Stato degli attacchi criptati nel 2020

Il team di ricerca Zscaler™ ThreatLabz si propone di condividere informazioni utili su come gli aggressori stiano accelerando il loro utilizzo della crittografia SSL/TLS per aggirare le difese tradizionali

GENNAIO-SETTEMBRE 2020

Sommario

Informazioni su ThreatLabZ

ThreatLabz è il team di ricerca sulla sicurezza globale di Zscaler. Oltre al suo lavoro di protezione dei clienti Zscaler dalle minacce emergenti, il team analizza il traffico aziendale che attraversa il cloud Zscaler. Con l'esperienza maturata dal team nell'ambito della sicurezza informatica, della scienza dei dati e nell'IA/apprendimento automatico, insieme al volume di dati analizzati per oltre 120 miliardi di transazioni giornaliere sulla piattaforma cloud Zscaler Zero Trust Exchange™, ThreatLabz ha una posizione privilegiata per fornire informazioni utili sulle tendenze legate al traffico aziendale e alla sicurezza.

Quando ThreatLabz scopre una nuova campagna di attacco o malware con tecniche o capacità non comuni, i ricercatori distruggono questi file e analizzano il loro codice cosi' da scoprire esattamente come sono programmati per riuscire a eludere il rilevamento, rilasciare carico utile, rubare informazioni, controllare i dispositivi, spiare l'utente, propagarsi e diffondersi. I risultati delle nostre analisi vengono messi gratuitamente a disposizione della comunità della sicurezza sul **blog di ricerca di Zscaler**.

Per quanto concerne nello specifico le tendenze SSL, i ricercatori di ThreatLabz hanno recentemente scoperto, analizzato e segnalato le minacce sfruttando i canali criptati. Puoi saperne di piu' leggendo i seguenti post:

- **I siti VPN falsi diffondono infostealer**
- **Abuso dello strumento StackBlitz per ospitare pagine di phishing**
- **Skimmer JavaScript**
- **Minaccia persistente avanzata (APT) Higaisa**

Per vedere il cloud Zscaler in azione, visualizza il **pannello di controllo dell'attività del cloud**, che mostra il numero di transazioni in fase di elaborazione e le minacce che vengono bloccate ogni secondo.

Il traffico SSL nasconde malware. A bizzeffe.

A far infuriare gli esperti di sicurezza, c'è una convinzione sulla crittografia SSL che è così radicata quanto fuorviante: "Pensavo che bastasse che un sito Web utilizzasse la crittografia SSL per essere sicuro".

La crittografia SSL è stata progettata per proteggere il traffico da occhi indiscreti, ma anche gli aggressori l'hanno sfruttata per nascondere gli attacchi, trasformando l'uso della crittografia in una potenziale minaccia, senza un'adeguata ispezione.

I criminali informatici conoscono perfettamente ciò che sanno gli esperti di sicurezza: la crittografia SSL/TLS è il metodo standard per proteggere i dati in transito. Questi stessi criminali informatici utilizzano i medesimi metodi di crittografia standard del settore, ideando modi intelligenti per nascondere malware all'interno del traffico criptato ed eseguire attacchi che aggirano il rilevamento. Infatti, tra gennaio e settembre, il cloud Zscaler ha bloccato 6,6 miliardi di minacce alla sicurezza nascoste all'interno del traffico criptato, che ammontano a una media di 733 milioni di blocchi al mese, un dato davvero sorprendente. Questa media mensile rappresenta un aumento di quasi il 260% rispetto al 2019, quando il cloud Zscaler bloccava una media di 283 milioni di minacce al mese nel traffico criptato.

L'ispezione del traffico criptato deve essere una componente chiave fra le armi di difesa della sicurezzadi qualsiasi organizzazione. Il problema è che i tradizionali strumenti di sicurezza locali, come i firewall di nuova generazione, fanno fatica a fornire le prestazioni e la capacità necessarie per decrittografare, ispezionare e ricrittografare il traffico in modo efficace. Tentare di ispezionare tutto il traffico SSL porterebbe a un netto arresto delle prestazioni (e produttività), ecco perché molte organizzazioni consentono ad almeno una parte del proprio traffico criptato di passare senza essere ispezionato, come ad esempio il traffico proveniente da provider di servizi cloud e da altri considerati "attendibili". Si tratta di una carenza molto critica. La mancata ispezione di tutto il traffico criptato rende le organizzazioni vulnerabili agli attacchi nascosti di phishing, malware e altro ancora, il che potrebbe rivelarsi disastroso.

Tra gennaio e settembre, il cloud **Zscaler ha identificato e fermato 6,6 miliardi di minacce** nascoste all'interno del traffico criptato.

Il team ThreatLabz ha analizzato il traffico criptato attraverso il cloud Zscaler per i primi nove mesi del 2020, valutandone l'uso nei settori specifici. L'obiettivo dell'analisi consisteva nel capire non solo il volume di traffico che utilizza la crittografia, ma anche le minacce nascoste all'interno di quel traffico. Alcuni dei punti salienti includono:

- **La maggior parte del traffico Internet è criptato:** l'80% di tutto il traffico utilizza la crittografia SSL/TLS per impostazione predefinita.
- **Crescita esplosiva in volume:** aumento del 260% delle minacce basate sull'SSL negli ultimi nove mesi, accelerato dal picco di app di collaborazione con base cloud durante la pandemia di COVID-19.
- **Assistenza sanitaria sotto attacco:** la sanità è stata il settore più bersagliato con 1,6 miliardi di minacce criptate identificate e bloccate, seguita dal settore finanziario e manifatturiero.
- **Aumento dell'abuso dei servizi di condivisione file con base cloud:** oltre il 30% di tutti gli attacchi con base SSL si nascondono nei servizi di collaborazione, come Google Drive, OneDrive, AWS o Dropbox.
- **Ransomware nascosti in aumento:** aumento di oltre 5 volte dei ransomware diffusi tramite il traffico web criptato.

Anche i criminali informatici usano l'SSL/TLS: ecco perché ispezionare il traffico criptato è importante

La crittografia del traffico Internet tramite SSL (Secure Sockets Layer), e la sua alternativa più moderna TLS (Transport Layer Security), rappresenta lo standard globale per la protezione dei dati in transito e la stragrande maggioranza del traffico Internet attuale è criptato.[1] Il problema è che anche i criminali usano la crittografia per nascondere malware e altri exploit (sistemi di attacco). Ciò significa che il traffico che passa attraverso i canali criptati non può più essere attendibile semplicemente in virtù di un certificato digitale.

I criminali informatici hanno creato sofisticate catene di attacchi che iniziano con un'email di phishing dall'aspetto innocuo, contenente un exploit o malware nascosto. Se un utente ignaro fa clic, l'attacco passa quindi alla fase di installazione del malware e, infine, all'esfiltrazione di preziosi dati aziendali.

