SOPHOS

Sophos Threat Report 2024: il cybercrime colpisce anche le aziende più piccole

Il ransomware resta la più grave cyberminaccia per le piccole imprese. Ma ci sono anche altri rischi in agguato.

Sophos X-Ops

Indice dei Contenuti

Quadro di riferimento

Il cybercrimine colpisce persone provenienti da diverse realtà, ma a subirne maggiormente l'impatto sono le piccole imprese. Anche se i notiziari tendono a focalizzarsi principalmente sugli attacchi informatici contro aziende di grandi dimensioni ed enti governativi, in realtà sono le piccole imprese (le organizzazioni con meno di 500 dipendenti, in senso lato) a essere più vulnerabili agli hacker e a subire, in proporzione, conseguenze più pesanti in seguito a un cyberattacco. La mancanza di tecnici esperti, gli scarsi investimenti nella cybersecurity e il budget limitato da dedicare alle tecnologie in generale sono tutti fattori che contribuiscono a questo livello di vulnerabilità. E il costo di riparazione dei danni causati da un attacco informatico può persino costringere molte aziende di piccole dimensioni a chiudere i battenti.

Le piccole imprese non sono una questione da poco. Secondo la Banca Mondiale, più del 90% delle aziende in tutto il mondo è costituito da piccole e medie organizzazioni, nelle quali lavora il 50% delle persone con un lavoro retribuito a livello globale. Negli Stati Uniti, le piccole e medie imprese contribuiscono a oltre il 40% dell'attività economica totale (in questo report utilizzeremo i termini piccole e medie imprese, aziende oppure organizzazioni in modo intercambiabile, per rifletterne le analogie nei nostri dati).

Nel 2023, oltre il 75% dei casi di risposta agli incidenti dei clienti nei quali è intervenuto il servizio Incident Response di Sophos X-Ops riguardava imprese di piccole dimensioni. Le informazioni raccolte su questi casi, in aggiunta ai dati di telemetria ottenuti dal software di protezione dei nostri clienti in imprese di piccole e medie dimensioni, hanno contribuito a fornirci un'ulteriore prospettiva esclusiva sulle minacce che ogni giorno colpiscono queste organizzazioni.

Riepilogo

In base ai dati e alla ricerca sulle minacce condotta da Sophos, si osserva che il ransomware continua a essere la minaccia con l'impatto più significativo sulle organizzazioni più piccole. Tuttavia, esistono anche altre minacce che costituiscono una minaccia molto importante per le piccole imprese:

- Il furto dei dati è l'obiettivo principale della maggior parte dei malware che colpiscono le piccole e medie imprese: programmi di intercettazione delle password o dei tasti digitati, più altri spyware sono la causa di quasi la metà dei rilevamenti di malware. Il furto delle credenziali attraverso phishing e malware può mettere in pericolo i dati delle piccole imprese situati sulle piattaforme cloud o in possesso dei provider di servizi; inoltre, le violazioni della rete possono essere sfruttate per colpirne anche i clienti
- Gli autori degli attacchi hanno intensificato l'uso della distribuzione di malware basato sul web (attraverso il malvertising o l'ottimizzazione dei motori di ricerca a scopo malevolo, detta "SEO poisoning"), per superare gli ostacoli costituiti dal blocco delle macro pericolose nei documenti; inoltre, sfruttano sempre più spesso le immagini dei dischi per causare il sovraccarico degli strumenti di rilevamento del malware
- I dispositivi non protetti connessi alle reti aziendali (inclusi i computer non gestiti e privi di software di protezione, i computer configurati in maniera errata e i sistemi che eseguono software non più supportati dall'azienda produttrice) sono tra i principali punti di accesso per qualsiasi tipo di attacco cybercriminale contro le piccole aziende
- Gli autori degli attacchi sfruttano sempre più frequentemente l'uso improprio dei driver (driver vulnerabili di aziende legittime o driver pericolosi che sono stati firmati con certificati rubati oppure ottenuti in maniera fraudolenta) per eludere le difese antimalware nei sistemi gestiti e disattivarle
- Gli attacchi e-mail hanno iniziato a evolversi dal semplice social engineering fino a diventare un'interazione più attiva e diretta con le vittime, basata su interi thread di e-mail e risposte, per dare maggiore credibilità all'esca
- Gli attacchi rivolti agli utenti dei dispositivi mobili, incluse le truffe di social engineering legate all'uso improprio di servizi di terze parti e piattaforme social, sono cresciuti in maniera esponenziale, colpendo sia singoli individui che piccole aziende. Possono variare dalla compromissione delle e-mail aziendali (Business Email Compromise) e dalla violazione dei servizi cloud, fino alle truffe di pig butchering (shā zhū pán (殺豬盤))

Da dove provengono i nostri dati

I dati utilizzati nelle nostre analisi provengono dalle seguenti fonti:

- Report dei clienti: dati di telemetria dei rilevamenti effettuati dai software di protezione Sophos in esecuzione sulle reti dei clienti, che offrono ampia visibilità sulle minacce individuate e analizzate dai SophosLabs (in questo report, detti "dati dei SophosLabs")
- Dati sugli incidenti nei quali è intervenuto il servizio Managed Detection and Response (MDR), raccolti durante le escalation effettuate in seguito al rilevamento di attività dannosa nelle reti dei clienti di MDR (in questo report, detti "dati di MDR")
- Dati del team Incident Response (IR), tratti dagli incidenti rilevati sulle reti dei clienti per le aziende con 500 dipendenti o meno e una quantità esigua (o inesistente) di sistemi di rilevamento e risposta gestiti (in questo report, detti "dati di IR")

Per un'analisi più approfondita dei dati tratti esclusivamente dai casi gestiti dal nostro team di IR (inclusi i casi dei clienti con più di 500 dipendenti), consigliamo la lettura della nostra pubblicazione gemella Active Adversary Report (AAR). A meno che non venga indicato altrimenti, le conclusioni tratte in questo report si basano sulla combinazione dei dati ottenuti, adeguatamente normalizzati.

Il bersaglio principale sono i dati

La maggiore sfida di cybersecurity affrontata dalle piccole imprese (nonché dalle organizzazioni di qualsiasi dimensione) è la protezione dei dati. Oltre il 90% degli attacchi segnalati dai nostri clienti include una forma di furto di dati o di credenziali; i metodi utilizzati possono essere diversi: attacco ransomware, estorsione di dati, accesso remoto non autorizzato o semplicemente furto diretto dei dati.

Gli attacchi di tipo Business Email Compromise (BEC), nel corso dei quali un cybercriminale assume il controllo degli account e-mail per commettere una frode o per altri scopi malevoli, sono un problema molto grave per le piccole e medie imprese. Attualmente, gli attacchi BEC non vengono trattati nella nostra pubblicazione gemella (Active Adversary Report, AAR); tuttavia, in base alle stime degli autori dell'AAR, nel 2023 il nostro team Incident Response ha identificato la frequenza di questi tipi di attacco come superiore a quasi tutti gli altri incidenti, seconda solo al ransomware.

Le credenziali rubate, inclusi i cookie del browser, possono essere utilizzate per gli attacchi BEC, per l'accesso a servizi di terze parti come i sistemi finanziari basati sul cloud, e per l'infiltrazione in risorse interne che possono poi essere sfruttate a scopo di frode o altri tipi di lucro. Possono anche finire nelle mani di "broker di accesso", che le rivendono a chiunque voglia utilizzarle: Sophos ha rintracciato forum clandestini nei quali veniva offerto l'accesso alle reti di diverse aziende di piccole e medie dimensioni.

