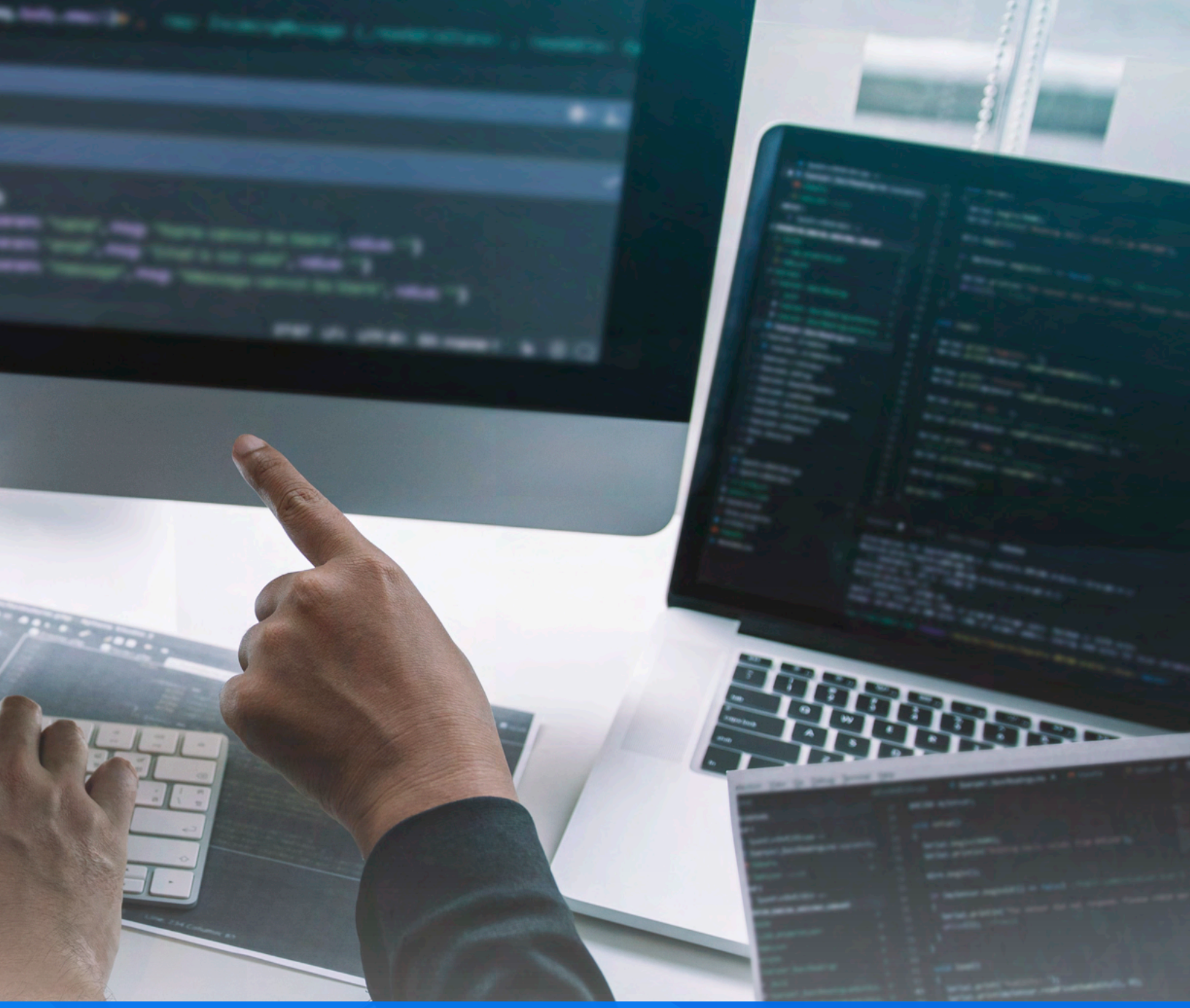

GLI ULTIMI DATI SUGLI

Attacchi criptati

REPORT 2021

zscaler™

INDICE

Il traffico HTTPS è sicuro?

Vi è della confusione a riguardo, e questo sembra ripercuotersi sulle attività di protezione dei dati in azienda. L'HTTPS (ovvero il TLS, precedentemente SSL) è lo standard di settore per la crittografia e protegge i dati in transito. Il suo compito consiste nel preservare la riservatezza dei contenuti da chiunque intenda spiarli. Tuttavia, questo protocollo è solamente un veicolo; la crittografia non indica che il contenuto sia intrinsecamente sicuro. Il malware può essere criptato e trasmesso con la stessa facilità dei file legittimi e, in realtà, oltre l'80% dei malware viaggia su questi canali.

Questo sembra un concetto semplice, ma la realtà è che la maggior parte delle aziende non ispeziona tutto il traffico criptato.
Molte di queste non lo ispezionano affatto. Considerato che la maggior parte del traffico si sposta su canali criptati, perché le aziende non dovrebbero ispezionarlo? Ma la domanda principale è: cosa si rischia non ispezionandolo?

A quanto pare, si rischia parecchio. Tra gennaio e settembre del 2021, Zscaler ha bloccato 20,7 miliardi di minacce sul canale HTTPS, un aumento di oltre il 314% rispetto ai 6,6 miliardi di minacce bloccate nel 2020, a loro volta aumentate di quasi il 260% rispetto all'anno precedente.

I criminali informatici stanno diventando sempre più esperti nelle loro tattiche di attacco e beneficiano delle reti di affiliazione e degli strumenti "as-a-service" disponibili sul dark web. Questa disponibilità ha portato a un'esplosione di attacchi sofisticati che sono fonte di costante preoccupazione per i team addetti alla sicurezza informatica. I ransomware, in particolare, colpiscono le aziende di tutto il mondo con attacchi di alto profilo che causano danni di decine di milioni di dollari. La crittografia dei malware è un passaggio banale nella sequenza di attacco.

Con l'incremento dei ransomware e di altri tipi di minacce, e la continua adozione di modelli di lavoro ibridi in cui i dipendenti si connettono da qualsiasi luogo, le aziende, per proteggersi al meglio, devono necessariamente ispezionare tutto il traffico on-premise e off-premise. Questa ispezione richiede però molte risorse, ed eseguirla su larga scala con strumenti di sicurezza legacy basati su hardware, come i firewall di nuova generazione, è praticamente impossibile. Per non compromettere le prestazioni e farlo in modo efficace, potrebbe essere necessario un numero di dispositivi da cinque a sette volte maggiore. Di conseguenza, sono molte le aziende che consentono il passaggio senza ispezione di almeno una parte del loro traffico criptato. Questo è un problema, e ora spiegheremo il perché.

Gli attacchi sui canali criptati sono incrementati del **314%** dal 2020 al 2021.

Risultati principali

Zscaler Zero Trust Exchange ospita il più grande insieme di dati sulla sicurezza al mondo, raccolti da oltre 300 trilioni di segnali e 160 miliardi di transazioni giornaliere, che equivale a 15 volte il volume delle ricerche condotte su Google ogni giorno. ThreatLabz, il team di ricerca delle minacce di Zscaler, ha analizzato questi dati dai primi nove mesi del 2021 e ha esaminato le minacce nel traffico criptato durante questo periodo. L'analisi che segue rivela alcune informazioni importanti sul panorama delle minacce criptate. Ecco i risultati principali:

- **Le minacce su HTTPS sono aumentate:** Zscaler ha registrato un incremento delle minacce di oltre il 314% all'interno del traffico criptato per il secondo anno consecutivo.
- **Il settore tech è molto preso di mira:** gli attacchi alle aziende tech sono aumentati del 2344%, mentre quelli contro le aziende di vendita al dettaglio e all'ingrosso sono incrementati dell'841%.
- **Assistiamo a una tregua per i servizi essenziali:** la sanità è stata il target principale nel 2020, ma le minacce sono rapidamente calate, così come gli attacchi contro le organizzazioni governative. I grandi attacchi, come quello contro Colonial Pipeline, hanno portato a una maggiore attenzione da parte delle autorità giudiziarie, e di conseguenza si è perso interesse verso questi obiettivi.
- **Il Regno Unito e gli Stati Uniti sono i principali target degli attacchi criptati.** Seguono India, Australia e Francia.
- **Le tattiche stanno cambiando:** i malware sono aumentati del 212%, il phishing è incrementato del 90%, mentre i malware di cryptomining sono in calo del 20%. Questo è indice di un cambiamento nelle tendenze degli attacchi, con i ransomware che stanno guadagnando sempre più popolarità.
- **Proteggere l'organizzazione con lo zero trust:** il modo migliore per difendersi dalle minacce criptate consiste nell'utilizzare un'architettura cloud zero trust basata su proxy, che riduca la superficie di attacco e consenta di ispezionare tutto il traffico in entrata e in uscita.

Gli attacchi alle aziende tech sono aumentati di **20 volte**

La crittografia moderna, che include SSL (Secure Sockets Layer) e il suo successore TLS (Transport Layer Security), viene utilizzata a livello globale per proteggere la maggior parte del traffico Internet. Se la percentuale di traffico legittimo che viene criptato aumenta, lo stesso accade per il traffico malevolo. Nel 2021, Zscaler ha bloccato più di 20,7 miliardi di minacce in un periodo di 9 mesi.

La crittografia offre in realtà diversi vantaggi agli aggressori: in primo luogo, è meno probabile che i team addetti alla sicurezza ispezionino il traffico criptato, e, inoltre, i file criptati sono più difficili da proteggere con fingerprint, e questo consente ai malware di insinuarvisi senza essere rilevati.

Sono vari i tipi di attacchi che i criminali possono nascondere all'interno del traffico criptato. I malware sono senz'altro la categoria principale e rappresentando quasi il 91% degli attacchi.

