SOPHOS
Cybersecurity delivered.

Sophos Threat Report 2023

I Team Di Sicurezza Affrontano Criminali Informatici Sempre Più Evoluti

Sophos X-Ops

Indice dei contenuti

Joe Levy
CTO Sophos

Lettera da parte del Chief Technology Officer

Ogni volta che ci avviciniamo alla fine dell'anno, è tradizione nel settore della cybersecurity, passare in rassegna gli ultimi 12 mesi e riconoscerli come i più significativi nella storia del nostro settore. Anche se nel 2022 non si sono verificati eventi del calibro di Aurora, Stuxnet, WannaCry o il cyberattacco a Colonial Pipeline, quest'anno, purtroppo, si è guadagnato un posto negli annali della cybersecurity a causa del conflitto in Europa, il più serio negli ultimi 50 anni.

Questa guerra presenta risvolti importanti per la cybersecurity, perché è sorta quando il paese promotore del ransomware, che ha anche la reputazione di essere uno dei principali sostenitori dell'attività cybercriminale, nonché isola felice per gli hacker, ha invaso la nazione confinante.

Dopo l'invasione dell'Ucraina, era inevitabile che il governo russo incoraggiasse (o arruolasse direttamente) le imprese cybercriminali locali per condizionare l'opinione pubblica internazionale, cercando di farla schierare dalla sua parte e sabotando le simpatie che il presidente ucraino avrebbe potuto raccogliere a livello globale. Ed è proprio questo che è accaduto quando vari promotori di disinformazione e gang di ransomware e malware hanno unito le forze a sostegno dell'aggressione russa.

Tuttavia, finora queste attività sono state un fallimento catastrofico. Il pubblico globale aveva già da tempo una pessima opinione dei criminali del ransomware, fin da quando, durante la pandemia, queste gang avevano attaccato gli ambiti più vulnerabili e più essenziali per la risposta alla crisi, inclusi il settore della sanità, le organizzazioni di ricerca medica, le aziende indispensabili per mantenere operative le varie supply chain, senza dimenticare l'industria alimentare e le fonti di energia, nonché addirittura il settore dell'istruzione. Le gang di ransomware non si erano di certo attirate la simpatia del pubblico, ma ora avevano suscitato maggiore collera a livello globale, pronunciandosi nettamente a favore dell'invasione della Russia, e dichiarando che qualsiasi organizzazione che si fosse opposta si sarebbe trovata nell'occhio del mirino.

Tuttavia, altri membri delle stesse gang basati in Ucraina vedevano la situazione da un'altra prospettiva. Ha così avuto inizio un botta e risposta di fughe di informazioni, che ha reso pubblici alcuni dei segreti più riservati e mai divulgati prima, che hanno aperto una finestra sul modus operandi delle gang di criminali informatici. A quanto pare la guerra ha causato una scissione, potenzialmente permanente, tra gli hacker ucraini e le loro controparti russe (e bielorusse).

Allo stesso tempo, mentre la Russia era occupata a promuovere la sua guerra di aggressione, la Cina ha intrapreso azioni cybercriminali di portata colossale, colpendo non solo i paesi confinanti e quelli che considerava decisivi per una potenziale "nuova via della seta", ma persino lo stesso settore della sicurezza informatica. In una serie di attacchi sempre più sfrontati contro aziende in prima linea nell'ambito della protezione delle informazioni e della rete, le gang di cybercriminali cinesi (probabilmente sponsorizzate dal governo) hanno preso di mira i prodotti di sicurezza per hardware realizzati da quasi tutte le aziende nei settori della sicurezza informatica e delle infrastrutture.

In un senso molto tangibile e personale, sembra che nel 2022 la lotta sia diventata ancora più spietata e che le due nazioni che rappresentano il maggior rischio di sicurezza informatica per il resto del mondo abbiano gettato la maschera, smettendo di fingere di non essere coinvolte nei più gravi casi di violazione e attacco alle infrastrutture, nonché nell'interruzione dei servizi per l'istruzione, il commercio internazionale e la sanità. L'impressione è invece che vogliano sbandierare pubblicamente il tutto, come per sfidarci a controbattere.

Quello che abbiamo fatto, che è anche quello che Sophos continuerà a fare in futuro, è potenziare le iniziative già in atto, per proteggere sia i nostri clienti che noi stessi. La nostra azienda ha intrapreso un percorso a lungo termine, volto a incrementare l'efficacia del rilevamento e dell'intervento automatico in presenza di comportamenti tipici del ransomware. Siamo diventati talmente abili a sabotare gli hacker, che questi stessi criminali stanno focalizzando sempre di più la loro attenzione nell'eludere il nostro rilevamento, invece di investire tempo e fatica nelle proprie minacce.

Al tempo stesso, alla luce degli attacchi sferrati dalle gang di cybercriminali cinesi e russe ai danni delle infrastrutture di sicurezza, avere fiducia nei propri vendor di cybersecurity è ora ancora più fondamentale. Siamo convinti che, per guadagnarsi e mantenere la fiducia dei loro clienti, i vendor debbano comunicare in maniera trasparente i propri investimenti in ambito di sicurezza, specialmente quando il vendor si occupa della fornitura di servizi e prodotti di protezione informatica. Sophos gestisce un Trust Center che fornisce approfondimenti sulle nostre attività relative ad avvertimenti tecnici e divulgazione di informazioni; offre anche test di sicurezza, programmi che premiano l'identificazione di bug e i nostri piani di analisi e risposta agli incidenti. Investiamo continuamente nella protezione della nostra infrastruttura interna, per renderla sicura contro attacchi e Advanced Persistent Threat; inoltre, potenziamo la protezione degli hardware e dei software in esecuzione negli ambienti dei nostri clienti. Il successo in questi ambiti sarà incrementale, poiché i criminali non hanno smesso di cercare di individuare e sfruttare nuove vulnerabilità. Sembra anzi che ultimamente si impegnino ancora di più a destabilizzare la sicurezza dei firewall, degli switch e degli access point di rete di qualsiasi vendor. In aggiunta, continuiamo a promuovere nelle nostre soluzioni l'applicazione di configurazioni sicure per impostazione predefinita; abbiamo poi introdotto nei nostri prodotti e servizi anche funzionalità molto utili, quali controlli dell'integrità dei sistemi e correzione dei criteri, potenziando così il profilo operativo e lo stato di sicurezza generale.

Le minacce continueranno a evolversi, e Sophos si adatterà instancabilmente a tutti i nuovi sviluppi, continuando a garantire i migliori risultati in termini di cybersicurezza.

Il background: la guerra in Ucraina

Se la guerra può essere considerata un'estensione dell'azione politica che usa altri mezzi, e se il conflitto informatico non è altro che un'ulteriore diramazione delle operazioni militari, è logico che la questione ucraina sia, on-line, molto simile alla situazione nella vita reale. Al momento della pubblicazione di questo documento, il panorama delle minacce ha un aspetto spaventoso all'interno dei confini ucraini, mentre nel resto del mondo occidentale causa problemi meno diffusi, ma pur sempre gravi. Inoltre, suscita molta agitazione, poiché il potenziale di estensione del conflitto, la disinformazione e il disagio generale rimangono comunque molto elevati.

Un conflitto locale, con ripercussioni a livello globale

Com'era prevedibile, la rapida escalation degli attacchi russi contro l'Ucraina del 24 febbraio ha portato alla luce truffatori che non aspettavano altro se non un'opportunità di guadagno a scapito della sofferenza e della costernazione globale.

A inizio marzo abbiamo notato un incremento nella quantità di e-mail provenienti da associazioni di beneficenza fasulle, che chiedevano donazioni per l'Ucraina. Nei primi giorni della guerra, i funzionari ucraini avevano fatto appelli al mondo intero per chiedere un contributo a sostegno della loro difesa militare e questi appelli includevano anche richieste di donazioni in criptovalute, a favore del Ministero del Tesoro del paese. I truffatori hanno subito approfittato dell'opportunità presentata dalle criptovalute, inviando milioni di e-mail di spam che si ricollegavano a questa richiesta, ma cambiando l'indirizzo del portafoglio della criptovaluta; includevano infatti destinatari che non erano associati né al governo ucraino, né a organizzazioni di beneficenza oppure ONG legittime. Durante il weekend del 5 e 6 marzo, il volume di messaggi di spam che chiedevano donazioni a favore di questi conti fasulli è stato talmente elevato da costituire la metà di tutto lo spam che abbiamo ricevuto in quel periodo di tempo: un volume scandalosamente alto. Fortunatamente, la campagna si è placata nel giro di pochi giorni.

Le truffe correlate all'Ucraina, rappresentate come percentuale del volume di spam in un giorno, marzo 2022

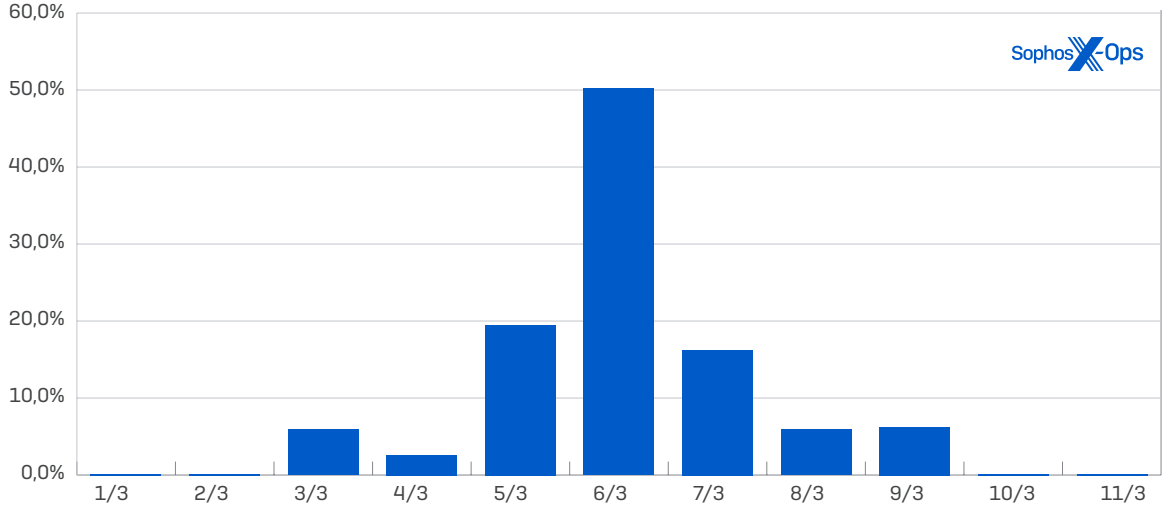

Fig.1. La crescita esponenziale, seppure di breve durata, del volume di e-mail di spam contenenti richieste di donazioni a favore di portafogli di criptovalute appartenenti a organizzazioni fasulle.

Giunti a maggio, sono emerse anche centinaia di siti fasulli che chiedevano "donazioni"; poiché i dati di pagamento avevano molti elementi in comune, sospettiamo che, come nel caso dei messaggi di spam iniziali, questi siti fossero gestiti da un numero relativamente limitato di entità. Questi attacchi erano tutt'altro che sofisticati dal punto di vista tecnico: la loro caratteristica principale era il fatto che utilizzassero come esca il nome del paese o dei suoi leader politici, per poi dare seguito al tutto sfruttando vulnerabilità ed exploit già noti.

Ad esempio, quel mese, in una campagna di spam particolarmente degna di nota, la gang di malware Emotet ha distribuito una serie di documenti Word dannosi, con titoli provocatori, sulla falsa riga della propaganda russa (ad esempio: "USA e alleati forniranno armi chimiche all'Ucraina.doc"), nel tentativo di diffondere il proprio malware. I documenti dannosi distribuiti in questo attacco sfruttavano un exploit della vulnerabilità CVE-2021-40444 per infettare i computer delle vittime che aprivano i documenti in computer a cui mancava quella patch di Office, che era stata rilasciata nell'autunno precedente.

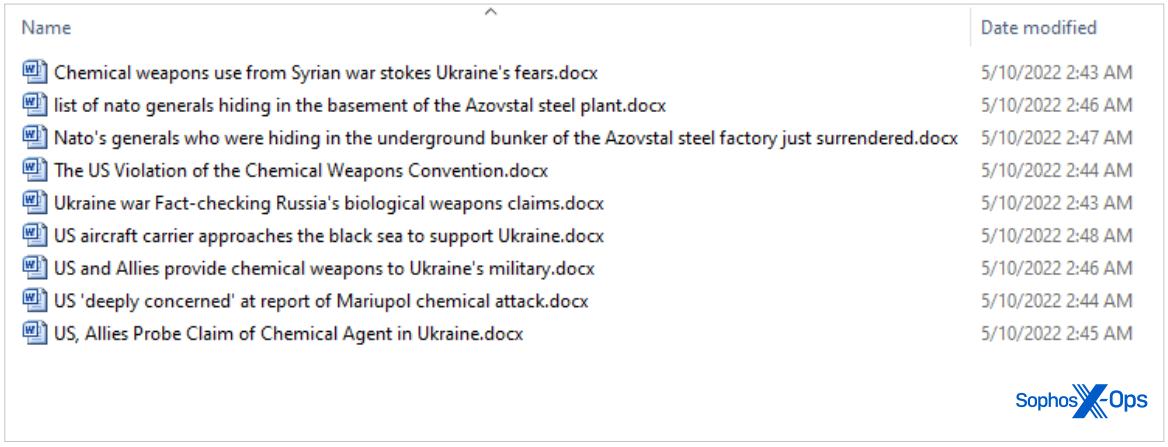

Fig.2. Alcuni titoli di documenti dannosi di spam Emotet sull'Ucraina, con dichiarazioni false e terrificanti.

Per quanto riguarda gli attacchi informatici a livello governativo fuori dai confini ucraini, al momento della pubblicazione di questo documento uno di questi due incidenti di alto profilo non è riconducibile a una fonte confermata. Secondo fonti ufficiali ucraine, l'attacco a ViaSat, che ha colpito i servizi satellitari dei clienti in Ucraina e in altri paesi europei poco prima dell'invasione, è sicuramente attribuibile alla Russia. Ma il sabotaggio di siti web di aeroporti occidentali nel mese di ottobre è più difficile da interpretare: è stato un attacco a livello governativo allo scopo di intimidire gli alleati dell'Ucraina, oppure è stata opera di hacker indipendenti?

La seconda ipotesi sembra essere quella più plausibile. Il sabotaggio e gli attacchi DDoS con tecnologie limitate (che hanno colpito anche siti web aeroportuali e hanno cercato di interferire con i voti dell'Eurovision) sono stati un'altra caratteristica delle prime giornate della guerra. Tuttavia, con il trascinarsi del conflitto verso un altro inverno e con la tensione elevata che caratterizza il clima internazionale, alcuni utenti che non lavorano in ambito tecnologico si sono trovati alle prese con le assurdità di KillNet, il collettivo di hacker simpatizzanti per la Russia.

Al centro di tutto

In territorio ucraino, il quadro mostra risvolti più strani e più cupi. Diversi attacchi rivolti al governo ucraino hanno seguito gli stessi pattern osservati nelle campagne dei cybercriminali: e-mail di social engineering, malware commerciale e strumenti di sicurezza offensiva utilizzati in maniera impropria. In un caso in particolare, un'e-mail contraffatta conteneva un link che sosteneva fosse un "aggiornamento per l'antivirus", ma in realtà era un beacon di Cobalt Strike. In un altro attacco (di cui parleremo in uno dei prossimi paragrafi di questo report), un ladro di informazioni metteva in vendita un'elevata quantità di dati su cittadini e organizzazioni governative dell'Ucraina. Non c'era nessuna richiesta di riscatto, solo una violazione volta a divulgare dati di natura sensibile.

Nel frattempo, sebbene siano due paesi diversi, in Ucraina e in Russia ci sono persone che sono da tempo complici in crimini informatici, con varie gang di ransomware che hanno affiliati in entrambe le nazioni. Quando è scoppiata la guerra, il nazionalismo ha causato divisioni interne in alcune gang.

La conseguenza più spettacolare è che lo scisma tra membri russi e ucraini in alcuni collettivi di ransomware e nei loro affiliati potrebbe aver causato la nascita di Conti Leaks, un dump di log di chat della gang dell'omonimo ransomware. Un account Twitter chiuso poco dopo la sua creazione e chiamato @TrickbotLeaks ha poi doxxato (ovvero rivelato informazioni personali o private su) presunti membri delle gang di cybercriminali Trickbot, Conti, Mazo, Diavol, Ryuk e Wizard Spiders.

Cosa si può dedurre da questo melodramma? Questi eventi forniscono ulteriori prove a dimostrazione del fatto che, come sostengono da anni numerosi ricercatori occidentali, il Servizio federale per la sicurezza della Federazione Russa (FSB) intrattiene rapporti molto stretti con diverse gang di ransomware, e che è possibile che abbia persino assegnato ad alcune di queste entità l'incarico di attaccare specificamente Conti.