Ciò che rende gli attacchi così nefasti è il fatto che anche l'exploit o il malware nascosto è criptato, il che cambia completamente la sua struttura del file. I sistemi di sicurezza informatica si basano sulla struttura di un file (o "impronta digitale") per identificare le minacce in arrivo; se è strutturato in un certo modo, il sistema sa di doverlo bloccare. Tuttavia, ogni volta che un file viene criptato, ottiene un'impronta digitale nuova che non viene riconosciuta come una minaccia.

L'ispezione SSL è l'unico modo efficace per bloccare i file dannosi che vengono diffusi [utilizzando questi servizi], poiché i sistemi di sicurezza non sono in grado di bloccare quello che non riescono a vedere.

[1] https://transparencyreport.google.com/https/overview?hl=en

Tendenze del traffico SSL

Le imprese hanno ampiamente accettato il fatto che la crittografia sia un requisito per la protezione dei dati in transito dall'intercettazione e dallo sfruttamento. Nella nostra analisi, abbiamo riscontrato che il settore dell'istruzione ha crittografato la percentuale più elevata del proprio traffico, seguito dal settore manifatturiero, finanziario e dalla sanità. Tuttavia tutti i settori, tra cui la vendita al dettaglio/ingrosso, i servizi, la tecnologia e la comunicazione e l'amministrazione pubblica hanno dati che si avvicinano in modo piuttosto omogeneo. Durante il periodo di analisi, tra gennaio e settembre 2020, abbiamo osservato che l'uso della crittografia in tutti i settori si attestava in media al 75%, con un picco di oltre l'80%.

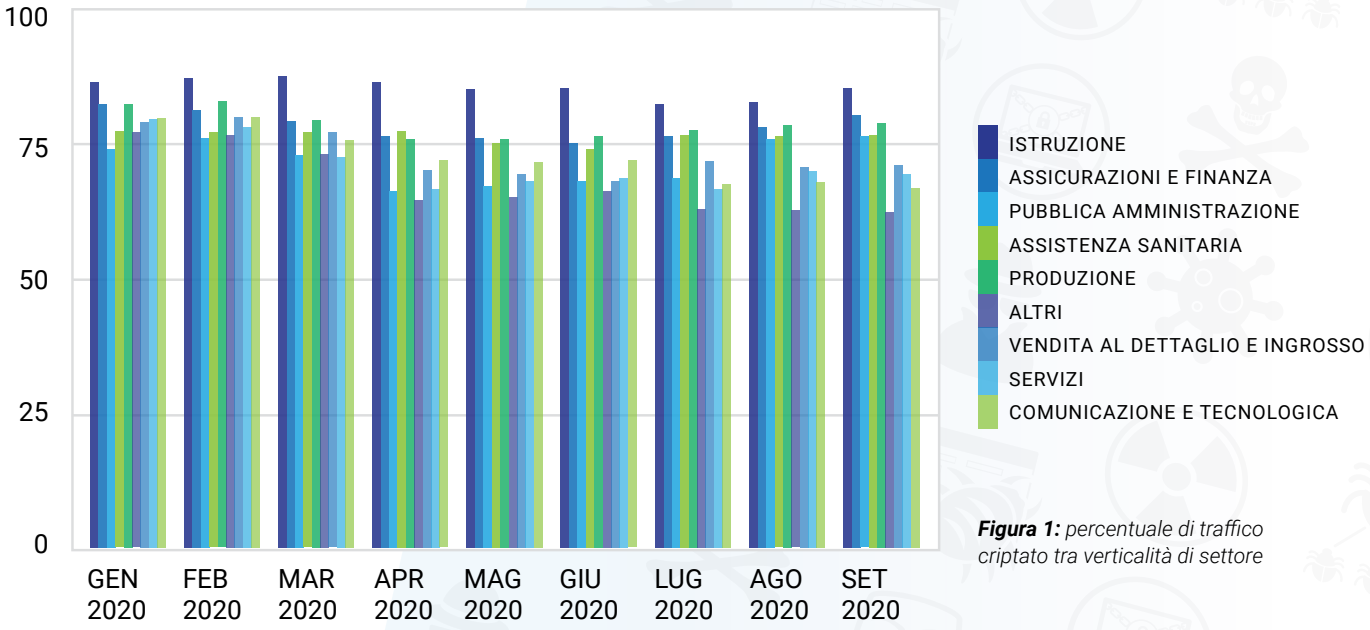


Figura 1: *percentuale di traffico criptato tra verticalità di settore*

Elevati tassi di traffico criptato sono stati osservati in ogni verticalità di settore, il che significa che tutte le organizzazioni devono considerare come ispezionare l'SSL/TLS per ricercare le minacce.

Secondo la nostra ricerca, le minacce si rivolgono maggiormente al settore sanitario con attacchi malware criptati, rispetto a qualsiasi altro settore. Tra gennaio e settembre 2020, il settore sanitario ha rappresentato il 25,5% di tutte le minacce avanzate bloccate sui canali criptati nel cloud Zscaler, seguito da quello finanziario/assicurazioni al 18,3%, manifatturiero al 17,4% e la pubblica amministrazione al 14,3%.

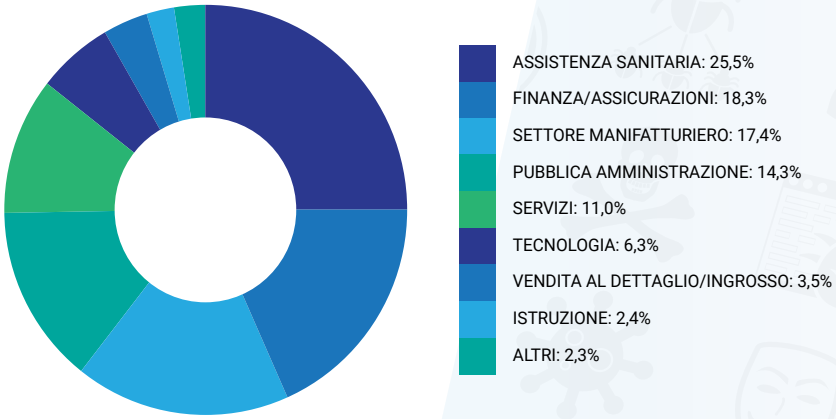


Figura 2: *minacce avanzate bloccate sui canali criptati per settore*

Nonostante la pandemia globale abbia reso i loro servizi più importanti che mai, le organizzazioni sanitarie sono state prese di mira dal maggior numero di minacce distribuite tramite canali criptati. Gli aggressori hanno anche sfruttato la pandemia per lanciare nuove campagne, con siti contraffatti che offrivano notizie, prodotti e cure. Nei primi tre mesi del 2020, ThreatLabz ha riferito un picco del **30.000%** di minacce correlate al COVID.

Focus settoriale sulla sanità

Il settore sanitario è stato il bersaglio di oltre 1,69 miliardi di tentativi di attacchi su canali criptati più di qualsiasi altro settore. La stragrande maggioranza degli attacchi contro questo settore è avvenuta tramite URL dannosi (84,2%). Gli URL dannosi possono essere consegnati agli utenti tramite e-mail, messaggi di testo, popup o annunci pubblicitari sulla pagina, con conseguente download di malware, spyware, ransomware, compromissione degli account e altro ancora.