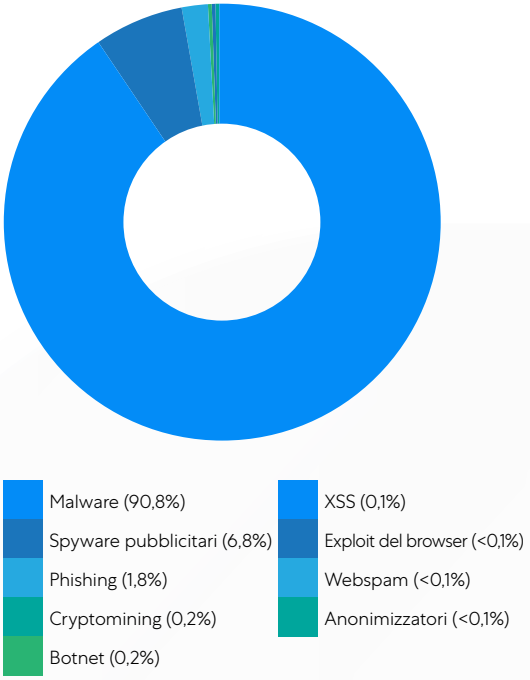

Figura 1: *frequenza degli attacchi sui canali criptati*

I malware rappresentano il **91%** degli attacchi

Tuttavia, anche altri tipi di attacchi sono in aumento. Rispetto al 2020, gli attacchi di spyware pubblicitari, exploit del browser, malware, phishing e botnet sono tutti aumentati nel 2021. Gli unici tipi di attacchi in calo sono rappresentati dal cryptomining (che prevede il controllo totale dei computer per effettuare il mining di criptovalute), il cross-site scripting o XSS (in cui il codice dannoso viene iniettato all'interno di siti web legittimi) e gli attacchi con anonimizzatore (che utilizzano i proxy per non rendere tracciabile gli aggressori). Negli ultimi anni, gli attacchi di cryptomining hanno subito un calo di popolarità, perché i ransomware sono diventati un'opzione più redditizia. In questo report, i ransomware sono inclusi nella categoria dei malware.

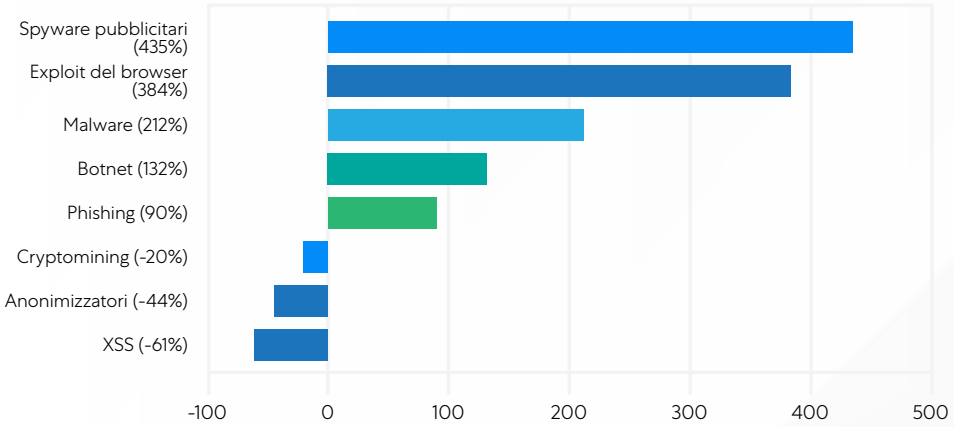

Figura 2: *variazione annua degli attacchi sui canali criptati*

Attacchi web

Il web è pieno di siti dannosi, e questi includono anche quelli con protocollo HTTPS. La scarsa igiene di internet consente alle minacce di persistere per molto tempo: Zscaler ha riscontrato più di 13.000 attacchi da siti infettati da Coinhive, anche se quest'ultimo è chiuso da oltre due anni. Una delle categorie più comuni di attacchi web che sfrutta il protocollo HTTPS è rappresentata da skimmer JavaScript, come **Magecart**, che vengono utilizzati per rubare dati di pagamento online.

Famiglia	Attacchi	Tipo
Nicehash	5.644.273	Cryptomining
Magecart	2.573.304	Skimming dei pagamenti
Adload	1.626.905	Webspam
Covid19	972.223	Malware
Webshell	934.873	Malware
Coinhive	13.670	Cryptomining

I siti web infetti possono rimanere infetti per **anni** dopo il lancio di un attacco.

Phishing

Il phishing continua a essere una delle tattiche principali attraverso cui gli utenti vengono indotti a fare clic sui link presenti nelle e-mail che contengono malware nascosti. Tutti i servizi di posta elettronica e condivisione dei file sono vulnerabili agli attacchi, ma la popolarità di Microsoft 365 l'ha reso di gran lunga il target principale nel 2021, con oltre 15 milioni di tentativi di attacco bloccati dalla piattaforma Zscaler in un periodo di osservazione di nove mesi.

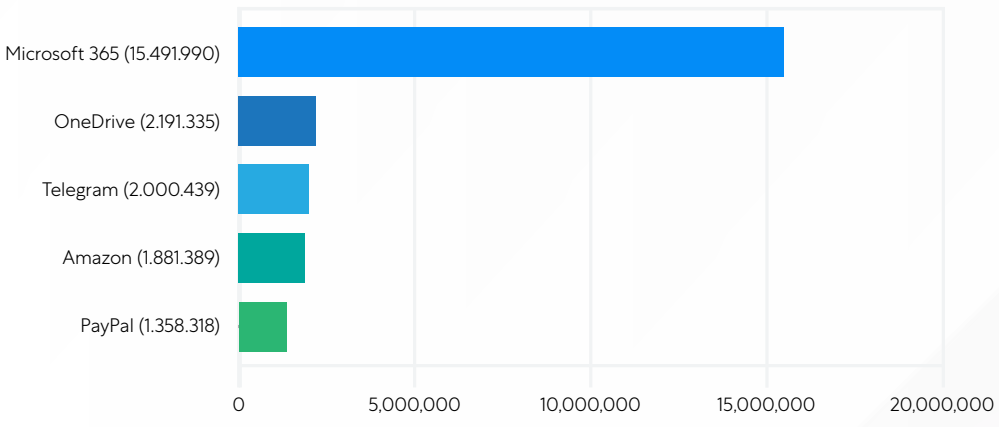

Figura 3: *attacchi di phishing criptati*

Malware

I malware sono stati la principale categoria degli attacchi del 2021. In genere, vengono scaricati da link infetti presenti nelle e-mail o sui siti web. Sebbene la maggior parte delle aziende disponga di una qualche forma di protezione contro i malware, gli aggressori stanno perfezionando le proprie tecniche, creando nuove varianti di malware in grado di aggirare le tecnologie di fingerprinting. Naturalmente, le aziende che non ispezionano il proprio traffico criptato non disporranno di alcuna visibilità sui malware (nemmeno su quelli conosciuti) finché questi non saranno entrati nei loro sistemi. Di seguito sono riportate alcune delle famiglie di malware prevalenti durante il 2021. Più avanti, verranno illustrati i casi di studio tecnici di quattro di queste famiglie che ne dimostrano le sequenze di attacco.

Famiglia	Attacchi malware
njRAT	355.753
Ursnif	336.540
Azorult	199.334
Hancitor	137.421
Emotet	58.867
Qakbot	30.199
Smokeloader	4269

I dati personali, nello specifico quelli che consentono di identificare le persone (Personal Identifiable Information, PII) sono **il bersaglio principale** dei tentativi di furto dei dati.

Furto di dati

Gli aggressori utilizzano i canali criptati non solo per infiltrarsi nei sistemi, ma anche per esfiltrare i dati. I tipi di dati esfiltrati più comuni sono quelli nazionali e fiscali, come Aadhar (India), TFN (Australia), Social Security (Stati Uniti) e BSN (Paesi Bassi). Il secondo obiettivo più comune è costituito da informazioni finanziarie e carte di credito, seguite da proprietà intellettuale e dati sanitari. La tabella seguente mostra i tentativi di furto di dati nell'arco di soli tre mesi.

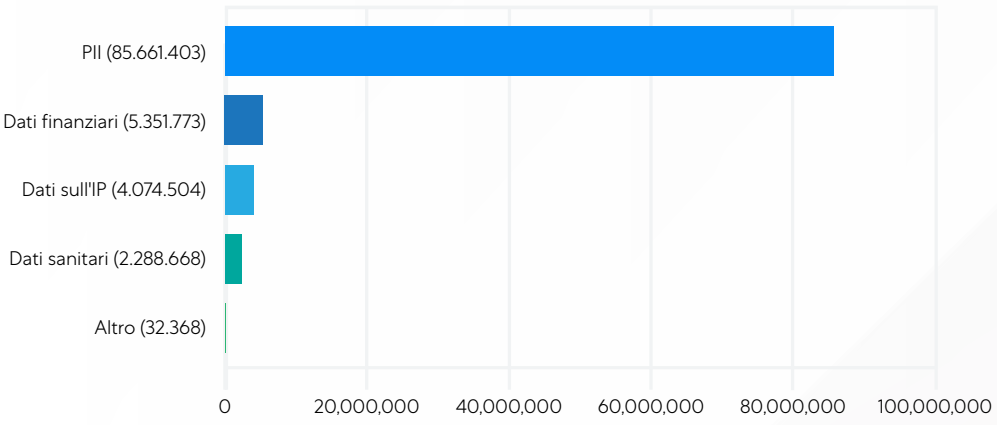

Figura 4: *tentativi di furto dei dati*

Attività di comando e controllo

I server di comando e controllo (C&C) vengono utilizzati per una serie di ragioni, tra cui l'esecuzione di payload di seconda fase negli attacchi mirati, l'esfiltrazione di dati e il controllo dei computer da utilizzare nelle botnet. Le botnet sono reti di dispositivi sotto il controllo di un utente malintenzionato che consentono attacchi coordinati su larga scala. Le botnet sono state utilizzate per attacchi DDoS (Distributed Denial of Service), violazioni finanziarie, mining di criptovalute e intrusioni mirate.

Gli aggressori utilizzano diversi strumenti per inviare richieste callback ai propri server C&C. Alcuni di questi, tra cui Smoke Loader e Gumblar, sono bot progettati specificamente per questo. Altri, come Cobaltstrike e Poshc2, sono strumenti penetration testing riconvertiti dagli aggressori. Di seguito sono riportate le percentuali di tentativi di callback con questi strumenti:

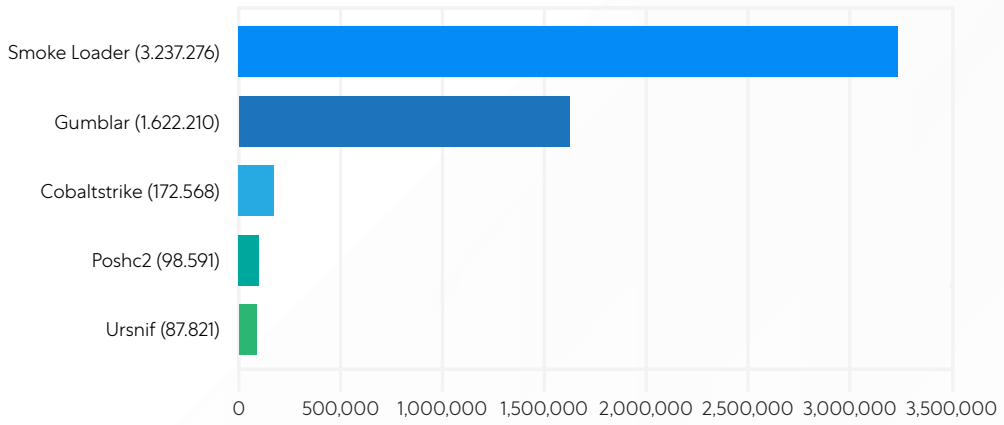

Figura 5: *attività di comando e controllo*

Gli aggressori interagiscono con quasi il **70%** delle applicazioni criptate esposte al web.

