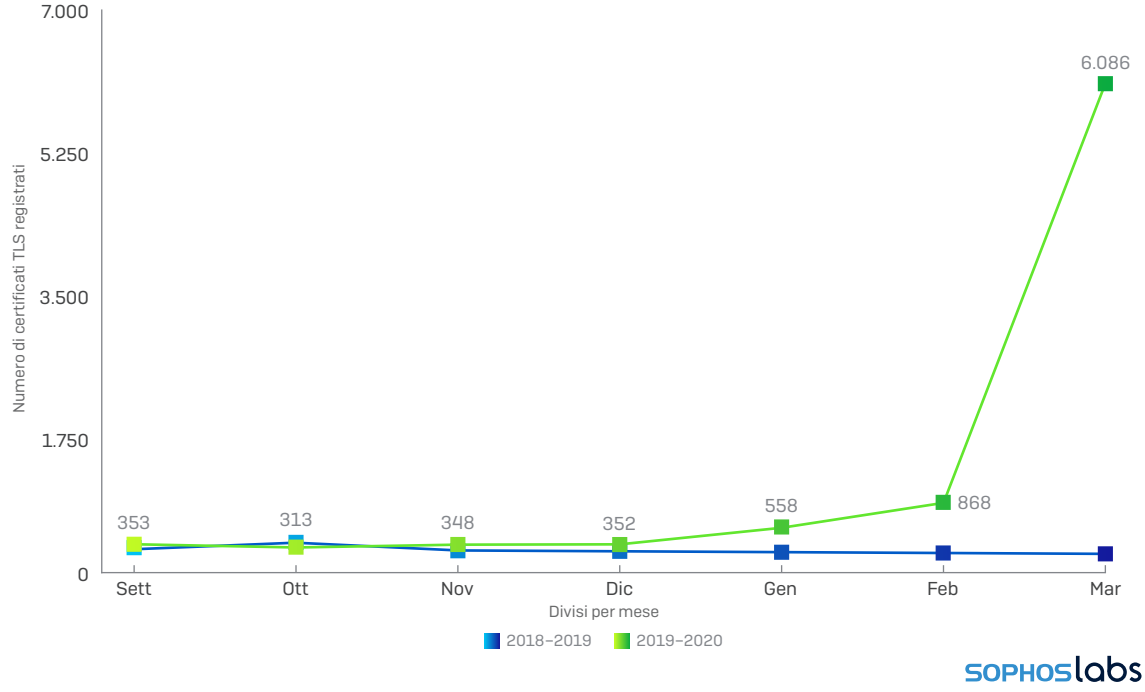


Fig.18. Le registrazioni di certificati TLS con riferimenti alla pandemia sono aumentate quasi di pari passo con le registrazioni di domini. Fonte: SophosLabs.

Abbiamo osservato una media giornaliera di più di 200 richieste di certificato per domini inerenti al COVID-19 nel mese di marzo, con un tasso che ha continuato a salire nei mesi successivi. A giugno, la media era di 625 al giorno, mentre a ottobre ha raggiunto il picco di 951 nuove richieste di certificati TLS al giorno.

Nella maggior parte dei casi, questi domini continuano a dimostrarsi legittimi o innocui, sebbene molti rimangano inattivi e privi di contenuti, il che indica che i proprietari potrebbero lasciarli “maturare” per utilizzarli in futuro a scopo di verifica della reputazione.

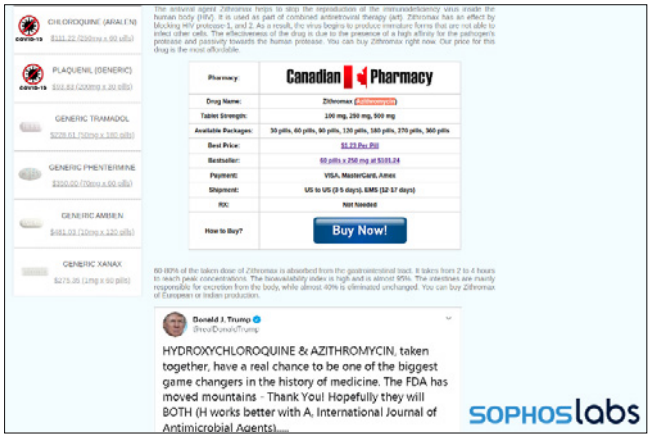


Fig.19. Neppure le classiche truffe basate sui farmaci sono riuscite a resistere alle nuove cure miracolose proposte su Twitter, e hanno persino incluso i tweet nei loro annunci. Fonte: SophosLabs.

Una piccola percentuale (meno dell’1%) ha dimostrato di essere associata a phishing o malware. Molti sono fugaci, con nomi host che non possono essere usati anche solo poco più di 24 ore dopo.

Lo smart working aumenta l'importanza della protezione del cloud computing

All'inizio dei lockdown da COVID-19 a marzo 2020 è cominciato un processo di transizione mai osservato prima, ma tuttora in corso, che ha coinvolto persone e posti di lavoro. Con molta probabilità, il modo in cui lavoriamo, andiamo a scuola, ci divertiamo o partecipiamo a eventi e conferenze è cambiato per sempre. Il cloud computing ha svolto un ruolo fondamentale in questa rapida evoluzione, ma presenta molte sfide.