Purtroppo, nessun aspetto di questo conflitto interno ha portato a una riduzione a lungo termine dell'attività globale del ransomware. Il 2022 ha avuto inizio con vari interventi degli ufficiali dell'FSB, che hanno arrestato sia membri della gang di ransomware-as-a-service REvil (a gennaio) che di una gang non identificata che si occupava di frodi basate sulle carte di credito (a febbraio); quest'anno ha anche visto l'estradizione verso gli Stati Uniti dei membri di REvil per un processo condotto nei primi di marzo. Tuttavia, giunti a metà anno questo tipo di collaborazione internazionale per la lotta contro il crimine era diventato ormai impensabile, e ci sono state varie indicazioni di un ritorno di REvil o di un servizio che si spacciava per questo ransomware. Nel frattempo, la guerra continua.

Gli aspetti economici del malware

Sebbene molti degli aspetti relativi al panorama delle minacce abbiano subito un'evoluzione l'anno scorso, quella più significativa potrebbe essere la continua crescita dell'economia cybercriminale. Questo ecosistema si è progressivamente trasformato in una vera e propria industria autonoma, con una rete di servizi di assistenza ben sviluppata e un approccio professionale e collaudato.

Le aziende IT hanno effettuato il passaggio verso linee di soluzioni "as-a-service", e l'ecosistema del cybercrimine ha seguito a ruota questo esempio. Broker di accesso, ransomware, malware per il furto di informazioni, opzioni di distribuzione del malware e altri elementi delle operazioni del cybercrimine sono diventati tutti molto più accessibili per gli aspiranti cybercriminali.

Uno dei motivi alla base di questa tendenza è l'economia emergente del cybercrimine. Esistono marketplace criminali, ad esempio Genesis, che permettono ai cybercriminali alle prime armi di acquistare facilmente malware e servizi di distribuzione del malware, per poi rivendere in blocco credenziali prelevate illecitamente e altri tipi di dati. I broker di accesso sfruttano exploit commerciali di software vulnerabili per infiltrarsi in centinaia di reti; a questo punto, rivendono questi accessi (spesso più volte) ad altri criminali. E gli affiliati che utilizzano il ransomware e altri hacker acquistano credenziali e accessi per sferrare attacchi a maggiore rischio, puntando a un bottino più sostanzioso per le loro attività criminali.

L'industrializzazione del ransomware ha facilitato l'evoluzione degli "affiliati" del ransomware, trasformandoli in vere e proprie attività professionali, specializzate nell'uso degli exploit. Con l'uso improprio di strumenti di sicurezza offensiva, software legittimi di amministrazione e supporto tecnico, nonché prodotti malware-as-a-service e altri exploit e malware acquistati sul mercato nero, gli hacker che abbiamo osservato sembrano convergere verso uno stesso punto: set di strumenti, tattiche e pratiche che non possono più essere associate ad attività di ransomware ben definite, a tentativi di spionaggio internazionale o ad altri motivi specifici. La specialità di queste gang di professionisti è ottenere (o acquistare) l'accesso ai sistemi, per rivenderlo a qualsiasi hacker disposto a pagare la somma richiesta, oppure, in alcuni casi, a più hacker con obiettivi diversi.

Per il loro business model, queste gang hanno copiato sotto vari punti di vista l'industria dei servizi cloud e web. Analogamente a come i reparti IT aziendali hanno adottato un modello "as-a-service" per un ventaglio sempre più esteso di funzionalità, ormai quasi tutti gli aspetti dei toolkit di cybercrimine possono essere affidati a fornitori di opzioni crime-as-a-service, che promuovono i loro "servizi" on-line, su pagine web clandestine. Esploreremo velocemente nove varianti di questi servizi, riservandone una decima, che meritano un'analisi più approfondita.

Nove acerrimi nemici

Access-as-a-service: vendita (individuale o in blocco) sul mercato nero di account e sistemi, che includono credenziali di Remote Desktop Protocol (RDP) e VPN, account, database, web shell e vulnerabilità che possono essere soggette a exploit.

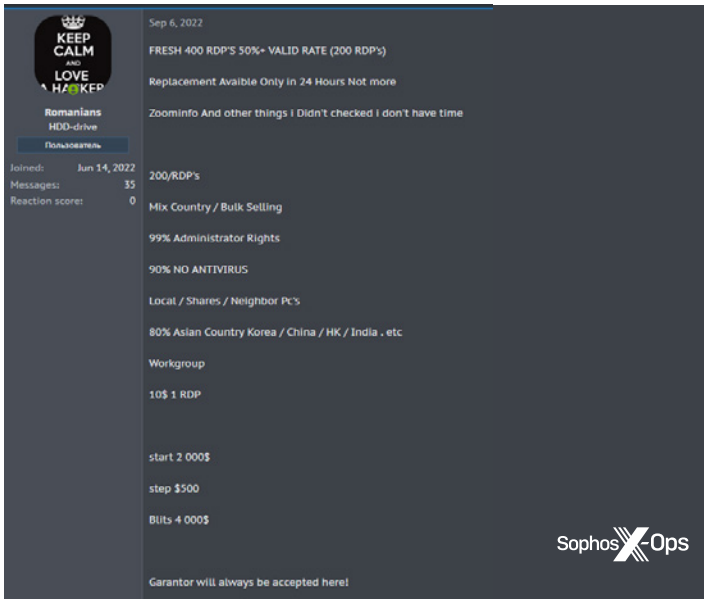

Fig.3. Un broker di accesso pubblicizza la sua mercanzia, alla ricerca di una vendita rapida.

Fig.4. Vendita all'asta dei dati di un'azienda con sede nell'UE

Distribution/spreading-as-a-service per il malware: agevolazione del processo di distribuzione del malware all'interno di aree geografiche o settori specifici o più estesi. Dagli annunci che abbiamo visto per questi servizi non emergono chiaramente le dinamiche di ogni caso, ma tra i potenziali vettori ci possono essere attacchi di tipo "watering hole", exploit delle vulnerabilità, o l'inclusione di elementi tipici dei prodotti AaaS (access-as-a-service).

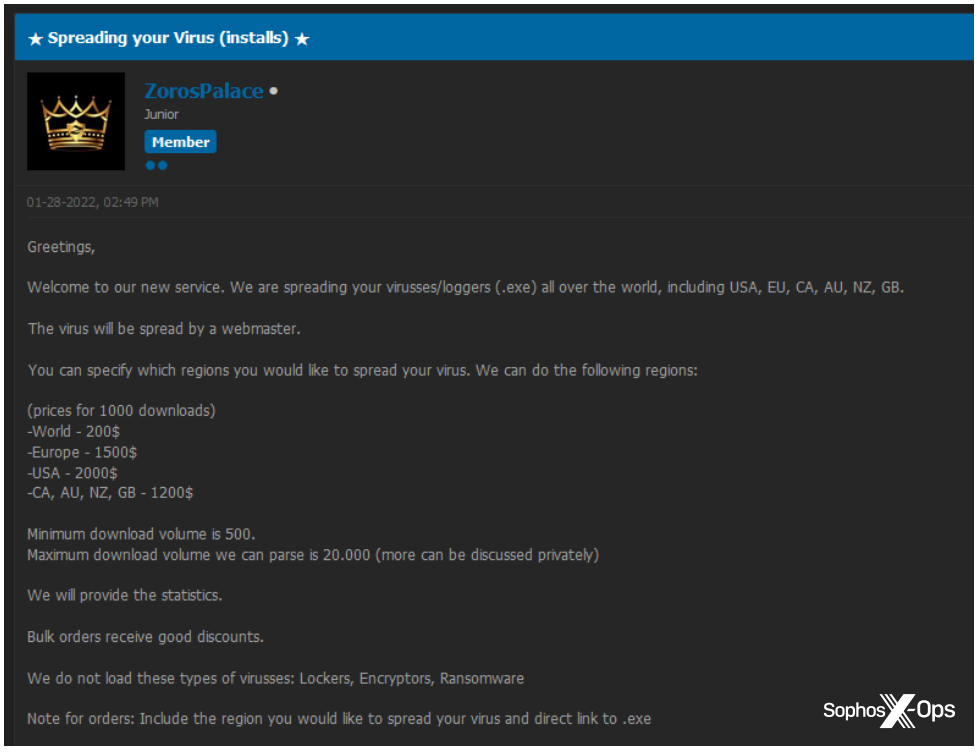

Fig.5. Un servizio appena avviato offre opzioni di propagazione del malware.

Phishing-as-a-service: offerta di servizi end-to-end per le campagne di phishing, incluse opzioni di clonazione dei siti web, hosting, e-mail realizzate per eludere i filtri antispam e appositi pannelli per monitorare i risultati.

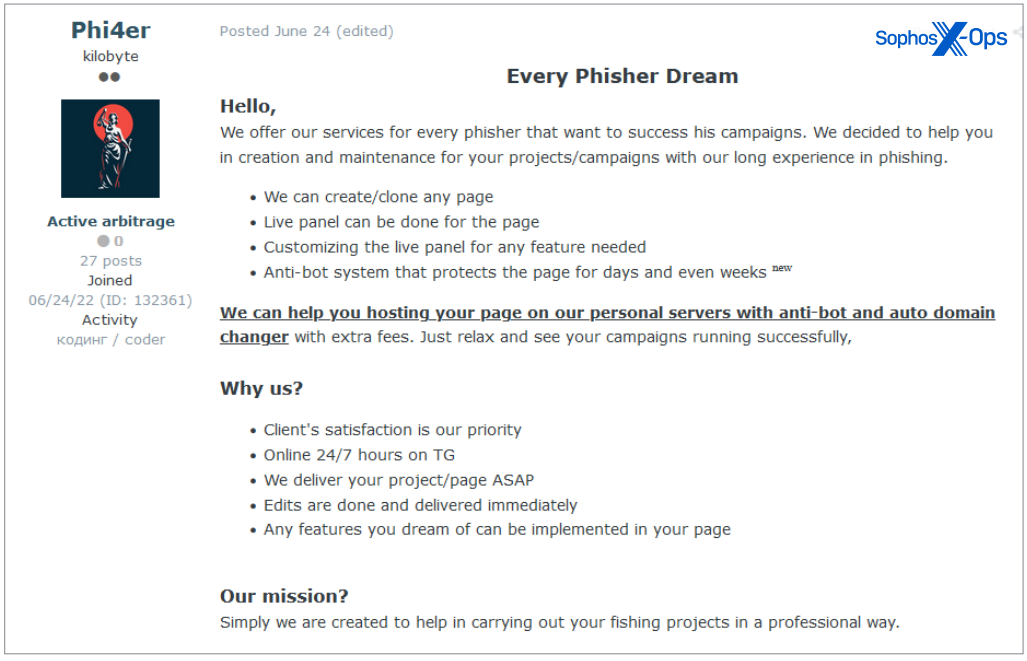

Fig.6. Una suite di servizi di phishing che garantisce supporto per i clienti.

OPSEC-as-a-service: un servizio particolarmente interessante, che abbiamo osservato come opzione inclusa in un pacchetto di Cobalt Strike su un forum di cybercriminali. Il venditore offre assistenza agli acquirenti per mezzo di un servizio OPSEC, che può essere acquistato con un pagamento unico o come abbonamento mensile, e che è progettato per mascherare le infezioni da Cobalt Strike e minimizzare il rischio di rilevamento e identificazione.

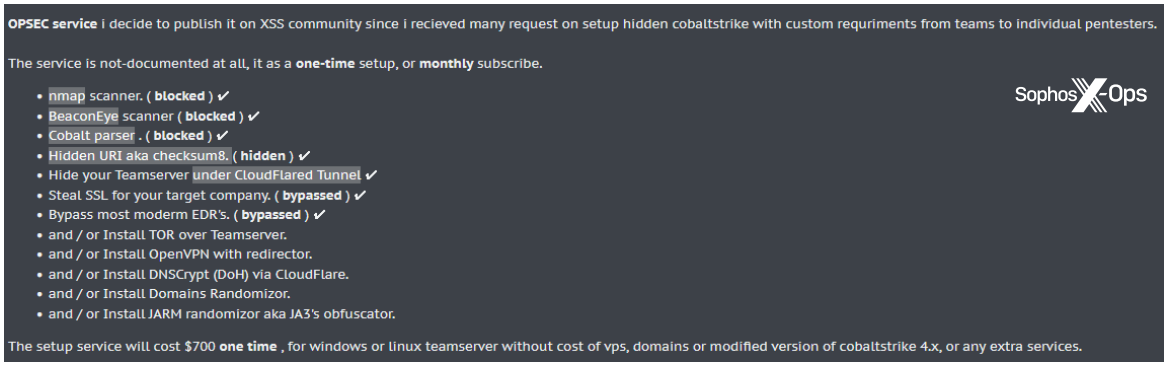

Fig.7. I fornitori di servizi specializzati aiutano i cybercriminali a coprire le proprie tracce.

Crypting-as-a-service: molto comune e venduto in diversi forum, il crypting-as-a-service è progettato per cifrare il malware in modo che possa eludere il rilevamento, specialmente quello di Windows Defender e SmartScreen, ma marginalmente anche quello di altri prodotti antivirus. Nell'esempio riportato di seguito, il servizio è stato offerto per un pagamento unico di 75 $ o per un abbonamento mensile di 300 $, con uso illimitato del servizio.

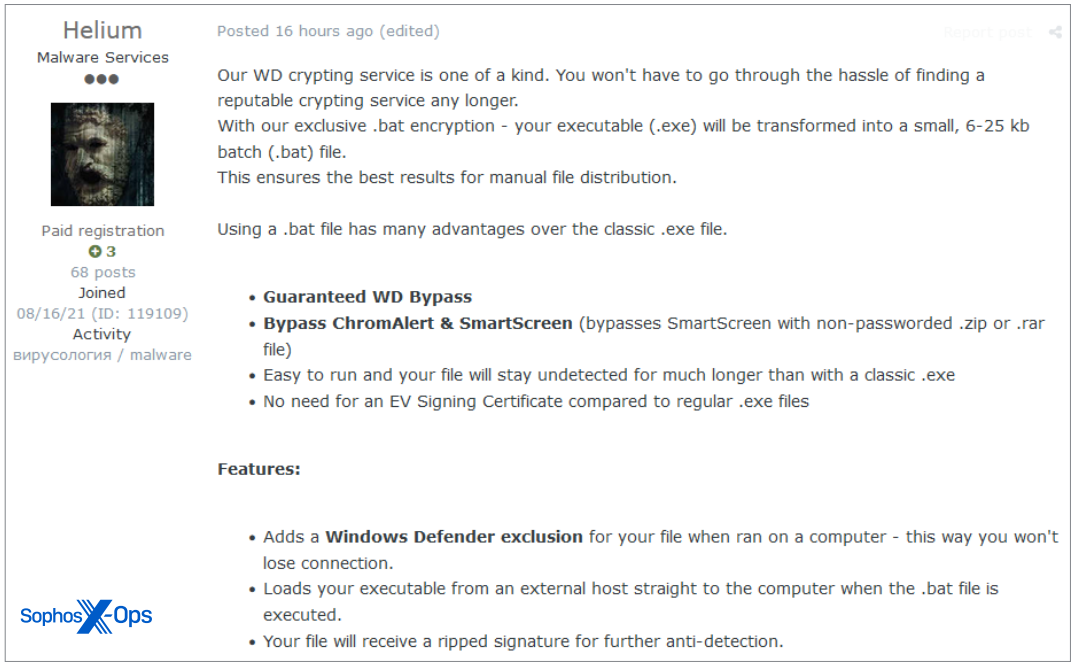

Fig.8. Nel tentativo di eludere il rilevamento, un servizio specializzato offre la possibilità di trasformare i file .exe in file .bat.

Scamming-as-a-service: abbiamo notato alcuni esempi di annunci per "kit di truffa" (scamming) sui forum cybercriminali, specialmente nell'ambito delle criptovalute,. Non era sempre chiaro cosa fosse in vendita, ma un annuncio offriva una "Pagina di truffa su Elon Musk che regala BTC" al prezzo di 450 $. Questa truffa è molto diffusa, e lo è stata fin dal 2018; è comparsa varie volte su Twitter, Medium e persino in un video manipolato con deepfake.

Vishing-as-a-service: un servizio di voice phishing ("vishing"), con cui un cybercriminale offre un sistema vocale a noleggio per ricevere telefonate, in combinazione con un "sistema di intelligenza artificiale" che permette al cliente di reindirizzare la vittima su un bot invece di un essere umano.