Attività di credential stuffing e di exploit

Questi canali vengono utilizzati dagli aggressori non solo per distribuire malware nel traffico criptato, ma anche per tentare attacchi con interazione umana tramite l'exploit di applicazioni criptate.

Il team Threatlabz raccoglie inoltre informazioni da una rete di esche distribuite a livello globale, utilizzando la tecnologia Zscaler Deception, per studiare tattiche, tecniche e procedure degli aggressori (TTP). Le esche vengono utilizzate per attrarre gli aggressori e non vi è interazione da parte di utenti legittimi, pertanto qualsiasi interazione è segno di attività malevola. ThreatLabz ha scoperto che:

1. Quasi il 70% di tutte le esche di applicazioni abilitate SSL ha registrato un'interazione, il che indicherebbe che il 70% delle applicazioni abilitate SSL è suscettibile di tentativi di attacco.
2. Nel contesto delle applicazioni web esca esposte a internet, quasi il 48% degli attacchi alle credenziali è stato diretto verso le e-mail e le VPN esca.
    - Le e-mail esca sono stati bersagli diffusi per lo stuffing di credenziali rubate.
    - Per le VPN si è verificato lo sfruttamento di CVE (Vulnerabilità ed esposizioni comuni) recentemente divulgate.
3. La tecnica riscontrata più frequentemente è stata la ricerca di file ".git", probabilmente con l'obiettivo di individuare server web configurati in modo errato per rivelarne il codice sorgente. Sebbene questa tecnica sia presente già da diverso tempo, è ancora estremamente diffusa durante la fase di ricognizione che precede la violazione.

Attacchi mobili

Smartphone e tablet continuano a essere bersagli molto comuni per gli aggressori, da colpire con exploit attraverso l'uso di applicazioni fittizie. Dopo l'infezione iniziale, molte delle nuove e prevalenti varianti di malware per dispositivi mobili utilizzano la comunicazione di rete SSL per le proprie attività di comando e controllo, tra cui il recupero di payload o la ricezione di comandi per svolgere attività malevole ed esfiltrare i dati. Le famiglie di malware come Hydra, Joker e quella appena scoperta di GriftHorse, sfruttano l'SSL per le proprie attività post-infezione.

Malware GriftHorse

La campagna di malware GriftHorse Android, emersa di recente, ha causato oltre 10 milioni di vittime in tutto il mondo e ha rubato denaro un ammontare stimato di centinaia di milioni di euro. Dopo l'infezione, alle vittime viene richiesto di inviare un numero di telefono per ricevere un premio. A loro insaputa, il numero di telefono viene abbonato a un servizio SMS premium che addebita al piano telefonico colpito più di 30 € al mese. Il trojan comunica con i server C&C in tre fasi e sfrutta il protocollo SSL per le attività di post-infezione.

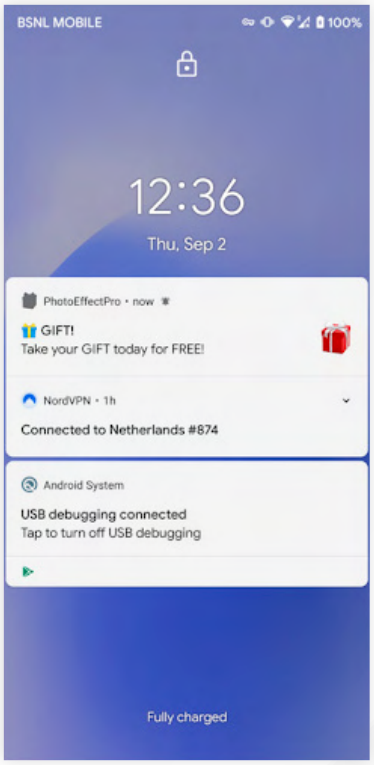

Figura 6: *attacco del malware GriftHorse*

Malware Joker

Joker è una delle famiglie di malware più note che prende di mira i dispositivi Android attraverso il Google Play Store. Zscaler ha bloccato quasi 22.000 tentativi di callback da malware Joker su TLS, che viene utilizzato per attività di comando e controllo. Nonostante il pubblico ne sia a conoscenza, il malware continua a farsi strada nel mercato ufficiale delle applicazioni di Google adottando cambiamenti nel codice, nei metodi di esecuzione o nelle tecniche di recupero dei payload. Joker è un tipo di spyware ed è progettato per rubare messaggi SMS, elenchi di contatti e informazioni sui dispositivi e per iscrivere la vittima a servizi WAP (Wireless Application Protocol) premium.

Il malware Hydra

Hydra è uno degli esempi più diffusi e abili di malware bancari. Le sue funzionalità includono lo screencasting, che consiste essenzialmente nel filmare le attività che si svolgono sullo schermo dell'utente nel corso del tempo. Hydra è inoltre in grado di installare app da remoto che consentono agli aggressori di osservare e controllare i dispositivi infetti, e questo lo rende una minaccia molto seria. Hydra sfrutta i certificati SSL per svolgere attività di comando e controllo.

Settore

Se si effettua un confronto tra il 2021 e il 2020, i risultati variano molto in base al settore. Sette dei settori considerati nel nostro studio hanno registrato percentuali di attacco più elevate su canali criptati, mentre per due settori si è verificata una diminuzione, e fra questi c'è il settore più preso di mira dello scorso anno: quello della sanità.

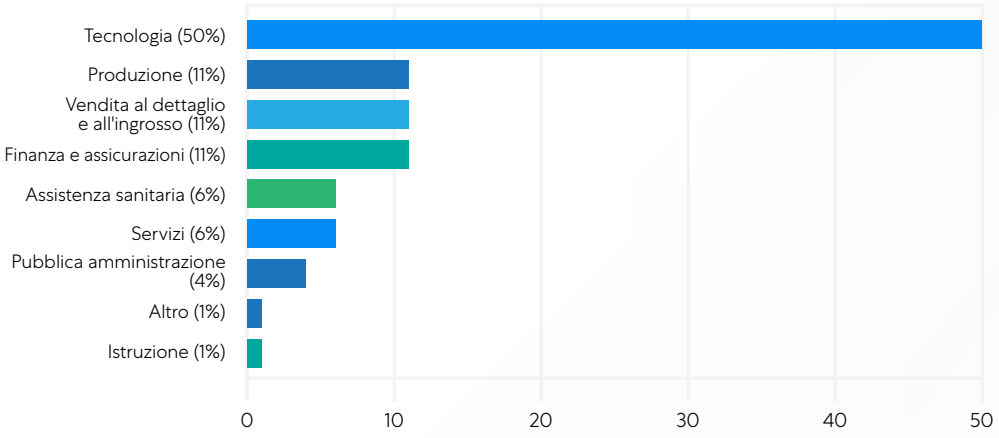

Figura 7: *volume di attacchi per settore*

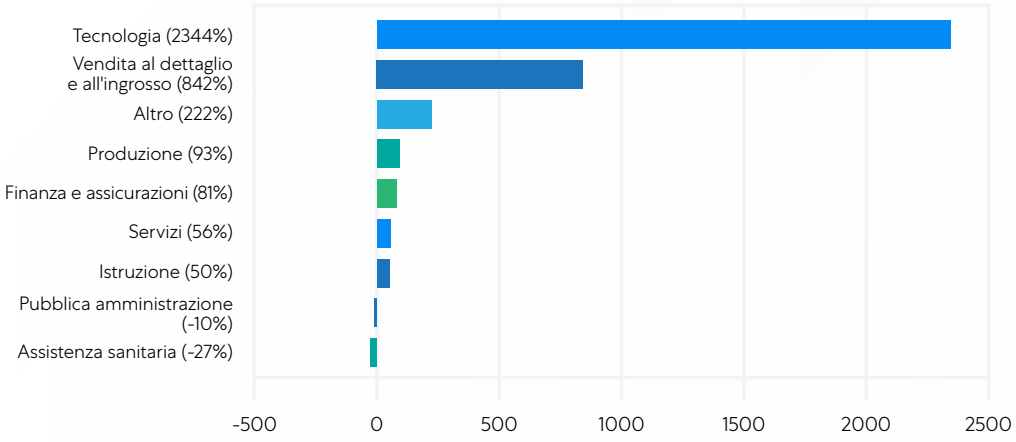

Figura 8: *attacchi per settore; confronto tra il 2021 e il 2020*

I settori del tech e della vendita al dettaglio hanno registrato un aumento notevole delle percentuali di attacco

Gli attacchi alle aziende tecnologiche sono aumentati di ben 23 volte, e attualmente rappresentano più della metà di tutti gli attacchi osservati. Il settore tecnologico è colpito in continuazione da malware e a un ritmo molto più elevato rispetto agli altri settori. La dipendenza del settore dalla tecnologia per quasi tutte le funzioni aziendali offre agli aggressori un'ampia superficie di attacco da sfruttare. Questa condizione è resa ancora più critica dall'improvvisa necessità di supportare tutte le attività dei lavoratori a distanza, dalle connessioni da remoto alle teleconferenze, dalle app SaaS ai carichi di lavoro nel cloud pubblico.

Le aziende tech sono degli obiettivi interessanti anche per il ruolo che svolgono nella catena di approvvigionamento di altre aziende. Un attacco riuscito alla catena di approvvigionamento può dare agli aggressori l'accesso a centinaia o addirittura migliaia di vittime, come si è visto nei casi di Kaseya, SolarWinds e molti altri.

Anche i settori della vendita al dettaglio e all'ingrosso hanno vissuto un anno problematico, con le percentuali di attacco che sono aumentate di più di 8 volte. Gli attacchi a questi settori rappresentavano solo il 3,5 del totale nel 2020, ma nel 2021 hanno raggiunto l'11%. Si è verificato un aumento significativo dei contenuti dannosi, tra cui skimmer, JavaScript malevoli e payload di malware rivolti ai fornitori operanti nella vendita al dettaglio e nell'e-commerce tramite i canali TLS.

Mentre il mondo inizia a tornare alla normalità e le aziende e gli eventi pubblici riaprono in tutto il mondo, molti dipendenti continuano a lavorare in ambienti relativamente poco sicuri. Ottenere l'accesso ai sistemi POS principali è una prospettiva estremamente invitante per i criminali informatici, in quanto apre le porte a ingenti profitti.