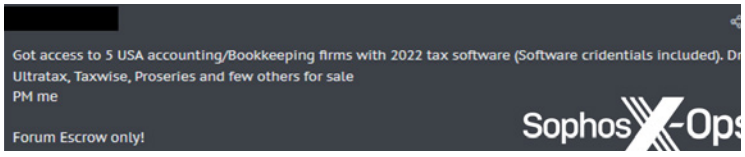

Figura 1: Un post in un forum che promuove l'accesso a un'azienda di contabilità statunitense di piccole dimensioni

Figura 2: Un post in un forum che promuove l'accesso a un'azienda di piccole dimensioni in Belgio

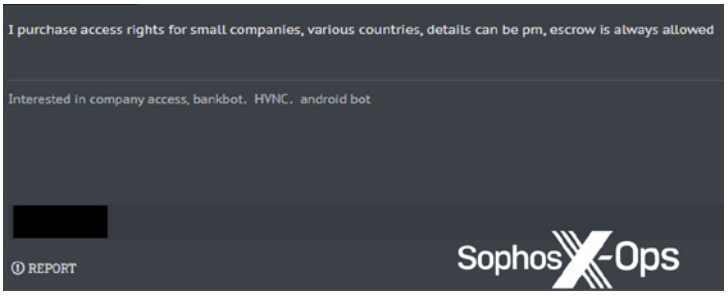

Figura 3: Un cybercriminale che offre di acquistare l'accesso a sistemi di piccole imprese

Figura 4: L'accesso a un'azienda di piccole dimensioni in Italia viene offerto in vendita su un forum criminale

In base alla categoria, quasi metà del malware rilevato nel 2023 aveva come obiettivo i dati delle vittime prese di mira. Nella maggior parte dei casi, si trattava di malware classificato specificamente come "stealer", ovvero malware che acquisisce credenziali, cookie del browser, tasti digitati e altre informazioni che possono essere trasformate in un guadagno, se vendute come accesso o sfruttate per ulteriori tentativi di exploit.

Tuttavia, a causa della natura modulare del malware, è difficile classificare interamente il malware per funzione: quasi tutti i malware sono in grado di rubare qualche informazione dai sistemi delle vittime. Inoltre, questi rilevamenti non includono altri metodi di furto di credenziali, quali il phishing tramite e-mail o SMS e altri attacchi di social engineering. Oltretutto, esistono anche altri bersagli, come i sistemi macOS e i dispositivi mobili, che vengono sfruttati da malware, applicazioni potenzialmente indesiderate e social engineering per prelevare illecitamente le informazioni degli utenti, specialmente quelle di natura finanziaria.

Categorie di malware per numero di aggiornamenti delle firme nel 2023

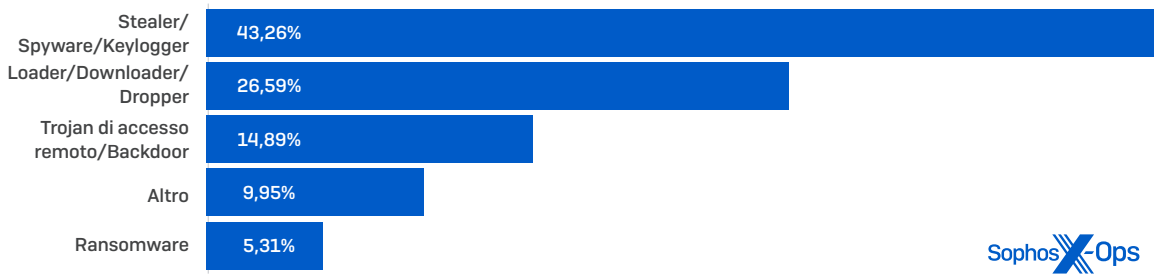

Figura 5: Rilevamenti di malware per il 2023 in base al tipo, secondo i dati dei SophosLabs e di MDR

Quasi il 10% del malware rilevato non rientra nelle quattro categorie principali indicate sopra. La categoria "Altro" include, per citare alcuni esempi, i malware che colpiscono i browser per inserirvi annunci dannosi, che reindirizzano i risultati di ricerca per guadagnare con i clic degli utenti, che modificano in altro modo le informazioni o che raccolgono dati per generare un guadagno per lo sviluppatore del malware.

Alcuni stealer hanno obiettivi molto specifici. I "Discord Token Stealer", realizzati per rubare le credenziali del servizio di messaggistica di Discord, vengono spesso sfruttati per diffondere altro malware attraverso i server di chat o la rete di distribuzione di contenuti di Discord. Tuttavia, altri stealer importanti (Strela, Raccoon Stealer e la famigerata famiglia di stealer RedLine) sono molto più aggressivi con i loro obiettivi: prelevano infatti archivi di password dal sistema operativo e dalle applicazioni, nonché cookie del browser e altre informazioni relative alle credenziali. Raccoon Stealer ha anche utilizzato la "copia negli appunti" per le transazioni digitali, che sostituisce gli indirizzi dei portafogli di criptovalute copiati negli appunti con l'indirizzo di un portafoglio controllato da chi distribuisce il malware.

Principali stealer per numero di segnalazioni di clienti individuali nel 2023

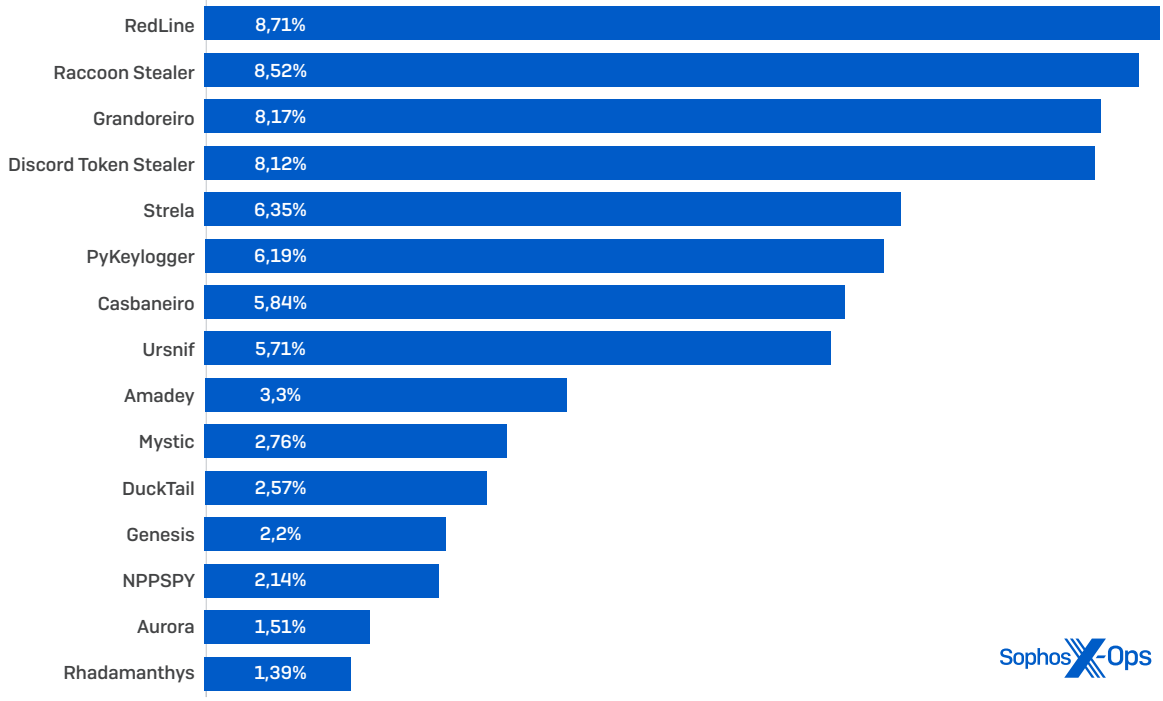

Figura 6: I rilevamenti di malware di tipo info stealer nel 2023, tratti dai dati di telemetria dei clienti Sophos raccolti dai SophosLabs

Sophos ha osservato un aumento nel numero dei malware info stealer che colpiscono macOS, e siamo convinti che questa tendenza continuerà ad aumentare. Questi stealer (alcuni dei quali vengono venduti in forum e canali Telegram clandestini per somme che possono raggiungere i 3.000 $) sono in grado di raccogliere informazioni su sistemi, browser e portafogli elettronici.