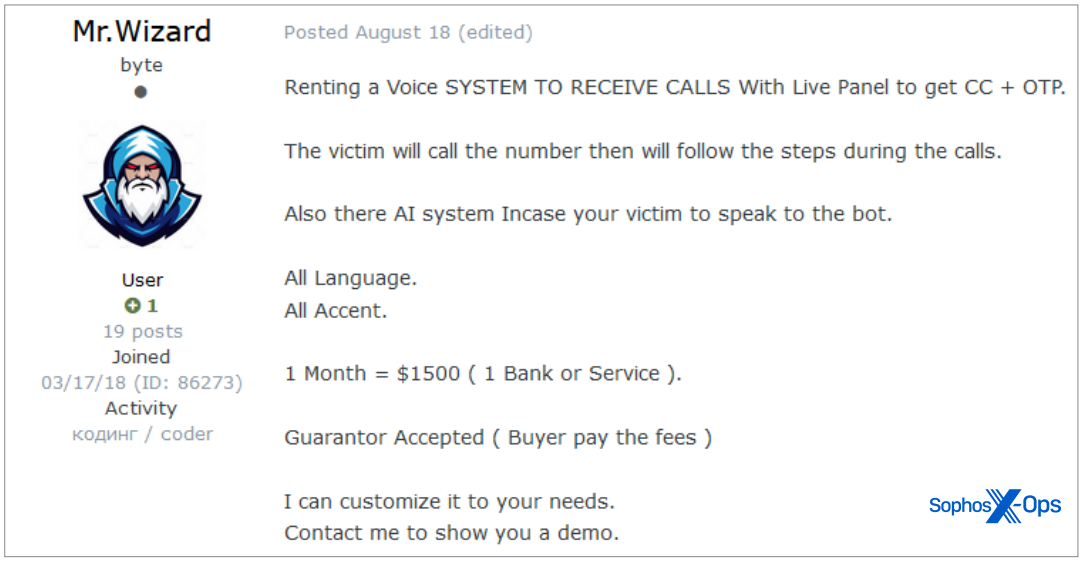

Fig.9. Un offerta di vishing-as-a-service, che include "ogni lingua, ogni accento".

Spamming-as-a-service: un classico, ma ancora molto diffuso sui forum criminali, lo spamming-as-a-service offre opzioni di spam in blocco attraverso un'ampia scelta di meccanismi, inclusi SMS ed e-mail. In alcuni casi, l'hacker offre di configurare l'intera struttura partendo da zero, altre volte invece gestisce l'infrastruttura e la sfrutta per inviare messaggi di spam personalizzati.

Scanning-as-a-service: ecco, infine, un servizio particolarmente interessante che viene offerto sui forum frequentati dai cybercriminali e che prevede l'accesso a una suite di strumenti commerciali legittimi (inclusi Metasploit, Invikti, Burp Suite, Cobalt Strike e Brute Ratel) per individuare, e presumibilmente sfruttare, eventuali vulnerabilità. Come possiamo vedere nella Figura 10, ai prezzi erano stati applicati sconti non indifferenti. A quanto pare, l'intera infrastruttura è stata creata e viene gestita dal venditore, che sostiene altrove che "basta solo attendere l'e-mail con i risultati della scansione".

Fig.10. Un fornitore di scanning-as-a-service elenca gli accessi a diverse suite di strumenti commerciali molto diffusi.

L'evoluzione dai primi passi alla maturità tecnologica

La crescita dell'industria "as-a-service" e la maggiore commercializzazione dei mercati clandestini hanno causato una trasformazione profonda nell'aspetto e nella funzionalità dei marketplace criminali. In un forum di spicco, ad esempio, gli utenti possono acquistare spazi pubblicitari e far visualizzare banner promozionali animati, destinati alle varie migliaia di utenti del forum. Va notato che uno degli annunci riportati nell'esempio che segue riguarda appunto Genesis, che abbiamo menzionato in questo documento e che è un marketplace di cui abbiamo già parlato in passato.

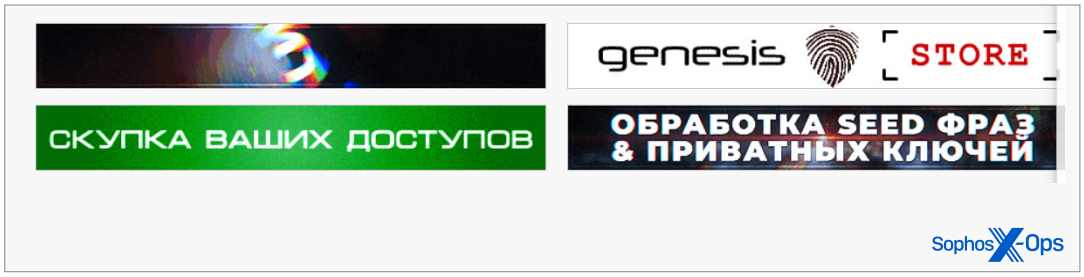

Fig.11. Un forum criminale mostra annunci per vari marketplace e servizi.

I cybercriminali sono anche sempre più consci dei vantaggi di un design e un layout ben curati. Anni fa, gli annunci relativi a malware e servizi correlati erano tendenzialmente semplici: post con un'enorme quantità di testo, che contenevano elenchi di funzionalità e opzioni. Oggi, invece, questi tipi di annunci sono spesso accompagnati da immagini dal forte impatto visivo, realizzate per dare ai prodotti un aspetto professionale e legittimo, con differenziazione del brand.

Fig.12. Il servizio Zed Point afferma di essere in grado di offrire informazioni che potrebbero agevolare l'alterazione o il furto di identità.

Fig.13. NoCryi raccoglie e conserva l'accesso a cookie di sessione rubati.

I marketplace non promuovono soltanto prodotti e servizi. Con il continuo sviluppo dell'economia criminale e il suo progressivo trasformarsi in una vera e propria professione, le offerte di lavoro e i post di reclutamento sono diventati sempre più comuni. Molti dei marketplace più importanti hanno pagine dedicate alla ricerca di collaboratori, sia per chi desidera un impiego (di solito come "penetration tester", un eufemismo che spesso significa affiliato di ransomware), che per chi offre lavoro.

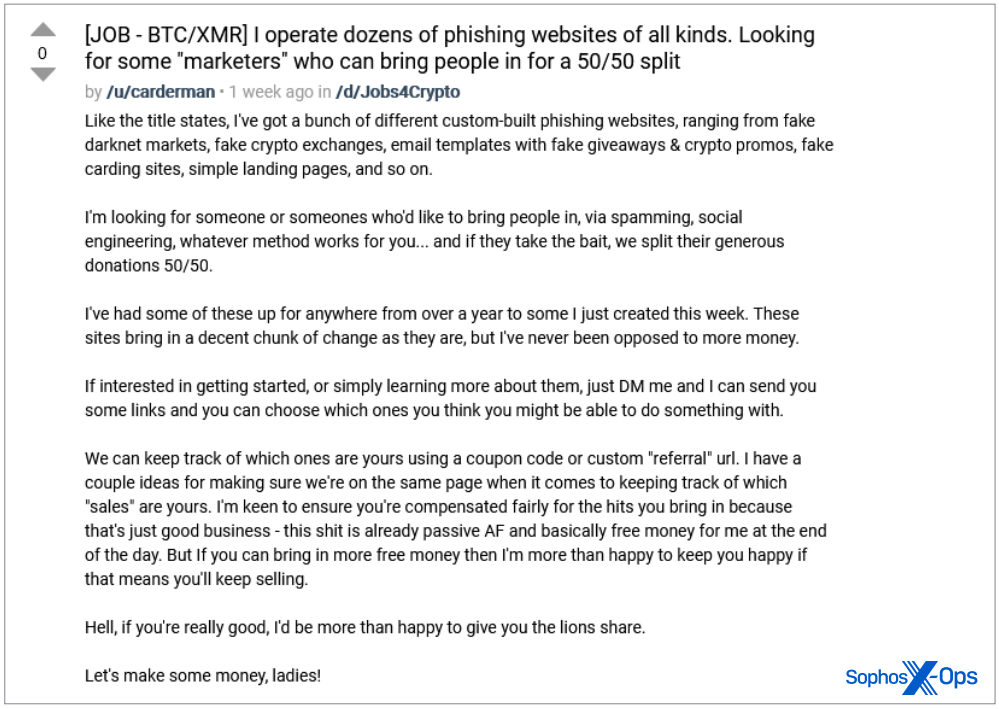

Fig.14. Le collaborazioni tra entità con set di competenze diverse permette di ottenere maggiore efficienza.

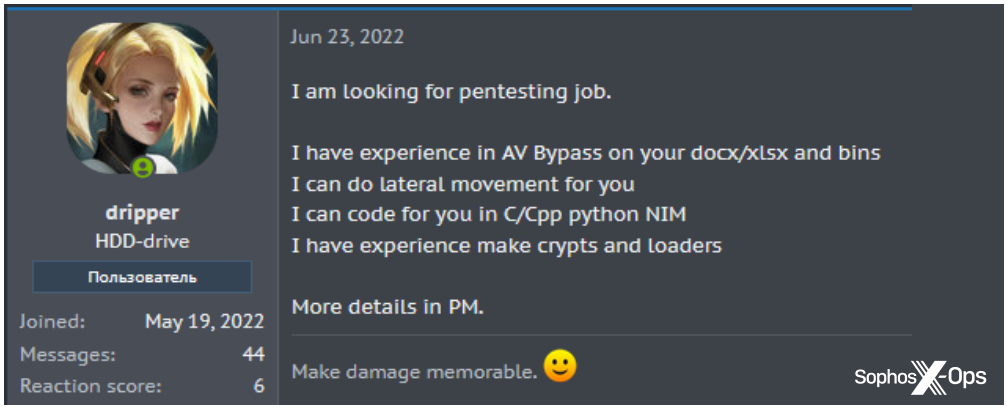

Fig.15. Un "penetration tester" esperto cerca lavoro presso un'entità già avviata.

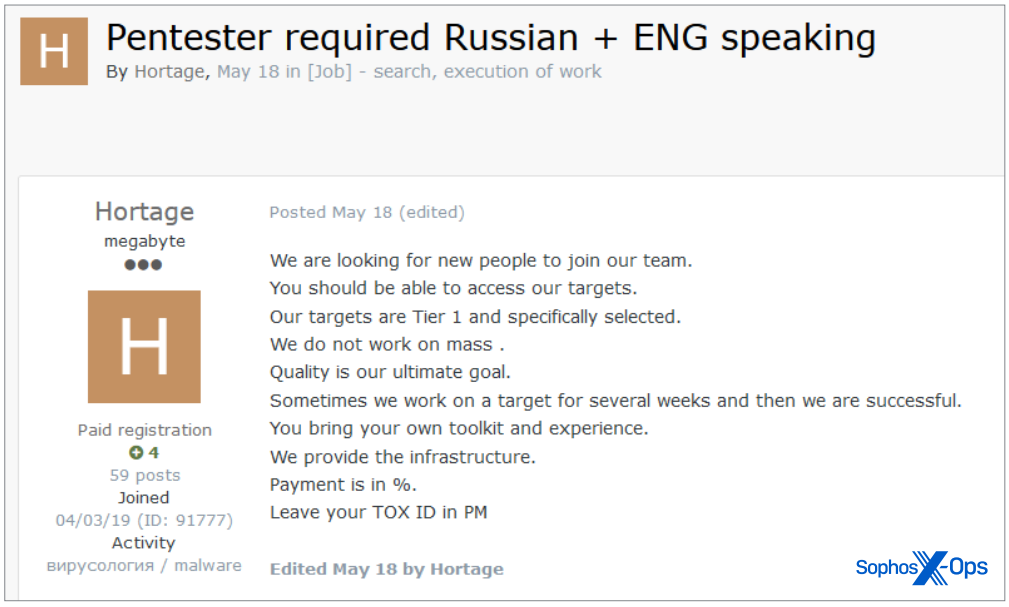

Fig.16. Una gang dii cybercriminali già operativa cerca altri membri.

Infostealer

I servizi dedicati al furto di informazioni sono parte dell'infrastruttura su cui si basa l'economia del malware. Sono simili, ma più estesi, delle opzioni "[elemento dannoso]-as-a-service" appena elencate. Grazie al malware-as-a-service e al malware-deployment-as-a-service, i cybercriminali alle prime armi possono cominciare con un investimento minimo, anche se hanno competenze tecniche che non vanno oltre la capacità di accedere ad alcuni pannelli di controllo web e di visitare i marketplace per la compravendita di credenziali.

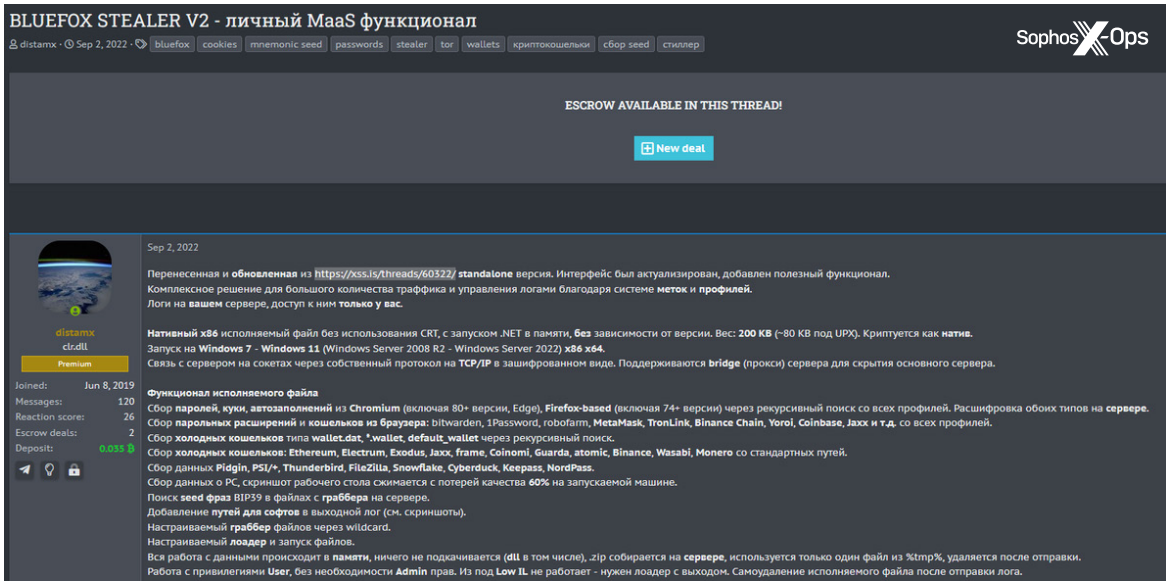

Fig.17. I servizi dedicati al furto di informazioni sono molto gettonati nell'ecosistema del cybercrimine, che favorisce la specializzazione.

Il cybercriminale imprenditoriale può poi rivendere le credenziali rubate su vari marketplace clandestini. In alcuni casi, queste credenziali sono solamente dati acquisiti fortuitamente da transazioni di criptovalute cifrate e altri metodi di monetizzazione del malware.

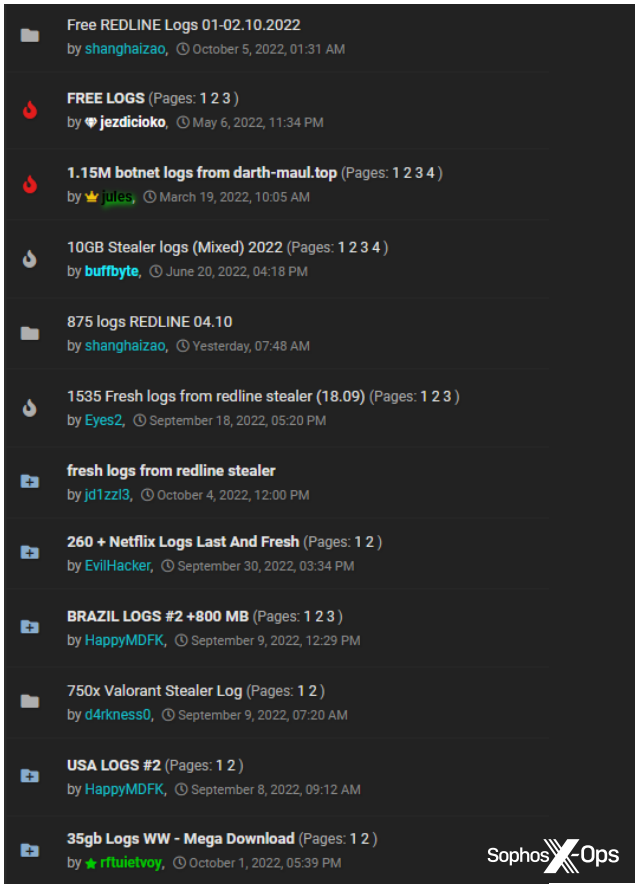

Fig.18. "Log" che sono stati rubati e messi in vendita; includono password e altre credenziali

Infine, l'ecosistema degli infostealer è a conoscenza del fatto che i responsabili di cybersecurity sono interessati alle sue azioni. E per non smentire la propria natura, riconosce anche in questo una buona opportunità di guadagno. Un forum clandestino, XSS, ha recentemente cercato di monetizzare il lavoro svolto da ethical hacker che hanno eseguito lo scraping dei loro forum, offrendo un abbonamento annuale di 2.000 $ per la raccolta di una quantità illimitata di dati.

