Il Report “State of Encrypted Attacks 2021” di Zscaler rivela un'impennata del 314% delle minacce al protocollo HTTPS

Il massiccio aumento degli attacchi informatici contro il settore della tecnologia e della vendita al dettaglio conferma la necessità immediata di una sicurezza Zero Trust

Risultati principali

- *Le minacce sul protocollo HTTPS sono aumentate del 314% rispetto all'anno precedente, superando una crescita del 250% per il secondo anno consecutivo.*
- *Gli attacchi contro le aziende di tecnologia sono aumentati del 2.300% rispetto all'anno precedente; gli attacchi contro le aziende di vendita al dettaglio e all'ingrosso sono aumentati dell'800%.*
- *Gli attacchi contro i settori della sanità e della pubblica amministrazione sono in calo rispetto all'anno precedente.*
- *Regno Unito, Stati Uniti, India, Australia e Francia sono i primi cinque obiettivi degli attacchi crittografati.*
- *Il malware è aumentato del 212%, il phishing del 90%, mentre gli attacchi di cryptomining sono diminuiti del 20%.*

Milano, 12 novembre 2021 - Zscaler, Inc. (NASDAQ: ZS), leader nella sicurezza cloud, ha annunciato oggi il rilascio del suo report annuale “State of Encrypted Attacks” che ha tracciato e analizzato oltre 20 miliardi di minacce bloccate sul protocollo HTTPS, originariamente progettato per la comunicazione sicura sulle reti. Lo studio di quest'anno ha riscontrato un aumento di oltre il 314% rispetto all'anno precedente nelle aree geografiche che includono Asia-Pacifico, Europa e Nord America, sottolineando la necessità di un modello di sicurezza Zero Trust e di una maggiore ispezione del traffico rispetto a quanto la maggior parte delle aziende possa fare con i modelli di sicurezza basati su firewall tradizionali.

Zero Trust Exchange di Zscaler analizza più di **190 miliardi di transazioni giornaliere**, estraendo oltre **300 trilioni di segnali** che forniscono visibilità sui dati aziendali su una scala senza pari. Il team di ricerca di ThreatlabZ ha sfruttato questa grande quantità di dati per fornire approfondimenti specifici sui rischi per la sicurezza derivanti dai canali crittografati nei settori chiave. Sette tra i settori coinvolti nello studio hanno sperimentato tassi di attacco più elevati provenienti da minacce nel traffico SSL e TLS, mentre il settore più bersagliato dello scorso anno, quello sanitario, ha visto una diminuzione del 27% a partire da gennaio 2021. Al contrario, con il 50% degli attacchi, il settore tecnologico è stato afflitto da un tasso di minacce molto più alto rispetto ad altre tipologie di aziende. Oggi nelle realtà aziendali, più dell'80% del traffico Internet è crittografato, il che significa che le imprese devono garantire una sicurezza completa a tutti i loro telelavoratori. I criminali informatici utilizzano tattiche sempre più sofisticate, e stanno sfruttando canali crittografati nelle varie fasi degli attacchi malware e ransomware.

"*La maggior parte dei team IT e della sicurezza delle aziende riconoscono questa realtà, ma spesso si trovano in difficoltà nell’implementare le policy di ispezione del traffico SSL/TLS a causa della mancanza di risorse di calcolo e/o di preoccupazioni per la privacy*", ha dichiarato **Deepen Desai, CISO e VP Security Research and**

Operations di Zscaler. "*Di conseguenza, i canali crittografati creano un punto cieco significativo nel loro livello di sicurezza. Il nuovo report di Zscaler sullo stato degli attacchi crittografati dimostra che il modo più efficace per prevenire tali minacce è tramite un'architettura proxy scalabile e basata sul cloud per ispezionare tutto il traffico crittografato, essenziale per una strategia globale di sicurezza zero trust*".

Il crimine informatico ai massimi storici

Tra gennaio e settembre 2021, Zscaler ha bloccato più di 20 miliardi di minacce su HTTPS, il valore è aumentato del 314% in più rispetto all'anno precedente. I criminali informatici stanno diventando sempre più scaltri e hanno beneficiato di reti di affiliazione e degli strumenti malware-as-a-service disponibili sul dark web.

I criminali informatici possono usare vari tipi di attacchi per nascondersi nel traffico crittografato ma i contenuti pericolosi hanno rappresentato uno sbalorditivo 91% degli attacchi, un aumento del 212% rispetto all'anno scorso. Al contrario, il malware cryptomining è sceso del 20%, riflettendo un cambiamento più ampio nelle tendenze di attacco, con il ransomware che diventa l'opzione più redditizia.

Settore tecnologico sotto assedio

Il report svela che gli attacchi contro le aziende del settore tecnologico, al dettaglio e all'ingrosso hanno visto un aumento significativo delle minacce. Gli attacchi contro il settore della tecnologia sono aumentati di uno sbalorditivo 2.300%, mentre il settore della vendita al dettaglio e all'ingrosso ha visto gli attacchi aumentare di oltre l'800%. Poiché un maggior numero di rivenditori offre l'opportunità di fare shopping online durante la stagione degli acquisti natalizi, ci si aspetta che i criminali informatici prenderanno di mira più soluzioni di ecommerce e piattaforme di pagamento digitale con malware e attacchi ransomware. Tale situazione, è esacerbata dall'improvvisa necessità di supportare i telelavoratori con connettività da remoto per app di teleconferenza e i carichi di lavoro del cloud pubblico.