Il ransomware continua a essere una delle minacce più gravi per le piccole imprese

Sebbene il ransomware rappresenti una percentuale relativamente bassa dei rilevamenti totali di malware, è pur sempre la minaccia che causa i danni più devastanti. Il ransomware colpisce aziende di qualsiasi dimensione in tutti i settori, ma abbiamo notato che tende ad attaccare più frequentemente le piccole e medie imprese. Nel 2021, la Ransomware Task Force dell'Institute for Security and Technology ha rivelato che il 70% degli attacchi ransomware aveva colpito aziende di piccole dimensioni. Anche se la quantità complessiva di attacchi ransomware ha subito variazioni nel corso degli anni, le nostre statistiche confermano questa percentuale.

Il ransomware LockBit è risultato la minaccia più presente nei casi di sicurezza delle piccole imprese nei quali è intervenuto il team Sophos Incident Response nel 2023. LockBit è un ransomware as a service distribuito da diversi affiliati, ed è stato il malware più diffuso nel 2022, secondo il grafico nella Figura 7.

Incidenti di ransomware nelle piccole imprese, gestiti da Sophos Incident Response nel 2023

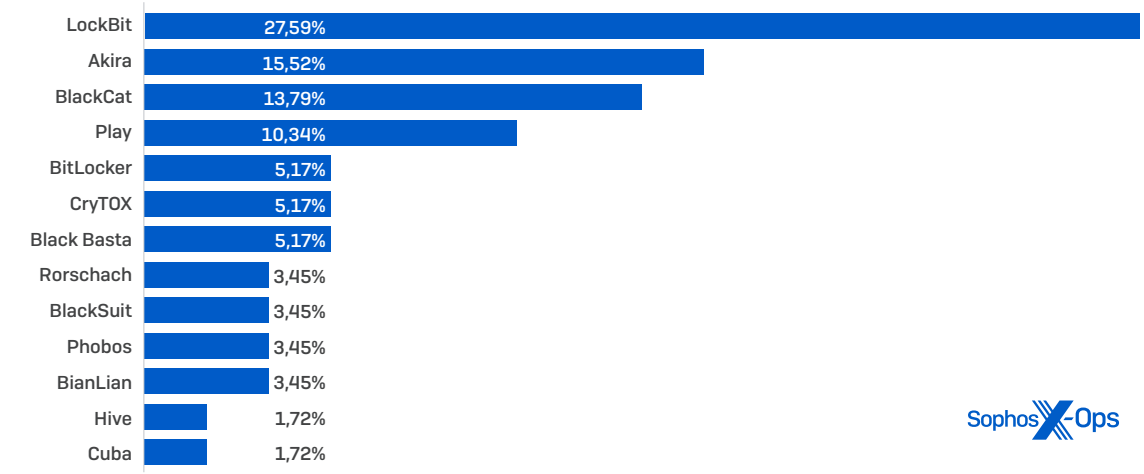

Figura 7: Una ripartizione dei ransomware che hanno causato incidenti nelle piccole imprese, analizzati da Sophos Incident Response nel 2023; le cifre riflettono i dati raccolti sul campo durante gli interventi di IR nei sistemi di clienti che generalmente non avevano implementato alcuna protezione Sophos

I 20 ransomware principali per numero di segnalazioni di clienti individuali nel 2023

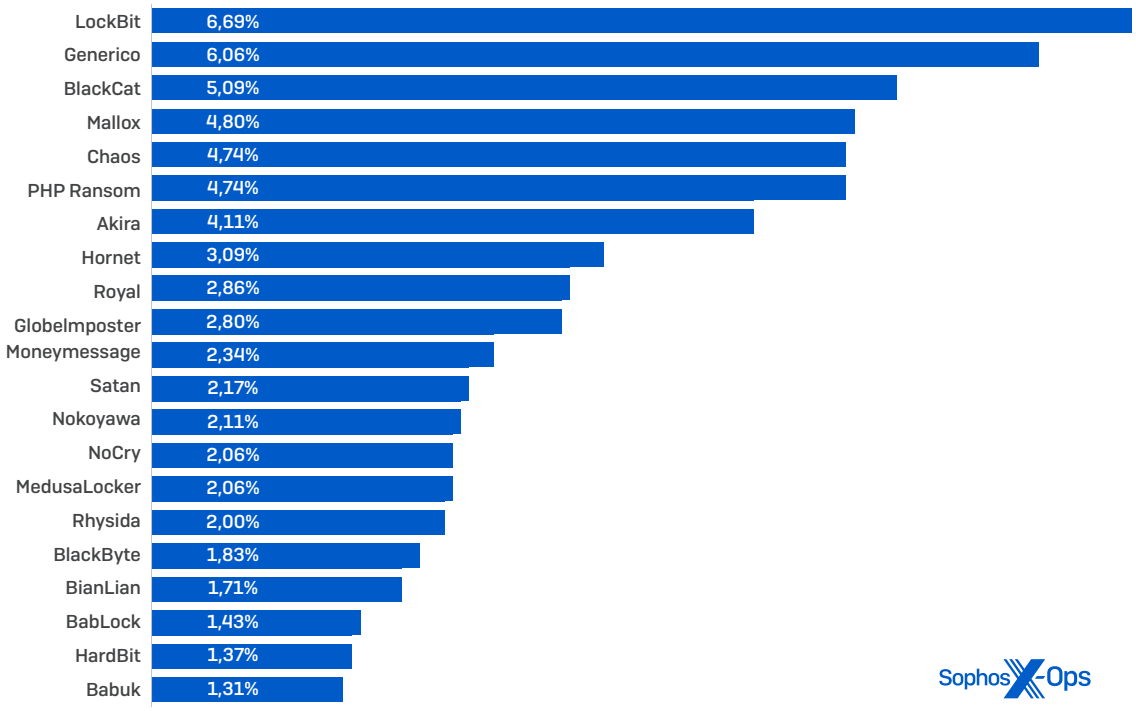

Figura 8: I principali tentativi di distribuzione del ransomware rilevati dal software di protezione endpoint Sophos e presenti nei dati dei SophosLabs di tutti i clienti nel 2023, rappresentati come percentuale di tutto il ransomware rilevato; "Generico" indica vari tipi di ransomware rilevati con una firma generica, che non appartengono a un'altra definizione

LockBit è stato il malware osservato più frequentemente dal team Sophos Managed Detection and Response (MDR, che include il team Incident Response e i rispettivi dati), con una quantità di incidenti nei quali è stato effettuato un tentativo di distribuzione del ransomware pari al triplo rispetto al malware più simile, Akira.