Gli attacchi al settore sanitario e governativo sono diminuiti

Dopo aver rappresentato il target principale nel 2020, gli attacchi alle organizzazioni sanitarie sono diminuiti del 27% nel 2021. Lo stesso vale per gli attacchi alle organizzazioni governative, che si sono ridotti del 10%. I grandi attacchi ransomware, che hanno avuto un impatto sui servizi critici, tra cui quelli contro SolarWinds, Colonial Pipeline e l'Health Service Executive irlandese, hanno attirato l'attenzione delle maggiori autorità giudiziarie, rendendo questi settori troppo difficili da attaccare al momento. Inoltre, diverse famiglie di ransomware hanno promesso di non colpire il settore sanitario e altri servizi essenziali durante la pandemia, anche se queste promesse non sono state del tutto mantenute.

Area geografica

I cinque Paesi più colpiti dagli attacchi criptati sono Regno Unito, Stati Uniti, India, Australia e Francia:

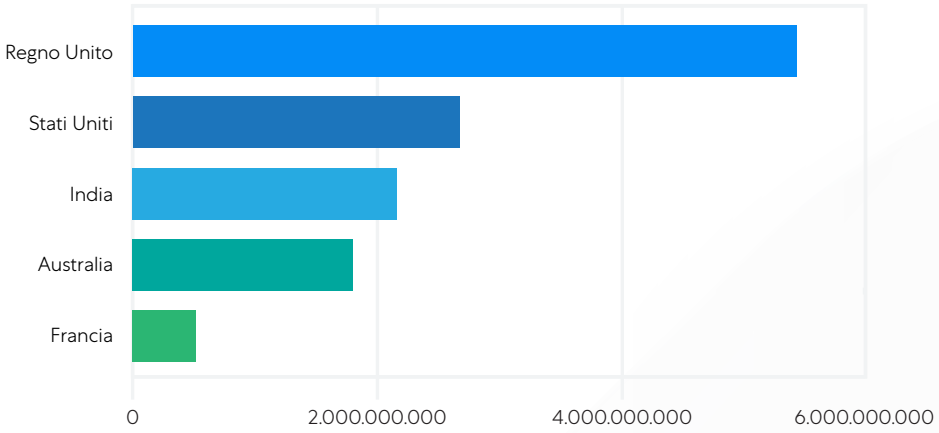

Figura 9: *i Paesi più attaccati*

Ognuno di questi Paesi rappresenta un grande hub tecnologico e la loro percentuale di attacchi subiti è aumentata insieme agli attacchi contro il settore. ThreatLabz ha osservato attacchi in 255 Paesi diversi in tutto il mondo, compresi Paesi di piccole dimensioni che in genere non vengono colpiti. Questo include oltre 7,5 milioni di attacchi nelle isole dei Caraibi e in località come le Isole Faroe, Saint-Barthélemy e le Isole Falkland. Questa situazione è una conseguenza della possibilità di lavorare da qualsiasi luogo, che ha portato diversi dipendenti a stabilirsi in luoghi remoti.

Con il Regno Unito che guida la classifica dei Paesi più colpiti in Europa, il Vecchio Continente ha subito il maggior numero di tentativi di attacco su canali criptati:

Regione	Conteggio
Europa	7.234.747.361
APAC	4.925.542.601
America del Nord	2.778.360.051
America del Sud	226.320.069
Africa	146.865.982
Medio Oriente	137.494.862
America centrale	127.354.294
Caraibi	7.543.056
Antartide	16.144

La possibilità di lavorare da qualsiasi luogo ha ampliato la portata geografica degli attacchi informatici.

Man mano che le aziende si evolvono per supportare i nuovi modelli di lavoro, è sempre più importante garantire la sicurezza delle proprie risorse e del traffico. Inoltre, è fondamentale riconoscere che la crittografia da sola non è in grado di fornire questo livello di sicurezza: i canali criptati vengono utilizzati dagli aggressori con la stessa frequenza dei canali non criptati.

La conclusione: **il traffico va ispezionato! Tutto quanto!**

Con gli strumenti legacy l'ispezione completa è costosa e negativa per le prestazioni. Inoltre, le normative che richiedono policy diverse per diversi tipi di dati possono contribuire a rendere il tutto ancora più complicato. Fortunatamente, esistono strategie consolidate che consentono alle aziende di ispezionare il traffico criptato su larga scala, senza influire negativamente sulle prestazioni dei sistemi o complicare il raggiungimento della conformità. Il nostro consiglio è:

- Decriptare, rilevare e prevenire le minacce in tutto il traffico HTTPS con un'architettura basata su proxy e nativa del cloud in grado di ispezionare tutto il traffico per ogni utente.
- Mettere in quarantena gli attacchi sconosciuti e bloccare i malware "paziente zero" con una sandbox basata su IA che trattenga i contenuti sospetti per sottoporli all'analisi, a differenza degli approcci di tipo "pass-through" basati su firewall.
- Garantire una sicurezza uniforme per tutti gli utenti e tutte le sedi, per assicurare che tutti dispongano dello stesso livello di sicurezza in ogni momento, che siano a casa, in sede o in viaggio.
- Ridurre istantaneamente la superficie di attacco partendo da un approccio zero trust in cui il movimento laterale non può esistere. Le app sono invisibili agli aggressori e gli utenti autorizzati accedono direttamente alle risorse di cui hanno bisogno, e non all'intera rete.

Questa soluzione richiede scalabilità e prestazioni che possono essere fornite solo da un'architettura basata su proxy e nativa del cloud, come Zscaler Zero Trust Exchange™. Una piattaforma di sicurezza in cloud soddisfa i requisiti di decriptazione e ispezione aumentando in modo flessibile la potenza di calcolo di cui ha bisogno e fornisce un'applicazione coerente delle policy in più sedi. Una strategia multistrato e difensiva, che riduca la superficie di attacco e supporti completamente l'ispezione HTTPS per far emergere le minacce nascoste, è essenziale per garantire la protezione delle aziende.

Il modo migliore per bloccare le minacce criptate consiste nell'ispezionare il traffico criptato nell'ambito di una strategia olistica di sicurezza zero trust.

IN CHE MODO ZSCALER ZERO TRUST EXCHANGE BLOCCA LE MINACCE CRIPTATE

Le strategie e le architetture zero trust sono i mezzi più efficaci per proteggere le aziende dalle minacce informatiche in rapida evoluzione. Lo zero trust parte attivamente dal presupposto che si stia subendo un attacco e che l'infrastruttura sia già stata violata. Come conseguenza di questa ipotesi, vengono messi in atto i controlli di sicurezza per impedire la riuscita del presunto attacco.

La maggior parte degli attacchi avanzati avviene in tre fasi distinte. La prima fase comporta la compromissione iniziale di un endpoint o di una risorsa esposta a internet. Una volta all'interno, l'aggressore avvia la propagazione laterale, eseguendo la ricognizione e stabilendo un punto di ingresso nella rete. Infine, passa all'azione per raggiungere i propri obiettivi, e questo in genere implica l'esfiltrazione dei dati. Zscaler Zero Trust Exchange riduce globalmente il rischio in ognuna di queste tre fasi di attacco, fornendo diversi controlli di sicurezza in ogni fase:

Prevenzione da compromissioni

Protezione di utenti, server, carichi di lavoro e dispositivi IoT/OT riducendo al minimo la superficie di attacco e ispezionando tutto il traffico.

Prevenzione del movimento laterale

Blocco degli aggressori prima che si muovano sulla rete e che identifichino i target di alto valore.

Prevenzione del furto di dati

Ispezione di tutti i dati diretti a internet per evitare la perdita di dati e lo sfruttamento dei dispositivi non gestiti.

Compromissione iniziale: per interrompere l'accesso iniziale, il primo passo da compiere è ridurre il numero di punti di ingresso nel proprio ecosistema. È quindi necessario controllare la propria superficie di attacco, rimanere aggiornati con le patch di sicurezza e correggere eventuali errori di configurazione esistenti. Inoltre, è bene eliminare tutte le applicazioni esposte a internet, posizionandole invece dietro un proxy cloud che agisca da intermediario per la connessione. In questo modo, si fornisce agli aggressori una sola porta di entrata e uscita, che è più semplice da monitorare. Inoltre, come abbiamo ripetutamente consigliato, è fondamentale ispezionare tutto il traffico, in quanto nulla può essere ritenuto attendibile. Zscaler esegue l'ispezione HTTPS su vasta scala nell'ambito della sua piattaforma di servizi e, man mano che il traffico aumenta, la potenza viene aumentata all'istante e in base alla necessità, senza che vi sia l'esigenza di acquistare, ordinare o ricevere apparecchiature.

Movimento laterale: con lo zero trust, non esiste una "rete attendibile". È fondamentale presupporre che chiunque abbia accesso a un'applicazione sia potenzialmente ostile e limitare pertanto i potenziali danni. Per ridurre l'accesso, è possibile usare la microsegmentazione, anche per gli utenti autenticati. La soluzione di accesso zero trust di Zscaler, Zscaler Private Access™, collega gli utenti direttamente all'applicazione di cui hanno bisogno senza mai esporre la rete, creando un segmento uno a uno che viene intermediato e autenticato da Zero Trust Exchange. Si tratta di una segmentazione zero trust nel suo formato più puro ed è molto meno complessa rispetto alla segmentazione della rete utilizzata dalle tecnologie legacy che si fonda su regole. Zscaler utilizza inoltre le Deception technology per attirare gli aggressori con esche posizionate strategicamente che, in presenza di aggressori che tentano di muoversi lateralmente o di eseguire ricognizioni, avvisano i team di sicurezza.

Callback di comando e controllo (C&C): una volta installato, il malware tenta generalmente di contattare un server di comando e controllo (C&C). Questo contatto consente agli aggressori di assumere il controllo dei server, emettere comandi aggiuntivi, scaricare ulteriori malware o rubare dati. L'ispezione del traffico in uscita è importante quanto quella del traffico in entrata per interrompere queste comunicazioni e proteggere i dati sensibili. Zscaler è in grado di ispezionare i dati criptati in entrata e in uscita, con sofisticate funzionalità di protezione contro la perdita di dati per identificare e bloccare tutto il traffico dannoso in uscita.