Il settore sanitario è spesso il bersaglio di attacchi informatici, a causa della presenza di sistemi legacy (per via della prolungata approvazione da parte della FDA) nell'ambiente. Tali sistemi legacy non dispongono di controlli di sicurezza e sono spesso soggetti ai problemi noti. Senza controlli unificati, visibilità e applicazione delle policy centralizzate, tali organizzazioni finiscono per ritrovarsi con delle lacune nei controlli di sicurezza, che i criminali informatici tentano di sfruttare.

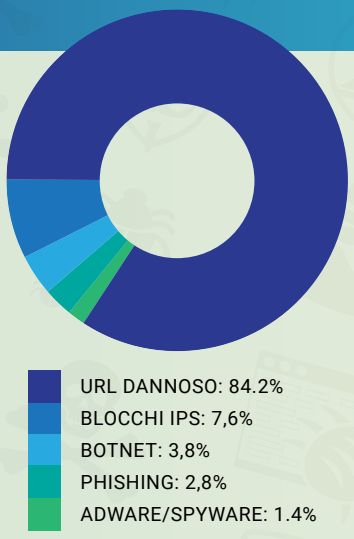


Figura 3: *minacce tramite canali criptati indirizzate al settore sanitario*

Gli attacchi stanno diventando sempre più avanzati

Gli utenti vengono spesso avvisati dai professionisti IT di controllare attentamente l'URL di un sito falso o sospetto per ricercare la presenza di errori, errori ortografici o altri indicatori che potrebbero confermarne la non legittimità. Oggigiorno i criminali informatici stanno sfruttando tecniche, come il domain squatting (appropriazione indebita di nomi di dominio) e l'attacco omografico IDN, per far apparire i loro siti praticamente indistinguibili da quelli reali.

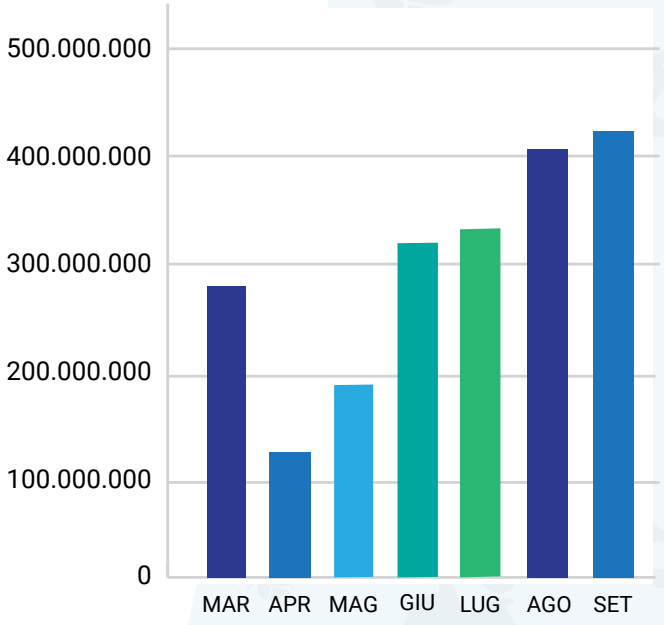
Il domain squatting consiste nel registrare un dominio di primo livello simile a un marchio noto (ad esempio gmali.com) allo scopo di erogare attacchi di phishing, rubare credenziali o distribuire malware.

Un attacco omografo, come il domain squatting, viene usato per ingannare le persone portandole a cliccare sui link utilizzando caratteri, come il numero "1" invece di una lettera "l" nell'URL di Apple (https://www.app1e.com).

Abuso dei servizi di archiviazione cloud

I servizi di archiviazione cloud sono emersi come un mezzo molto popolare di attacco. Tali servizi sono ottimi per la condivisione sicura dei file tramite trasmissione basata su SSL sul web. Ma dal momento che i criminali informatici sanno che la maggior parte delle organizzazioni non è in grado di ispezionare il traffico SSL su larga scala e che i servizi cloud sono generalmente "attendibili", lanciano attacchi che sembrano provenire da questi servizi.

Da marzo a settembre 2020, il cloud Zscaler ha bloccato **due miliardi di minacce** nel traffico criptato, la maggior parte delle quali riguardava contenuti dannosi ospitati su Google, AWS, Dropbox e OneDrive. Queste minacce sono quasi raddoppiate tra marzo e settembre e rappresentavano quasi il 30% di tutte le minacce SSL/TLS criptate in quei mesi.



Da marzo a settembre, il cloud Zscaler ha bloccato **due miliardi di minacce** nel traffico SSL, provenienti dai provider di servizi di archiviazione cloud.

Figura 4: *minacce avanzate bloccate su TLS/SSL provenienti dai principali servizi di archiviazione cloud*

La Figura 5 mostra come i servizi cloud vengano sfruttati per ospitare e distribuire malware. I criminali informatici predispongono il carico utile del malware (spesso un file downloader di fase 1) su uno o più servizi e distribuiscono gli URL come parte di una campagna di spam via e-mail. L'utilizzo di servizi leader come Google, Microsoft, Amazon e Dropbox migliora le possibilità che gli utenti finali facciano clic sul link.

I criminali informatici sfruttano inoltre i certificati SSL con caratteri jolly appartenenti a tali fornitori di servizi. Se il traffico dei provider di servizi cloud viene considerato sicuro e non viene controllato, i malintenzionati hanno gioco facile nel distribuire un carico utile di malware sui canali criptati ed eludere le soluzioni di sicurezza basate sul filtro URL, come anti-spam, protezione dell'e-mail, firewall e altro ancora. **Un'e-mail di phishing con un collegamento a un file dannoso, ospitato in un servizio affidabile con base cloud, può eludere le tradizionali soluzioni di sicurezza della posta elettronica.**