Principali malware osservati negli incidenti gestiti nel 2023 da MDR, in base al numero di incidenti

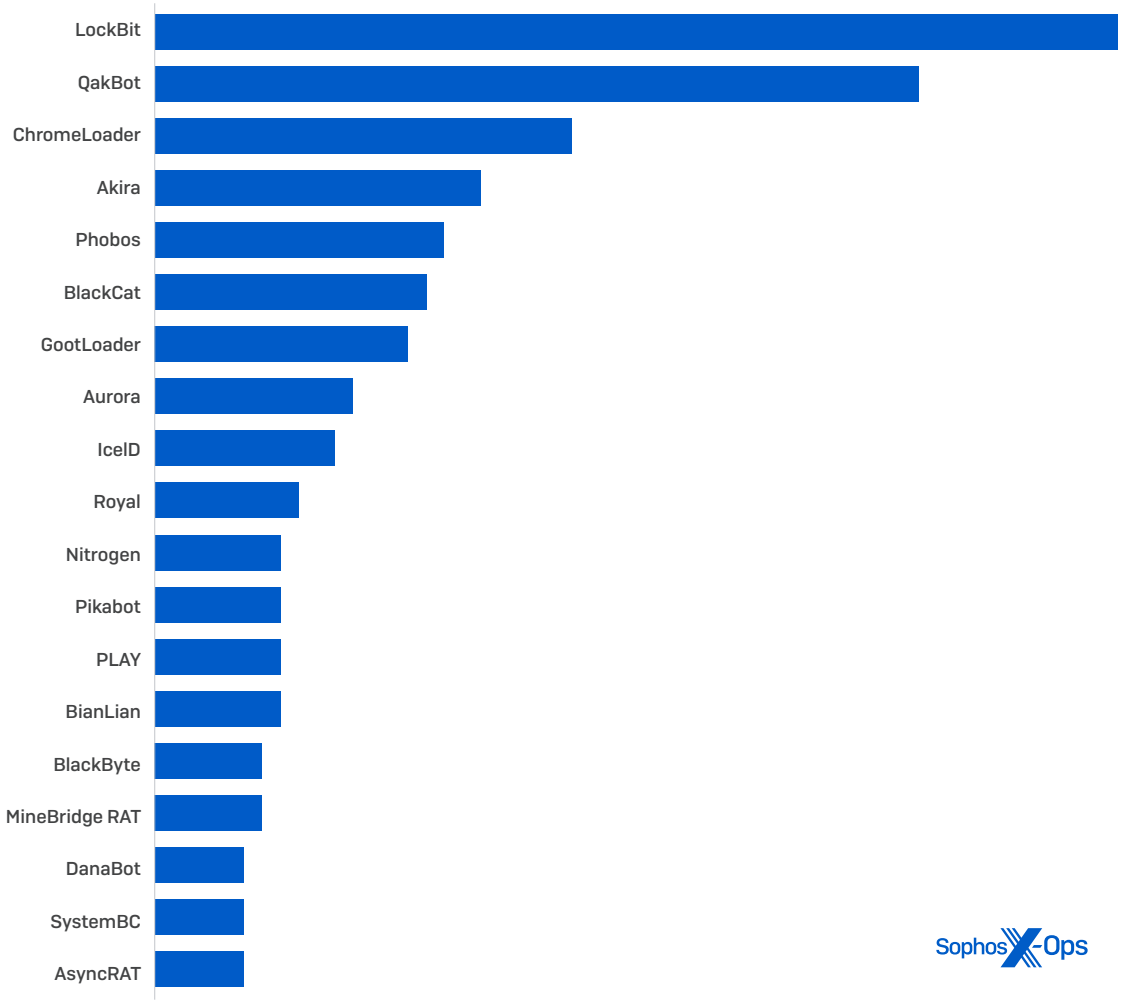

Figura 9: Il malware osservato più frequentemente negli incidenti nei quali è intervenuto il team Sophos Managed Detection and Response nel 2023, come indicato nei dati di MDR. Si notino le differenze tra questo grafico e quello della Figura 8; oltre alla prevalenza di LockBit nel 2023, si osserva che, sebbene sia presente un'ampia selezione di famiglie di ransomware che hanno cercato di infettare i sistemi, solo un sottoinsieme di queste famiglie raggiunge uno stadio che richiede l'intervento diretto di MDR. Si noti che i risultati non sono esclusivi: ciò significa che un unico incidente potrebbe includere più di un solo rilevamento

Il 2023 è stato caratterizzato da un fenomeno che è diventato sempre più comune con il passare dei mesi: l'uso del ransomware eseguito da remoto, sfruttando un dispositivo non gestito nelle reti delle organizzazioni per cercare di crittografare i file su altri sistemi della rete attraverso l'accesso ai file di rete.

Incidenti di remote ransomware, 2022-2023

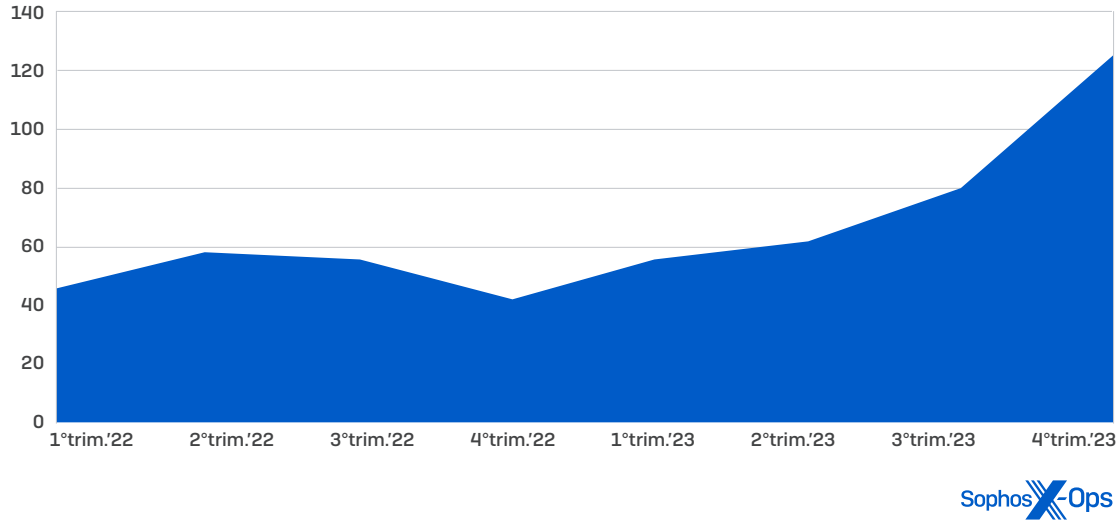

Figura 10: Gli ultimi due anni di dati di telemetria dei clienti raccolti da Sophos indicano un incremento generale nella percentuale di tentativi di attacchi ransomware che includono il remote ransomware: un problema attuale che si è ripresentato con maggiore insistenza, specialmente nella seconda metà del 2023

Questi tipi di attacchi sono in grado di infiltrarsi nei sistemi sfruttando server, dispositivi personali e appliance di rete non protetti, che si connettono alle reti Windows delle organizzazioni. Un sistema di difesa che agisce in profondità può impedire a questi attacchi di causare un'interruzione completa del servizio, ma le organizzazioni possono comunque essere vulnerabili alla perdita e al furto dei dati.

I sistemi Windows non sono gli unici a essere colpiti dal ransomware. Sono infatti sempre più frequenti gli sviluppatori di ransomware e altri tipi di malware che sfruttano linguaggi multipiattaforma per costruire versioni mirate per i sistemi operativi macOS e Linux e le piattaforme hardware supportate. Nel mese di febbraio 2023, è stata individuata una variante Linux del ransomware ClOp, utilizzata in un attacco verificatosi a dicembre 2022; da allora, Sophos ha osservato versioni esfiltrate di ransomware LockBit che colpivano macOS direttamente sul processore di Apple, e Linux su diverse piattaforme hardware.

Cybercrime as a service

Il panorama del malware continua a essere da dominato da ciò che abbiamo definito con il termine "Malware as a Service" (MaaS), ovvero l'uso di framework di distribuzione del malware offerti dai cybercriminali per altri cybercriminali, attraverso marketplace clandestini. Tuttavia, il panorama del MaaS ha risentito dell'impatto dei miglioramenti della sicurezza nelle piattaforme e degli interventi di neutralizzazione messi in atto dalle forze dell'ordine.

Dopo un decennio di prevalenza nell'ambito della distribuzione del malware, Emotet è svanito, dopo essere stato annientato da Europol ed Eurojust a gennaio 2021. Lo stesso si può dire, in maniera minore, per QakBot e TrickBot, dopo che sono stati fermati dalle forze dell'ordine ad agosto 2023. Anche se QakBot si è ripresentato in forma minore, è stato ampiamente sostituito dai suoi successori Pikabot e DarkGate.