Zscaler Zero Trust Exchange interrompe l'intera sequenza di attacco e offre un'ispezione HTTPS su larga scala utilizzando un approccio multistrato dotato di un'ispezione delle minacce in linea, sandboxing e prevenzione sulla perdita dei dati, oltre a una vasta gamma di ulteriori capacità di difesa. Inoltre, l'effetto cloud di Zscaler prevede che tutte le minacce identificate nella piattaforma globale aggiornano automaticamente le protezioni per tutti i clienti di Zscaler, quindi il loro posizionamento in termini di sicurezza è in costante miglioramento, grazie al contributo fornito da ciascun cliente Zscaler in tutto il mondo. La soluzione Zscaler Zero Trust Exchange, supportata dal security cloud più grande del mondo, accelera la trasformazione aziendale, garantendo la protezione di utenti e applicazioni indipendentemente dalla loro posizione, utilizzando l'identità basata sul contesto e l'applicazione delle policy.

Di seguito sono riportate le famiglie di malware nuove e diffuse che sfruttano il TLS individuate da ThreatLabz durante il 2021.

njRAT

Sono stati osservati 355.753 blocchi di download tramite TLS.

Riepilogo

njRAT, noto anche come Bladabindi, è un trojan di accesso remoto (RAT) scritto nel framework .Net in grado di consentire il controllo completo del sistema infetto, oltre a fornire una serie di funzionalità all'aggressore da remoto. Può registrare le attività della tastiera dell'utente, rubare dati dalle macchine compromesse ed esfiltrare i dati verso un server remoto. È stato individuato per la prima volta nel giugno del 2013.

Per eludere il rilevamento, questo malware può utilizzare una o tutte le seguenti tecniche:

1. Offuscamento utilizzando packer noti, come ConfuserX, ecc.
2. Anti-virtualizzazione: verifica della presenza di "vboxservice.exe", "vboxtray.exe", "vmtoosd.exe", "SDBIE. DLL", ecc.
3. Controllo degli strumenti di analisi: controllo di processi quali processviewer.exe, processhacker.exe, ecc.

Strategia di distribuzione

Gli aggressori distribuiscono njRAT utilizzando varie strategie, come le e-mail e il web. Alcuni dei più diffusi vettori di attacco sono:

- Utilizzo di kit di exploit come Lord EK e Rig EK.
- File di MS Office basati su macro inviati come allegati di e-mail o ospitati in corrispondenza di un URL.

Persistenza

Per consentirne la persistenza, questo malware può utilizzare uno dei seguenti meccanismi o entrambi:

1. Creazione di una voce di registro in esecuzione automatica in HKCU\Software\Microsoft\Windows\CurrentVersion\Run o HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
2. Autocopiarsi nella cartella di avvio

Rete

njRAT utilizza un DNS dinamico per i server di comando e controllo (C&C) e comunica utilizzando un protocollo TCP personalizzato su una porta configurabile. Di recente si è visto che njRAT v2.0 utilizza cdn.discordapp.com per il rilascio del proprio carico utile, che funziona tramite il protocollo HTTPS. Può utilizzare anche Filebin.net, che utilizza anch'esso l'HTTPS, per mascherarsi sotto forma di gioco craccato.

Smoke Loader

ThreatLabz ha registrato 4.269 blocchi per il download e 3.237.276 blocchi per callback su TLS.

Riepilogo

Smoke Loader è stato creato dagli ambienti informatici criminali russi nel 2011. Quest'anno, Smoke Loader ha compiuto 10 anni ed è ancora molto attivo. Viene utilizzato principalmente come strumento di download per scaricare ed eseguire malware aggiuntivi. Si tratta di un kit malevolo fornito con un bot e un pannello C&C basato su PHP, insieme a un manuale utente. Questo malware viene spesso venduto sul dark web a 1650 dollari per un pacchetto completo.

Tecniche di elusione

Smoke Loader viene spesso iterato attraverso elenchi di processi per individuare un processo in cui insinuarsi e utilizza il metodo di propagazione dell'iniezione per insinuarsi in explorer.exe. Sfrutta inoltre armi con più trucchi anti-VM; ad esempio, controlla se il percorso dell'eseguibile contiene la stringa [A-F0-9]{4}.vmt e controlla anche tutti i processi in esecuzione per cercare le stringhe "qemu-ga.exe", "qga.exe", "windanr.exe" "vboxservice.exe" "vboxtray.exe", "vmtoosd.exe", "pr_toos.exe", "vbox" e "vmmemc" e, se ne trova una, il binario esce. Cerca inoltre i nomi dei processi in esecuzione, come "procmon.exe", "ProcessHacker.exe", "Wireshark.exe" e molti altri e, se viene trovato uno di questi processi, il binario esce.

Meccanismo di persistenza

Genera un ID univoco per ogni computer colpito, basato sulla concatenazione del nome del computer, di un numero statico a codifica fissa (diverso tra le campagne) e del numero di serie del volume dell'unità di sistema. L'ID viene quindi generato come hash MD5 della stringa concatenata e aggiunto di nuovo con l'MD5 del numero di serie del volume. Il malware utilizza questo ID univoco per diversi scopi, quali la creazione di nomi di file casuali per due file rilasciati: la prima è una copia dell'eseguibile di Smoke Loader e la seconda è un file lnk creato nella cartella di avvio che viene invocato come attività pianificata.

Comunicazione di rete

I domini C&C vengono criptati utilizzando semplici operazioni XOR. Pertanto, Smoke Loader invia una richiesta POST al server C&C. Il carico utile viene criptato utilizzando RC4 prima dell'invio. La richiesta POST restituisce una risposta "404 Not Found"(404 Non trovato), ma contiene un carico utile nel corpo della risposta. Smoke Loader è diventato un downloader diffuso per diverse famiglie di malware e lo si vede scaricare malware come Avemaria, ospitato su pastebin.com, che funziona su HTTPS, così come si possono osservare comunicazioni simili per altri malware che utilizzano l'HTTPS.

QakBot

Sono stati osservati 30.199 blocchi di download tramite TLS.

Riepilogo

QakBot è un trojan bancario, noto anche come Qbot o Pinkslipbot, attivo dal 2007. Il suo scopo principale consiste nel rubare le credenziali bancarie. Viene distribuito tramite e-mail di spam e induce gli utenti a scaricare allegati malevoli o a fare clic su link dannosi. Il download di un documento o di un file di script scarica anche il payload principale del Qakbot nel sistema infetto. In alcuni casi, è stato distribuito tramite kit di exploit e scaricato da altri malware come TrickBot. Si è evoluto nel corso tempo, e ha aggiunto funzionalità, come tecniche di web injection per il furto di credenziali, di numeri di carte di credito, social security number, indirizzi e-mail e sequenze di tasti, ed è dotato di funzionalità backdoor.

Meccanismo di persistenza

QakBot stabilisce la persistenza creando un tasto RUN ("esegui") nella posizione di avvio automatico ed eseguendo il malware a ogni accesso. Inoltre, crea attività pianificate per eseguire il carico utile una volta alle 05:33 ed eliminare l'attività pianificata dopo l'esecuzione.

> *HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run\{Random}*
> *C:\Windows\SysWOW64\schtasks.exe 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn {Random}/tr '\'% AppData%\Roaming\Microsoft\{Random}\{Random.exe}\' /I {Random}' /SC ONCE /Z /ST 05:33 /ET 05:45*

Comunicazione di rete

In una delle campagne, JavaScript scarica il modulo aggiornato di QakBot *ebook[.]w3wvg.com/datacollectionservice.php3* e lo esegue. Il carico utile di scaricamento è criptato e lo script lo decrittografa prima di rilasciarlo nel sistema e rubare le seguenti informazioni dal computer della vittima:

- Indirizzo IP
- Nome dell'host
- Nome utente
- Versione del sistema operativo
- Credenziali bancarie

Utilizza WebInject per alterare la comunicazione tra la macchina della vittima e i siti Web bancari e ruba le credenziali. Per comunicare con il server di comando e controllo tramite TLS (Transport Layer Security), come mostrato nella schermata sottostante, QakBot utilizza un handshake TLS invece dell'SSL (Secure Sockets Layer).

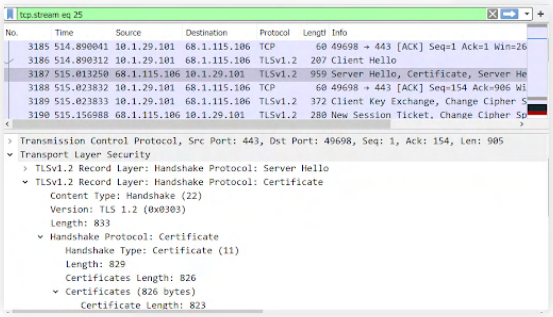

Figura 10: *QakBot utilizza un handshake TLS*

Solarmarker

Riepilogo

Il malware noto come Solarmarker/Jupyter Infostealer/Yellow Cockatoo/Polazert è un ladro di informazioni altamente modulare, nonché un keylogger. Di solito, questo malware si integra con le applicazioni potenzialmente indesiderate (PUA) conosciute, come PDFSam, utilizzando Innopack per creare un pacchetto in cui è presente sotto forma di file di programma legittimo. L'infezione da Solarmarker avviene solitamente utilizzando l'avvelenamento da SEO, ovvero una vecchia tecnica utilizzata come esca per far scaricare file da Internet alle vittime. Il download del pacchetto malware avviene tramite HTTPS.

Tecniche di elusione

Questo malware viene distribuito utilizzando installatori come MSI e Innopack. Ciò viene fatto per aumentare le dimensioni del vettore iniziale, affinché superino i 50 MB, che è un valore superiore rispetto alle dimensioni di invio di alcuni repository di malware e sandbox. MSI viene utilizzato anche per eludere il rilevamento degli endpoint e le soluzioni antivirus, poiché l'esecuzione di PowerShell da parte di MSI è meno sospetta di un'esecuzione di uno script PowerShell.

Meccanismo di persistenza

Nelle campagne recenti, questo malware rilascia un file .lnk nella directory del menu Start\Programmi\Avvio dell'utente. Con il file .lnk inserito in questa directory, verrà eseguito all'avvio e avvierà la backdoor.