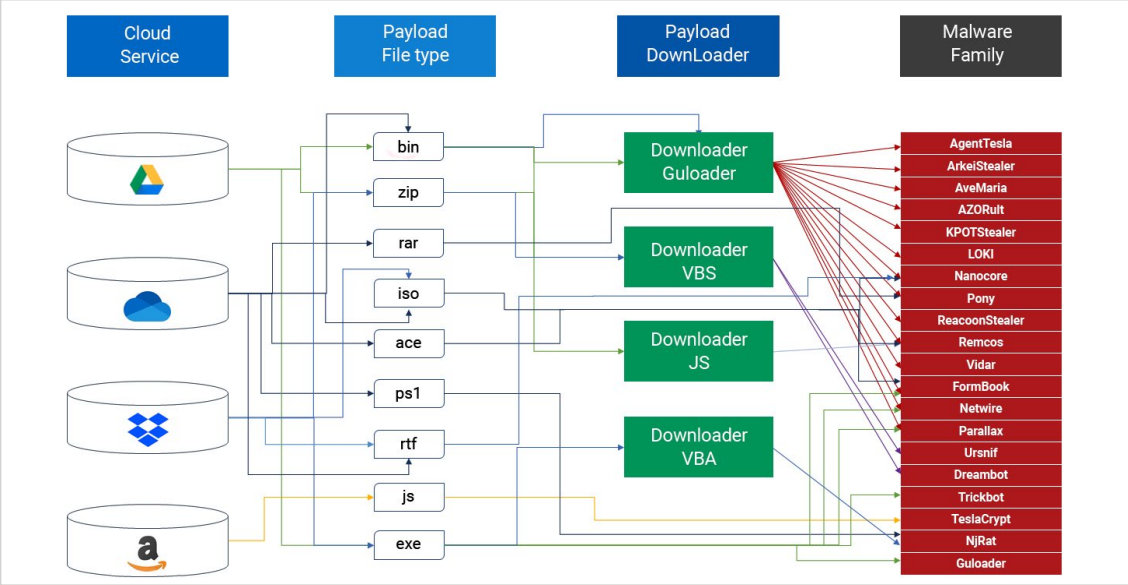


Figura 5: *carico utile di malware fornito tramite servizi cloud*

L'esempio seguente mostra gli URL del servizio di archiviazione cloud OneDrive. In questo esempio, i primi due URL sono dannosi e comportano il download di malware appartenenti alle famiglie "Trojan EdLoader" e "Backdoor LokiBot". Tuttavia, il terzo URL è legittimo e scarica il file effettivo dell'utente. Il sottodominio e l'URI (Uniform Resource Identifier) vengono visualizzati come schemi di stringhe casuali, che rendono impossibile distinguere gli URL legittimi da quelli dannosi. L'ispezione SSL è l'unico modo efficace per bloccare i file dannosi che vengono diffusi utilizzando questi servizi, poiché i sistemi di sicurezza non sono in grado di bloccare quello che non riescono a vedere.

Figura 6: *stringhe casuali nei sottodomini rendono impossibile distinguere gli URL dannosi da quelli legittimi*

Attacchi mobili

Anche gli smartphone sono diventati dei bersagli popolari. Allo stesso modo in cui i criminali informatici contraffanno le pagine web, creano app false che sembrano legittime. Ad esempio, un trojan bancario Android chiamato Cerberus utilizza un nome e un'icona di un'applicazione per imitare la legittima applicazione Google Play. Dopo che un utente ignaro fa clic sull'app falsa, invia una notifica per ottenere il l'autorizzazione al "servizio di accessibilità". (il servizio di accessibilità assiste gli utenti con disabilità nell'utilizzo di dispositivi Android e app).

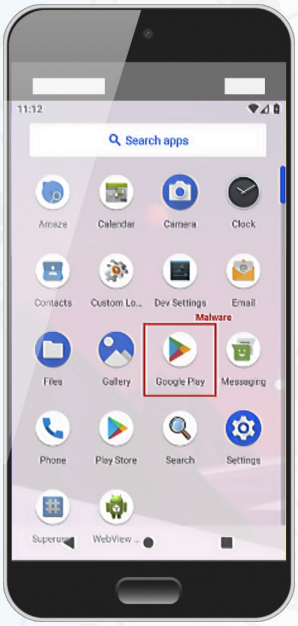


Figura 7: *app Google Play contraffatta*

Capita cosi' che molti utenti "accettino" una notifica senza leggerla attentamente. In questo caso, facendo clic su "Consenti", si consente all'app di vedere il contenuto di altre app visualizzate sullo schermo ed eseguire una varietà di azioni, senza che l'utente ne sia a conoscenza.

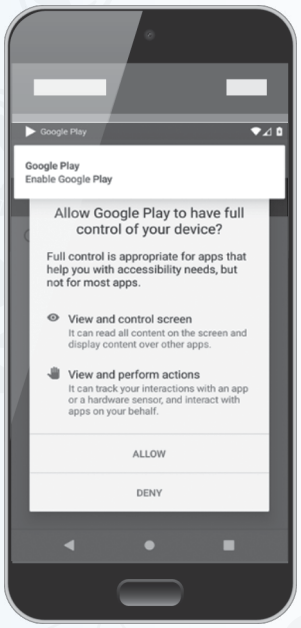
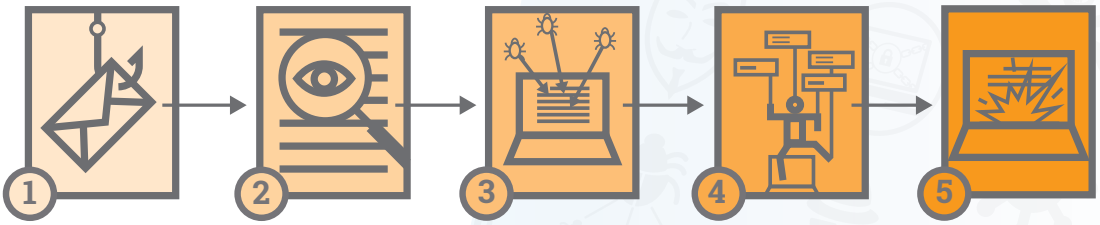


Figura 8: *notifica sull'app Google Play contraffatta*

Il malware si appropria delle credenziali delle app bancarie, di Gmail o dell'autenticazione a due fattori di Google, quindi le esfiltra. Può anche intraprendere altre azioni malevoli, come rubare delle registrazioni audio e messaggi di testo. Ma può andare peggio. Dopo che viene consentita al malware l'autorizzazione al servizio di accessibilità, il medesimo può impedire all'utente di disabilitare l'autorizzazione e può rendere difficile la disinstallazione dell'app.

Anatomia di un attacco



La consegna può includere un'e-mail di phishing con un exploit o un malware nascosto all'interno. Il malware viene consegnato quando un utente lo scarica o fa clic su un link nell'e-mail.

Lo sfruttamento è ciò che accade quando il programma cerca le vulnerabilità che può sfruttare nel sistema ed eseguire il codice.

L'installazione si verifica quando il malware viene caricato sul computer della vittima.

Un callback C&C (Command-and-control) si ha quando il malware tenta di comunicare con i server C&C, spesso per ottenere istruzioni o inviare dati rubati.

La detonazione è il passaggio in cui il malware può installare malware aggiuntivo, esfiltrare dati o eseguire altre azioni programmate dal server C&C.

Analisi della catena di attacco

Phishing

Poiché il phishing è, in genere, la prima fase di un attacco informatico multifase che comporta il furto di credenziali, abbiamo analizzato gli oltre **193 milioni di tentativi di phishing** forniti su canali criptati, ma identificati e bloccati dal cloud Zscaler tra gennaio e settembre 2020. Abbiamo analizzato i tentativi per verticalità di settore. Con le singole strutture che spesso utilizzano infrastrutture e sistemi IT diversi (il che le rende potenzialmente più vulnerabili), il settore manifatturiero è stato l'obiettivo più bersagliato e ha ricevuto il 38,6% dei tentativi di phishing, seguito dal settore dei servizi con il 13,8%.