Le aziende tecnologiche sono un obiettivo allettante anche a causa del loro ruolo nella supply chain. Un attacco di successo alla catena di approvvigionamento come accaduto nei casi Kaseya e SolarWinds può fornire ai criminali informatici l'accesso a un insieme prezioso di informazioni sugli utenti. Inoltre, mentre il mondo inizia il suo ritorno alla normalità, le imprese e stanno riaprendo e gli eventi in presenza stanno ripartendo in tutto il mondo, molti dipendenti lavorano ancora in ambienti non sufficientemente protetti. Riusciere a ottenere l'accesso ai sistemi critici dei punti vendita è estremamente allettante per i criminali informatici, perché può portare ingenti guadagni.

In calo gli attacchi ai servizi essenziali

Gli attacchi alle strutture sanitarie – tra i più numerosi nel 2020 - sono diminuiti del 27% nel corso del 2021. Allo stesso modo, gli attacchi contro il settore della pubblica amministrazione sono diminuiti del 10%. Gli attacchi ransomware che hanno preso di mira i servizi essenziali, tra cui quello che ha colpito Colonial Pipeline e l'Health Services Executive dell'Irlanda, hanno attirato l'attenzione dei più alti livelli governativi, compresa la Casa Bianca, che ha recentemente firmato un ordine esecutivo per migliorare la sicurezza informatica della nazione.

"Dopo essere stati i più frequentemente presi di mira nel 2020, i settori della sanità e della pubblica amministrazione si sono trovati con l'urgenza di rinnovare i loro standard di sicurezza con architetture moderne, che si basano in gran parte sull'approccio Zero Trust. C'è stato anche un aumento delle attività di controllo da parte del governo e un giro di vite delle forze dell'ordine sui gruppi di criminali informatici in risposta agli attacchi di alto profilo contro servizi critici come quello al sistema di oleodotti Colonial Pipeline",

ha affermato Desai. "Come risultato di questi due fattori, quest'anno abbiamo osservato una diminuzione degli attacchi contro gli enti governative e le strutture sanitarie".

Altri Paesi presi di mira

Zscaler ThreatLabz ha osservato attacchi in oltre 200 paesi e territori in tutto il mondo, compresi piccoli paesi che non sono obiettivi comuni come le isole dei Caraibi. Inoltre, la diffusione del telelavoro ha portato i dipendenti a trovarsi in luoghi fuori dai soliti grandi hub tecnologici come la San Francisco Bay Area, New York, Londra, Parigi, Sydney.

I cinque paesi più colpiti dagli attacchi crittografati includono il Regno Unito (5.446.549.767), gli Stati Uniti (2.674.879.625), l'India (2.169.135.553), l'Australia (1.806.003.182) e la Francia (519.251.819).

Nel complesso, l'Europa è in testa con 7.234.747.361 attacchi, seguita da Sud Est asiatico (4.924.732.36) e Nord America (2.778.360.051).

Proteggere la propria azienda

Man mano che le aziende supportano i nuovi modelli di lavoro abilitati al digitale, è sempre più importante garantire che le loro risorse e il traffico verso tali risorse siano sicuri. Per ridurre la minaccia degli attacchi crittografati, Zscaler ThreatLabz raccomanda l'adozione di una strategia di sicurezza Zero Trust che permetta di:

- **Prevenire le violazioni:** sicurezza completa per tutti gli utenti e tutte le sedi per garantire che tutti abbiano sempre lo stesso livello di sicurezza, che siano a casa, in ufficio o all'estero. Utilizzare un'architettura cloud-native e basata su proxy per ispezionare tutto il traffico per ogni utente e decifrare, rilevare e prevenire le minacce che possono nascondersi nel traffico HTTPS.
- **Prevenire gli spostamenti laterali:** l'utilizzo di un'architettura Zero Trust con funzionalità di deception per ridurre la superficie di attacco e prevenire i movimenti laterali dei criminali informatici. Questo tipo di architettura rende le applicazioni invisibili agli aggressori mentre permette agli utenti autorizzati di accedere direttamente alle risorse necessarie e non all'intera rete.
- **Prevenire la perdita dei dati:** quarantena degli attacchi sconosciuti o delle app compromesse in un ambiente sandbox basato sull'intelligenza artificiale per fermare malware e ransomware. A differenza degli approcci basati sul firewall, questo trattiene tutti i contenuti sospetti per l'analisi, assicurando che i tentativi di violazione vengano fermati prima che siano in grado di accedere ai sistemi sensibili e rubare informazioni critiche per l'operatività aziendale.

Il report completo può essere scaricato qui.

Metodologia

Il team di ThreatLabz ha analizzato i dati del cloud di sicurezza Zscaler, che monitora oltre 190 miliardi di transazioni al giorno in tutto il mondo. Zscaler ha bloccato oltre 20,7 miliardi di minacce trasmesse tramite canali crittografati da gennaio 2021 a settembre 2021.

A proposito di 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 da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basato su SASE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi

Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it

Tel. +39 02 91339811