Tutto questo non ha avuto alcuna ripercussione sul famigerato trojan di accesso remoto AgentTesla, che ha scalato la classifica e si trova ora al primo posto nel mercato dei MaaS. L'anno scorso, secondo i nostri dati di telemetria, è stato il malware rilevato più spesso dalla protezione endpoint nel 2023, nonché quello più presente negli endpoint in generale (oltre ai file .LNK generici dannosi e al malware offuscato); inoltre, ha costituito il 51% dei rilevamenti nel framework di distribuzione del malware.

Principali framework di distribuzione del malware per numero di segnalazioni di clienti individuali nel 2023

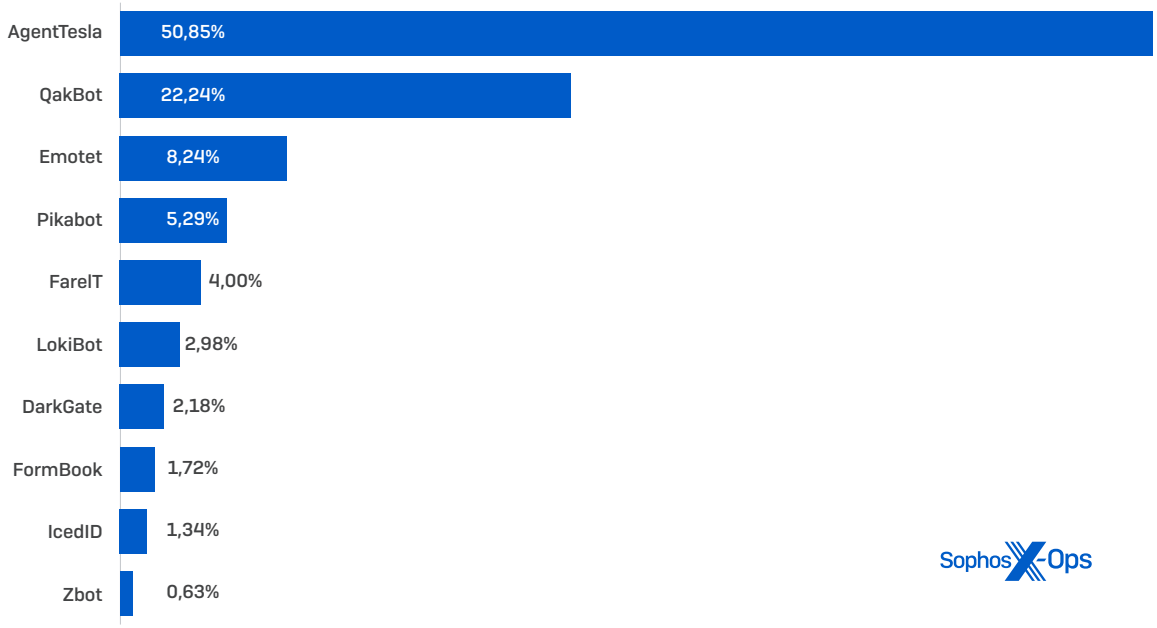

Figura 11: Una ripartizione dei framework più comunemente utilizzati dagli autori degli attacchi per distribuire il malware, in base al numero di rilevamenti su endpoint effettuati nelle reti dei clienti protetti con Sophos; le statistiche di QakBot rappresentano i rilevamenti prima dell'intervento internazionale delle forze dell'ordine contro l'infrastruttura di questa minaccia, avvenuto ad agosto 2023

Alla ricerca di un canale di distribuzione diverso

Gli attacchi malware richiedono una sorta di accesso iniziale, che di solito prevede l'uso di una delle seguenti tattiche:

- E-mail di phishing
- Allegati e-mail pericolosi
- Exploit di vulnerabilità nei sistemi operativi e nelle applicazioni
- Aggiornamenti fasulli del software
- Exploit e uso inappropriato di Remote Desktop Protocol
- Furto di credenziali

In passato, per ottenere questo accesso iniziale, i criminali che sfruttano MaaS si affidavano principalmente agli allegati e-mail pericolosi. Tuttavia, i cambiamenti introdotti nelle impostazioni di sicurezza predefinite della piattaforma Microsoft Office hanno avuto un impatto significativo sul mercato dei MaaS. Con l'implementazione di cambiamenti da parte di Microsoft nelle applicazioni Office, volti a bloccare per impostazione predefinita le macro VBA (Visual Basic, Applications Edition) nei documenti scaricati da Internet, è ora diventato più difficile per i cybercriminali che usano MaaS poter sfruttare il loro metodo preferito per diffondere il malware.

Tutto questo ha portato ad alcune evoluzioni nei tipi di allegati utilizzati dagli hacker, che tendono ora a utilizzare quasi esclusivamente allegati con file PDF. Ci sono state, tuttavia, alcune eccezioni degne di nota. All'inizio del 2023, gli hacker di QakBot hanno iniziato a sfruttare i documenti OneNote per eludere il problema dei cambiamenti introdotti in Excel e Word, inviando documenti che nascondevano link a file di script che venivano attivati quando la vittima cliccava su un pulsante all'interno di un blocco appunti di OneNote.

Nel 2021, abbiamo osservato che alcuni tipi di "malware as a service" come la backdoor Raccoon Stealer avevano iniziato a dipendere principalmente dalla distribuzione tramite web, spesso sfruttando tecniche di ottimizzazione dei motori di ricerca (SEO) per ingannare le vittime e convincerle a scaricare il loro malware. Nel 2022, abbiamo rilevato la tattica "SEO poisoning" nell'ambito di una campagna dell'info stealer SolarMarker. La diffusione di questi metodi è di nuovo in aumento e gli autori degli attacchi che li sfruttano sono ora molto più sofisticati.

Abbiamo notato diverse campagne di rilievo che utilizzavano gli annunci web e il SEO poisoning per colpire le vittime. Una di queste era stata condotta da una gang che usava malware e che abbiamo denominato "Nitrogen"; la gang pubblicava su Google e Bing annunci legati a parole chiave specifiche, per indurre le vittime a scaricare un programma di installazione software dannoso da un sito web fasullo, che utilizzava la brand identity di uno sviluppatore di software legittimo. La stessa tecnica di malvertising era stata impiegata in correlazione con vari altri malware di accesso iniziale, incluso l'agente botnet Pikabot, l'info stealer IcedID e le famiglie di malware backdoor Gozi.

Nel caso di Nitrogen, gli annunci avevano come target personale IT non specializzato e offrivano download di vari strumenti, ad es. un software di desktop remoto molto conosciuto per offrire supporto agli utenti finali, e alcune utilità per il trasferimento sicuro dei file. I programmi di installazione contenevano quello che promettevano, ma distribuivano anche un payload di Python dannoso che, al momento del lancio del programma di installazione, scaricava una shell remota di Meterpreter e beacon di Cobalt Strike. In base ad altri risultati ottenuti dai ricercatori, si può concludere che con molta probabilità si trattasse del primo passo di un attacco del ransomware BlackCat.

Strumenti “a duplice applicazione”

Cobalt Strike, il noto kit software di “adversary simulation e red team operations”, continua a essere sfruttato non solo da organizzazioni legittime di test, ma anche dai veri criminali informatici. Non è tuttavia l’unico software sviluppato per uso commerciale a essere utilizzato dai cybercriminali. E ormai non è nemmeno quello più comune.

Spesso gli strumenti di desktop remoto e compressione dei file, i sistemi più usati per il trasferimento dei file, e i software open source per i test di sicurezza vengono sfruttati dagli hacker per gli stessi motivi per cui vengono utilizzati dalle piccole e medie imprese: per semplificare le attività.