Comunicazione di rete

Solarmarker viene servito utilizzando il protocollo TLS e distribuito utilizzando l'avvelenamento da SEO. Poiché, in genere, questo malware viene impacchettato con altri installatori, la sua comunicazione di rete viene in qualche modo offuscata dalle comunicazioni dei packer legittimi. La maggior parte dei programmi utilizza TLS e HTTPS, mentre la comunicazione dannosa avviene tramite l'HTTP utilizzando le richieste POST. L'indirizzo IP è presente nel codice binario. I dati utente vengono inviati utilizzando un JSON, come mostrato di seguito.

```
{
    "{\"action\":\"ping\",\"",
    Deimos.a.a(new char[]
    {
        'h',
        'w',
        'i',
        'd'
    }),
    "\":\"",
    A_0.g,
    "\",\"pc_name\":\"",
    Deimos.a.h(),
    Deimos.a.b(),
    "\",\"os_name\":\"",
    Deimos.a.e(),
    Deimos.a.b(),
    "\",\"arch\":\"",
    Deimos.a.f() ? "x64" : "x86",
    Deimos.a.b(),
    "\",\"rights\":\"",
    Deimos.a.d() ? "Admin" : "User",
    Deimos.a.b(),
    "\",\"version\":\"",
    A_0.a,
    "\",\"",
```

Figura 11: *dati utente inviati utilizzando JSON*

BlackMatter

Riepilogo

BlackMatter ha iniziato a essere distribuito a luglio del 2021. Gli operatori ransomware di BlackMatter utilizzano tecniche di doppia estorsione e sono noti per pubblicare i dati sensibili rubati delle vittime sul loro sito Web, qualora il riscatto non venga pagato. Fornisce RaaS (Ransomware as a Service) e lo si è visto pubblicare un annuncio su un forum alla ricerca di broker in grado di fornire l'accesso iniziale a reti compromesse di grandi dimensioni: gli operatori di BlackMatter pagano i broker per l'accesso alla rete. Il ransomware BlackMatter utilizza combinazioni di RSA+Salsa20 nel processo di crittografia. Questo ransomware aggiunge le estensioni ".{Caratteri alfanumerici casuali}" ai file dopo la crittografia. Rilascia la richiesta di riscatto "{Caratteri alfanumerici casuali}.README.txt".

Elusione e offuscamento

Il ransomware BlackMatter elimina le copie shadow sul computer di una vittima, per impedire il ripristino del sistema. Termina i processi relativi alla produttività, come Outlook, Oracle e Blocco note, in modo che il ransomware possa crittografare più file. Dopo l'esecuzione, aumenta anche i privilegi tramite un'interfaccia COM. Utilizza l'offuscamento delle stringhe e una tecnica di risoluzione dinamica dell'API Win32.

Comunicazione di rete

BlackMatter raccoglie informazioni quali la versione del bot, l'ID del bot, il nome dell'host, il nome utente, le informazioni sul disco, il sistema operativo, l'architettura di sistema e le informazioni sui file criptati. Comunica tramite HTTPS e utilizza il TLS per la crittografia, come mostrato nella schermata di seguito. Se il carico utile non riesce a comunicare con l'HTTPS, utilizza l'HTTP per comunicare con il server di comando e controllo.

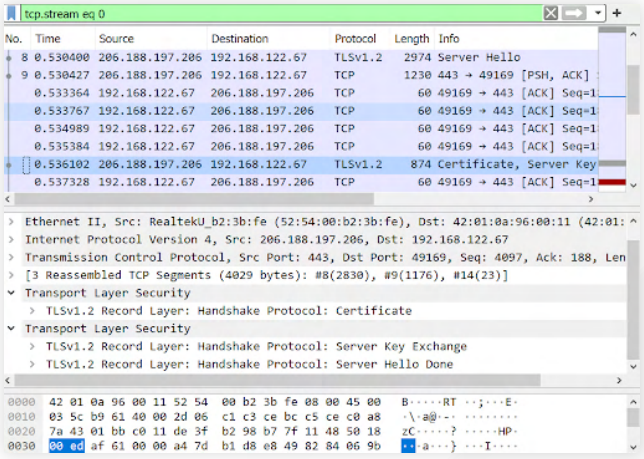

Figura 12: *BlackMatter utilizza il TLS per la crittografia*

REvil/Sodinokibi

Riepilogo

Il ransomware REvil, noto anche come Sodinokibi, è stato individuato per la prima volta nell'aprile del 2019, distribuito tramite e-mail di spam, kit di exploit e account RDP compromessi; Sodinokibi sfrutta spesso anche le vulnerabilità in Oracle WebLogic. Sodinokibi crittografa ogni file e aggiunge l'estensione .{caratteri alfanumerici casuali}. Utilizza una combinazione di algoritmi di scambio di chiavi basati su Salsa20 e ECDH nel processo di crittografia. Rilascia la nota di riscatto "{caratteri alfanumerici casuali}-readme.txt" e cambia lo sfondo nel sistema infetto.

Elusione e offuscamento

REviL ha la capacità di utilizzare tecniche di bypass dell'UAC per eseguire funzioni con privilegi elevati nel contesto del processo corrente. Utilizza inoltre varie API di Windows per determinare la lingua predefinita di sistema, installata sul computer, e procede all'esecuzione delle attività dannose solo se la lingua di sistema non è presente nella whitelist preconfigurata. Tali controlli linguistici vengono spesso eseguiti dai ceppi di ransomware per prevenire l'infezione delle vittime in aree geografiche specifiche.

Comunicazione di rete

REvil raccoglie nome utente, nome dell'host, nome del dominio, layout della tastiera, sistema operativo, informazioni sull'unità, architettura della CPU e dettagli sulla chiave di crittografia dal sistema di una vittima e invia queste informazioni al suo server di comando e controllo utilizzando l'HTTPS. L'elenco dei domini è presente nella configurazione integrata nel carico utile.

Microsoft Office 365

Abbiamo osservato l'abuso di siti di hosting legittimi e di editor di codice online, come glitch.me, CodeSandbox, Cloudflare Workers e altro ancora, utilizzati per ospitare contenuti di phishing. Questi siti servono le pagine di phishing tramite HTTPS e aiutano nello sviluppo rapido del Web. Di seguito sono riportati alcuni esempi di questi siti di phishing.

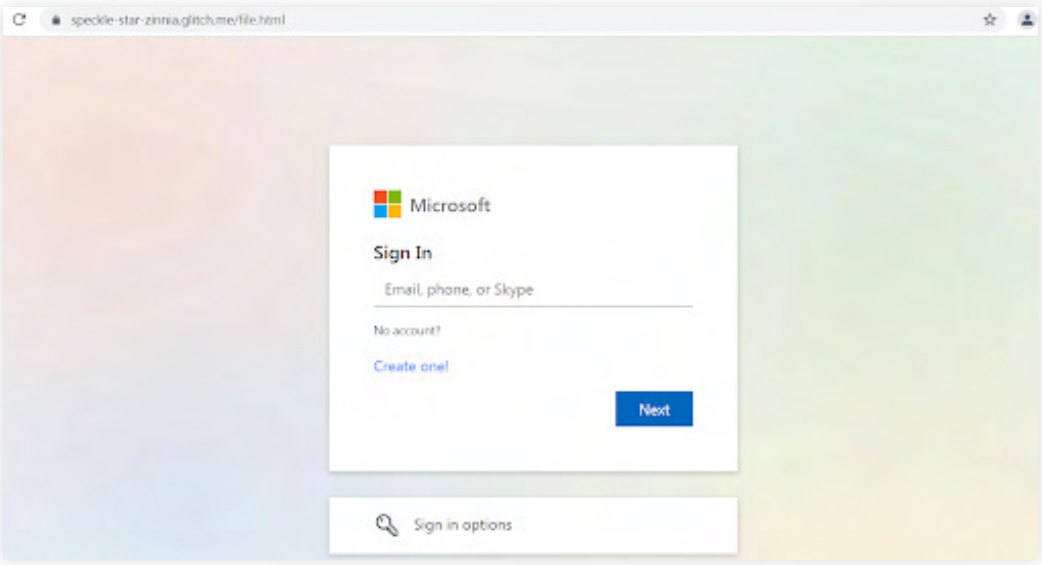

Figura 13: *esempio di sito di phishing*

Queste pagine di phishing utilizzano l'offuscamento multistrato e alcune parti del codice sorgente vengono offuscate con un mix di offuscatori JavaScript e codifica Base64.

Figura 14: *esempio di offuscamento multistrato*

Di seguito è riportato un altro caso di offuscamento multistrato.

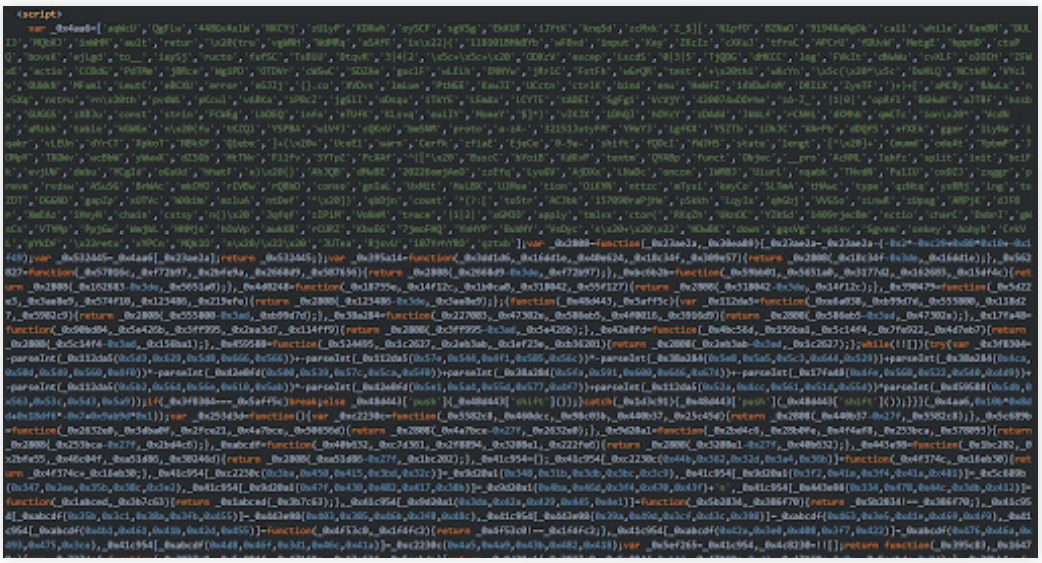

Figura 15: *esempio di offuscamento multistrato*

Questi siti di phishing creano inoltre impronte digitali degli indirizzi IP e reindirizzano a un sito Microsoft legittimo se l'IP appartiene all'elenco di aziende mostrato nella schermata seguente.

```
$.ajax({
        type: "GET",
        url:'https://pro.ip-api.com/json/?key=tPiZVEq18Ne6eQ1&fields=66846719',
        dataType: "json",
        success: function (res) {
        var e833200 = res.as + " " + res.asname + " " + res.isp;
          if (
          e833200.toLowerCase().indexOf("phish".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Paypal".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("namecheap".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Google".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Amazon".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("M247".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("AVAST".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Kaspersky".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("BullGuard".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Wintek Corporation".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("McAfee".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("commodo".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bitdefender".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Contina".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Symantec".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("fireeye".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("NetCraft".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("YandexBot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("barracuda".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mimecast".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("appriver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("proofpoint".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlscan".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlredirectresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bingbot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("trendmicro".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("spam".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("crawler".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mozilla".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("msnbot".toLowerCase()) >= 0
```

Figura 16: *elenco di aziende*

Amazon

Abbiamo osservato casi di phishing di Amazon tramite HTTPS. Uno di questi casi è illustrato nella schermata qui sotto. Possiamo notare che la regione di consegna predefinita sono gli Stati Uniti, il che fornisce informazioni sull'obiettivo di questa campagna di phishing.