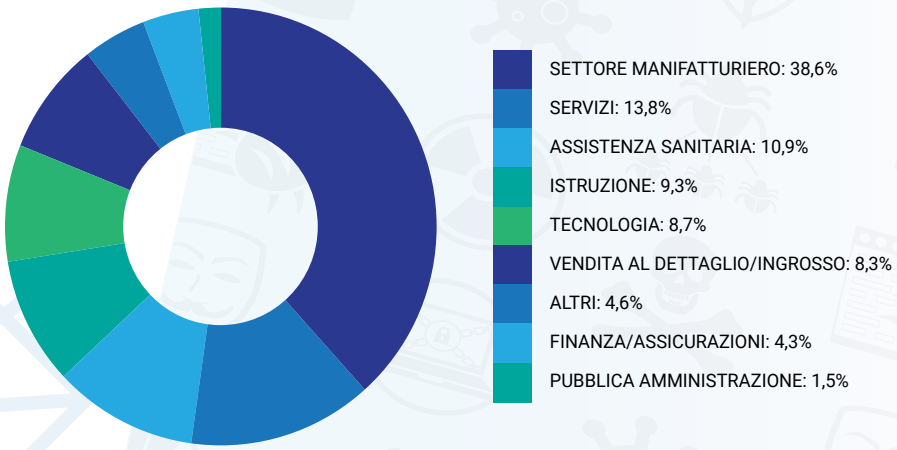


Figura 9: *minacce di phishing bloccate sui canali criptati per settore*

Servizi aziendali e marchi oggetto di phishing

Un tentativo di phishing include spesso un sito web falsificato che imita un marchio preso di mira. In altre parole, arriva un'e-mail e indica all'utente di fare clic su un link che lo porta su un sito falso. A quel punto all'utente viene richiesto di inserire un nome utente/password o altre informazioni importanti, che possono essere utilizzate dai criminali informatici per portare a termine degli attacchi.

La nostra ricerca ha riscontrato che il marchio più soggetto a phishing è stato Microsoft. Gli attacchi sono dotati di varie proprietà Web a tema Microsoft (Office 365, SharePoint, OneDrive e così via), con cui i criminali informatici cercano di rubare le credenziali dei servizi aziendali. Il secondo attacco di phishing più diffuso riguardava truffe di "Supporto tecnico", che, in genere, utilizzano un reindirizzamento Web dannoso da siti Web compromessi che dichiarano che la macchina dell'utente è stata violata e che il "supporto Microsoft" risolverà il problema (una volta che le informazioni della carta di credito sono state inviate dall'utente).

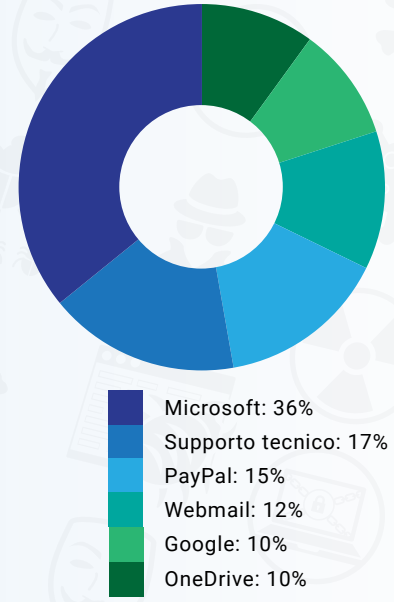


Figura 10: *marchi e servizi aziendali più frequentemente oggetto di phishing*

Anche PayPal e Google sono stati tra i principali marchi falsificati da tali attacchi di phishing. I siti contraffatti sembrano sinistramente simili ai siti reali, rendendo difficile individuare le differenze.

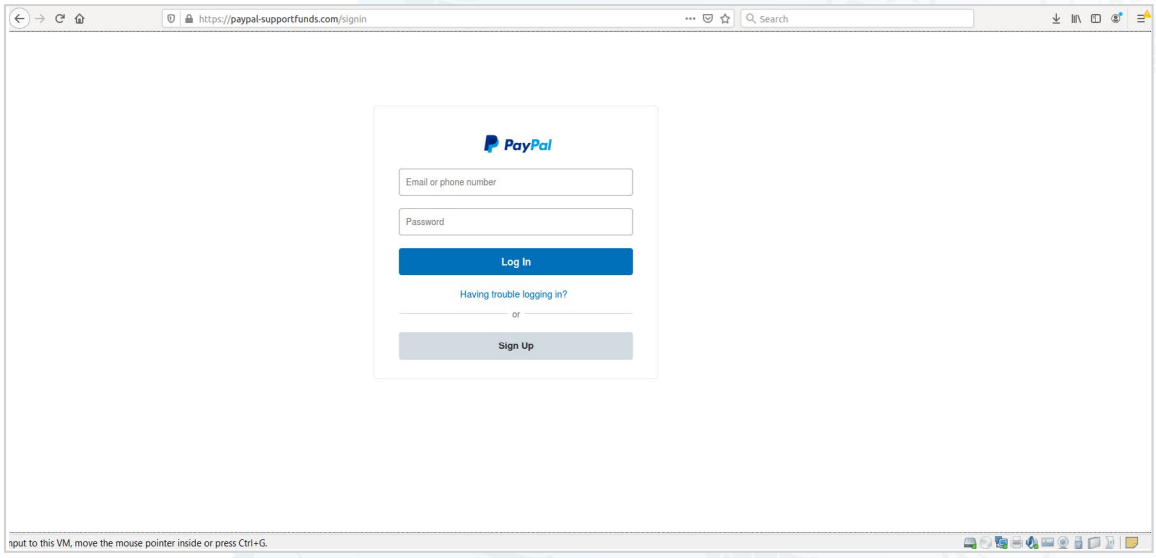


Figura 11: *il sito di phishing di PayPal su HTTPS*

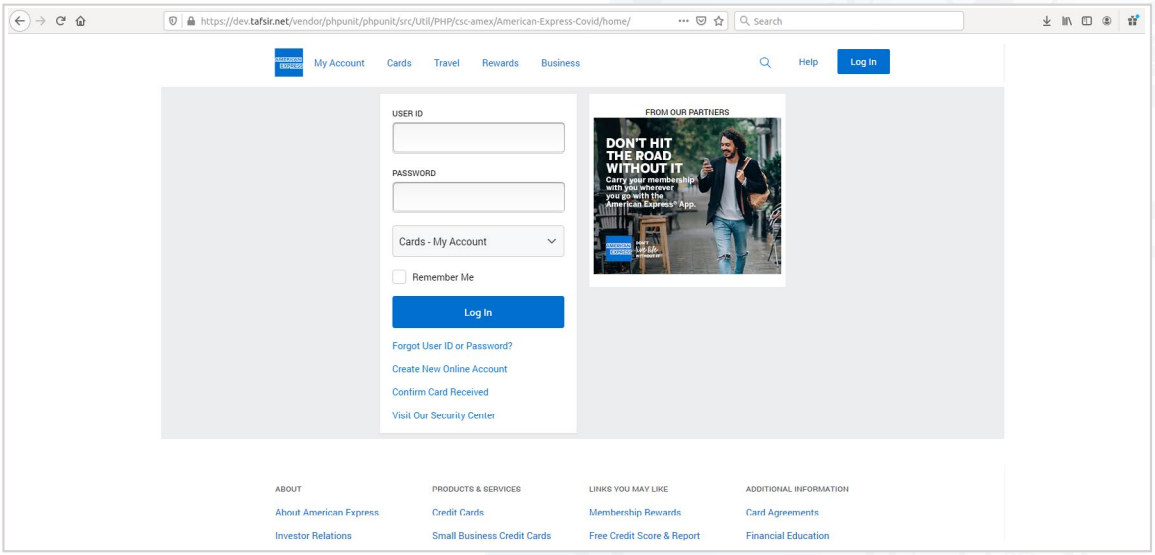


Figura 12: *sito di phishing di American Express su HTTPS*

Phishing di Netflix su HTTPS

L'utilizzo di servizi di intrattenimento in streaming, come Netflix, è aumentato durante la pandemia e gli aggressori informatici l'hanno notato. I malintenzionati colpiscono i servizi di streaming per appropriarsi delle credenziali dell'utente attraverso il phishing, e, come si vede nella Figura 13, è difficile distinguere tali pagine false da quelle reali.