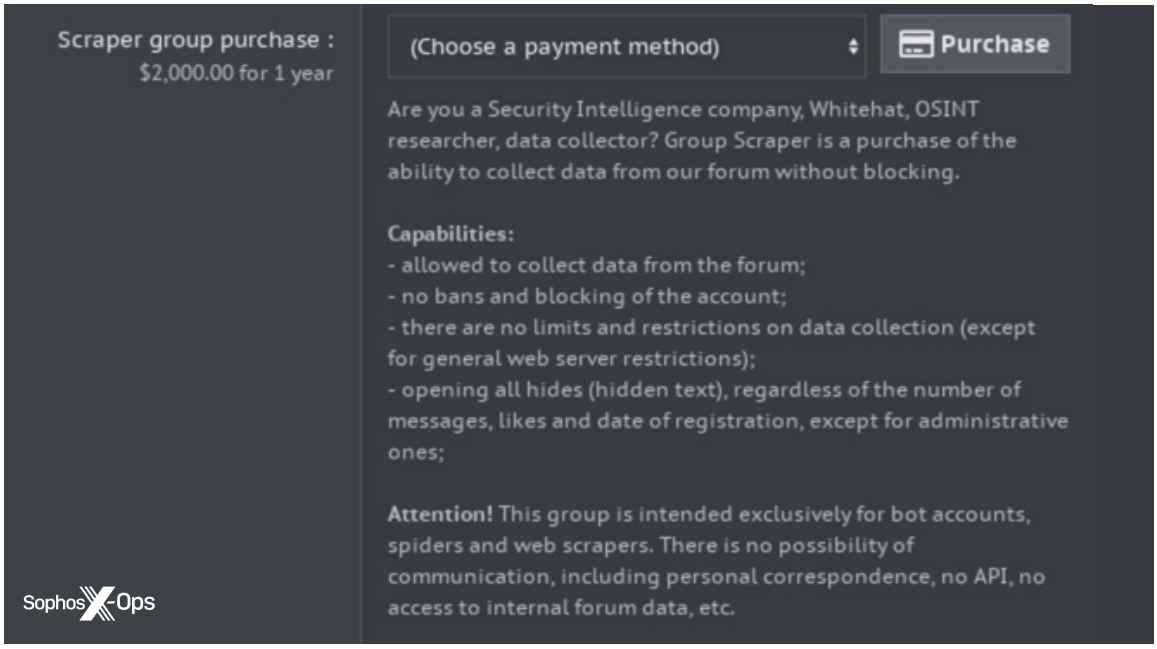

Fig.19. Un forum offre accesso a pagamento a strumenti di scraping BlueHat, nel tentativo di tenere d'occhio le attività criminali (la seconda immagine fornisce il testo tradotto dal russo all'inglese).

Quella del malware infostealer è una definizione molto ampia. Include vari tipi di malware che vengono menzionati in un altro paragrafo di questo report, inclusi strumenti di accesso remoto (RAT), keylogger, "clipper" focalizzati sulle criptovalute e altro malware che si occupa del furto illecito di credenziali, cookie del browser, transazioni di criptovalute o qualsiasi altro dato che può essere rubato rapidamente e rivenduto o riutilizzato per altri scopi dannosi.

Gli infostealer hanno fornito i cookie di Slack che sono poi stati utilizzati dalla gang Lapsus$ per ottenere accesso alla rete aziendale di Electronic Arts nel 2021. Sono stati coinvolti in maniera molto simile anche in altre attività più recenti, che prevedevano l'impiego di token di sessione di applicazioni web rubati; questi token hanno poi permesso ai criminali di ottenere un accesso più persistente ed esteso, che variava da attacchi di tipo Business Email Compromise fino al ransomware.

Infostealer, raffigurati in base alla percentuale di computer univoci

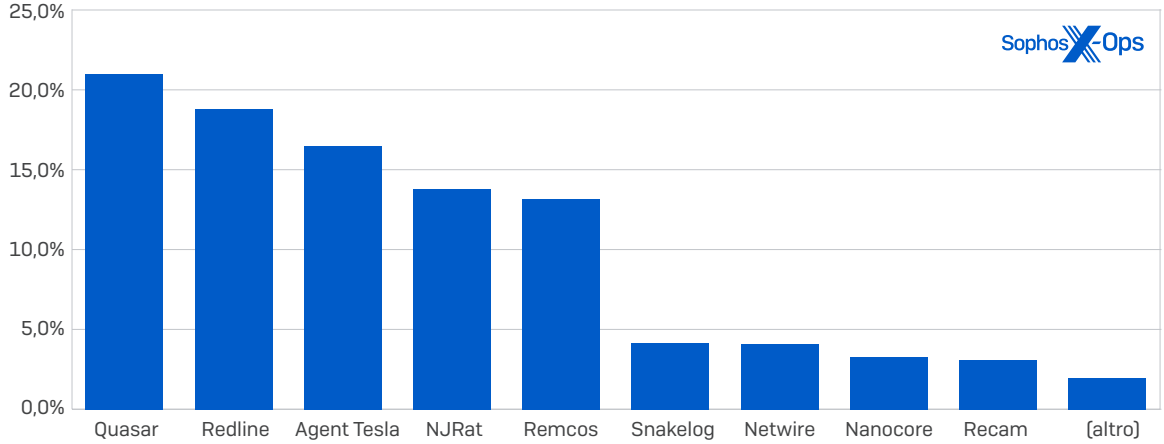

Fig.20. Quasar, Redline e Agent Tesla costituiscono la maggior parte del malware infostealer; Quasar è stato rilevato in più di un quinto dei computer infettati in un periodo di sei mesi.

Chi nutre un particolare interesse verso gli infostealer potrà notare l'assenza nel grafico del tristemente famoso Raccoon Stealer. Dopo la sua comparsa nel 2019, questo malware di origine ucraina focalizzato su Windows era momentaneamente svanito dal panorama all'inizio del 2022, in seguito a un intervento collaborativo tra l'FBI e le forze dell'ordine olandesi e italiane. È poi riapparso verso fine anno, sotto nuova gestione. Lo sviluppo di una nuova versione era cominciato a giugno, e il completamento del nuovo rilascio è stato poi annunciato a settembre sul canale Telegram dei suoi autori. Tuttavia, sebbene il nuovo lancio sia stato ampiamente pubblicizzato, finora abbiamo osservato pochissimi casi recenti del nuovo Raccoon Stealer. A fine ottobre, il Dipartimento di Giustizia degli Stati Uniti ha formalizzato un rinvio a giudizio a carico di un cittadino ucraino attualmente in custodia presso le autorità olandesi, con l'accusa di cospirazione a operare il servizio.

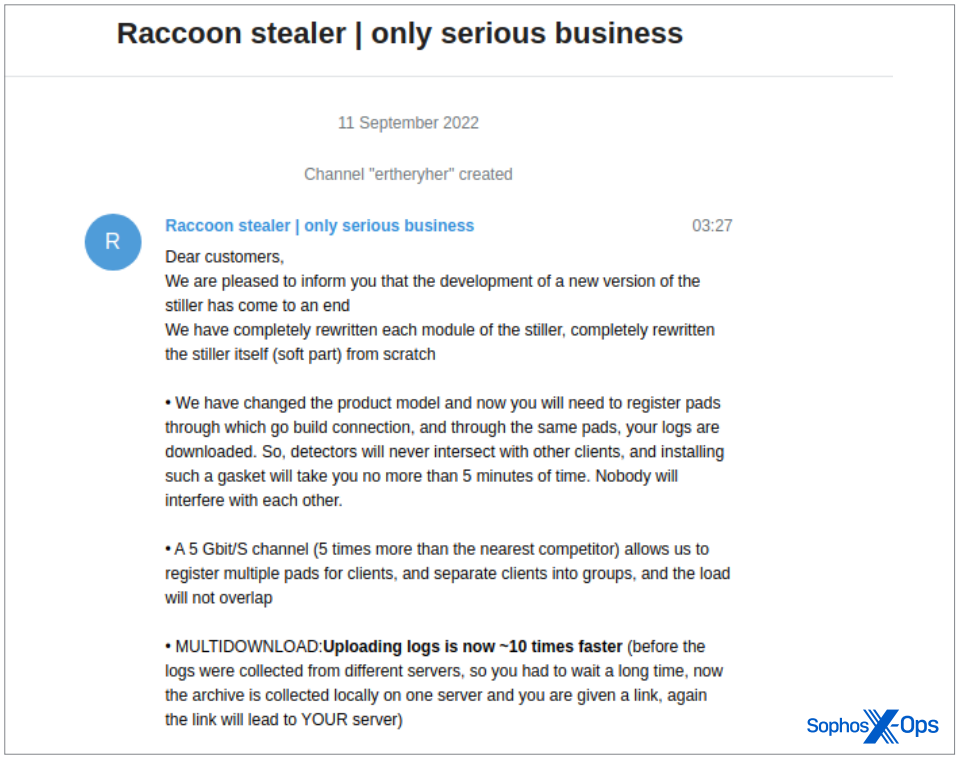

Fig.21. Settembre: Raccoon Stealer annuncia il rilascio dell'ultima versione sul canale Telegram della gang.

Gli infostealer si diffondono attraverso vari canali. Uno dei più comuni è tramite i downloader-as-a-service, che sfruttano il social engineering per ingannare gli utenti e indurli a scaricare file di archivio o immagini di dischi che, in teoria, dovrebbero contenere programmi di installazione di software legittimi. Di solito questi contenuti vengono spacciati per versioni "craccate" degli originali, che dovrebbero aiutare a risparmiare sui costi di licenza. I download includono anche i programmi di installazione di diversi pacchetti di malware. Solitamente questi siti di download sfruttano tecniche di ottimizzazione del motore di ricerca per essere posizionati in cima ai risultati delle ricerche contenenti termini che fanno riferimento a software "craccati". Altre distribuzioni a pagamento possono essere effettuate tramite botnet come Emotet o Qakbot/Qbot.

Spesso alcuni infostealer, come Agent Tesla, adottano approcci più mirati, creando e-mail dannose, scritte appositamente per colpire un gruppo di vittime in particolare. Contengono allegati camuffati da documenti urgenti, ma che in realtà sono programmi di installazione di malware.

Gli infostealer possono, tuttavia, essere distribuiti in maniera ancora più mirata. Sophos ha rilevato casi in cui gli hacker avevano utilizzato una backdoor distribuita tramite Cobalt Strike per avviare un malware di furto dei cookie e altri malware per il furto di credenziali, agendo direttamente dall'interno della rete. Hanno cercato di prelevare cookie del browser da sistemi che includevano un server; questi cookie avrebbero potuto essere sfruttati per assumere l'identità di utenti legittimi e ottenere accesso alle risorse web dell'organizzazione, per poi procedere a un ulteriore movimento laterale.

Sophos ha implementato misure diverse per bloccare gli infostealer, aggiungendo anche la protezione contro il furto dei cookie per impedire che gli infostealer cerchino di appropriarsi illecitamente dei cookie di sessione.

L'evoluzione del ransomware

Sebbene alcuni collettivi di ransomware abbiano riscontrato vari problemi l'anno scorso, anche (ma non solo) per via dell'instabilità geopolitica e di qualche procedimento penale, dalle vecchie gang ne sono emerse di nuove. L'attività del ransomware rimane quindi una delle minacce cybercriminali più ricorrenti per le organizzazioni. Le attività e i meccanismi sfruttati dai cybercriminali del ransomware, sia in termini di elusione del rilevamento che di incorporazione di tecniche innovative, continuano a evolversi.

Alcune gang di ransomware hanno adottato nuovi linguaggi di programmazione, nel tentativo di rendere più difficile il loro rilevamento, o di compilare file eseguibili più facili da avviare su più sistemi operativi o piattaforme. Il motivo potrebbe tuttavia essere anche il semplice fatto che sono gli sviluppatori dei payload del malware a utilizzare nuovi strumenti e nuove competenze. Gli sviluppatori dei ransomware BlackCat e Hive hanno adottato il linguaggio di programmazione Rust, mentre il malware BlackByte è compilato con Go (detto anche GoLang).

Il ransomware più prevalente rilevato da Sophos Rapid Response nei primi dieci mesi del 2022 è stato LockBit, seguito a ruota da BlackCat e Phobos (si noti tuttavia che la categoria "altro" costituisce più di un quinto delle famiglie osservate, il che indica che il panorama del ransomware non è limitato a poche famiglie di alto profilo). La distribuzione è, con molta probabilità, piuttosto simile alla distribuzione totale degli attacchi ransomware a livello globale.

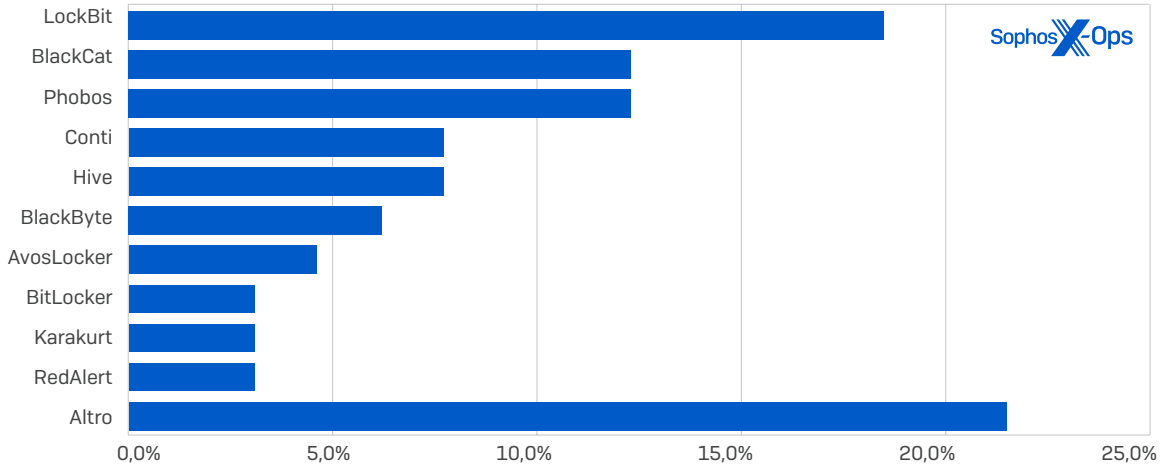

Fig.22. Entità di alto profilo quali LockBit, BlackCat e Phobos sono comuni, ma il panorama osservato da Rapid Response è estremamente vario.

Oltre a utilizzare più linguaggi, il ransomware ha anche diversificato i tipi di vittime: infatti non si focalizza più solo su Windows. RedAlert, o N13V, cifra sia i server ESXi Windows che Linux, e lo stesso vale per Luna (un altro ceppo di ransomware basato su Rust). Ma non sono solo i criminali "di seconda categoria" ad adottare questa strategia: a inizio anno i ricercatori hanno rilevato una variante di LockBit per ESXi Linux. L'ampliamento delle piattaforme prese di mira implica maggiori opportunità per i cybercriminali: una superficie di attacco più estesa, più pressioni sulle vittime e potenzialmente un minore rischio di rilevamento, in quanto la maggior parte delle misure antiransomware è progettata per Windows. Il panorama delle minacce che colpiscono Linux, Mac e le piattaforme per i dispositivi mobili verrà discusso in maggiore dettaglio in un altro paragrafo di questo report.

Abbiamo anche osservato alcuni sviluppi nella modalità di distribuzione del ransomware sui sistemi compromessi. Due incidenti di ransomware analizzati a inizio anno dal nostro team dei SophosLabs, uno avente come protagonista Darkside e uno il ransomware Exx, includevano l'uso improprio di applicazioni altrimenti innocue per eseguire il sideload di DLL. Nel caso di Darkside, il cybercriminale aveva sfruttato un programma per la rimozione dei virus, mentre Exx aveva utilizzato uno strumento di aggiornamento di Google. Dopo anni in cui è stato oggetto di estremo interesse per alcuni hacker con target di nicchia, il sideload di DLL sta diventando rapidamente una tattica molto diffusa tra i cybercriminali, poiché può aiutarli a eludere il rilevamento, eseguendo payload dannosi, camuffati da processi legittimi.

Per quanto riguarda la distribuzione e diffusione del ransomware, i cybercriminali continuano a improvvisare e ad adattarsi. Abbiamo osservato l'uso improprio di Impacket, una raccolta di moduli Python open-source da utilizzare con i protocolli di rete per ottenere la capacità di muoversi lateralmente nelle reti compromesse. Il toolset di Impacket include opzioni di esecuzione da remoto, intercettazione delle credenziali e dump di script, oltre a exploit di vulnerabilità note e moduli di enumerazione.

Tutte queste caratteristiche lo rendono un pacchetto molto desiderabile per i cybercriminali che utilizzano il ransomware. È destinato all'uso come strumento legittimo per lo svolgimento di test di sicurezza, ma analogamente a Metasploit e Cobalt Strike, possiede opzioni e funzionalità che attirano clienti poco raccomandabili. Per rimanere in tema, anche Brute Ratel è stato utilizzato per distribuire payload, come accennato prima. La diffusione del fenomeno che vede un incremento dell'utilizzo improprio di strumenti di sicurezza legittimi ("duplice applicazione") costringe i responsabili di difesa informatica ad avere una conoscenza esatta di qualsiasi elemento presente nella rete, del motivo della sua presenza e di ogni utente che abbia i diritti necessari per utilizzarlo.