Sophos MDR ha osservato l’uso improprio di queste utilità, che definiamo “strumenti a duplice applicazione”, nell’ambito dei processi post-exploit degli autori degli attacchi:

- **Individuazione:** Advanced IP Scanner, NetScan, PC Hunter, HRSword
- **Persistenza:** AnyDesk, ScreenConnect, DWAgent
- **Accesso con credenziali:** Mimikatz, Veeam Credential Dumper, LaZagne
- **Movimenti laterali:** PsExec, Impacket, PuTTY
- **Raccolta ed esfiltrazione dei dati:** FileZilla, WinSCP, MEGASync, Rclone, WinRAR, 7-Zip

In base ai dati di Sophos MDR, AnyDesk e PsExec sono stati entrambi osservati in un numero di incidenti superiore rispetto a Cobalt Strike, come possiamo vedere di seguito:

Principali strumenti “a duplice applicazione” osservati negli incidenti gestiti da MDR nel 2023, in base al numero di incidenti

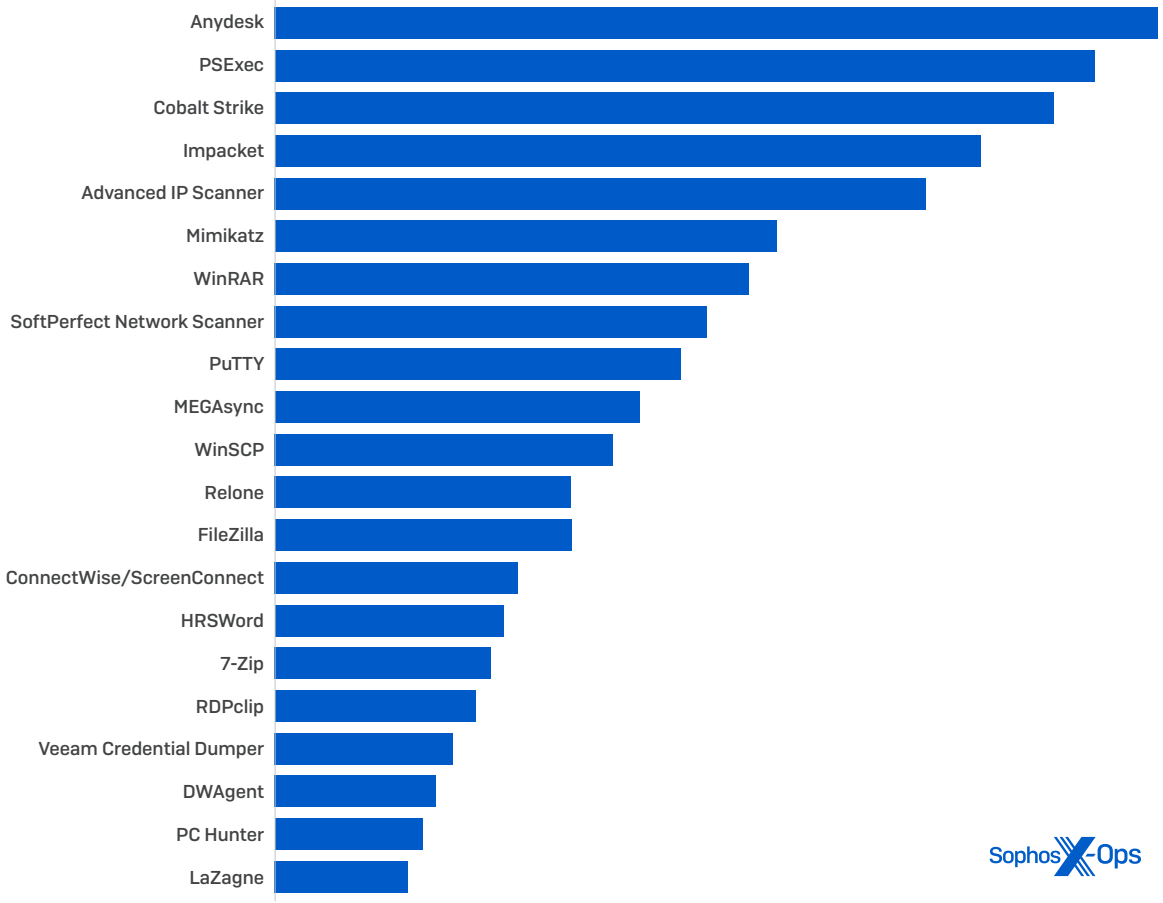

Figura 12: Gli strumenti “a duplice applicazione” più frequentemente osservati negli incidenti di sicurezza, in base al numero di casi in cui ciascuno di essi è stato osservato nei dati di Sophos MDR

Attacchi zero-day e non zero-day

A maggio 2023, Progress Software ha segnalato la presenza di vulnerabilità nella popolare piattaforma sicura per il trasferimento di file gestito della propria azienda, MOVEit, tra le quali era presente una vulnerabilità che era stata sfruttata da almeno una gang di criminali informatici. L'azienda avrebbe poi rivelato ulteriori vulnerabilità, rilasciando diverse patch per risolverle.

Gli attacchi sono stati attribuiti ad hacker associati alla gang di ransomware Cl0p. I cybercriminali si sono serviti della vulnerabilità per distribuire web shell sulle interfacce web esposte al pubblico dei server di MOVEit Transfer; in alcuni casi, queste web shell sono riuscite a mantenere la persistenza anche dopo l'applicazione delle patch da parte dei clienti di Progress

MOVEit è stata solo un esempio di moltissime vulnerabilità "zero-day" che i team di sicurezza informatica delle aziende hanno dovuto affrontare nel 2023. Nel mese di febbraio, GoAnywhere, un altro sistema di trasferimento dei file, ha rivelato una vulnerabilità che una gang affiliata a Cl0p aveva cercato di sfruttare. In più, una vulnerabilità nell'esecuzione del codice remoto nei prodotti software per server di stampa PaperCut MF e NG è stata sfruttata dalla gang di ransomware Bl00dy a marzo e ad aprile, dopo essere stata segnalata dagli sviluppatori a gennaio.

In alcuni casi, non è possibile applicare patch per queste vulnerabilità. Ad esempio, una vulnerabilità nelle appliance Barracuda Email Security Gateway identificata a giugno era talmente grave da non poter essere risolta e ha pertanto richiesto la sostituzione completa delle appliance fisiche e virtuali. Una gang cybercriminale cinese ha continuato a sfruttare le appliance vulnerabili per il resto del 2023.

Le vulnerabilità nei software e nei dispositivi non devono per forza essere recenti per essere sfruttate dagli hacker. Spesso gli autori degli attacchi cercano di colpire software non più supportati, ad esempio quelli di firewall di rete e server web obsoleti, sapendo che non verranno rilasciate patch.

Attacchi alla supply chain e malware con firme digitali

Le piccole imprese devono anche pensare alla sicurezza dei servizi da cui dipendono per gestire la propria azienda, nonché delle rispettive infrastrutture informatiche. Gli attacchi alla supply chain non colpiscono solo le organizzazioni a livello governativo. Abbiamo infatti osservato che gli attacchi rivolti ai Managed Services Provider stanno diventando un elemento sempre più rilevante nella strategia del ransomware.

Nel 2023, il team Sophos MDR è intervenuto in cinque casi che avevano colpito aziende di piccole dimensioni, i cui attacchi erano stati causati da un exploit nel software di monitoraggio e gestione da remoto (RMM) di un loro provider di servizi. Gli autori dell'attacco si erano serviti dell'agente di RMM NetSolutions in esecuzione nei computer delle organizzazioni prese di mira per creare nuovi account di amministrazione nelle reti delle vittime e successivamente per distribuire strumenti di desktop remoto, esplorazione della rete e implementazione di software. In due di questi casi, gli hacker sono riusciti a distribuire il ransomware LockBit.