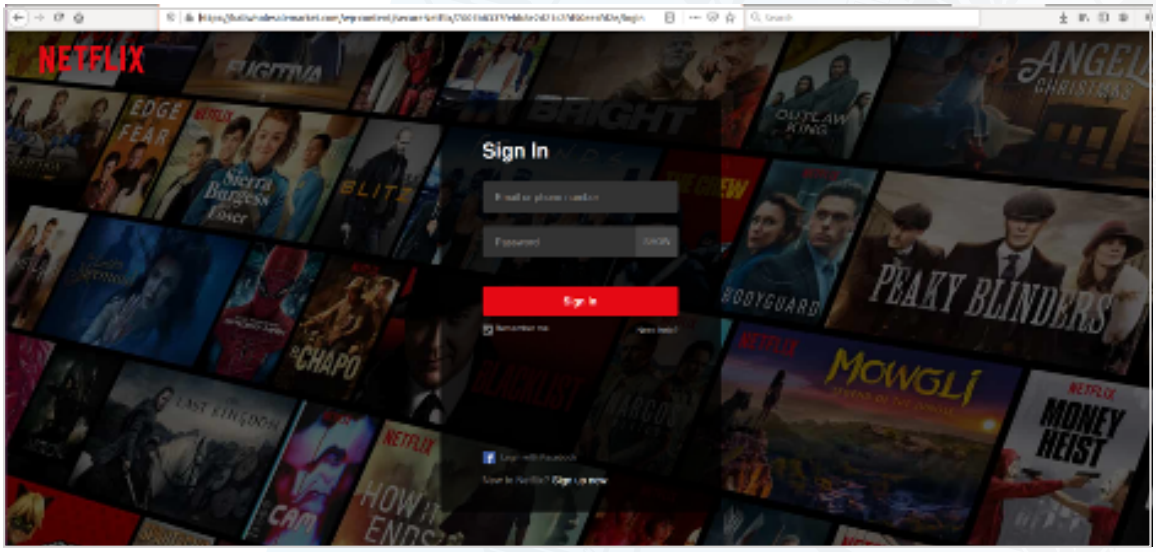


Figura 13: *immagine del phishing di Netflix*

Truffa di supporto tecnico su HTTPS rivolta agli utenti Microsoft

La Figura 14 mostra una pagina truffaldina del supporto tecnico Microsoft. Facendo clic sull'URL viene visualizzato il certificato HTTPS verificato da Microsoft. Il certificato in uso mostra che gli aggressori utilizzano Azure (un altro marchio noto) nel tentativo di enfatizzare la parvenza che si tratti di una pagina legittima inviata da Microsoft.

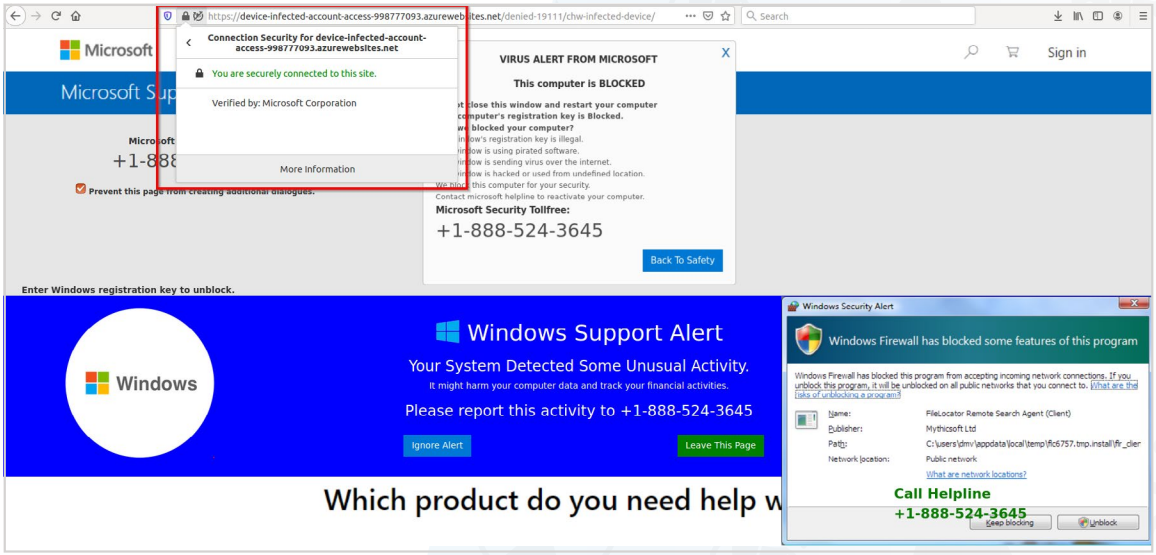


Figura 14: *truffa del supporto tecnico su HTTPS rivolta agli utenti Microsoft*

Exploit del browser

Gli exploit del browser consentono agli aggressori di sfruttare una vulnerabilità in un sistema operativo e modificare le impostazioni del browser di un utente all'insaputa di quest'ultimo. Il cloud Zscaler ha bloccato più di 658.000 minacce di sfruttamento dei browser, rivolte al settore manifatturiero (26,5%) e finanziario/assicurativo (19,9%), che rappresentano gli obiettivi principali.

L'industria manifatturiera è stata spesso l'obiettivo di attacchi informatici perché (almeno tradizionalmente) questo settore si è rivelato altamente frammentato, con singole strutture, ciascuna che utilizzava infrastrutture IT diverse e più sistemi disgiunti. Come in altri settori senza controlli unificati e visibilità e applicazione delle policy centralizzate, la sicurezza è incompleta e i criminali informatici continuano a sfruttare questi buchi.