Le gang di ransomware sembrano esplorare anche opportunità più generiche, per diversificare le loro attività. Un esempio importante è l'aumento dei siti di divulgazione di informazioni riservate (leak), nei quali i cybercriminali pubblicano dettagli sulle proprie vittime. Tradizionalmente, il modello è piuttosto semplice: se le organizzazioni pagano le somme richieste, i loro dati non vengono pubblicati su questo sito. Se però non lo fanno, il loro destino è segnato. Quest'anno, tuttavia, si sono osservati degli sviluppi molto interessanti in questo ambito.

Essendo indubbiamente una delle più importanti gang di ransomware, LockBit ha dimostrato di essere un passo avanti rispetto agli altri. Il suo nuovo sito di divulgazione delle informazioni riservate che accompagna la nuova versione del ransomware, ovvero LockBit 3.0 (detto anche LockBit Black, probabilmente perché molte delle sue capacità e gran parte del codice sembrano essere basate sul ransomware BlackMatter), contiene alcune opzioni innovative. Ad esempio, uno dei metodi studiati dalla gang per ottenere un pagamento è offrire ai visitatori, o alla vittima, la possibilità di distruggere o acquistare i dati rubati, oppure di ritardare il conto alla rovescia della pubblicazione.

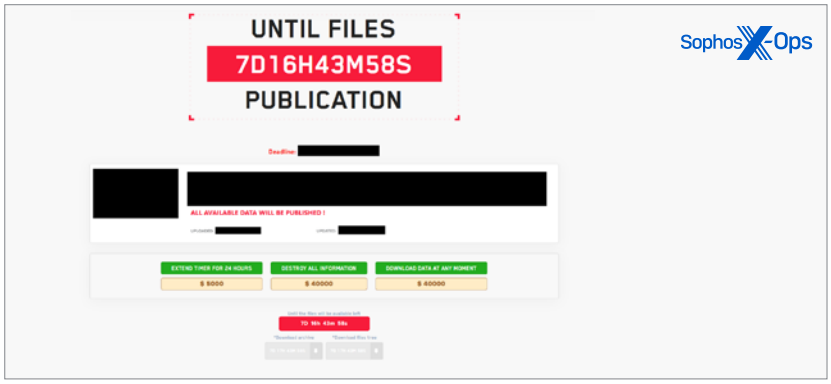

Fig.23. Alla vittima di LockBit viene proposta l'opzione di ritardare il conto alla rovescia del ransomware o di scaricare (o eliminare permanentemente) i dati.

Anche altre gang di ransomware, come Karakurt e AvosLocker, hanno cominciato a cavalcare la stessa onda, organizzando aste per vendere i dati rubati. Altre ancora, come Snatch, promettono di rendere disponibili informazioni riservate con un modello di abbonamento. Alcuni siti offrono un'opzione extra per la visibilità post-divulgazione: se una vittima paga, vengono mantenute segrete non solo le informazioni sottratte, ma anche il fatto che si è verificata una violazione (se la condizione della vittima era già stata pubblicata sui siti di divulgazione di informazioni riservate, ne verrà rimossa ogni menzione). Potenzialmente, questa opportunità rischia di rendere la vittima complice di occultamento di attività che in molti paesi richiederebbero la segnalazione a enti normativi.

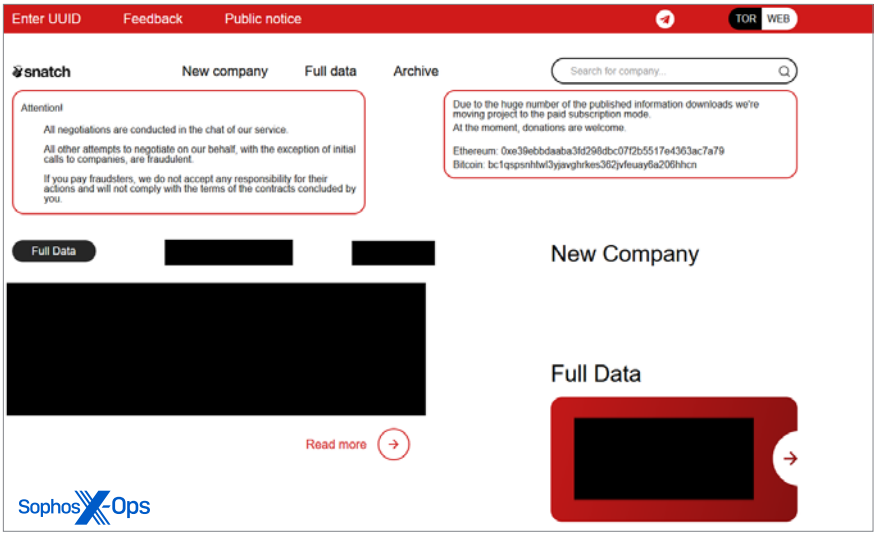

Fig.24. Il ransomware Snatch passa a un modello di abbonamento.

Ma LockBit è andata persino oltre, con innovazioni non solo nel prodotto principale, ma anche nelle interazioni con la comunità dei cybercriminali e nel suo posizionamento all'interno di essa. Il suo nuovo sito di divulgazione di informazioni riservate, ad esempio, mette in palio premi per l'identificazione di bug, con compensi che variano "da 1.000 $ a 1 milione di $", per attività volte, in ultima analisi, a potenziare il servizio:

- Comunicazione privata della presenza di bug nel sito web o nel malware stesso
- Doxxing del leader del programma di affiliazione di LockBit, con dettagli su come sono state ottenute le informazioni, presumibilmente al fine di aiutare LockBit a potenziare l'efficacia della sua OPSEC. Questo è il premio da un milione di dollari
- Vulnerabilità nel messenger di TOX (un pacchetto di messaggistica istantanea molto utilizzato dagli hacker)
- Idee su come migliorare il ransomware LockBit
- Divulgazione di informazioni relative a vulnerabilità nel proprio dominio .onion o in altri aspetti della rete TOR

LockBit non è la prima gang di cybercriminali a offrire premi per l'identificazione di bug: a novembre 2021 All World Cards, un importante collettivo che si occupava di frodi basate sulle carte di credito, attivo in diversi forum di cybercrimine in lingua russa, ha offerto premi fino a 10.000 $ per l'individuazione di vulnerabilità nel loro store. E probabilmente, non sarà neppure l'ultimo caso di questa tendenza. È un metodo efficace per svolgere penetration test e valutazione delle vulnerabilità in crowdsourcing, garantendo allo stesso tempo massima riservatezza sui risultati, che rimangono noti solo ai ricercatori e agli hacker.

Fig.25. All World Cards rivela un programma con una ricompensa modesta per l'individuazione di bug, verso la fine del 2021.

Infine, abbiamo notato un paio di ransomware o gang di divulgazione di informazioni riservate meno noti che, a differenza dei loro parenti più famosi, sembrano avere motivazioni politiche. Il primo è un sito di divulgazione di informazioni riservate dedicato alla condivisione di contenuti tratti da violazioni ai danni di cittadini e organizzazioni governative in Ucraina, sebbene non sia chiaro quale sia l'origine dei dati e se siano il frutto di un attacco ransomware.

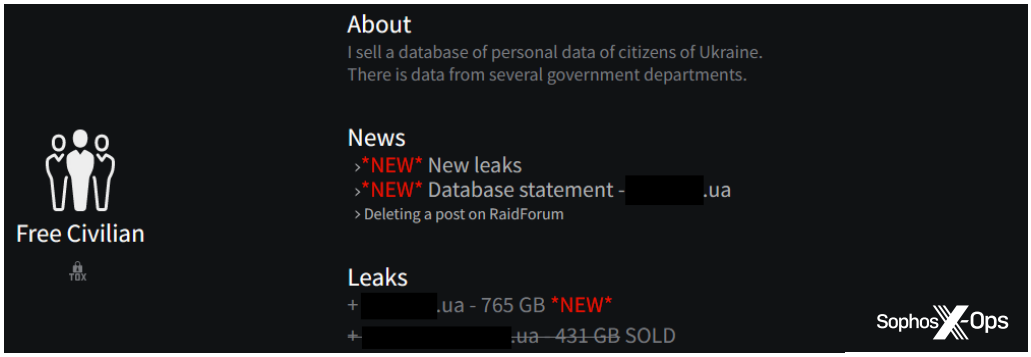

Fig.26. Cittadini ucraini nell'occhio del mirino di hacker che colpiscono le vittime di questo paese

Il secondo è una gang che si chiama Moses Staff e che sembra colpire le organizzazioni israeliane con tattiche simili a quelle del ransomware, senza però esigere un riscatto.

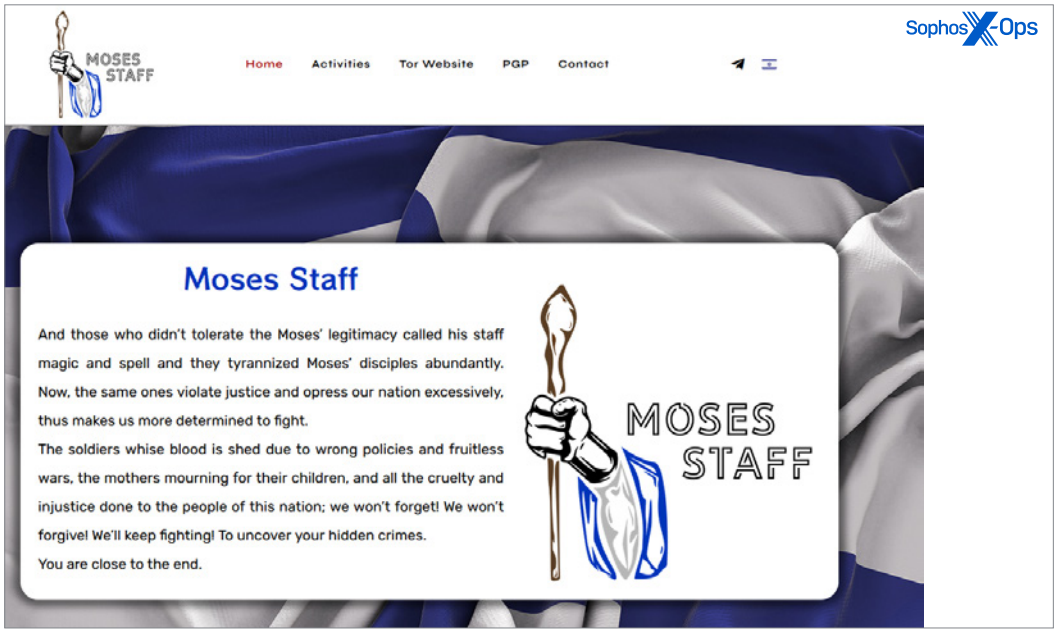

Fig.27. Una gang anti-israeliana sfrutta tattiche simili a quelle del ransomware per attaccare questa nazione

Gli strumenti di attacco

Per la maggior parte dei responsabili di cybersecurity, capire chi ha sferrato gli attacchi è leggermente meno fattibile di quanto lo sia conoscerne il "come". In questo paragrafo analizzeremo come gli hacker moderni sfruttano strumenti legittimi di sicurezza offensiva per i propri scopi nefasti. Gli strumenti di penetration testing sono ovviamente ottimi candidati per le attività criminali, ma non sono gli unici software di sicurezza legittimi a essere utilizzati in modo improprio; passeremo ora in rassegna altre tecniche, incluso l'impiego di strumenti di accesso remoto (RAT) altrimenti innocui. Subito dopo, esamineremo l'incremento del volume dei "LOLBin" (una tecnica che sfrutta in modo improprio i file binari già presenti nei sistemi delle vittime) e l'aumento degli hacker che si servono di driver legittimi di terze parti e DLL per integrare di nascosto il proprio codice dannoso, superando i controlli delle infrastrutture di protezione. Infine, dedicheremo del tempo a due specie di malware che hanno particolarmente suscitato il nostro interesse nel 2022: un ransomware che colpisce gli upgrade dei software di protezione endpoint e un software "miner" che ruba risorse alle vittime per minare criptovalute. Concluderemo quindi il report puntando i riflettori sul panorama delle minacce che colpiscono Linux, Mac e i dispositivi mobili.

L'uso di strumenti di sicurezza offensiva legittimi per fini molto pericolosi

L'applicazione impropria degli strumenti di sicurezza offensiva (software destinati all'uso da parte dei team di IT security durante le simulazioni di attacchi attivi) è molto comune in numerose campagne di ransomware. Come abbiamo visto l'anno scorso, l'uso di copie piratate dello strumento di penetration testing commerciale Cobalt Strike si è rivelato molto diffuso tra hacker quali gli affiliati di ransomware. Gli strumenti open-source sviluppati dalla comunità di sicurezza offensiva rimangono quelli maggiormente rilevati tra tutti gli strumenti di attacco dei cybercriminali. Alcuni esempi includono lo strumento di raccolta di credenziali Mimikatz (alcune versioni del quale costituiscono circa due quinti dei rilevamenti univoci nei dati di telemetria di Sophos), altre utilità di exploit basate su PowerShell (come PowerSploit) e componenti di "Meterpreter" connessi alla piattaforma di exploit parzialmente open-source MetaSploit.

Tuttavia, le copie piratate di strumenti di sicurezza offensiva pubblicamente disponibili sul mercato sono diventate un componente standard di attacchi più complessi e professionali. Come indicato in precedenza, alcune gang pubblicano annunci alla ricerca di personale dotato di esperienza con questi strumenti. In più, le copie piratate di Cobalt Strike e della versione commerciale di Metasploit sono ora talmente comuni che spesso vengono pubblicati link a copie gratuite di questi software su siti clandestini (sebbene alcuni contengano in realtà del malware).

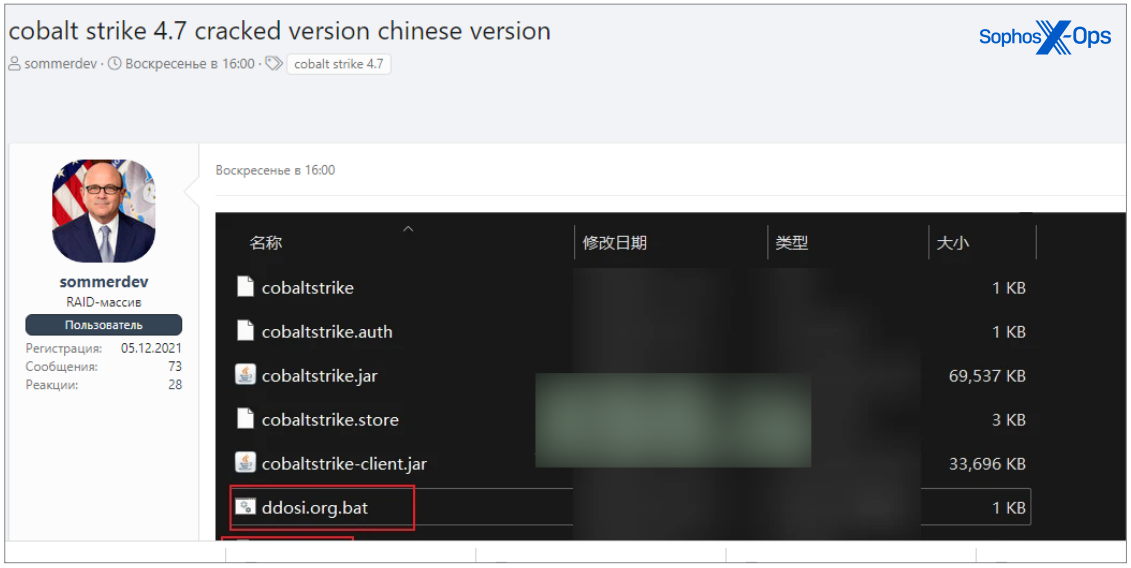

Fig.28. Una versione in lingua cinese di Cobalt Strike 4.7 craccata e messa in vendita.

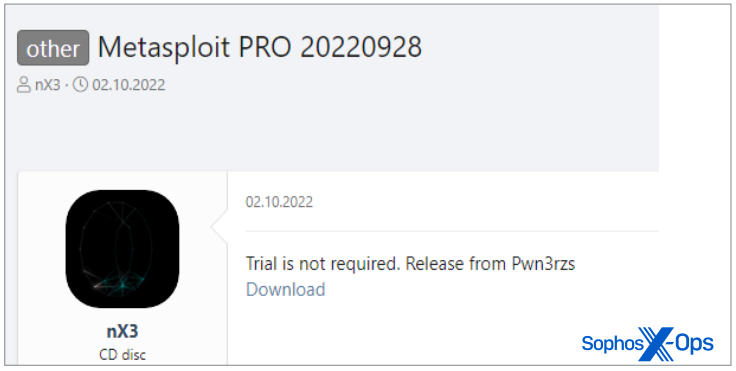

Fig.29. La versione a pagamento di Metasploit viene piratata e resa disponibile per il download.