È difficile proteggersi contro attacchi che sfruttano software attendibili, specialmente quando questi software offrono agli hacker la possibilità di disattivare la protezione endpoint. Le aziende di piccole dimensioni e i provider di servizi che le assistono devono monitorare attentamente gli avvisi che indicano che la protezione endpoint è stata disattivata nei sistemi presenti nella loro rete: questo potrebbe infatti essere un segnale che indica che un hacker ha ottenuto accesso con privilegi elevati attraverso una vulnerabilità della supply chain, oppure tramite altri software che a prima vista potrebbero sembrare legittimi.

Nel 2023, ad esempio, abbiamo notato varie istanze di autori degli attacchi che sfruttavano driver del kernel vulnerabili di software obsoleti che avevano ancora firme digitali valide; altri exploit riguardavano software malevolo creato intenzionalmente, che utilizzava firme digitali ottenute in maniera fraudolenta(inclusi driver del kernel dannosi firmati digitalmente con il programma Microsoft Windows Hardware Compatibility Publisher, WHCP), per eludere il rilevamento degli strumenti di sicurezza ed eseguire codice in grado di disattivare la protezione antimalware.

I driver del kernel operano a un livello di base del sistema e, durante l'avvio del sistema operativo, vengono tipicamente caricati prima di altri software. Questo significa che in molti casi possono eseguirsi prima che venga avviato il software di sicurezza. Le firme digitali svolgono in un certo senso la stessa funzione di un lasciapassare: in tutte le versioni di Windows a partire da Windows 10 versione 1607, i driver del kernel devono essere in possesso di una firma digitale valida, altrimenti non vengono caricati dai sistemi operativi Windows nei quali è attivato l'Avvio protetto.

A dicembre 2022, Sophos ha comunicato a Microsoft di aver scoperto dei driver del kernel dannosi che presentavano certificati firmati da Microsoft. Poiché avevano certificati firmati da Microsoft, questi driver sono stati accettati per impostazione predefinita come software innocui, il che ne ha permesso l'installazione e le successive azioni di disattivazione delle protezioni endpoint sui sistemi nei quali erano stati installati. Microsoft ha rilasciato un advisory sulla sicurezza e a luglio 2023 ha revocato diversi certificati di driver malevoli che erano stati ottenuti con WHCP.

Anche i driver non malevoli possono essere soggetti a exploit. Abbiamo osservato vari casi in cui driver e altre librerie di versioni obsolete e persino attuali di prodotti software sono stati sfruttati dagli autori degli attacchi per il "sideload" del malware nella memoria di sistema.

Abbiamo anche rilevato l'uso di driver di Microsoft negli attacchi. Una versione vulnerabile di un driver dell'utilità Microsoft Process Explorer è stata utilizzata diverse volte da alcuni criminali del ransomware, nel tentativo di disattivare i prodotti di protezione endpoint; ad aprile 2023, abbiamo documentato la presenza di uno strumento che è stato chiamato "AuKill", che sfruttava questo driver in più attacchi, cercando di distribuire i ransomware Medusa Locker e LockBit.

A volte siamo stati fortunati e abbiamo intercettato i driver vulnerabili prima che potessero essere soggetti a exploit. A luglio, l'attività di un driver in un prodotto di sicurezza di un altro vendor ha attivato le regole di comportamento di Sophos. A far scattare l'allarme è stato un test di simulazione di attacco di un cliente, ma la nostra indagine sull'evento ha rivelato tre vulnerabilità, che abbiamo segnalato al vendor del software interessato e per le quali sono poi state rilasciate patch.

Con il social engineering, gli spammer cercano di spingersi oltre

In un'era caratterizzata da chat su dispositivi mobili con messaggi crittografati end-to-end, c'è chi può considerare le e-mail come un metodo di comunicazione antiquato; tuttavia, sembra che gli spammer non se ne siano accorti, o che semplicemente questo non gli interessi. Sebbene si continui a osservare il metodo tradizionale BEC, nel quale un cybercriminale finge di essere un dipendente che chiede a un altro dipendente di inviare carte regalo, ultimamente gli spammer stanno dando sfogo alla loro creatività.

L'anno scorso il team di sicurezza Sophos per la messaggistica si è imbattuto in una miriade di nuovi stratagemmi e tecniche di social engineering, progettati per eludere i tradizionali controlli delle e-mail. I messaggi in cui l'autore di un attacco inviava un allegato o un link tramite e-mail senza alcun contatto precedente sono ormai fuori moda: ora è molto più probabile che gli spammer più abili inizino prima una conversazione, per poi passare all'attacco finale nelle e-mail di follow-up.

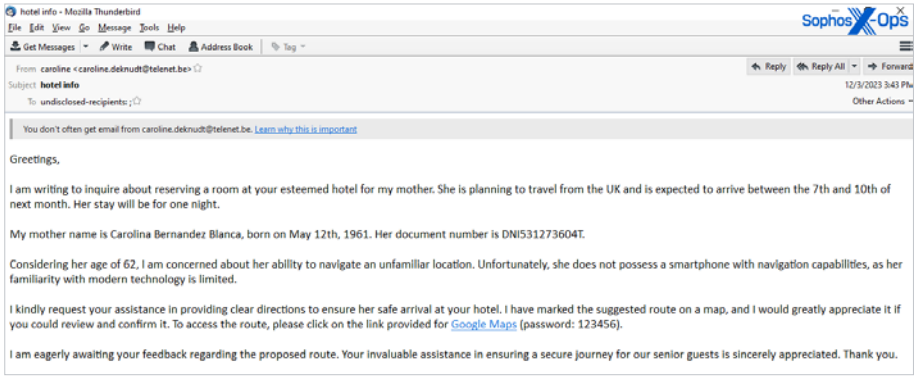

Figura 13: È solo dopo aver ricevuto una risposta dalla potenziale vittima che lo spammer tende a inviare un'e-mail con un link a un file dannoso all'interno di un file di archivio ZIP protetto da password

Abbiamo osservato questa metodologia in attacchi nei quali gli spammer fingono di essere operatori di un servizio di consegna e chiamano clienti aziendali al telefono, chiedendo di aprire un'e-mail con contenuti ingannevoli. Nel 2023 abbiamo anche visto spammer che colpivano diversi settori inviando inizialmente un sollecito o un reclamo tramite e-mail, seguito da un link per scaricare un file malevolo camuffato da documento legittimo, dopo che l'azienda aveva risposto alla prima e-mail.

Tradizionalmente, la prevenzione antispam prevede processi di ispezione dei contenuti dei messaggi, con decisioni prese in base a tali contenuti. Gli spammer hanno sperimentato vari metodi per sostituire i contenuti testuali dei loro messaggi con immagini incorporate: in alcuni casi, le immagini sembravano essere un messaggio scritto, mentre altre volte i malintenzionati avevano provato a usare codici QR o immagini che sembravano essere fatture (con numeri di telefono che gli autori dell'attacco cercavano di convincere la vittima a chiamare), nel tentativo di eludere il rilevamento.

Figura 14: Un allegato PDF in un messaggio di spam, nel quale è incorporata l'anteprima sfocata e illeggibile di una fattura, con un link a un sito web che ospita un payload dannoso

Con gli allegati dannosi, gli hacker hanno cercato di spingersi oltre; si è osservato persino un ritorno dei PDF ingannevoli, contenenti link a script o siti web dannosi, a volte utilizzando un codice QR incorporato. La famiglia di malware QakBot ha ampiamente abusato del formato dei documenti Microsoft OneNote, ovvero del blocco appunti (o file .one), per distribuire payload, prima di essere stata fermata verso fine anno in un intervento coordinato di neutralizzazione. I cybercriminali hanno anche sfruttato il formato di file MSIX (un tipo di formato di file di archivio utilizzato da Microsoft per distribuire app attraverso il Windows App Store), come stratagemma per sfuggire al rilevamento.