Il provisioning di autorizzazioni di accesso eccessive, la visibilità limitata sulle risorse e sugli asset nel cloud e la mancanza di adeguati controlli possono rendere gli ambienti cloud più vulnerabili alle minacce informatiche, mentre il malware imperversa sul cloud tanto quanto sugli ambienti fisici. Il cryptojacking è il tipico esempio di un problema in costante crescita che riguarda il cloud. I processi di cryptomining basati sui cicli informatici sono già abbastanza pericolosi quando si eseguono su computer fisici e incidono sulle bollette elettriche. Tuttavia, quando si eseguono su istanze cloud, causano un effetto collaterale ancora più devastante: alla vittima viene addebitato l'utilizzo dei servizi cloud per i cicli di CPU utilizzati dalle workstation virtuali che svolgono i difficili calcoli matematici necessari per far guadagnare agli hacker l'equivalente in criptovaluta di pochi centesimi di Euro.

Inoltre, in molti casi, la forza lavoro in remoto subisce attacchi ransomware durante i quali i cybercriminali isolano l'infrastruttura cloud nello stesso modo in cui bloccano i computer fisici. Dopotutto, il ransomware è in grado di cifrare dischi rigidi o spazi di archiviazione degli oggetti con la stessa semplicità delle risorse di archiviazione fisiche. Le organizzazioni con infrastrutture cloud colpite dal ransomware potrebbero essere costrette a pagare non solo per l'utilizzo dei cicli di CPU necessari per cifrare i dati, ma anche per il riscatto.

Organizzazioni colpite da incidenti di sicurezza nel corso dell'ultimo anno

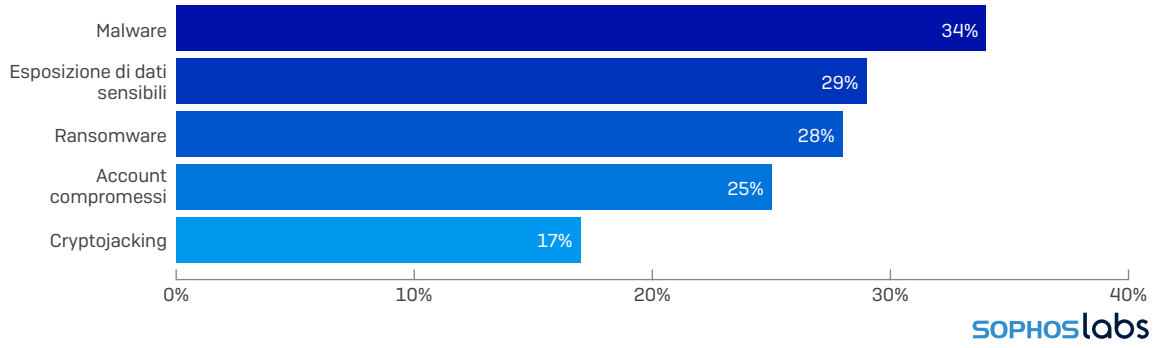


Fig.20. Nel nostro Report sulla cloud security per il 2020, abbiamo intervistato più di 3.500 professionisti del settore IT in merito alla loro esperienza di utilizzo del cloud e abbiamo rilevato che molti dei problemi di sicurezza che affliggono le reti fisiche si sono spostati su quelle virtuali. Fonte: SophosLabs.

Durante il lockdown, i reparti IT delle organizzazioni hanno avuto bisogno di trovare un modo per impostare una helpdesk virtuale che svolgesse le stesse funzioni di cui si occupava la loro helpdesk fisica prima della chiusura degli uffici. Le principali necessità di cambiamento dettate dal COVID-19 sono state introdotte in tre ondate.

Durante le prime settimane di lockdown, si è cominciata a formare la prima ondata: un'ondata di accesso. Milioni di dipendenti si sono trovati improvvisamente impossibilitati a recarsi sul posto di lavoro, per cui hanno avuto bisogno di accedere alle risorse dell'ambiente della propria organizzazione da remoto. Il rapido aumento della richiesta di strumenti di accesso tramite VPN (Virtual Private Network) o sistemi zero-trust ha sovraccaricato le risorse esistenti. Oltre alle VPN, le organizzazioni si sono trovate ad aver bisogno di nuovi firewall e altre appliance di sicurezza, nonché a dover installare sistemi di Unified Threat Management moderni per incrementare la sicurezza dei rudimentali firewall layer-3 dei servizi cloud.

Nel mondo pre-COVID-19, le VPN venivano utilizzate relativamente poco, in quanto il numero di dipendenti fisicamente presenti sul posto di lavoro superava quelli in viaggio o connessi da remoto. Giunti a maggio e poi a giugno, la VPN per questi dipendenti era ormai diventata un'ancora di salvezza indispensabile (se non persino insostituibile), che manteneva operative le organizzazioni.

Tuttavia, queste organizzazioni hanno capito velocemente che non era consigliabile che i dipendenti utilizzassero i dispositivi personali per accedere alla VPN da casa, e la scarsa disponibilità di nuovi laptop è diventata una nuova sfida per le organizzazioni che già faticavano a gestire le esigenze informatiche di una forza lavoro distribuita. Senza una quantità adeguata di computer fisici, le organizzazioni si sono provvisoriamente affidate alla risorsa apparentemente illimitata delle virtual machine per soddisfare la propria esigenza di un'area di lavoro sicura. Ha così avuto inizio la seconda ondata: l'ondata dei desktop virtuali.

Con l'aumentare del numero di dipendenti che cominciavano a utilizzare desktop aziendali virtuali, la soluzione più pratica ed economicamente vantaggiosa è stata passare all'hosting sul cloud. Tuttavia queste risorse dovevano essere protette.

Improvvisamente, i reparti IT hanno dovuto supportare centinaia o migliaia di VM dei dipendenti, e altrettanto improvvisamente è sorta la necessità di strumenti in grado di compilare un inventario e configurare in maniera sicura la sempre più elevata quantità di server virtuali, desktop virtuali e altri servizi cloud: l'ondata della gestione del cloud.