Cobalt Strike è stato coinvolto nel 47% degli incidenti risolti dal team Sophos Rapid Response nei primi tre trimestri del 2022. Gran parte di questi incidenti è correlata al ransomware o ad attività "pre-ransomware", in casi in cui i cybercriminali sono stati intercettati grazie all'uso di tecniche, strumenti e pratiche associate a scenari di attacchi ransomware imminenti. Tuttavia, Cobalt Strike è stato osservato anche in attacchi rivolti ai governi, come nella campagna di SolarWinds del 2020 e negli attacchi mirati a vittime in Ucraina, sferrati da hacker schierati con la Russia.

Cobalt Strike, da solo, costituisce l'8% di tutti i rilevamenti univoci di strumenti di attacco. Inoltre, il suo protocollo di comunicazione è stato implementato in altri strumenti sviluppati dagli hacker. TurtleLoader, per esempio, ne contiene versioni che si connettono alla loro rete di comando e controllo (C2) tramite il protocollo di connessione di Metasploit o Cobalt Strike. Queste entità in grado di sfruttare strumenti diversi presentano sfide molto interessanti per i responsabili di cybersecurity, specialmente se si considera il fatto che la protezione dei sistemi contro gli attacchi coinvolge vari livelli di difesa.

E non si può mai abbassare la guardia, perché ci sono sempre nuovi pericoli in agguato. Al momento della pubblicazione di questo documento, abbiamo ad esempio osservato l'aumento degli attacchi basati su Brute Ratel, in seguito al suo nuovo rilascio e al ritorno della disponibilità di questo toolkit per i cybercriminali; per ora i rilevamenti di Brute Ratel sono quasi insignificanti, in quanto emergono in meno dell'1% dei rilevamenti che abbiamo in memoria. Nel 2023, siamo convinti che ci sarà un cambiamento in questa situazione, a causa della proliferazione delle versioni craccate del prodotto.

Rilevamenti di strumenti di attacco particolarmente degni di nota (computer univoci in un periodo campione di 6 mesi)		
Strumento di attacco	**Percentuale di computer infettati**	**Note**
Mimikatz	24,7%	Utilità open-source di dump delle credenziali post-exploit
Apteryx	14,5%	Una versione compilata di Mimikatz
Suite PowerSploit	11,7%	Open-source, senza supporto ufficiale dal 2020
SrpSuite	8,3%	Suite open-source di PowerShell realizzata da FuzzySecurity
Cobalt Strike	8,0%	Software sviluppato internamente, spesso piratato/craccato
Meterpreter	7,8%	Payload Metasploit di attacco open-source, supporto commerciale disponibile
Nishang	6,8%	Framework e script/payload per l'uso con PowerShell
TheFatRat	6,2%	Backdoor/automazione dei payload Metasploit open-source
TurtleLoader	5,4%	Backdoor, spesso osservato in combinazione con Metasploit o Cobalt Strike
JMeter	5,1%	Metasploit basato su Java
Juicy Potato	5,0%	Exploit open-source del Servizio trasferimento intelligente in background (strumento di privilege escalation)
winPEAS	4,8%	Script per la privilege-escalation e il furto di informazioni
Swrort	4,6%	Backdoor basata su Metasploit
Empire	4,5%	Framework open-source post-exploit, fusione tra PowerShell Empire e Python EmPyre, senza supporto ufficiale da luglio 2019

Sophos X-Ops

Fig.30. La percentuale di computer infetti analizzati da Sophos in cui era presente lo strumento indicato, più maggiori informazioni su alcuni degli strumenti; dati raccolti in un periodo di sei mesi (da aprile a settembre 2022), gli strumenti rilevati in meno del 4,5% dei computer univoci sono stati omessi per questioni di spazio.

Fino a settembre 2022, gli sviluppatori di Brute Ratel sostenevano di avere completo controllo sull'accesso allo strumento tramite la fornitura di licenze. Eppure, gli hacker associati alla gang di ransomware Conti avrebbero, a quanto pare, creato società fasulle per acquistare la piattaforma, ed è stato osservato almeno un caso in cui una licenza è stata esfiltrata da un dipendente di un cliente legittimo. Da settembre, copie piratate di un rilascio recente di Brute Ratel sono diventate ampiamente disponibili in alcuni marketplace clandestini.

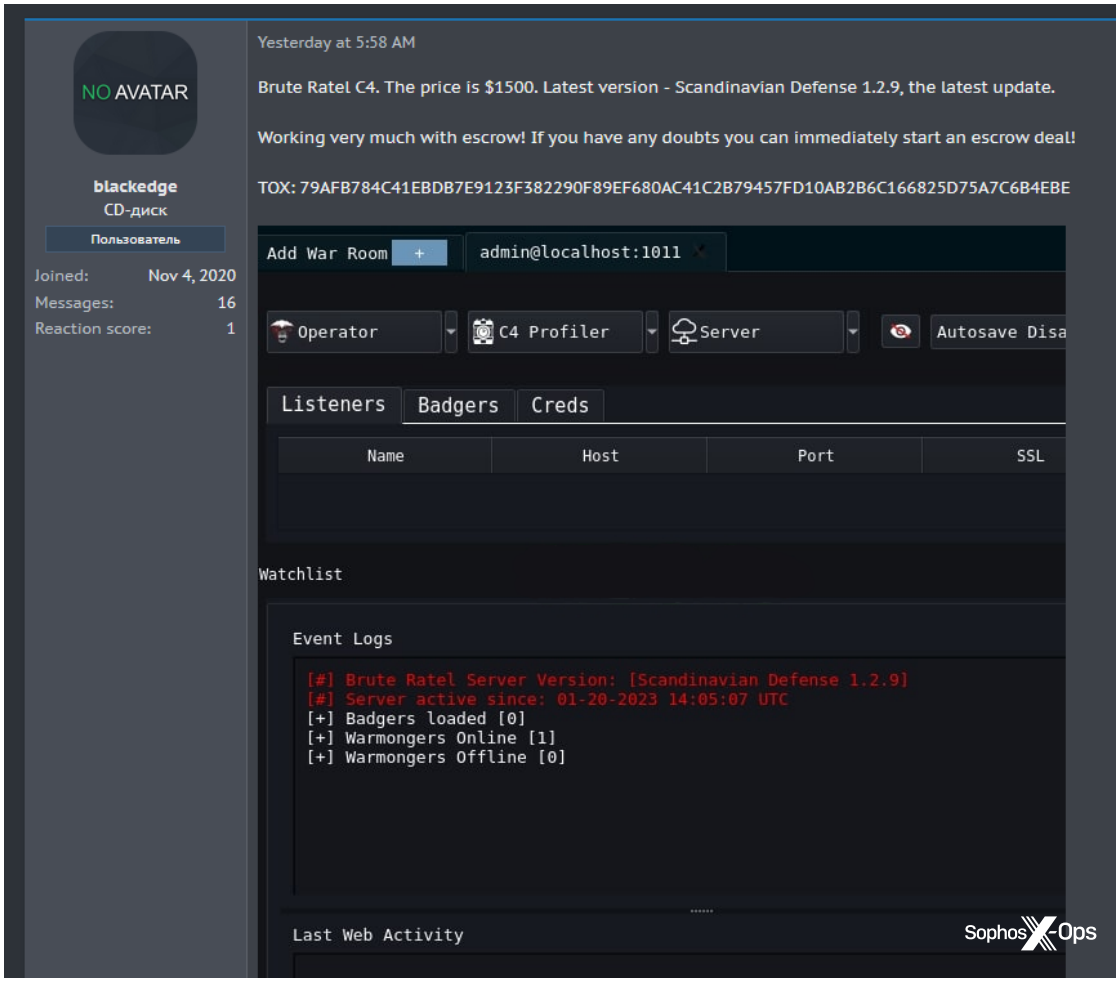

Fig.31. Una versione craccata di Brute Ratel fa la sua comparsa sul mercato nero.

Finora abbiamo offerto solo un'infarinatura degli attacchi associati a componenti di Brute Ratel. Durante la valutazione di un incidente svolta da Sophos MDR, abbiamo notato che i cybercriminali hanno provato prima a usare Cobalt Strike. Quando Cobalt Strike è stato rilevato, hanno poi cercato di distribuire Brute Ratel, e anche questo tentativo è stato bloccato.

Tuttavia, è molto probabile che ci saranno altri incidenti in futuro. Come possibile conseguenza diretta della maggiore disponibilità di Brute Ratel, recentemente i nostri ricercatori hanno osservato agenti di Brute Ratel propagati da Qakbot, con dinamiche molto simili alla diffusione dei beacon di Cobalt Strike in passato.

Altri strumenti di sicurezza utilizzati in modo improprio

Brute Ratel non è l'unico a essere stato "convertito" in uno strumento pericoloso: i cybercriminali offrono anche molti altri strumenti di sicurezza legittimi, che sono in vendita nei marketplace clandestini. Alcuni esempi includono: Core Impact (un framework di penetration testing), Nexpose (un programma di analisi che rileva le vulnerabilità), VirusTotal Enterprise e Carbon Black (una piattaforma di protezione endpoint.

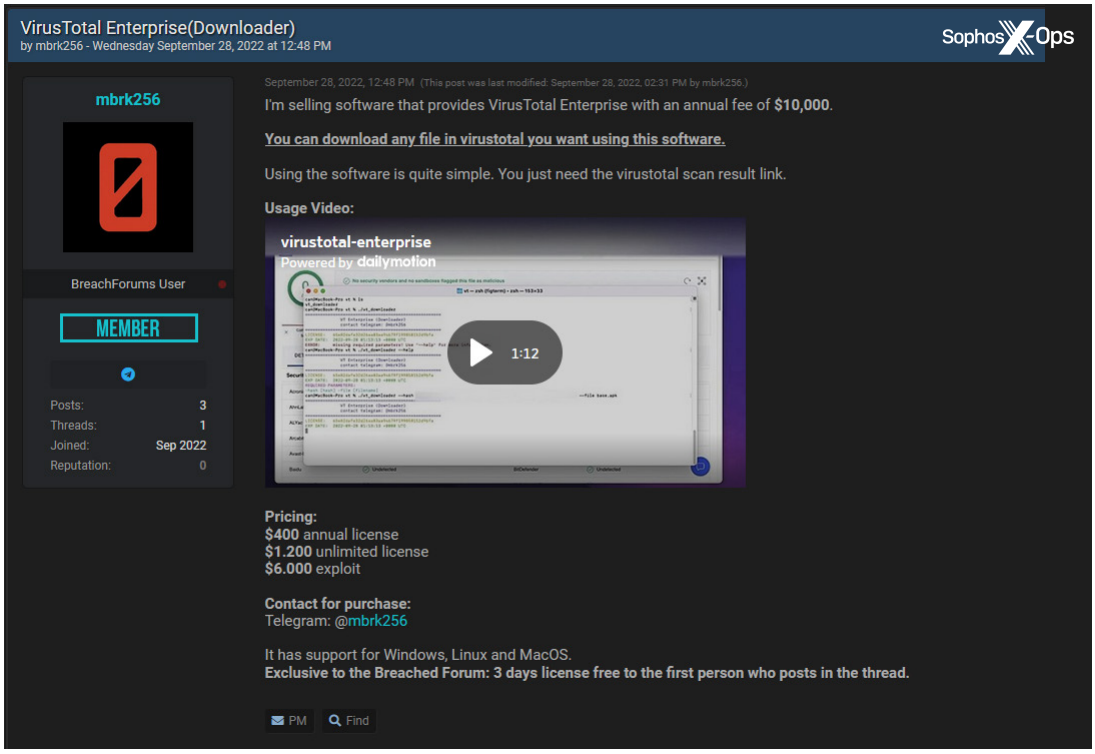

Fig.32. VirusTotal Enterprise, vittima dello scraping di dati

I casi di utilizzo di questi strumenti perfettamente legittimi da parte dei cybercriminali possono essere diversi: gli hacker possono dissezionare le piattaforme EDR e di protezione endpoint per eseguire test alla ricerca di vulnerabilità e tattiche di evasione; possono automatizzare gli exploit e la scansione alla ricerca di vulnerabilità tramite penetration testing e framework di exploit; infine possono ottenere campioni e informazioni di "controspionaggio" sfruttando strumenti come VirusTotal.

Strumenti di accesso remoto a duplice applicazione

Tra gli innumerevoli strumenti di sicurezza acquisiti in maniera illecita o semplicemente utilizzati in modo improprio all'interno del panorama delle minacce, meritano una menzione speciale gli strumenti di accesso remoto. A causa della frequenza con cui questi strumenti legittimi vengono trasformati in utilità sfruttate a scopo illecito (un esempio inquietante di "duplice applicazione"), i responsabili di IT security devono mantenere costantemente un occhio vigile sui sistemi, per intercettare eventuali indizi di uso improprio e comportamenti discutibili.

Gli strumenti di accesso remoto possono essere impiegati per stabilire una connessione persistente ai sistemi compromessi, che possono così diventare il punto di partenza di un attacco. Alcuni dei principali strumenti di accesso remoto includono:

- NetSupport Manager (NetSupport)
- TeamViewer Remote Access (TeamViewer)
- ConnectWise Control/Screenconnect Remote Access (ConnectWise)
- AnyDesk (AnyDesk Software)
- Atera (Atera Networks)
- Radmin (Famatech)
- Remote Utilities (Remote Utilities)
- Action1 RMM (Action1)

Questi strumenti possono essere installati dai cybercriminali per sferrare il loro attacco, oppure da broker di accesso che rivendono poi a terze parti l'accesso persistente alle reti compromesse. Alcuni hacker richiedono esplicitamente accesso ai sistemi della vittima con questi strumenti su siti web clandestini:

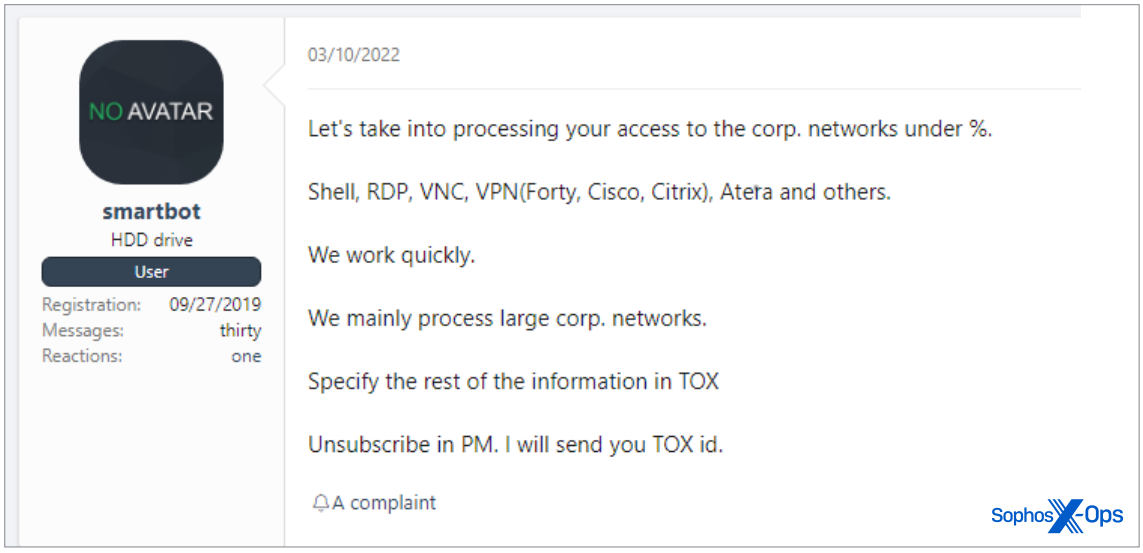

Fig.33. Offerta di accesso a reti violate tramite strumenti compromessi

Atera è uno strumento che è stato rilevato come parte di molteplici tentativi di incursione nei casi analizzati da Sophos, inclusa una serie di distribuzioni non riuscite di malware attraverso la vulnerabilità Log4J, nonché in diversi incidenti che sono stati oggetto di indagine del team Sophos Rapid Response. Nei tentativi di exploit tramite Log4J, che colpivano principalmente i server VMware Horizon, gli hacker hanno cercato di eseguire uno script PowerShell da remoto, per scaricare e installare l'agente di Atera in modo invisibile all'utente (più un altro strumento di accesso remoto utilizzato in maniera illecita: Splashtop Streamer), con una licenza di prova gratuita. Negli incidenti risolti da Rapid Response, sono state individuate installazioni di Atera effettuate sfruttando server di Microsoft Exchange vulnerabili. Alcuni incidenti recenti osservati da Rapid Response hanno avuto come protagonisti i cybercriminali della gang di ransomware BlackCat, che hanno utilizzato in maniera impropria TeamViewer ed AnyDesk.