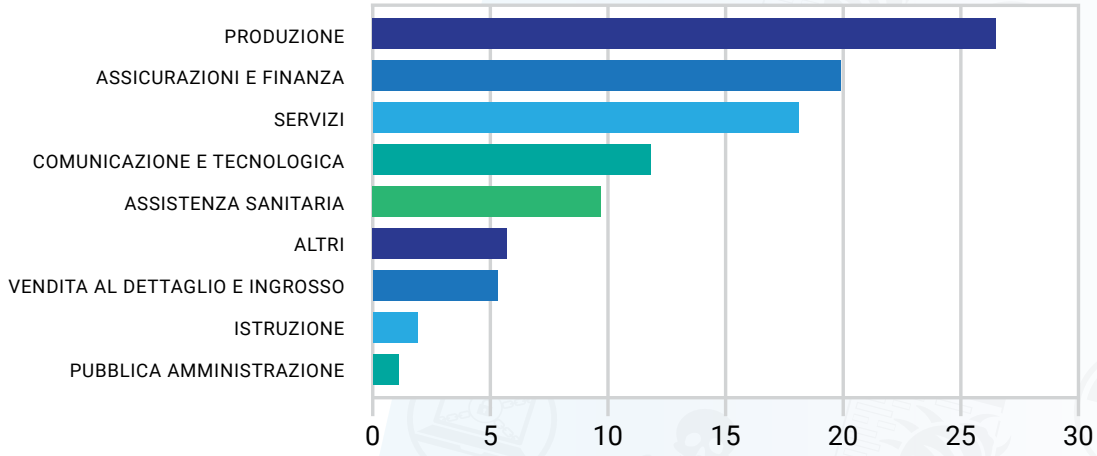


Figura 15: *exploit dei browser bloccati sui canali criptati per settore*

Ransomware

Zscaler ThreatLabz ha visto aumentare gli attacchi ransomware erogati sui canali SSL/TLS del 500% da marzo 2020. Con la maggior parte dei dipendenti che lavorano in remoto e accedono alle applicazioni interne, si è rilevato un incremento delle attività di ransomware mirate alle verticalità dei settori più a rischio e più facilmente spinti a pagare eventuali riscatti.

Tecnologia e comunicazione (40,5) e sanità (26,5) sono state tra le verticalità di settore più colpite dagli attacchi ransomware su canali criptati.

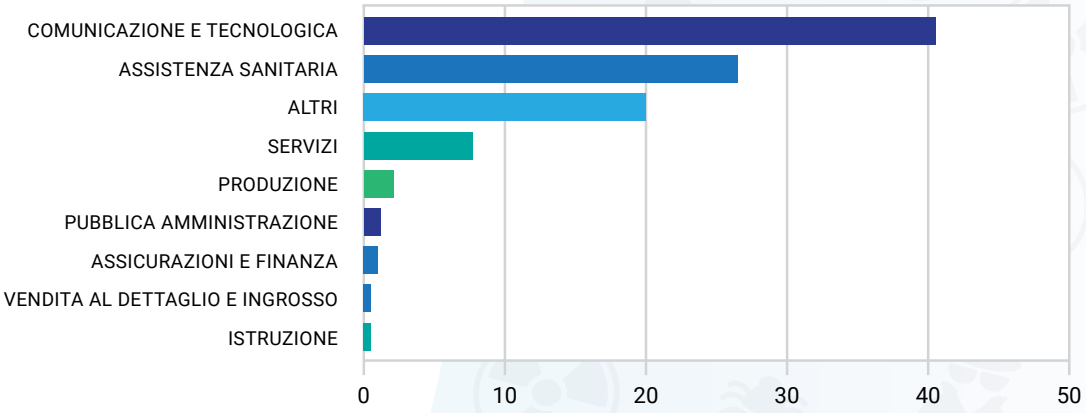


Figura 16: *ransomware bloccati su canali criptati per settore*

Le principali famiglie di ransomware viste in questi attacchi includono le varianti FileCrypt/FileCoder, seguite dalle varianti della famiglia Sodinokibi, Maze e Ryuk. Un cambiamento notevole evidenziato in molte di queste varianti di famiglie di ransomware durante l'ultimo anno consiste nell'aggiunta di una funzione di esfiltrazione dei dati. Questa nuova funzionalità consente alle bande ransomware di esfiltrare i dati sensibili dalle vittime, prima di crittografare i dati. Questi dati esfiltrati sono come una polizza assicurativa per gli aggressori: anche se l'organizzazione colpita ha dei buoni backup, pagherà il riscatto per evitare che i propri dati vengano esposti.

Malware

Il malware è un mezzo persistente, che consente a un criminale informatico di avere un accesso continuo alla macchina di una vittima. Il malware viene spesso installato dopo aver sfruttato con successo delle vulnerabilità o tramite attacchi di ingegneria social. È di gran lunga il tipo di attacco più spesso rilevato dai ricercatori di Zscaler, con oltre **2,6 miliardi di minacce malware** bloccate durante la nostra analisi.

I settori che gestiscono informazioni di identificazione personale (PII) sono frequenti obiettivi dei malware. Nella nostra analisi la sanità e il settore finanziario/assicurazioni hanno visto il maggior numero di attacchi malware bloccati su canali criptati, rispettivamente al 27,4 e al 19,6%.

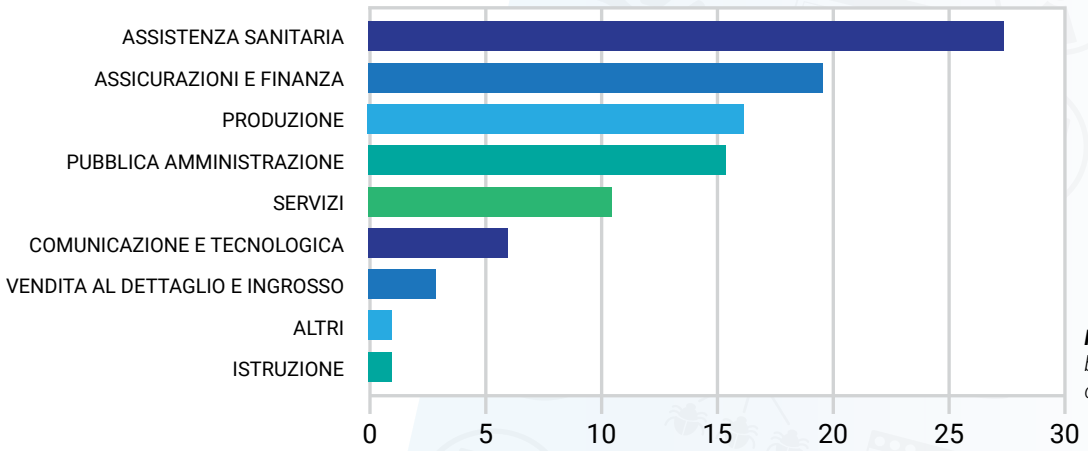


Figure 17: *malware bloccati sui canali criptati per settore*

Attività C&C (command-and-control) di malware su canali crittografati

La comunicazione C&C è un'altra parte chiave della catena di attacco. Se il malware ha eluso il rilevamento ed è stato installato con successo sul dispositivo di un utente finale, richiama il server C&C per iniziare a esfiltrare dati e lanciare ulteriori attacchi. I carichi di lavoro dei malware sono spesso programmati per rimanere dormienti e attendono i comandi dal server, prima di avviare qualsiasi attività dannosa. Emotet e TrickBot sono state le due famiglie di malware più diffuse osservate durante la nostra analisi.