Cronologia di attacco

Fig.21. Un attacco di cryptojacking che abbiamo analizzato ha avuto inizio dopo che uno sviluppatore ha incorporato per errore le proprie credenziali cloud nel codice archiviato in un repository pubblico. L'hacker ha individuato e successivamente utilizzato queste credenziali per sferrare l'attacco, sfruttando le API native del provider di servizi cloud e lanciando centinaia di istanze di VM per minare Bitcoin. Allo stesso tempo, ha automatizzato le funzionalità di queste istanze per renderle più difficili da terminare. Successivamente, ha revocato l'accesso degli altri utenti legittimi.
Fonte: SophosLabs.

L'era del COVID-19 è caratterizzata da enormi trasformazioni in ogni ambito dell'esistenza umana, incluso il modo in cui molte persone lavorano. In un recente sondaggio condotto da Reuters, il 97% dei CEO e dei CTO intervistati ha dichiarato che il lockdown ha accelerato la loro transizione a nuove tecnologie. Ma in tempi di limitazioni di budget e incertezze, quasi un CTO su tre ha indicato che il proprio compito consisteva nell'implementare questi cambiamenti in maniera meno dispendiosa possibile.

Nell'ultimo Report sulla cloud security di Sophos è emerso che la maggior parte degli incidenti di sicurezza che hanno colpito il cloud computing erano dovuti principalmente a due motivazioni di base: credenziali rubate o prelevate tramite phishing, oppure configurazioni errate che hanno portato a casi di violazione. Sette intervistati su dieci tra gli oltre 3.700 responsabili IT che hanno partecipato al sondaggio, hanno affermato che l'infrastruttura cloud supportata dalla loro organizzazione aveva subito una violazione nei 12 mesi precedenti al sondaggio.

CCTC entra in azione con una risposta rapida alle minacce

Fig.22. Fonte: Sophos.

A una settimana dall'inizio del lockdown da COVID-19, Joshua Saxe, Chief Scientist presso Sophos, ha lanciato un appello globale alla ricerca di volontari. Questa catena umana virtuale è presto diventata la COVID-19 Cyber Threat Coalition (CCTC), un'organizzazione composta da più di 4.000 membri aventi un unico obiettivo: impegnarsi a contrastare qualsiasi tipo di minaccia o di stratagemma di social engineering che cercasse di sfruttare, in maniera esplicita o implicita, la paura generale del pubblico suscitata dal COVID-19.

"Non sono un vigile del fuoco, per cui non saprei come aiutare in caso di incendio, ma posso assistere un team che si occupa di potenziare le difese delle infrastrutture critiche, come gli ospedali", dichiara Nick Espinosa, analista di sicurezza e podcaster residente a Chicago, membro della CCTC.

È stata un'iniziativa indispensabile. Fin dall'inizio del lockdown, i cybercriminali hanno disseminato spam, malware e moltissime altre minacce che utilizzavano, in forme diverse, il nuovo, terrificante gergo della pandemia. Come indicato nel testo principale del rapporto, a un certo punto le persone hanno cominciato a registrare migliaia di nuovi domini al giorno, contenenti le diciture COVID-19, corona o CoV nel nome. Sophos ha rintracciato domini correlati a certificati TLS con le stesse stringhe di testo nei dati del certificato, trovandone diverse altre migliaia.

La crescita dei membri della COVID-19 Cyber Threat Coalition

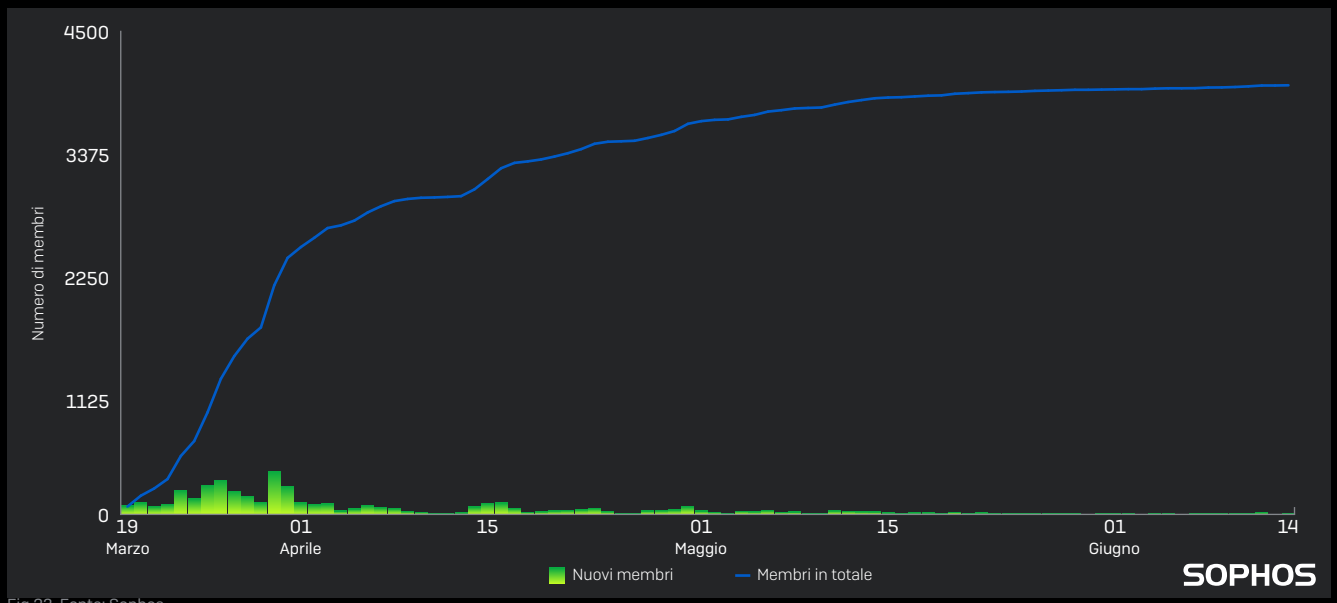


Fig.23. Fonte: Sophos.