In molti casi, l'utilizzo improprio di questi strumenti legittimi può essere rilevato e bloccato in base alla presenza di contesti anomali, come quando si osservano eventi di installazione insoliti (ad es. l'installazione di una versione di NetSupport tramite PowerShell in una directory inconsueta). In alcune situazioni, l'uso improprio di questi strumenti può anche essere evidente quando per la distribuzione viene impiegata una licenza di prova gratuita. Sophos implementa regole basate sui comportamenti che intercettano l'uso improprio delle licenze gratuite di Atera; inoltre, continua a sviluppare il rilevamento basato sui comportamenti, per individuare gli utilizzi impropri di questo tipo di software e di altri pacchetti di accesso remoto.

LOLBin e file eseguibili legittimi

Una delle principali caratteristiche degli attacchi sferrati dagli active adversary, ma anche di quelli completamente automatizzati, è l'impiego di file binari di tipo "Living-Off-the-Land", meglio noti come LOLBin. I cybercriminali approfittano di questi componenti nativi di Windows per eseguire comandi di sistema, eludere funzionalità di sicurezza preimpostate, scaricare ed eseguire file dannosi da remoto e muoversi lateralmente all'interno delle reti.

Il LOLBin più importante, ovvero la shell dei comandi Windows (cmd.exe), viene utilizzato dalla maggior parte delle backdoor e delle shell per eseguire comandi di sistema e lanciare malware; di conseguenza viene rilevato, anche se in forme diverse, in quasi ogni attacco malware. Windows offre diverse piattaforme di scripting: PowerShell, l'Host applicazioni HTML Microsoft (mshta.exe) e Windows Scripting Host (wscript.exe). Tutti questi strumenti possono essere sfruttati per eseguire chiamate API Windows, per scaricare ed eseguire altri contenuti malevoli, per avviare comandi di sistema e per raccogliere dati. Inoltre, la piattaforma PowerShell viene utilizzata da molti degli strumenti di attacco impiegati dai cybercriminali.

Un altro componente Windows adoperato frequentemente in maniera illecita, rundll32.exe, viene spesso adottato dagli hacker per caricare malware in formato DLL (libreria di collegamento dinamico). Esistono tuttavia altri file eseguibili legittimi e firmati che possono essere sfruttati in modo analogo e coinvolti in attività di esecuzione di backdoor o ransomware.

Altri LOLBin non sono altrettanto evidenti. L'utilità di gestione dei certificati Windows (certutil.exe) è in grado di recuperare contenuti da server web remoti, e viene pertanto chiamata molto frequentemente in causa dal ransomware e da altri cybercriminali, per scaricare e decodificare file dannosi. Bitsadmin.exe, l'utilità a riga di comando per il Servizio trasferimento intelligente in background (Background Intelligent Transfer Service, BITS), viene impiegata per trasferire file all'interno o all'esterno della rete colpita, senza bisogno che il processo che ha avviato il trasferimento rimanga attivo: una caratteristica che la rende ideale per il movimento laterale del malware o l'esfiltrazione dei dati.

Questo tipo di comportamento può essere rilevato e bloccato in vari modi. I comportamenti dannosi che sfruttano PowerShell e altri motori di scripting possono essere rilevati monitorando la Windows Antimalware Scan Interface (AMSI). Anche un'analisi dell'esecuzione dei LOLBin attraverso le chiamate di sistema o da una riga di comando può rilevare questo tipo di uso improprio.

I dieci principali LOLBin, in base alla percentuale di computer colpiti		
LOLBin	**Percentuale di rilevamenti non elaborati**	**Note**
cmd	92,26%	Interprete dei comandi predefinito
powershell	1,79%	Shell della riga di comando e di scripting più avanzata
certutil	1,09%	Programma della riga di comando installato come componente dei Servizi certificati
mshta	1,01%	Host applicazioni HTML Microsoft, permette l'esecuzione di .HTA (applicazione HTML)
bitsadmit	0,95%	Servizio trasferimento intelligente in background (Background Intelligent Transfer Service), utilizzato come componente di Windows Update per il trasferimento di file
wscript	0,93%	Host di scripting Windows che supporta l'esecuzione di JScript e VBScript
bcdedit	0,83%	Strumento da riga di comando per la gestione dei dati di configurazione di avvio
rundll32	0,52%	Utilizzato per caricare ed eseguire librerie di collegamento dinamico (DLL) a 32 bit
nltest	0,39%	Strumento che offre informazioni di diagnostica
procdump	0,21%	Applicazione da riga di comando che fornisce informazioni sui processi di sistema

Fig.34. L'onnipresente cmd.exe è senza ombra di dubbio il bersaglio generale più comune per l'uso improprio di LOLBin sui sistemi Windows (aprile-settembre 2022).

Modello "bring your own vulnerability"

Oltre ai LOLBin, spesso negli attacchi ransomware e in altri crimini informatici vengono utilizzati anche altri file eseguibili legittimi: in questo scenario, le app impiegate illecitamente vengono fornite dagli hacker. A volte si tratta di file eseguibili vulnerabili che possono essere utilizzati per eseguire il sideload di codice dannoso. Questo è avvenuto l'anno scorso, quando un componente obsoleto firmato da McAfee è stato sfruttato in un attacco ransomware AtomSilo per implementare una backdoor di Cobalt Strike.

Un'altra versione di questo metodo è la tecnica "Bring Your Own Vulnerable Driver" (porta il tuo driver vulnerabile), che sfrutta un driver legittimo e firmato, caratterizzato da una vulnerabilità soggetta a exploit, per ottenere accesso con privilegi limitati al sistema operativo. I ricercatori Sophos hanno ad esempio scoperto che i cybercriminali che distribuivano il ransomware BlackByte utilizzavano in maniera illecita RTCore64.sys e RTCore32.sys, i driver utilizzati dalla diffusissima utilità di overclocking della scheda grafica Micro-Star MSI AfterBurner 4.6.2.15658. Una vulnerabilità in questi driver (CVE-2019-16098) permette a un utente che ha effettuato l'autenticazione di leggere e scrivere nella memoria arbitraria, che in questo caso è stata utilizzata per eludere e disattivare alcuni software di sicurezza.

Altri incidenti recenti in cui si è osservata l'implementazione della tecnica Bring Your Own Vulnerable Driver includono l'uso improprio, nel mese di luglio, di un driver anti-cheat per il videogioco Genshin Impact, più una segnalazione a maggio di una variante del ransomware AvosLocker che sfruttava un driver antirootkit vulnerabile di Avast. In entrambi i casi, i driver sono stati soggetti a exploit per eludere o disattivare il software di protezione.

Complessivamente, il team Sophos Rapid Response ha osservato una quantità sufficiente di attività per derivarne diversi segnali di allarme estremamente utili, che aiutano a capire quando un attacco ransomware potrebbe essere imminente. Da un'indagine svolta sugli incidenti affrontati nei primi nove mesi del 2022, è emerso che almeno l'83% dei ransomware erano stati preceduti da indizi forieri della presenza di un problema. I cinque principali precursori di un attacco ransomware, con la rispettiva classificazione MITRE ATT&CK, sono stati:

- T1003 – Credential Access (accesso con credenziali) – OS Credential Dumping (dump delle credenziali del sistema operativo)
  - Dump delle credenziali, non cifrate o con hash, per estrapolare dal sistema operativo e dai software della vittima l'accesso agli account e informazioni relative alle credenziali degli utenti
- T1562 – Defense Evasion (Elusione delle difese) – Impair Defenses (Compromissione delle difese)
  - Modifica o disattivazione di componenti nell'ambiente della vittima, al fine di eludere o rallentare le soluzioni di protezione già implementate nei sistemi, incluse le misure di prevenzione e le opzioni di audit/log
- T1055 – Privilege Escalation – Process Injection
  - Inserimento di codice nello spazio degli indirizzi di processi attendibili, per permettere al codice degli hacker di eludere i sistemi di difesa e/o ottenere privilegi più elevati; il precaricamento e il sideload di DLL rientra in questa categoria
- T1021 – Lateral Movement (movimento laterale) – Remote Services (servizi remoti)
  - Uso di servizi remoti attraverso account validi/non protetti per accedere a un sistema e svolgere azioni con l'identità dell'utente che ha effettuato l'accesso, possibilmente attraverso uno strumento di amministrazione remota tradizionale o a duplice applicazione, come descritto sopra
- T1059 – Execution (esecuzione) – Command and Scripting Interpreter (interprete dei comandi e di scripting)
  - L'uso improprio di interpreti dei comandi e di scripting, nonché di script e file binari, oppure l'impiego degli stessi tramite terminali interattivi, shell o servizi remoti, come indicato sopra

Alcuni altri pattern osservati, anche se non classificati in maniera altrettanto nitida, sono molto interessanti dal punto di vista dei professionisti:

- Il 64% degli attacchi ransomware (nello specifico la distribuzione del ransomware) ha avuto inizio tra le 22:00 e le 06:00, ora locale
- Il periodo di tempo più comune per l'inizio di un attacco è stato il "turno di notte" tra lunedì sera e martedì mattina
- L'esfiltrazione avveniva circa due giorni prima della fase di richiesta di riscatto da parte del ransomware
- Il tempo medio di permanenza dei cybercriminali è stato 11 giorni

Il ransomware che colpisce gli upgrade della protezione endpoint

La voce "T1562 – Defense Evasion (Elusione delle difese) – Impair Defenses (Compromissione delle difese)" dell'elenco di precursori di un attacco ransomware merita un'analisi più approfondita. Uno degli sviluppi sempre più predominanti negli incarichi del team Rapid Response durante il 2022 conferma sia l'efficacia di Sophos in ambito di blocco del ransomware per impedire che causi ulteriori danni, sia il riconoscimento di questo successo da parte delle principali gang di ransomware e dei loro affiliati: ora gli attacchi ransomware includono regolarmente, come indicatore che precede la distribuzione del malware di cifratura, anche tentativi di accedere ai controlli amministrativi che gestiscono il profilo di sicurezza della vittima.

Come abbiamo visto in uno dei paragrafi precedenti, gli "active adversary" del ransomware, ovvero le persone che durante gli attacchi intervengono direttamente con attività "hands-on-keyboard", usano abitualmente strumenti di intercettazione o scraping delle password, allo scopo di acquisire le credenziali di un amministratore. I cybercriminali sfruttano impropriamente utilità come Mimikatz, originariamente creato come strumento volto a migliorare la sicurezza, per intercettare ed esfiltrare le password degli utenti dalle reti delle vittime dei loro attacchi.

Un tempo, le password di amministrazione venivano impiegate per assumere il controllo degli strumenti di gestione (ad es. i controller di dominio Windows), che potevano poi essere sfruttati per distribuire direttamente il ransomware. Tuttavia, negli attacchi più recenti, gli hacker tendono sempre più sovente a utilizzare queste credenziali per accedere ai controlli centrali, dai quali è possibile gestire la protezione endpoint. In alcuni casi, i cybercriminali hanno utilizzato immediatamente le credenziali rubate per accedere a quegli strumenti di gestione e disattivare le funzionalità antimanomissione degli strumenti di protezione endpoint. In altri casi, hanno semplicemente disattivato l'intera protezione endpoint.

Per sventare questi tipi di attacchi, Sophos e altre aziende hanno aggiunto opzioni di autenticazione a più fattori (MFA) alle pagine di accesso alla console di gestione centralizzata, nonché all'interno di dispositivi fisici come i firewall, che sono caratterizzati da accessi con diritti di amministrazione. Tuttavia, per poter usufruire dei massimi livelli di efficacia e per fermare i cybercriminali, gli utenti finali di questi prodotti (ovvero i responsabili di sicurezza e gli amministratori IT) devono pur sempre attivare queste funzionalità ed effettuare la registrazione. Sophos consiglia vivamente a tutti i suoi clienti di attivare queste opzioni di protezione il prima possibile.

Malware di cryptomining

I software utilizzati per il mining di criptovalute consumano la capacità di elaborazione delle risorse delle vittime per svolgere complicate attività di crittografia, nella speranza di guadagnare nuove "monete virtuali" (token). Solitamente, agiscono come parte di un pool connesso di processori o computer. Per molte criptovalute, il mining richiede hardware professionali, con unità di elaborazione grafica appositamente dedicate a queste attività, visto che richiedono una capacità di elaborazione estremamente elevata. Tuttavia, esiste ancora l'opportunità di sfruttare anche hardware generici per minare criptovalute; inoltre, ci sono reti in rapida crescita, composte da bot di mining che continuano a cercare di sfruttare sistemi vulnerabili e rubare le loro capacità di elaborazione a scopo di lucro.

Sebbene questi tipi di malware non mettano a repentaglio i dati delle organizzazioni, consumano moltissime risorse informatiche, incrementando i costi correlati all'energia elettrica e al raffreddamento dei dispositivi. Un malware di cryptomining spesso indica la presenza di altro malware, in quanto viene distribuito attraverso vulnerabilità di reti e software facilmente accessibili.

La maggior parte dei malware di cryptomining si concentra su Monero (XMR) e i motivi sono diversi. Le attività da svolgere per ottenere XMR non richiedono necessariamente l'uso di schede grafiche professionali, il che significa che questa criptovaluta può essere minata anche con server che non hanno hardware grafici particolarmente potenti. Inoltre, XMR è meno rintracciabile rispetto a molte altre criptovalute, e questo lo rende più desiderabile per le attività criminali.

I bot di mining sono spesso il primo malware a sfruttare le vulnerabilità appena rese note. La vulnerabilità di Java Log4J e gli exploit di ProxyLogon/ProxyShell in Microsoft Exchange Server sono state rapidamente sfruttate da botnet di cryptomining. In vari casi di ransomware osservati da Rapid Response, il team Sophos ha trovato prove della presenza di malware di cryptomining che utilizzava lo stesso punto di compromissione iniziale del ransomware, a volte diversi mesi prima dell'attacco ransomware.

I miner sono un problema che riguarda più piattaforme. Sebbene la maggior parte dei bot che diffondono malware di cryptomining rilevati da Sophos sia basata su Windows (e sebbene sfrutti PowerShell e altri motori di scripting Windows per l'installazione e la persistenza), esistono anche versioni per Linux di queste botnet, che spesso colpiscono appliance di rete o server web a cui non sono state applicate le patch più recenti.

Anche se i miner di XMR sono ancora molto diffusi e comuni, le fluttuazioni (principalmente verso il basso) del valore di alcune criptovalute hanno avuto un impatto significativo sui criminali che usano i cryptominer. Con la diminuzione del valore di XMR, è calata anche la redditività delle botnet di cryptomining, e sembra che questo fenomeno abbia avuto ripercussioni anche sull'impegno investito dagli hacker che le utilizzano, i quali sembrano trascurare le attività di ampliamento dei pool di mining. Alcune variazioni nei tassi di rilevamento delle distribuzioni di cryptominer hanno seguito le fluttuazioni del valore di XMR, come indica il grafico che segue. Si noti soprattutto il calo a metà giugno sia del valore di XMR, che dei rilevamenti dei cryptominer.

Rilevamenti dei miner di Monero e fluttuazione del prezzo di questa criptovaluta, aprile-settembre 2022

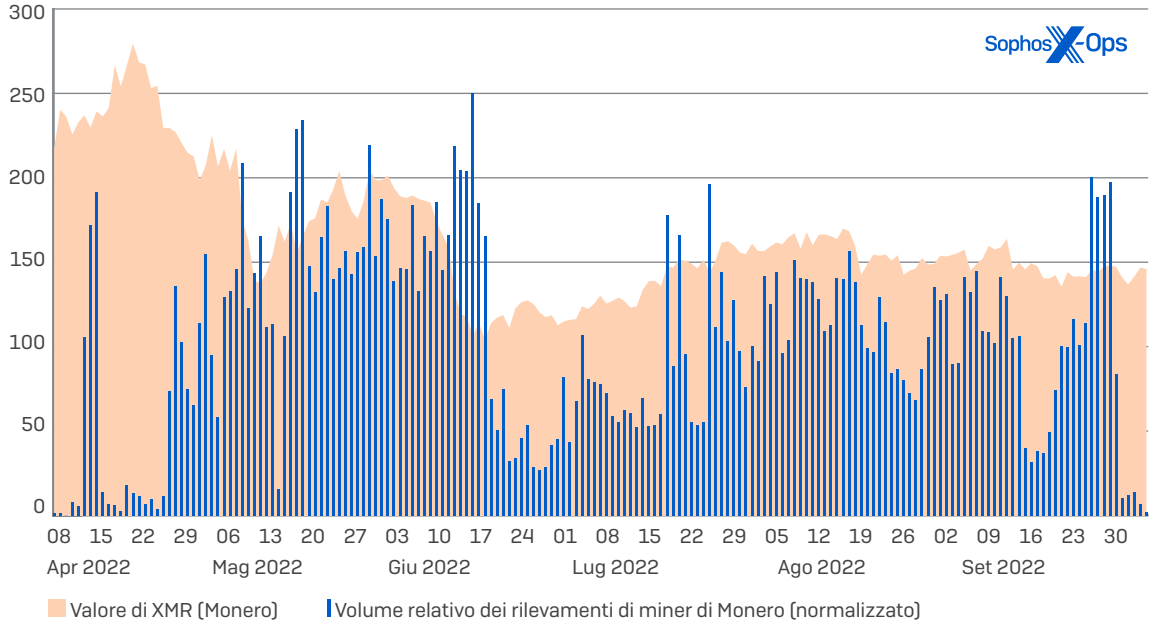

Fig.35. I rilevamenti di Monero l'anno scorso (indicati in blu, con totali normalizzati in base alla scala) mostrano congruenza con il valore di Monero durante lo stesso periodo (in arancione).