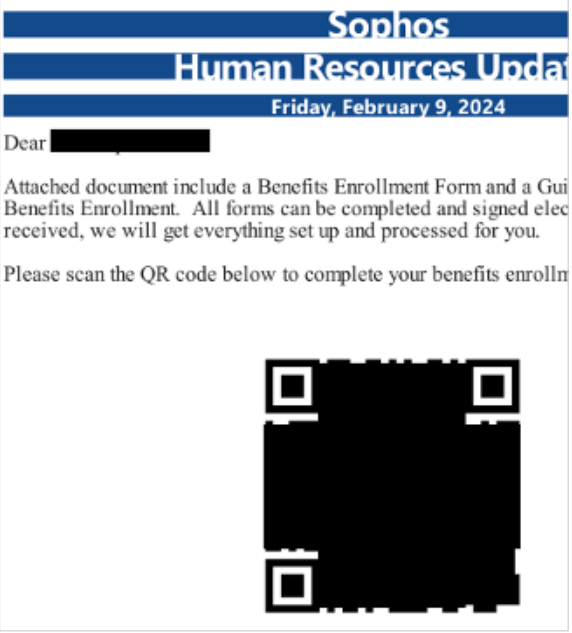
Sophos
Human Resources Updat
Friday, February 9, 2024
Dear [redacted]
Attached document include a Benefits Enrollment Form and a Gui
Benefits Enrollment. All forms can be completed and signed elec
received, we will get everything set up and processed for you.
Please scan the QR code below to complete your benefits enrolln

Figura 15: Un allegato PDF dannoso inviato a dei dipendenti Sophos, con un codice QR incorporato che porta a una pagina di phishing

E gli autori degli attacchi hanno utilizzato in maniera impropria anche i servizi di Microsoft: a fine anno, circa il 15% di tutto lo spam bloccato da Sophos era stato inviato sfruttando account e-mail creati nel sistema di messaggistica aziendale onmicrosoft.com.

Mobile malware e minacce di social engineering

Le aziende di piccole dimensioni dipendono dai dispositivi mobili per i propri sistemi informatici approvati o ad hoc. SMS, applicazioni di messaggistica e comunicazione, nonché app connesse ai servizi cloud (incluse applicazioni per POS mobili) sono tutti sistemi critici per le piccole imprese distribuite. I cybercriminali lo sanno e continuano a escogitare modi per colpire gli utenti dei dispositivi mobili per ottenere accesso ai dati o per truffare le loro vittime.

Spyware e "banker" sono famiglie di malware Android che suscitano particolare preoccupazione e che riteniamo continueranno a rappresentare una minaccia anche in futuro. Lo spyware viene utilizzato per raccogliere dati dal telefono e a volte persino per iscrivere a sua insaputa l'utente del dispositivo mobile a servizi a tariffa maggiorata, generando così un guadagno monetario diretto. Questo malware preleva dal dispositivo colpito dati personali (inclusi messaggi SMS e registri delle chiamate), che vengono poi venduti a truffatori, utilizzati come arma di ricatto, o entrambe le cose. Ci sono stati numerosi casi in cui le vittime sono arrivate a togliersi la vita come conseguenza diretta di un attacco spyware.

Queste applicazioni per dispositivi mobili malevole vengono distribuite in vari modi. Fingono di essere applicazioni legittime in Google Play o in app store di terze parti, spesso spacciandosi per applicazioni di prestiti. Vengono anche diffuse tramite link inviati per SMS.

I banker sono malware che colpiscono le applicazioni finanziarie, inclusi i portafogli di criptovalute, per raccogliere dati sui conti bancari e ottenere accesso ai fondi, utilizzando le autorizzazioni di accessibilità per mettere mano ai dati di natura sensibile presenti nel telefono.

C'è poi il fenomeno del "pig butchering," o ***sha zhu pan***. Abbiamo iniziato a monitorare, sia su iOS che su Android, le applicazioni fasulle legate a un tipo di truffa che avevamo inizialmente chiamato "CryptoRom"verso l'inizio del 2021; da allora, le truffe sono diventate sempre più sofisticate.

Le organizzazioni criminali che si nascondono dietro queste truffe (spesso pilotate dall'interno di complessi edilizi in cui lavorano persone che sono state praticamente sequestrate dalla criminalità organizzata) hanno rubato miliardi di dollari a vittime in tutto il mondo, colpendo frequentemente le piccole imprese. Nel 2023 una piccola banca nel Kansas è andata in fallimento ed è stata confiscata dall'FDIC dopo che il CEO aveva inviato 12 milioni di $ depositati dai clienti a degli scammer, nel tentativo di recuperare fondi che a quanto pare avrebbe perso in una di queste truffe. Questo tragico esempio mostra come una truffa solitamente associata alla vita privata di una persona possa avere ramificazioni più ampie e influire anche sulle piccole imprese.

Gli scammer che utilizzano le truffe sha zhu pan attirano le vittime sfruttando social media, app di incontri, altre app e piattaforme delle community, nonché persino SMS inviati "per errore". Tendono a colpire le persone alla ricerca di una connessione romantica o un'amicizia. Dopo aver trasferito la conversazione con la vittima su un'app di messaggistica sicura, come WhatsApp o Telegram, il cybercriminale cerca di guadagnarsene la fiducia, per poi presentare un'idea lucrativa nella quale dichiara di essere coinvolto direttamente e che di solito prevede l'uso di criptovalute.

Negli ultimi 12 mesi abbiamo osservato come le applicazioni fasulle utilizzate in queste truffe siano riuscite a infiltrarsi negli app store di Google Play o iOS. I criminali eludono le verifiche di sicurezza degli app store con un'app innocua, che rimane tale fino alla fine del processo di valutazione; successivamente, ne modificano i contenuti remoti per trasformarla in un'app di crypto trading fittizia. Gli scammer intascano immediatamente tutte le criptovalute depositate in queste app.

Recentemente abbiamo osservato anche alcune di queste truffe che adottano una tattica tipica di un'altra forma di truffa crypto che non richiede alcuna app fasulla: in questi casi, viene utilizzata la funzionalità "Web3" delle app di portafogli digitali per dispositivi mobili, per attingere direttamente dai fondi nei portafogli creati dalle vittime. Abbiamo identificato centinaia di domini associati a queste varianti di sha zhu pan basate sul "DeFi (Decentralized Finance) mining", e proprio come avviene per le app fasulle che identifichiamo, continuiamo a segnalarli e facciamo di tutto per fare in modo che vengano rimossi.

Conclusioni

Di sicuro non sono poche le minacce affrontate dalle piccole imprese, e il loro livello di complessità è spesso paragonabile a quello riscontrato negli attacchi rivolti ad aziende di grandi dimensioni ed enti governativi. Sebbene le somme che possono essere sottratte alle piccole imprese siano inferiori a quelle delle organizzazioni più estese, i cybercriminali non si fanno scrupoli a rubare ciò su cui riescono a mettere mano e per compensare intensificano il volume degli attacchi.

Le associazioni criminali contano sul fatto che le aziende più piccole sono spesso caratterizzate da difese meno efficaci e non implementano strumenti moderni e sofisticati per proteggere utenti e risorse. Il segreto per proteggersi in maniera efficace contro queste minacce è dimostrare che queste supposizioni sono infondate: educa i tuoi dipendenti, implementa l'autenticazione a più fattori in tutte le risorse connesse a Internet, applica le patch a server e appliance di rete il prima possibile e considera una migrazione delle risorse più difficili da gestire (ad esempio i server di Exchange) verso piattaforme e-mail SaaS.

In base alla nostra esperienza, la differenza principale tra le aziende per cui gli attacchi informatici hanno effetti devastanti e quelle che riescono invece a superarli con conseguenze minori è il tempo di risposta. Poter contare su esperti in grado di monitorare e rispondere alle minacce 24/7 non è più un optional per il 2024, bensì un must. Restare al sicuro non è impossibile. Richiede semplicemente una pianificazione completa e livelli multipli di protezione, in grado di regalarti tempo prezioso per rispondere agli attacchi e minimizzare i danni.

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

11/04/24 IT (NP)

SOPHOS