Data l'unicità della natura della minaccia del COVID-19, i messaggi di spam dannosi che approfittano della crisi globale suscitano particolare indignazione. "Abbiamo osservato un incremento esponenziale dell'hacking criminale che utilizzava come esca il COVID-19", sostiene Espinosa. Sono emerse campagne di spam in cui gli spammer camuffavano i messaggi, spacciandoli per comunicazioni ufficiali dell'Organizzazione Mondiale della Sanità, del CDC negli USA, dell'NHS nel Regno Unito, di aziende farmaceutiche, o di altri enti sanitari in altri paesi.

Gli analisti hanno anche riscontrato riferimenti al COVID-19 in stringhe contenute in file binari e utilizzate come variabili nei cosiddetti LOLscript dei pacchetti Living-Off-the-Land.

I membri della CCTC hanno condiviso campioni e dati di intelligence su tutti i tipi di incidenti utilizzando un canale Slack creato rapidamente. Nonostante un inizio piuttosto caotico, l'organizzazione ha presto assunto una rudimentale forma di struttura. "Moltissime persone si sono unite e hanno cominciato a condividere informazioni a raffica", dichiara Espinosa.Il risultato del lavoro della CCTC, attraverso le informazioni raccolte, è il suo feed di intelligence che elenca i nuovi indicatori di compromissione (IoC) rilevati. Il feed è disponibile gratuitamente per chiunque. Questi IoC sono un'ulteriore risorsa che si aggiunge alle tecnologie di sicurezza già esistenti; inoltre, possono essere utilizzati in maniera indipendente da qualsiasi vendor. Quando la CCTC è entrata in partnership con la Cyber Threat Alliance, i vendor di sicurezza membri della CTA hanno amplificato l'effetto protettivo dei dati di intelligence sulle minacce della CCTC, inserendoli nelle proprie strategie e offrendo protezione contro queste minacce.

"La rapida unione di tutti questi professionisti della sicurezza con un obiettivo comune è stata commovente", sostiene Espinosa. "Probabilmente all'inizio eravamo disorganizzati", prosegue, "ma il gruppo ha trovato rapidamente un ordine". La realizzazione della piattaforma di condivisione CCTC significa che chiunque in futuro si trovi a dover rispondere a una pandemia simile a quella da COVID-19 non dovrà ripartire da zero e potrà rispondere con maggiore tempestività alle minacce, con un meccanismo metaforicamente analogo a quello del sistema immunitario negli esseri umani.

MAI ABBASSARE LA GUARDIA: ECCO LE MINACCE CHE SFRUTTANO PIATTAFORME NON CONVENZIONALI

Viviamo in un mondo circondato da dispositivi informatici che non sono né computer né server: router, telefoni cellulari, firewall, smart TV, dispositivi di streaming, dispositivi VoIP, videocamere e videocitofoni, sistemi di archiviazione connessi alla rete, alcune marche di elettrodomestici e così via.

Tuttavia, il fatto che non abbiano l'aspetto di un computer tradizionale non significa che non possano anch'essi venire utilizzati impropriamente o in maniera illecita.

Il volume del malware Joker per Android è in aumento

Gli utenti Android si trovano nel mezzo di una corsa alle armi tra Google (proprietaria della piattaforma Android e del principale Google Play Store) e gli autori del malware, che vogliono che i propri malware vengano elencati tra i download disponibili sul Google Play Store. Google ha trascorso diversi anni a realizzare un sistema progettato in modo da ispezionare il codice sorgente delle app Android che richiedono l'inclusione nel Google Play Store. Questo sistema cerca blocchi di codice che indichino intenti dannosi o che possano portare a esiti non desiderabili per un utente Android. Gli sviluppatori delle app contenenti malware hanno dovuto impegnarsi molto per riuscire a eludere i controlli del codice del Google Play Store.

Joker, detto anche Bread, è un'app fraudolenta che utilizza SMS a tariffa maggiorata, nonché uno dei migliori esempi di famiglia di malware che si è evoluta per eludere questi controlli del codice. Dall'anno scorso, non appena il problema è stato identificato dai ricercatori, Google ha rimosso dal Google Play Store migliaia di queste app dannose modificate da Joker. Nonostante l'impegno costante nel debellare il malware, Joker continua a ritornare.

Joker assume le sembianze di varie app: utilità e strumenti, sfondi, programmi di traduzione, servizi di messaggistica, ovvero moltissimi cloni delle app più comuni. Non bisogna inoltre dimenticare che Joker potrebbe venire incorporato in un'app che ha lo stesso aspetto e la stessa modalità operativa della versione autentica di un'app già utilizzata. Le app di Joker hanno semplicemente del codice di malware ben nascosto in una delle librerie di terze parti comunemente utilizzate dagli autori per motivi legittimi durante la compilazione delle proprie app.