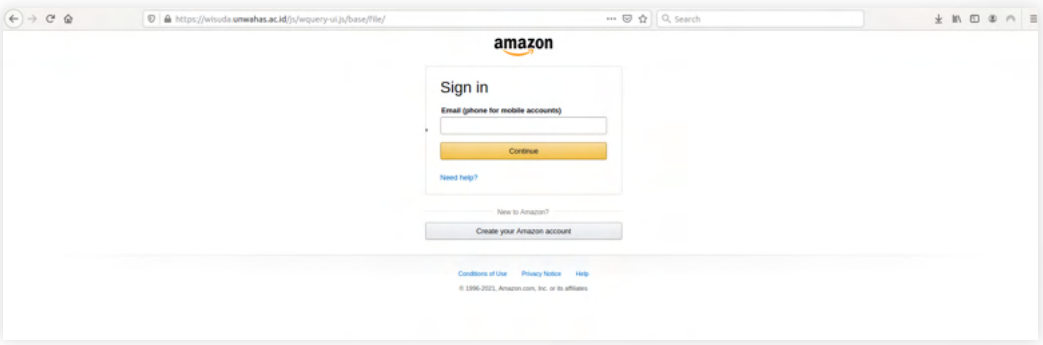

Figura 17: *istanza di phishing di Amazon tramite HTTPS*

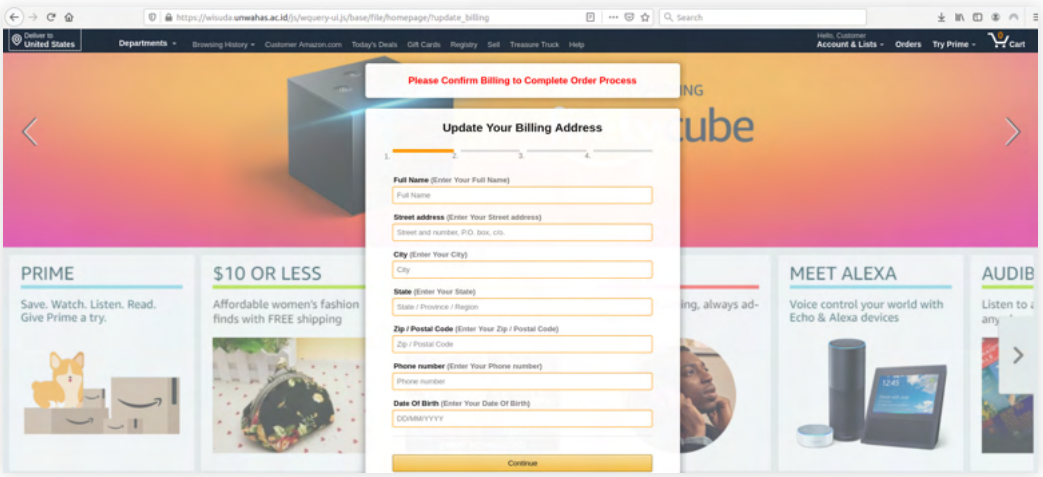

Figura 18: *istanza di phishing di Amazon tramite HTTPS*

Mostriamo di seguito la pagina sottoposta a defacing dall'aggressore nella posizione del sito Web che ospita il phishing di Amazon.

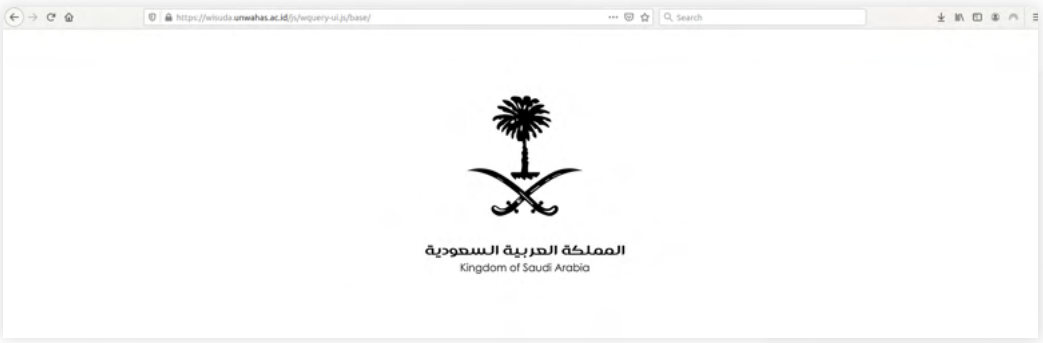

Figura 19: *pagina sottoposta a defacing dall'aggressore*

OneDrive

Abbiamo osservato gli aggressori servire le pagine di phishing di OneDrive tramite HTTPS. Queste venivano fornite da siti Web compromessi che ospitavano contenuti di phishing. Il codice sorgente viene codificato con la codifica esadecimale di base, per eludere il rilevamento da parte degli scanner di contenuti di phishing.

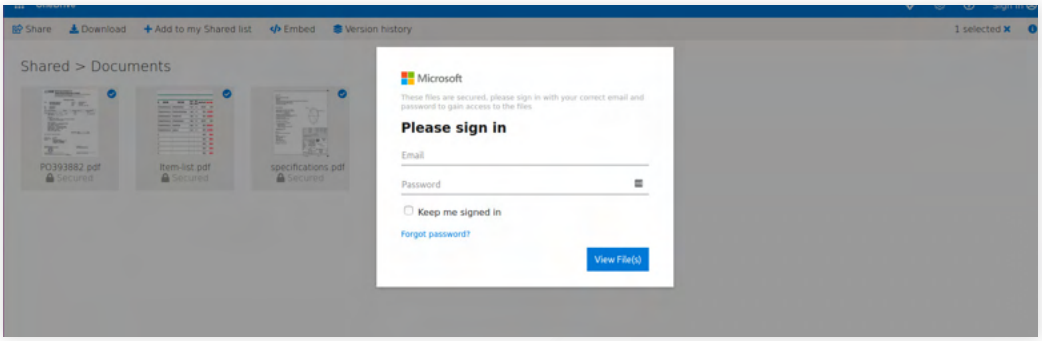

Figura 20: *istanza di phishing di OneDrive tramite HTTPS*

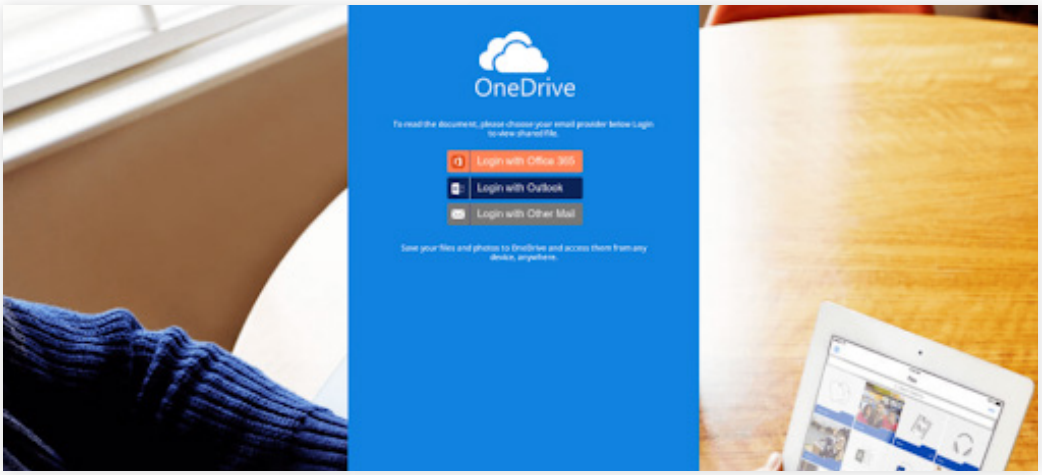

Figura 21: *istanza di phishing di OneDrive tramite HTTPS*

Figura 22: *parte codificata del codice sorgente*

Telegram

Abbiamo riscontrato casi di client Web non ufficiali di Telegram che utilizzavano l'HTTPS. Questi client Web non sono in grado di garantire la sicurezza. Queste pagine di phishing richiedono il numero di telefono dell'utente e inviano un'OTP a tale numero. Una volta che l'utente accede all'OTP sul sito Web non ufficiale, il client Web utilizza l'API di Telegram per recuperare il contenuto dell'utente e lo fornisce all'utente. Durante questa operazione, non vi è alcuna garanzia su come i messaggi dell'utente, l'elenco dei contatti e altri dati verranno utilizzati dai client Web dannosi. Di seguito viene riportato un esempio di tale sito Web.

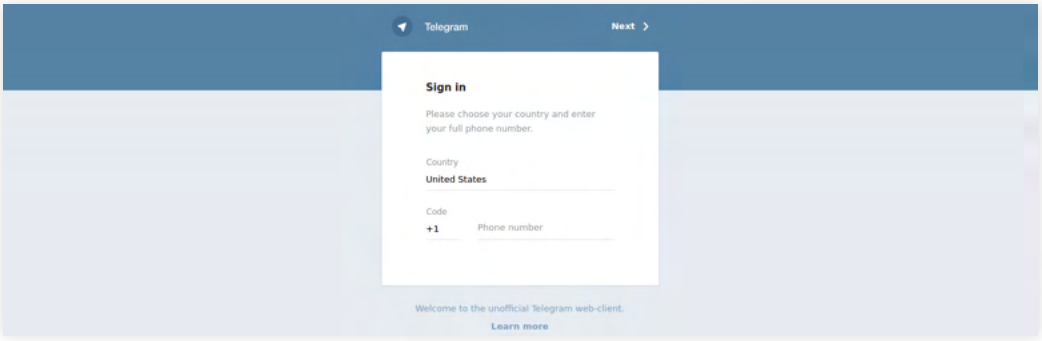

Figura 23: *istanza di client Web non ufficiale di Telegram che utilizza l'HTTPS*

Il fondatore di Telegram ha raccomandato l'uso dell'app ufficiale di Telegram per garantire la sicurezza.

Figura 20: *istanza di phishing di OneDrive tramite HTTPS*

PayPal

Abbiamo osservato l'attività di phishing di PayPal tramite HTTPS. Nel caso seguente, un sito Web di acquisti presenta l'opzione di pagamento PayPal compromessa.