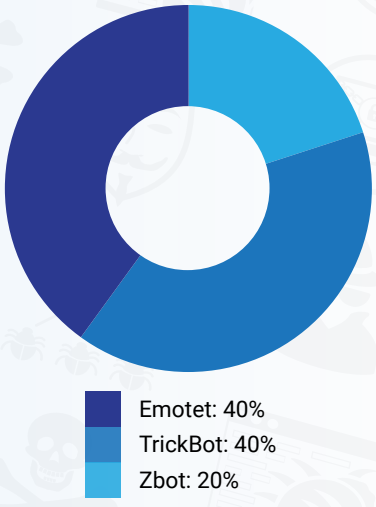


Figura 18: *attività C&C più comunemente bloccata sui canali crittografati*

Oltre a Emotet e TrickBot, abbiamo visto attività da Ursnif e Unruy. Emotet è stato il più utilizzato in tutti i settori, mentre TrickBot è stato il secondo tipo di malware più comunemente usato nel settore finanziario/assicurazioni e pubblica amministrazione. Ursnif è stato più spesso rilevato negli attacchi rivolti al settore sanitario e manifatturiero, mentre Unruy è stato il secondo tipo di malware più utilizzato negli attacchi indirizzati contro le istituzioni scolastiche.

Conoscere meglio i malware

Emotet: Emotet ha iniziato come trojan bancario nel 2014. In seguito si è trasformato in una minaccia molto rilevante, utilizzata principalmente per lo spam e il download di malware sui sistemi bersaglio. La CISA (U.S. Cyber Infrastructure Security Agency) ha definito Emotet tra i ceppi malware **più costosi e distruttivi** che interessano sia il settore pubblico che quello privato. Emotet ha dimostrato di essere resiliente e modulare, con miglioramenti regolari che ne rendono difficile il rilevamento da parte delle organizzazioni.

TrickBot: TrickBot è un successore del trojan bancario Dyre ed è diventato uno dei ceppi di malware più diffusi e pericolosi nel panorama delle minacce odierne. Spesso visto cooperare con altri tipi di malware, TrickBot è talvolta usato come un vettore di infezione iniziale, che trova la sua strada nell'host bersaglio o scarica altre famiglie di malware per ottenere il massimo da un'infezione.

Ursnif: il trojan Ursnif è una delle varianti più attive e prevalenti della famiglia di malware Gozi, conosciuta anche come Dreambot. Questo trojan è spesso diffuso da kit di exploit, allegati alle e-mail e link dannosi.

Unruy: Unruy è un trojan che visualizza annunci pubblicitari fuori contesto ed esegue clic su annunci al fine di raccogliere entrate per i suoi controller. Comunica con host in remoto e può anche scaricare ed eseguire file arbitrari per portare avanti le proprie attività.

Cos'è necessario per prevenire le minacce criptate

È sempre più importante riconoscere che il traffico SSL non è necessariamente sinonimo di traffico sicuro. Cosi' come è aumentato l'uso della crittografia, così è stato anche per il relativo utilizzo da parte degli avversari, per nascondere i loro attacchi. La necessità di ispezionare il traffico criptato è più vitale che mai. Molte organizzazioni seguono le procedure consigliate per la sicurezza e criptano il proprio traffico Internet. Tuttavia gli strumenti legacy, come i firewall di nuova generazione, spesso non dispongono delle prestazioni e della capacità di ispezionare il traffico SSL su larga scala. Nessuno può permettersi di arrestare le operazioni e i flussi di lavoro e pertanto molti team IT consentono alla maggior parte del traffico criptato di passare senza essere ispezionato.

Inoltre, esistono norme rigorose in merito al modo in cui le organizzazioni devono trattare i dati contenenti informazioni personali su clienti, pazienti e così via. Creare policy separate relative al modo in cui degli specifici tipi di dati devono essere ispezionati e replicarle in posizioni diverse è un'attività difficile e pertanto le organizzazioni spesso ignorano completamente questo processo.

Quindi, come è possibile proteggere la propria organizzazione dai pericoli nascosti nel traffico criptato senza intaccare le prestazioni? Con la maggior parte del traffico aziendale che oggi è criptato, come si può essere sicuri di decrittografare e ispezionare tutto, preservando la conformità per tutti gli utenti, dentro e fuori dalla rete?

- **Decrittografare, rilevare e prevenire le minacce in tutto il traffico SSL** con un proxy nato sul cloud, in grado di ispezionare tutto il traffico per ogni utente.
- **Mettere in quarantena gli attacchi sconosciuti e bloccare il malware paziente zero** con una quarantena basata sull'IA che confina i contenuti sospetti per sottoporli all'analisi, a differenza degli approcci passthrough basati su firewall.
- **Garantire una sicurezza coerente a tutti gli utenti e in tutte le sedi,** per assicurare che tutti dispongano dello stesso livello ottimale di sicurezza in ogni momento, sia che siano a casa, in sede centrale o in viaggio.
- **Ridurre istantaneamente la superficie di attacco,** partendo da una posizione di zero trust, dove il movimento laterale non può esistere. Le app sono invisibili agli aggressori e gli utenti autorizzati accedono direttamente alle risorse necessarie, non all'intera rete.

Questa soluzione richiede scalabilità e prestazioni che possono essere fornite solo da un'architettura nata sul cloud, basata su proxy, come Zscaler Zero Trust Exchange. Una piattaforma di sicurezza con base cloud soddisfa i requisiti di decrittografia e ispezione scalando elasticamente le risorse di elaborazione, e fornisce un'applicazione coerente delle policy in più sedi. Zscaler esegue l'ispezione SSL su larga scala come parte della propria piattaforma di servizi e, con l'aumentare del traffico, la capacità viene aggiunta istantaneamente e su richiesta: non ci sono apparecchi di applicazione da dimensionare, ordinare o spedire.

Nessun settore è immune alle minacce alla sicurezza. E dato che sempre più traffico viene criptato, ispezionare quel traffico è diventato un fattore mission-critical. Una strategia multifase di difesa in profondità, che supporti totalmente l'ispezione SSL, è essenziale per garantire che le aziende siano protette dall'escalation delle minacce che si nascondono nel loro traffico criptato.

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

Informazioni su ThreatLabZ

ThreatLabZ è il laboratorio di ricerca sulla sicurezza di Zscaler. Il suo Team di alto livello è responsabile della ricerca di nuove minacce, nonché garantisce la protezione costante delle migliaia di organizzazioni che utilizzano la piattaforma globale Zscaler. Oltre alla ricerca di malware e all'analisi comportamentale, i membri del team sono coinvolti nella ricerca e nello sviluppo di nuovi moduli prototipo per la protezione avanzata dalle minacce e conducono regolarmente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler soddisfino gli standard di conformità della sicurezza. ThreatLabZ pubblica regolarmente sul suo portale delle analisi approfondite delle 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 in linea del mondo. Scopri di più su zscaler.com o seguici su Twitter **@zscaler**.

zscaler™