Ci sono vari motivi per cui Joker riesce continuamente a eludere i controlli di sicurezza del codice del Google Play Store:

1. Le app dannose sfruttano l'offuscamento, che può variare dalla semplice sostituzione di una stringa all'utilizzo di complessi strumenti commerciali di creazione dei pacchetti, per rallentare le analisi ed eludere le verifiche del Google Play Store.
2. Quando lo "sviluppatore" di Joker avvia l'app, questa non contiene alcun codice dannoso. Questo stabilisce un precedente, ovvero un'occasione in cui l'app inclusa nel Google Play Store non conteneva minacce. Il codice dannoso fa la sua comparsa nell'app solo in un secondo momento, in seguito a un aggiornamento.
3. L'app agisce decifrando il proprio payload in fase di esecuzione, oppure lo scarica dinamicamente in un altro momento.

Il malware Joker utilizza codice nativo (JNI) invece del più comune codice DEX. Il codice nativo sfrutta il linguaggio C per la programmazione, che rallenta l'analisi alla ricerca di codice dannoso. DEX invece è una variazione del codice Java, per cui è molto più semplice da decompilare per renderlo leggibile in chiaro. Il malware utilizza questo codice JNI per inviare messaggi SMS, per generare un utile e come metodo per contattare la propria rete di comando e controllo. L'utilizzo di JNI e della segnalazione fuori banda utilizzando la rete telefonica invece di Internet può essere un fattore che aiuta Joker a eludere le scansioni automatiche di DEX non compatibili con JNI.

Joker si trova evidentemente in vantaggio nella battaglia contro l'analisi automatica di Google del codice delle nuove app. Per il 2021 non prevediamo un rallentamento della diffusione di Joker, che potrebbe anzi essere presto imitato da altri competitor.

Annunci e PUA diventano sempre più simili a vero e proprio malware

Gli annunci dannosi (malvertising) continuano a essere una delle principali cause di minacce per una serie di dispositivi. Recentemente abbiamo analizzato due trend attuali, riscontrati nelle minacce di malvertising, che non rientrano nell'ambio degli attacchi di malware: truffe relative alle attività di supporto tecnico che utilizzano il "blocco del browser" per le pagine web, e annunci che prendono di mira i dispositivi mobili e che sono associati ad app fraudolente o "fleeceware". Sophos classifica questi tipi di attacchi come "avvisi fasulli", ovvero annunci dannosi che cercano di incutere paura nelle vittime, inducendole a compiere un'azione che genererebbe un utile per i truffatori che hanno avviato l'attacco.

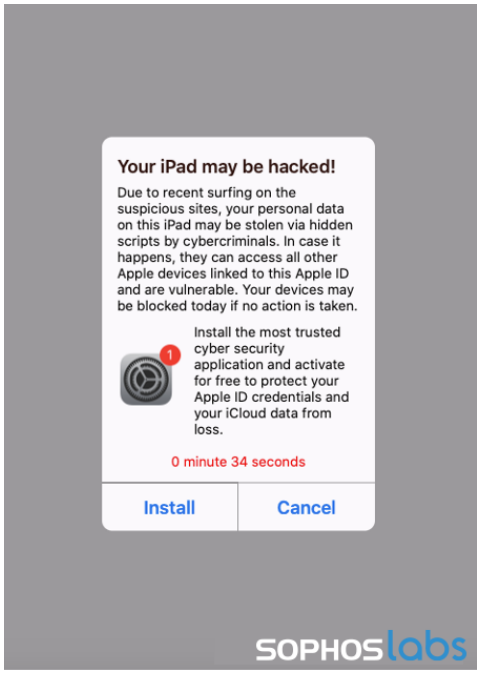


Fig.24. Fonte: SophosLabs

Solitamente, le truffe relative ad attività di supporto tecnico cercano di indurre le vittime a concedere accesso remoto ai propri computer, per poi convincerle ad acquistare software e servizi di supporto tecnico a prezzi esorbitanti, oppure a fornire dati di carta di credito da utilizzare a scopo fraudolento. Sebbene in passato queste truffe prevedessero chiamate dirette di telemarketing, oggi molti truffatori hanno adottato un modello che "attira" le vittime: utilizzano infatti annunci web per cercare di convincere gli utenti che i loro computer sono stati bloccati per motivi di sicurezza, inducendoli quindi a chiamare direttamente i truffatori.

Per raggiungere i propri obiettivi, i truffatori si servono di kit per i siti web contenenti script progettati per impedire a un utente di lasciare una pagina. Alcuni esempi possono includere variazioni degli attacchi "evil cursor" (che fanno sembrare che il puntatore del mouse si trovi in un posto diverso, oppure che lo rendono completamente invisibile) o "infinite download", che sovraccaricano il browser. Tutti gli avvisi cercano di imitare gli avvisi legittimi di Microsoft o Apple. Alcuni dei kit che abbiamo intercettato sfruttavano un bug che il team di sicurezza dei SophosLabs aveva rilevato in Firefox nei primi mesi dell'anno, mentre altri sferravano attacchi simili su altri browser. In ogni caso, venivano tutti diffusi tramite annunci web dannosi, nascosti dietro ad altri contenuti.