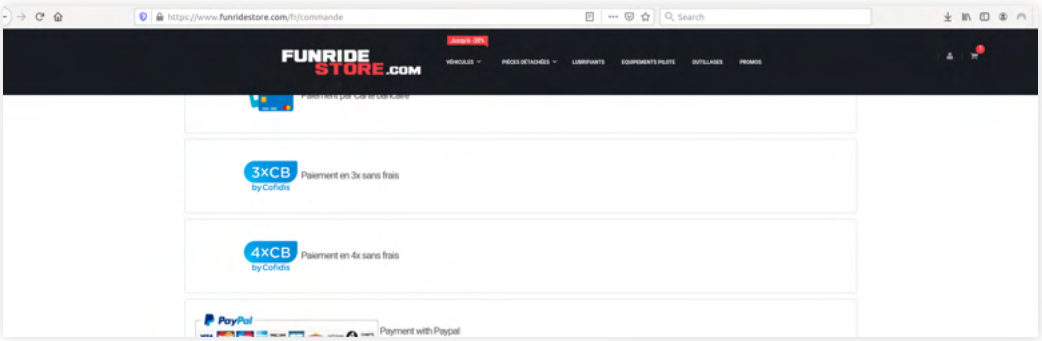

Figura 25: *istanza di attività di phishing di PayPal tramite HTTPS*

Se l'utente aggiunge articoli a un carrello, ci sarà una richiesta delle informazioni di spedizione e di contatto. Dopo aver inserito i dati, all'utente verranno fornite diverse opzioni di pagamento. Questo link di pagamento tramite PayPal è compromesso. Se l'utente sceglie l'opzione PayPal, verrà indirizzato alla pagina di phishing mostrata di seguito.

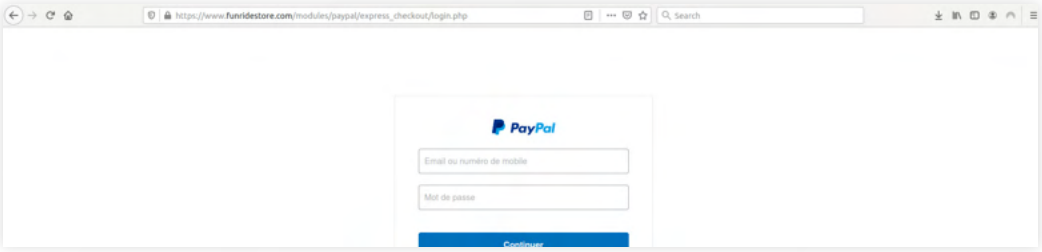

Figura 26: *pagina di phishing di PayPal*

Se vengono immesse le credenziali di PayPal, l'utente verrà reindirizzato all'URL di PayPal legittimo in cui l'utente può accedere e completare l'acquisto.

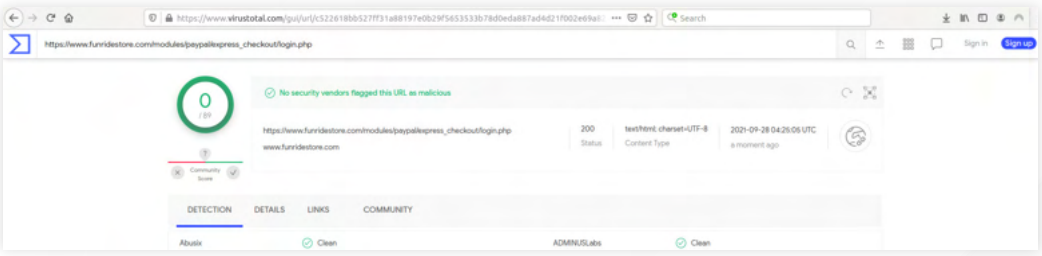

Figura 27: *pagina di phishing di PayPal*

Questo è un esempio interessante di ingegneria social. Mostra una pagina di acquisto legittima e il posizionamento del link di phishing di PayPal proprio là dove gli acquirenti si aspettano un link legittimo. I link di pagamento con carta di credito puntano a URL legittimi, solamente il link PayPal è stato compromesso.

Riscontriamo frequentemente l'uso di strumenti come Cobalt Strike, Mimikatz, LaZagne, tra gli altri, da parte degli aggressori per gli attacchi mirati, per eseguire la propagazione laterale, l'esfiltrazione dei dati e altre attività di C&C. Cobalt Strike rimane uno degli strumenti più utilizzati in molti di questi attacchi mirati.

Cobalt Strike

Sono stati riscontrati 24.410 blocchi per il download e 172.568 blocchi per callback tramite TLS.

Riepilogo

Cobalt Strike è uno strumento commerciale per la simulazione degli aggressori e le operazioni del Red Team. È un software completo di tutte le funzionalità, con profili di comando e controllo (C&C) predefiniti e configurabili, che gli consentono di modificare il proprio comportamento e gli indicatori di rete per simulare le tattiche, le tecniche e le procedure (TTP) di diverse famiglie di malware utilizzate per gli attacchi nel mondo reale. Sebbene sia uno strumento commerciale legittimo, è stato utilizzato ripetutamente dagli aggressori per attacchi reali. Vari gruppi APT, come quelli elencati di seguito, utilizzano il framework di Cobalt Strike:

- APT19
- DarkHydrus
- CopyKittens
- APT32
- Cobalt Group
- APT29
- Leviathan
- FIN6

Cobalt Strike è un malware senza file e supporta lo shellcode multifase, che può essere utilizzato per più scopi.

Comunicazione di rete

Cobalt Strike può essere configurato per comunicare su uno o più protocolli, utilizzando la funzionalità dei profili C&C malleabili:

- DNS (record TXT, A e AAAA)
- HTTP/HTTPS
- SMB (pipe denominate)
- TCP

Tecniche di elusione

Cobalt Strike viene spesso rilasciato come carico utile nella fase finale, che utilizza anche pipe denominate, ovvero socket che consentono la comunicazione tra i processi o anche gli host. Le funzioni post-sfruttamento di Cobalt Strike includono keylogger, Mimikatz e moduli screenshot.

Movimento laterale utilizzando credenziali rubate

Cobalt Strike utilizza le credenziali rubate per interagire con una condivisione di rete remota, usando SMB (Server Message Block), accedere a un computer utilizzando il protocollo RDP (Remote Desktop Protocol) e accedere a un servizio appositamente progettato per accettare connessioni remote, quali Telnet, SSH e VNC.

PoshC2

Sono stati riscontrati 98.591 blocchi per callback tramite TLS.

PosHC2 è un framework C&C con riconoscimento proxy, utilizzato per aiutare i tester di penetrazione per quanto concerne Red Team, post-sfruttamento e movimento laterale.

PoshC2 è scritto principalmente in Python3. PoshC2 si presenta sotto forma di impianti PowerShell/C# e Python2/Python3, con carichi utili scritti con codice sorgente in PowerShell v2 e v4, C++ e C#. Questi abilitano la funzionalità C&C su una vasta gamma di dispositivi e sistemi operativi, tra cui Windows, *nix e OSX.

PoshC2 può essere utilizzato con SharpSocks, che ammette il proxy Socks di tunnelling HTTPS inverso per C#, permettendo così l'esecuzione del traffico C&C su HTTPS.

Ursnif

Sono stati riscontrati 336.540 blocchi per il download e 87.821 blocchi per callback tramite TLS.

Riepilogo

Ursnif (noto anche come Gozi) è un trojan bancario, ma presenta varianti che includono componenti come backdoor, spyware, iniettori di file e altro ancora. È stato identificato per la prima volta nel 2006 e viene eseguito continuamente. Questo malware è distribuito utilizzando campagne di phishing specifiche per ogni Paese.

Meccanismo di persistenza

Ursnif utilizza due meccanismi per instaurare la persistenza:

1. Creazione di una nuova attività pianificata (con il nome "Power<parola_casuale>") (ad es. PowerSgs).
2. Se questo per qualche motivo non va a buon fine, utilizza la chiave di registro "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" per assicurarsi di mantenere la persistenza al riavvio del sistema.

Attività di rete

Una volta stabilito un avamposto sulla macchina, avvia il suo thread di lavoro principale, che interroga continuamente il server C&C per ottenere i comandi. Questo malware raccoglie informazioni sull'utente, come "utente", "server" e "ID", sotto forma di valori hash, e "uptime" (tempo di attività), che è un valore temporale che indica da quanto tempo è in esecuzione il dispositivo. "DNS" è il nome del computer e "whoami" è il nome utente completo. In alcuni casi, è stato riscontrato che questo malware contatta e trasmette le informazioni al proprio C&C utilizzando l'HTTPS.

Dridex

Sono stati riscontrati 50.088 blocchi per il download e 11.167 blocchi per callback tramite TLS.

Riepilogo

Dridex, noto anche come Bugat and Cridex, è un trojan specializzato nel furto di credenziali bancarie. Ha fatto la sua prima apparizione nel 2011, evolvendosi nel corso degli anni, ed è stato presente in diverse campagne di phishing che utilizzavano documenti di Microsoft Word ed Excel come carichi utili.

Tecniche di elusione

Dridex viene distribuito dalla botnet Cutwail o dal kit di exploit RIG. Utilizza campagne di phishing basate su tematiche attuali, come ad esempio il lancio di SpaceX.

Comunicazione di rete

Il carico utile del documento Dridex contiene C&C per la fase successiva. Il C&C viene contattato utilizzando l'HTTPS per scaricare un file DLL (Dynamic-Link Library), che è il carico utile finale che infetta l'utente e contatta ulteriori C&C. Una variante di Dridex, nota anche come DoppelDridex, nelle sue recenti campagne ha iniziato a utilizzare cdn.discordapp.com e Slack come C&C, che contiene il file DLL.

Scopri in che modo **Zscaler** è in grado di ispezionare tutto il traffico SSL senza influire sulle prestazioni o creare problematiche relative alla conformità. In alternativa, verifica la tua capacità di ispezionare il traffico SSL/TLS utilizzando il nostro strumento di **analisi dell'esposizione alle minacce di Internet.**

Informazioni su ThreatLabZ

ThreatLabZ è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti di alto livello è responsabile della ricerca di nuove minacce, nonché della protezione costante delle migliaia di aziende che utilizzano la piattaforma globale di Zscaler. Oltre alla ricerca di malware e all'analisi del comportamento, i membri del team si occupano di ricerca e dello sviluppo di nuovi prototipi per la protezione avanzata dalle minacce sulla piattaforma Zscaler e conducono regolarmente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano in linea con gli standard di conformità. ThreatLabZ pubblica regolarmente sul suo portale analisi approfondite sulle minacce nuove ed emergenti: **research.zscaler.com**.

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni, in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security inline del mondo.
Scopri di più su zscaler.com o seguici su Twitter **@zscaler.**

zscaler™