Ma la redditività dei cryptominer non ha avuto ripercussioni solo sul valore della valuta minata: ha infatti avuto un impatto significativo anche sulla longevità dei miner: molti, infatti, cercano e rimuovono miner simili dai server che attaccano. In alcuni casi, i cryptominer applicano addirittura patch per risolvere le vulnerabilità che hanno sfruttato, al fine di impedire che altri miner entrino nei sistemi e li rimuovano. Questa strategia garantisce persistenza quando le organizzazioni eseguono scansioni per l'individuazione di sistemi vulnerabili.

Oltre Windows: il panorama delle minacce che colpiscono Linux, Mac e i dispositivi mobili

Fino a questo punto del report abbiamo esaminato principalmente malware e strumenti di attacco che colpiscono Windows; è normale, visto che Windows è il target principale di gran parte dei cybercriminali. Tuttavia, Windows non è l'unico bersaglio a rischio all'interno di un'impresa, ed è sempre più comune sentir parlare di campagne di attacco su piattaforme multiple. Queste campagne vengono strutturate utilizzando linguaggi che supportano più piattaforme, come Go o Python (spesso incluso in PyInstaller), oppure framework come Electron. In alterntiva, vengono impostate preparando file binari per i framework più comuni. In questo ultimo paragrafo, daremo una rapida occhiata al panorama delle minacce che colpiscono Linux, Mac e i dispositivi mobili, precisando tuttavia che molti di questi cryptominer sono (pur sempre) presenti in tutte queste piattaforme e anche in altre.

Minacce Linux

I sistemi Linux sono da tempo nell'occhio del mirino dei cybercriminali, per via dei servizi che vengono frequentemente distribuiti su questo sistema operativo, come ad esempio: siti web aziendali, server delle virtual machine, appliance di rete, server di archiviazione e infrastrutture di applicazioni aziendali. I cybercriminali si stanno dedicando sempre di più allo sviluppo di ransomware e altro malware multipiattaforma che gli permetta di colpire queste risorse e incrementare i loro guadagni. Nei primi sei mesi da quando Sophos ha lanciato i suoi sistemi di protezione per Linux, abbiamo rilevato 14 singoli server Linux colpiti dal ransomware.

La maggior parte del malware destinato a sistemi Linux (nonché ad altre piattaforme server) viene sviluppato per minare criptovalute. Più del 40% dei nostri rilevamenti, e il 72% dei dispositivi individuali identificati come contenenti malware, deriva dai cryptominer.

Minacce Linux in base alla percentuale di rilevamenti su Linux		
Minaccia	**Percentuale di rilevamenti**	**Note**
Miner	43,0%	Rilevamento generico di miner
DDoS	27,1%	Rilevamento correlato a Mirai
Tsunami	12,3%	Client DDoS basati su IRC
Gognt	11,5%	Rilevamento generico per i malware compilati con Go
Rst	1,3%	Virus ventennale che infetta i file
Loit	1,1%	Exploit locale
Swrort	0,9%	Mettle (implementazione di Meterpreter) per Linux
SSHDoor	0,7%	Backdoor di SSH
XpMmap	0,6%	Exploit correlati alla memoria
DrtyCoW	0,6%	Exploit Dirty COW (CVE-2016-5195)
ProcHid	0,4%	Trojan che maschera i processi
Ngioweb	0,2%	Botnet proxy
Psdon	0,1%	Agente di Poseidon per il framework per red team Mythic
GoScan	0,1%	Programma di analisi di Go che cerca computer vulnerabili

SophosX-Ops

Fig.36. Nonostante il caos che regna nel panorama delle criptovalute nel 2022, i cryptominer sono purtroppo un tipo di infezione efficace su Linux.

I cryptominer hanno dominato i risultati relativi a Linux quest'anno, ancora di più di quanto non suggerisca la tabella. "Miner" è il termine di rilevamento generico utilizzato da Sophos per i cryptominer. I cryptominer possono essere rilevati anche sotto altri nomi: "Gognt", ad esempio, è il nostro rilevamento per le famiglie di malware compilato con Go che non sono correlate in nessun altro modo. Questo significa che è probabile che esistano altri cryptominer oltre al rilevamento "miner", il che vuol dire che ce ne sono molti di più di quelli mostrati in questa tabella.

Minacce Linux in base alla percentuale di rilevamenti univoci su Linux		
Minaccia	**Percentuale di computer univoci**	**Note**
Miner	74,3%	Rilevamento generico di miner
Gognt	5,1%	Rilevamento generico per le famiglie di malware compilati con Go
DDoS	4,3%	Rilevamento correlato a Mirai
Swrort	3,2%	Mettle (implementazione di Meterpreter) per Linux
DrtyCoW	3,1%	Exploit Dirty COW (CVE-2016-5195)
Ngioweb	2,8%	Botnet proxy
Tsunami	2,7%	Client DDoS basati su IRC
Roopre	0,9%	Backdoor che colpisce i server web
SSHBrut	0,9%	Programma di violazione delle password basato su attacchi brute force di SSH
Loit	0,8%	Exploit locale
Shell	0,8%	Malware che concede all'hacker accesso alla shell
Bckdr	0,6%	Rilevamento generico per le backdoor
Ransm	0,6%	Ransomware

Fig.37. Quando viene classificato in base ai singoli computer colpiti, l'impatto dei cryptominer su Linux è ancora più evidente.

Il secondo gruppo, per ordine di grandezza, di rilevamenti sui sistemi Linux colpiti è associato a Gognt e viene distribuito con toolkit di Distributed Denial of Service (DDoS). Quasi tutti questi malware attaccano vulnerabilità che sono state risolte nelle versioni più recenti di Linux, ma che persistono in una quantità piuttosto elevata di dispositivi e appliance a cui non sono state applicate le patch.

Esistono diverse backdoor e botnet tra le rimanenti minacce Linux. Tuttavia, la più interessante tra le altre minacce principali è probabilmente Tsunami: una backdoor di Linux estremamente longeva, che recentemente si è evoluta per attaccare anche server delle applicazioni Jenkins e WebLogic.

Minacce Mac

Nel 2022 abbiamo notato la disponibilità su siti come GitHub di quantità sempre più elevate di strumenti di attacco open-source e framework post-exploit/C2 (comando e controllo) che supportano macOS. La semplice presenza di codice nel repository non è necessariamente correlata a un'impennata imprevista di attacchi di ampia portata rivolti ai Mac; tuttavia, molto probabilmente indica quantomeno un incremento dell'interesse generale, nonché una certa volontà di condividere tale codice.

Le minacce prevalenti sulla piattaforma macOS continuano a essere le applicazioni potenzialmente indesiderate (Potentially Unwanted Application, PUA), che includono app in grado di installare plug-in per il browser Apple Safari (oltre ad altre piattaforme browser). Queste app inseriscono elementi nelle pagine web, al fine di reindirizzare gli utenti su contenuti fraudolenti o pericolosi.

Applicazioni potenzialmente indesiderate (PUA) su macOS, aprile-settembre 2022		
Rilevamento	**Percentuale di computer univoci**	**Note**
Adloadr	16,2%	Rilevamento generico di adware
Genieo	8,9%	Hijacking del browser (ricerca)
Bundlore	8,4%	Adware
Dynji	4,6%	Hijacking del browser (barra degli strumenti)
Pirrit	3,7%	Adware
AdvMac	3,2%	Adware
HistColl	3,0%	Raccolta dei dati del browser
Keygen	2,3%	Strumento di pirateria di software

Fig.38. Con un margine molto ampio, Adloadr è in cima all'elenco delle PUA rilevate sui Mac nei 2022.

Sophos X-Ops

L'applicazione Adloadr (una delle varie PUA prevalenti, classificabile come adware), ha fatto un balzo al primo posto nelle nostre statistiche di telemetria del 2022 per i Mac, con quasi il doppio delle infezioni su computer univoci, rispetto all'applicazione di hijacking del browser Genieo, che si trova al secondo posto.

Per quanto riguarda il malware, abbiamo osservato quantità elevate di NukeSped, Vsearch e Dwnldr: un trojan di accesso remoto, un pacchetto di adware e un downloader generico di trojan. Anche Chropex e ProxAgnt, due app di supporto associate alla famiglia di Adloadr, sono apparse nel nostro elenco di rilevamenti comuni.

Rilevamenti di malware su macOS, aprile-settembre 2022		
Rilevamento	**Percentuale di computer univoci**	**Note**
NukeSped	22,2%	Trojan di accesso remoto
VSearch	15,6%	Adware/hijacking del browser
Dwnldr	10,8%	Rilevamento generico di trojan
Agent	10,8%	Rilevamento generico di malware
Keygen	6,4%	Generatore di chiavi per eludere la protezione contro la copia
FkCodec	6,2%	Adware, finge di essere un programma di installazione di codec video
Chropex	5,0%	Adware, mostra anche comportamenti tipici dell'hijacking del browser
ProxAgnt	1,9%	Trojan
Swrort	1,5%	Trojan di accesso remoto

Fig.39. NukeSped, Vsearch e Dwnldr dominano la classifica dei principali rilevamenti di malware su macOS.

Sophos X-Ops

Fino a ottobre, abbiamo scoperto cinque nuove minacce macOS che sono emerse nel 2022; nessuna di queste cinque ha raggiunto quantità che ne permettessero l'inserimento nella nostra tabella, ma le stiamo osservando con estremo interesse, tenendo conto dei nuovi rilevamenti.

Nuove minacce macOS osservate nel 2022			
Mese	**Nome**	**Rilevamento**	**Note**
Gennaio	SysJoker	OSX/SysJoker	Backdoor multipiattaforma che supporta macOS
Gennaio	DazzleSpy	OSX/DazzleSpy	Tecnica di infezione correlata a MACMA, una backdoor che prendeva di mira gli attivisti pro-democrazia a Hong Kong
Marzo	Gimmick	OSX/Gimmick	Comunica attraverso API Google Drive per nascondere il traffico di rete agli occhi dei sistemi di monitoraggio
Maggio	pymafka/CrateDepression	Troj/Pymaf, OSX/Cobalt	Attacco alla supply chain in pacchetti ospitati su PyPI; alla fine distribuisce un beacon di Cobalt Strike
Ottobre	Alchimist	Exp/20214034-D	Framework di attacco multipiattaforma compilato con Go

Fig.40. Cinque nuove minacce macOS emerse nei primi dieci mesi del 2022.

Sophos X-Ops

Minacce dei dispositivi mobili

Ormai le applicazioni mobili sono diventate il modo più comune per interagire con Internet, e per questo motivo i dispositivi mobili si trovano ora al centro di una gamma sempre più estesa di nuovi tipi di cybercrimine. Sebbene la piattaforma Android continui a essere colpita da un flusso costante di malware, distribuito sotto forma di applicazioni fasulle e infostealer, sia Android che iOS sono diventate sempre di più frequentemente oggetto di applicazioni fraudolenti e fasulle. Oltretutto, i cybercriminali hanno scoperto nuovi modi di utilizzare il social engineering per infiltrarsi anche nel walled garden dei dispositivi mobili Apple.

Nei nostri rilevamenti, i malware injector, gli spyware e i malware associati all'internet banking continuano a dominare nell'ambito dei pacchetti Android .APK dannosi, accompagnati da app di generazione di clic per annunci fasulli. Tuttavia, le applicazioni potenzialmente indesiderate (incluse app che praticamente non fanno altro se non prelevare di nascosto pagamenti per "acquisti in-app" illegittimi) stanno diventando una minaccia sempre più pericolosa per gli utenti dei dispositivi mobili. L'anno scorso sono emerse diverse gang di truffe finanziarie molto sofisticate, che si servono di app fasulle. Nel Sudest asiatico, questi collettivi sono diventati una vera e propria industria.

Nel 2021 Sophos ha cominciato a monitorare una campagna di crimine organizzato che abbiamo battezzato CryptoRom. La campagna si basa su un tipo di frode informatica noto come sha zhu pan (杀猪盘, letteralmente "piatto per la macellazione dei maiali"), che gode del supporto di un collettivo ben organizzato, composto da sviluppatori di pagine web e applicazioni fraudolente, creatori di profili fasulli sui social e persone che sfruttano script di social engineering sui social media e sulle app di incontri per far cadere le vittime nelle loro trappole.

Nel mese di ottobre del 2021, abbiamo documentato l'espansione globale della campagna. La formula si è trasformata ed evoluta, passando da investimenti in criptovalute fasulle a investimenti derivati da criptovalute fasulle, espandendosi anche su altri finti mercati finanziari. Per conferire a queste macchinazioni un aspetto legittimo, il collettivo crea applicazioni e siti web per dispositivi mobili fasulli, che si spacciano per istituzioni finanziarie legittime. Molte di queste app si sono infiltrate senza destare sospetti negli app store, come è successo nel caso delle app di "mining di liquidità" individuate nell'Apple App Store e nel Google Play Store.

Nel frattempo, i truffatori hanno escogitato modi per colpire anche iOS, approfittando di Clip web e programmi di implementazione di test per sviluppatori di app, al fine di indurre gli utenti a installare le loro applicazioni sui dispositivi iOS. Queste strategie includono l'uso improprio del programma di distribuzione ad hoc "Super Signature" di Apple, del beta test "Test Flight" e degli schemi delle applicazioni aziendali, al fine di sfuggire ai controlli di sicurezza dell'Apple App Store. Lo stesso approccio può essere utilizzato per altri malware che colpiscono iOS, ma che, per il completamento dell'installazione, richiedono alcune attività di social engineering a danno della vittima.

Queste applicazioni sono costate alle vittime centinaia di milioni di dollari e fanno parte di un ecosistema di cybercrimine in costante evoluzione, che spazia dalle truffe romantiche a tentativi più estesi di social engineering su piattaforme quali Facebook, Twitter e LinkedIn. Le truffe continuano a evolversi e vengono imitate da altre gang di cybercriminali, che aggiungono particolarità uniche.

Sia Android che iOS sono vittime ideali anche per le campagne pubblicitarie dannose, che includono avvisi fasulli simili agli avvisi di sistema, ma che spesso cercano di reindirizzare gli utenti su un finto app store; successivamente, cercano di convincere questi utenti ad acquistare un'applicazione con costi di licenza nascosti, a installare altro malware o a svolgere entrambe le operazioni.

Sophos continua a esplorare nuovi modi per bloccare queste minacce e segnala i nuovi casi di utilizzo improprio degli app store agli sviluppatori dei rispettivi sistemi operativi mobili, non appena viene individuato un problema.

Conclusione

Nell'intero panorama delle minacce, ci sono due elementi che spiccano tra tutti gli altri: la crescente semplicità con cui gli aspiranti cybercriminali possono entrare in questo mondo e la commercializzazione di quelli che un tempo sarebbero stati considerati strumenti e tattiche delle "Advanced Persistent Threat" (minacce avanzate e persistenti). Sebbene quello degli strumenti di hacking, del malware e dell'accesso a reti vulnerabili sia da tempo un mercato molto florido, le lezioni apprese nella recente storia delle attività del ransomware e di altri hacker dotati di risorse economiche rilevanti stanno diventando rapidamente accessibili anche per la comunità estesa dei cybercriminali. E lo stesso si può dire degli strumenti di sicurezza disponibili in commercio, progettati per superare alcuni tipi di protezione.

Le condizioni geopolitiche hanno contribuito a rendere ancora più difficile la lotta al cybercrimine. Quest'anno, con l'aumento della tensione tra USA e Cina, la potenza asiatica ha terminato la collaborazione con le forze dell'ordine statunitensi per combattere il cybercrimine; nel frattempo, in seguito a un giro di vite della Cina sulle truffe di criptovalute e su altri tipi di cybercrimine all'interno dei propri confini, i criminali che parlano cinese hanno cominciato rapidamente a dedicarsi all'esportazione di queste attività criminali. E mentre la guerra in Ucraina ha, seppur brevemente, causato problemi ad alcune gang di cybercriminali di lingua russa, queste ultime hanno rapidamente ripreso le loro attività.

Contro queste minacce non esiste un sistema di difesa sicuro al 100%. Per impedire che la loro infiltrazione nei sistemi provochi danni irreparabili, occorre infatti una protezione attiva, e per molte organizzazioni il carico di lavoro della cybersecurity è troppo elevato per essere gestito in maniera autonoma. Sophos continua a lavorare assiduamente per incrementare la sua capacità di aiutare le organizzazioni di qualsiasi dimensione a proteggersi da un panorama delle minacce in costante evoluzione, offrendo soluzioni di protezione per endpoint e rete, oltre a servizi gestiti di Managed Detection and Response.

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

17/11/22 IT (NP)

SOPHOS