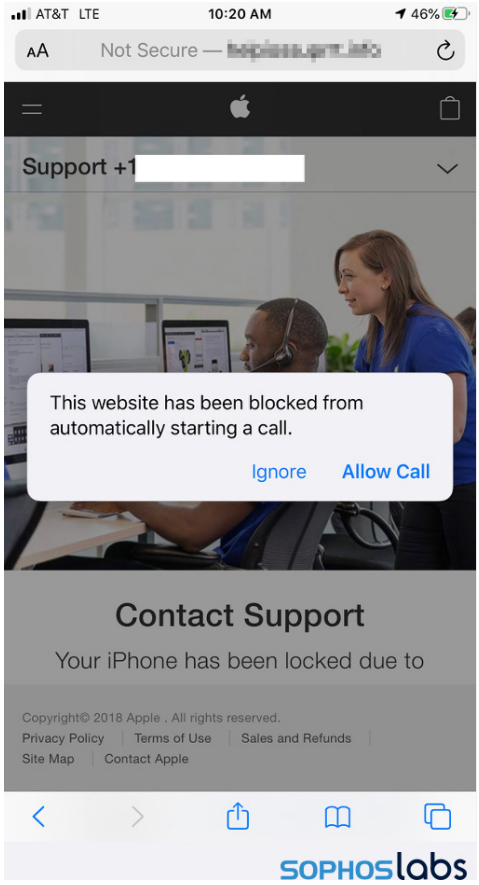


Fig.25. Fonte: SophosLabs

La stessa infrastruttura che supporta questi attacchi su browser di PC e Mac visualizza anche truffe relative ad attività di supporto tecnico e avvisi fasulli con link ad applicazioni potenzialmente indesiderate, incluse app che si spacciano per servizi VPN e strumenti di "pulitura", pubblicizzati come prodotti per la rimozione del malware con abbonamenti acquistabili (e in alcuni casi contenenti vero e proprio malware Android). Sophos ha individuato un gruppo di server che conducevano campagne volte a pubblicare questi tipi di annunci, utilizzando software realizzato da sviluppatori russi per questo scopo specifico.

Quando le risorse della vittima vengono utilizzate per attaccarla: utilizzo improprio degli strumenti di sicurezza a scopo criminale

Alcuni attacchi non prevedono alcun tipo di malware, né nelle fasi iniziali, né in quelle finali. Agiscono invece servendosi degli strumenti inclusi nei sistemi operativi dei computer di una rete. Altri criminali sfruttano invece i vantaggi di una serie di strumenti utilizzati da due figure fondamentali nel settore della sicurezza informatica: gli esperti di risposta agli incidenti e di penetration testing.

La comunità della sicurezza informatica ha coniato una definizione per questo stile di attacco che utilizza una quantità limitata (o inesistente) di malware e che preferisce invece sfruttare componenti già esistenti del sistema operativo di pacchetti software molto diffusi: Living-Off-the-Land (LOL). Solitamente questi attacchi utilizzano uno o più metodi di automazione impiegando scripting nativo, come ad es. PowerShell, file batch o script VBScript, collettivamente chiamati LOLscript. Gli attacchi si servono dei LOLscript per eseguire sequenze di comandi che utilizzano file binari Living-Off-the-Land (applicazioni), comunemente detti LOLbin.

I software originariamente progettati per i "read team" della sicurezza informatica prevedono un modello "bring-your-own-attack". In questo caso gli hacker scelgono di utilizzare strumenti di sicurezza commerciali normalmente utilizzati da amministratori di rete ed esperti di prenetration testing. Tra questi è possibile trovare strumenti quali Cobalt Strike e alcuni elementi del framework Metasploit, progettati per l'uso a scopo di valutazione di sicurezza e test tecnici.

Il set di strumenti utilizzati da uno dei pirati informatici creatore di Netwalker nella matrice di ATT&CK

ACCESSO INIZIALE	ESECUZIONE	PRIVILEGE ESCALATION	ELUSIONE DEI TENTATIVI DI DIFESA	ACCESSO CON CREDENZIALI	INDIVIDUAZIONE	MOVIMENTI LATERALI	IMPATTO
Exploit Tomcat	Script PowerShell	CVE-2020-0796	Caricamento senza file	mimikatz	SoftPerfect Network Scanner	psexec	Ransomware Netwalker
Exploit Weblogic	psexec	CVE-2019-1458	Strumento di rimozione dell'AV Eset	Mimidogz	NLBrute	TeamViewer	Ransomware Zeppelin
E-mail di phishing		CVE-2017-0213	Recupero delle password Eset di Gordon	Mimikittenz		Anydesk	Ransomware Smaug
		CVE-2015-1701	Strumento di disinstallazione dell'Agente di Sicurezza di Trend Micro	Editor delle credenziali di Windows			Esfiltrazione dei dati
			Disinstallazione di Microsoft Security Client	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

SOPHOSlabs

Fig.26. Il set di strumenti utilizzato da uno dei pirati informatici coinvolti negli attacchi di ransomware Netwalker, che includeva un assortimento completo di utilità Open Source, freeware e commerciali in diverse fasi dell'attacco. Fonte: SophosLabs.

Questi strumenti hanno un valore inestimabile per gli hacker e ciò è dovuto a una serie di motivi: poiché vengono spesso utilizzati in maniera legittima (a scopo di controllo o comunque per ottimizzare la sicurezza dei sistemi), può essere difficile per le soluzioni antivirus o di sicurezza rilevare immediatamente questi strumenti o le loro attività. Di conseguenza, Sophos si affida maggiormente alle analisi dei comportamenti tipici dei LOLscript per identificare un'eventuale attività malevola. Inoltre, ovviamente è più semplice sfruttare risorse già create, piuttosto che crearne di nuove.

Sebbene il loro utilizzo negli ultimi 12 mesi non sia stata una novità, nel 2020 LOLscript e reverse shell sono diventati elementi onnipresenti nei più complessi attacchi manuali di ransomware tramite violazione. Abbiamo infatti osservato un aumento sia della quantità che della varietà di questi strumenti di attacco.

Kill chain degli strumenti di attacco del RaaS Dharma

ACCESSO INIZIALE	ESECUZIONE	PRIVILEGE ESCALATION	ELUSIONE DEI TENTATIVI DI DIFESA	ACCESSO CON CREDENZIALI	INDIVIDUAZIONE	MOVIMENTI LATERALI	ESFILTRAZIONE	IMPATTO
Credential spray per RDP	PowerShell	CVE-2019-1388	Disattivazione della protezione antimalware	mimikatz	PCHunter	Oggetti Group Policy	Emailer di screenshot di PowerShell	Ransomware Dharma
Furto delle credenziali di RDP	WMI	CVE-2018-8120	Programma di disinstallazione di Revo	Remote Desktop Passview	Process Hacker	Desktop remoto	TOR	
	AutoIT	CVE-2017-0213	Programma di disinstallazione di IOBit	LaZagne	GMER	Gestione remota WinRM	dropmefiles[.]com	
	Riga di comando/ RDP			NLBrute	Advanced IP Scanner			
				Strumenti Hash Suite	NS2.EXE			

SOPHOSlabs

Fig.27. Fonte: SophosLabs.

Questi strumenti di attacco possono essere di natura molto diversa, da applicazioni disponibili sul mercato a repository GitHub Open Source, con funzionalità che possono includere:

- Framework di comando e controllo simili a quelli delle botnet
- Generazione e offuscamento di shellcode
- Elusione dell'antivirus e del rilevamento tramite sandbox
- Estrazione di password o credenziali
- Kerberoasting (per mantenere la persistenza dei privilegi di amministratore di dominio)
- La capacità di prelevare con attacchi brute force le password utilizzate da diversi servizi
- Esfiltrazione dei dati di sistema

Nel loro stato iniziale, la maggior parte di questi strumenti contiene payload innocui e a volte non include alcun payload. Tuttavia, in passato, grazie alle informazioni di contesto acquisite per mezzo delle nostre tecnologie di rilevamento basato sul comportamento, abbiamo osservato che molti di questi strumenti partecipavano ad attività malevole.

Secondo i nostri dati di telemetria, i dieci strumenti di attacco più comunemente utilizzati sono (in ordine di frequenza d'uso) Metasploit, BloodHound, mimikatz, PowerShell Empire, Cobalt Strike, Veil Evasion, Hydra THC, Enigma, Nishang e Shellter. Metasploit supera nettamente tutti gli altri, aggiudicandosi il titolo di strumento più comunemente osservato, con una frequenza di rilevamento doppia rispetto al secondo classificato, BloodHound.

Attualmente Sophos monitora l'utilizzo di 99 strumenti di attacco diversi; sembra molto improbabile che nel 2021 gli hacker demordano dallo sfruttare questi strumenti ben compilati.

Epidemiologia digitale

Qual è la percentuale dei dispositivi di elaborazione che sono stati infettati con malware non rilevato? Qual è la percentuale delle righe di comando eseguite da cybercriminali la cui presenza non è stata rilevata? Qual è la percentuale delle e-mail di phishing mirate che passano inosservate? Come cambiano tutti questi fattori in funzione del settore, della posizione geografica e dello stato di protezione della rete?

Sollevare queste domande può essere paragonato al chiedere: "Qual è la percentuale di persone infettate dal COVID-19?". In un contesto in cui molte persone potrebbero non essere mai state sottoposte a test per rilevare la presenza del virus, i test che vengono effettuati possono avere un alto tasso di falsi positivi e falsi negativi. In altre parole, è difficile.

Nonostante tutte le sfide, gli epidemiologi rispondono ogni giorno a domande critiche sul COVID-19. Purtroppo i ricercatori di cybersecurity non riescono a fare lo stesso per gli attacchi informatici. Siamo rimasti indietro rispetto agli epidemiologi in termini di strumenti, tecniche e procedure disponibili per affrontare in maniera logica le situazioni di incertezza. Non ci sono scuse ed è tempo di impostare strumenti che aiutino a comprendere la natura di ciascuna minaccia che affrontiamo, indicando i rischi in maniera accurata a chi dobbiamo proteggere e prendendo decisioni strategiche in merito a dove occorre concentrare maggiore attenzione.

Per svolgere il proprio compito in questa missione, il team Sophos AI ha intrapreso un progetto che prevede la compilazione di un set di modelli statistici liberamente ispirati a quelli epidemiologici, al fine di fornire una stima della prevalenza totale delle infezioni di malware. Abbiamo impostato una solida pipeline di raccolta dati, che preleva dati da 100 milioni di endpoint utilizzando metodi statistici bayesiani, per aiutarci a rispondere alle domande più difficili e a tracciare un quadro completo della performance dei nostri modelli "sul campo".

Consideriamo ad esempio questa domanda: "Qual è la quantità di malware che colpisce i nostri clienti settimanalmente e quanto ne viene rilevato?"

Se per tutti i file fosse possibile stabilire quali contengono malware e quali invece sono innocui, la questione sarebbe già risolta! Purtroppo ci sono due problemi.

1. Non conosciamo tutte le informazioni contestuali di un file: a tutti i prodotti endpoint capita prima o poi di non riuscire a rilevare del malware, e anche qualche falso positivo (un file normale segnalato come malware) ogni tanto è inevitabile
2. L'equilibrio tra file innocui e dannosi è pesantemente sbilanciato a favore di quelli innocui, per cui è poco probabile riuscire a determinare la vera natura di un file mediante analisi manuale. Occorrerebbe svolgere un'analisi approfondita di tutti i file ritenuti innocui dalla nostra soluzione endpoint, che ne rivelerebbe al massimo uno dannoso su varie migliaia

Per risolvere questi problemi abbiamo utilizzato la statistica bayesiana. In pratica, abbiamo impostato un modello "generativo" dei dati: un programma matematico in grado di dedurre parametri ("Qual è la quantità effettiva del malware?") e di trasformare i risultati di questo processo in simulazioni della quantità di rilevamenti endpoint che potrebbe essere osservata. Abbiamo quindi provato approssimazioni diverse, preso nota di quali di queste simulazioni riflettessero maggiormente la realtà osservata e siamo partiti dai risultati per risalire a valori plausibili del parametro investigato.

Supponiamo, ad esempio, di avere a disposizione 2.000 rilevamenti endpoint e una buona stima dei tassi di veri e falsi positivi in una settimana specifica. Possiamo simulare scenari con tassi di malware dello 0%, del 2%, del 5% e così via, per osservare le previsioni della simulazione per i rilevamenti sugli endpoint; se in corrispondenza di un tasso di malware specifico i risultati si avvicinano ai 2.000 rilevamenti, allora si tratta (probabilmente) di un valore plausibile.

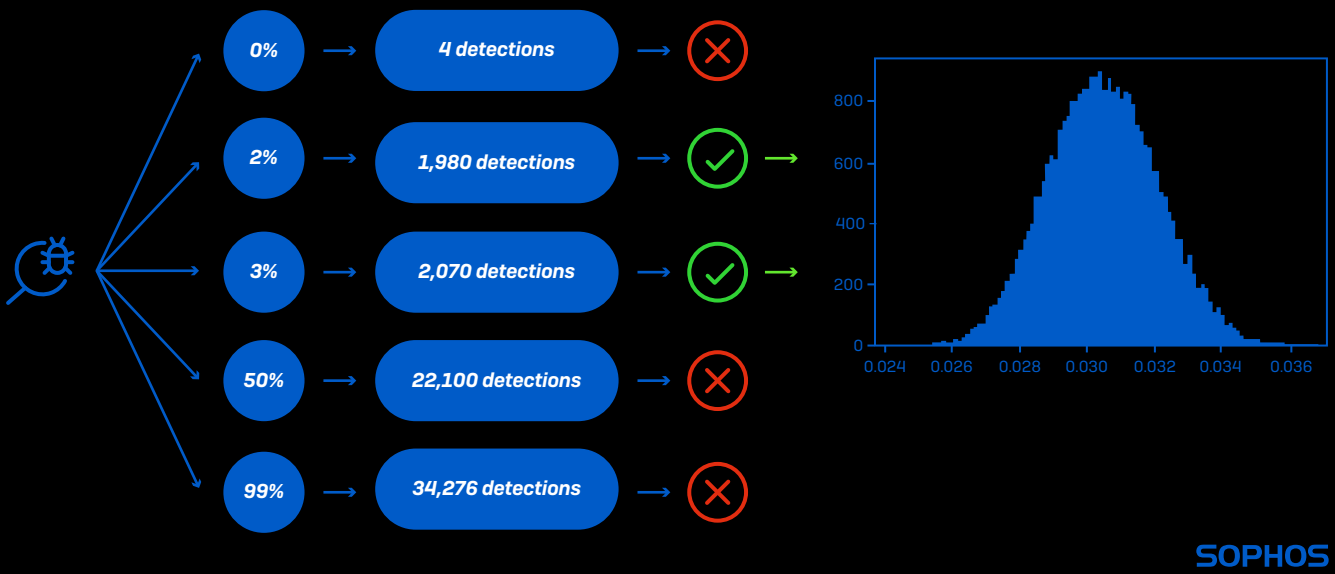


Fig.28. Proporre un tasso di malware, eseguire test, vedere se la simulazione corrisponde alla realtà osservata, annotare i tassi che restituiscono i risultati attesi e ripetere. Fonte: SophosAI.

Il processo può essere ripetuto milioni di volte per strutturare una distribuzione di valori plausibili per il tasso di malware. Poiché utilizziamo un approccio bayesiano, le barre di errore sono "incluse" nella stima. Nel nostro esempio, il modello ritiene che il valore più probabile della domanda "Quale percentuale dei file rappresenta file di malware?" sia di poco superiore al 3%, ma qualsiasi risultato compreso tra il 2,75% e il 3,35% circa è piuttosto plausibile.

Una volta raggiunta una buona approssimazione di questa statistica (quanti file su cento presentano la probabilità di essere file di malware sugli endpoint dei clienti), anche i mancati rilevamenti e i falsi positivi diventano relativamente semplici da stimare. Analizzando i dati ottenuti dal nostro sistema di rilevamento del malware basato sul deep learning per una settimana specifica del mese di maggio (senza attivare alcuna delle opzioni di rilevamento basato sulle firme digitali, sui comportamenti o sulla metodologia euristica), possiamo popolare una matrice completa di veri e falsi positivi e negativi, completando il nostro quadro di performance del modello. In questo caso si può notare che, sebbene siano presenti alcuni falsi negativi, il numero di falsi positivi è basso e con asimmetria tendente a zero, mentre il numero di veri positivi è alto e presenta un'asimmetria tendente a 161.000 (il numero totale dei risultati positivi nel campione). Osservando la scala, si nota che le tre quantità sono tutte trascurabili rispetto al numero di veri negativi, ovvero dei file che la nostra tecnologia di machine learning (ML) ha contrassegnato come innocui.

Il nostro strumento ispirato all'analisi epidemiologica ci ha permesso di stimare, se non persino trovare, dove si trovano i proverbiali aghi nel pagliaio dei nostri file PE.

Fig.29. Analisi del modello di machine learning dei veri e falsi positivi a inizio del mese di maggio del 2020. Fonte: SophosAI.

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

20-11-01 IT (DD)

SOPHOS