Boom di vendite online di accessi (hackerati) alle reti

Feb 11, 2021 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS, Scenario 0

Il fenomeno è in costante crescita e i pirati informatici fanno affari d'oro. Il giro d'affari stimato è di oltre 1 milione di dollari.

Un'organizzazione capillare, estremamente strutturata e che ormai ha le caratteristiche di una vera filiera. Il cyber crimine continua la sua evoluzione verso una dimensione estremamente professionalizzata e il fenomeno della compravendita di accessi alle reti di aziende e organizzazioni ne è la migliore dimostrazione.

Ad accendere i riflettori sul fenomeno è una ricerca condotta dalla società di sicurezza **KELA**, che nel suo studio pubblicato su Internet tratteggia un quadro decisamente preoccupante. Sui forum frequentati dagli hacker c'è un traffico continuo che alimenta un vero e proprio mercato.

Lo schema è semplice: **i pirati informatici che riescono a violare un qualsiasi network al posto di portare attacchi più "profondi" per monetizzare la loro attività, mettono in vendita l'accesso a qualsiasi "collega" che possa essere interessato**.

L’indagine dei ricercatori di KELA, che fa riferimento all’ultimo trimestre del 2020, ha messo a nudo un mercato in cui, solo nei tre forum specializzati in questo particolare traffico che i ricercatori hanno esaminato, hanno visto un’offerta di accessi a 250 reti compromesse, con un listino che, complessivamente, avrebbe un valore di **circa 1,2 milioni di dollari**.

In molti casi, però, i prezzi per gli accessi non sono nemmeno indicati: i pirati preferiscono trattare in privato la transazione e, di conseguenza, la somma complessiva potrebbe essere più alta.

La maggior parte degli accessi in vendita sfrutta protocolli RDP (Remote Desktop Protocol) e VPN (Virtual Private Network). Una tendenza segnalata da molti ricercatori che è cresciuta nel periodo della pandemia da Covid 19, in cui molte aziende hanno implementato sistemi di accesso in remoto per consentire ai dipendenti di lavorare dal proprio domicilio.

La ricerca di KELA, però, da un punto di vista quantitativo mette a nudo quella che potrebbe essere soltanto la punta dell'iceberg. **Come spiegano gli stessi autori del rapporto, molte transazioni avvengono in privato ed è possibile che una buona parte di queste non passi nemmeno per i forum analizzati**.

Condividi l'articolo

Dependency Confusion: l'attacco ha funzionato con 35 big dell'hi tech

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/11/boom-di-vendite-online-di-accessi-hackerati-alle-reti/?utm_source=rss&utm_medium=rss&utm_campaign=boom-di-vendite-online-di-accessi-hackerati-alle-reti

---

Dependency Confusion: l'attacco ha funzionato con 35 big dell'hi tech

Feb 10, 2021 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La tecnica sfrutta il sistema delle dipendenze a livello di sviluppo software. Ecco come un ricercatore ha scoperto di poter colpire Apple, Microsoft, PayPal e altri big del settore.

Nel panorama della cyber security, gli attacchi supply chain hanno posto di riguardo tra le preoccupazioni che tormentano gli esperti. Il motivo è semplice: a fronte di un'attività relativamente ridotta, permettono ai cyber criminali di colpire un considerevole numero di vittime.

La tecnica messa a punto da **Alex Birsan**, però, è qualcosa di ancora più pericoloso. IL ricercatore, infatti, ha trovato un punto debole che avrebbe consentito di colpire con estrema facilità (ed efficacia) numerose aziende nel settore tecnologico, compresi veri "mostri sacri" come **Apple**, **PayPal** e

Microsoft.

La tecnica, che il ricercatore ha battezzato con il nome di Dependency Confusion, sfrutta in pratica quel livello di "fiducia" per cui gli sviluppatori tendono a considerare affidabili i pacchetti di codice pubblicati online.

L'intuizione di Birsan fa leva sul sistema delle dipendenze, cioè quella complessa rete che consente agli sviluppatori di "richiamare" automaticamente pacchetti di codice in vari linguaggi di programmazione (Birsan ha preso di mira **Python**, **Node** e **Ruby**) che vengono estratti da repository dedicati, come **GitHub**.

Il ricercatore ha sviluppato una serie di tecniche che gli hanno consentito, in pratica, di pubblicare su Internet delle versioni infette dei pacchetti, sostituendo quelli esistenti o semplicemente rimpiazzando pacchetti che erano stati cancellati ma che vengono comunque richiamati dalle applicazioni sviluppate con il linguaggio corrispondente.

Il suo esperimento, spiega Birsan in un post pubblicato su Internet, ha dato risultati sorprendenti: **è infatti riuscito a caricare il suo codice malevolo sui sistemi di un gran numero di aziende di primo piano, dalle quali ha poi potuto estrarre informazioni sensibili**.

Per farlo, il ricercatore spiega di aver utilizzato un sistema di esfiltrazione basato su quesy DNS, che consentono di aggirare la maggior parte dei controlli di sicurezza.

L’esperimento avrebbe permesso alle aziende coinvolte (35 in tutto, di dimensioni notevoli) di individuare le vulnerabilità a questa tecnica di attacco e correggere i loro sistemi per mitigare il rischio di futuri intrusioni.

Condividi l’articolo

Florida: un pirata attacca il sistema idrico per avvelenare la città

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/10/dependency-confusion-lattacco-ha-funzionato-con-35-big-dellhi-tech/?utm_source=rss&utm_medium=rss&utm_campaign=dependency-confusion-lattacco-ha-funzionato-con-35-big-dellhi-tech

---

Florida: un pirata attacca il sistema idrico per avvelenare la città

Feb 09, 2021 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

Il cyber criminale ha alterato i sistemi per diffondere una quantità elevata di soda caustica nella rete idrica di Oldsmar. Colpa del Covid?

Nuovo capitolo nel settore degli attacchi hacker alle infrastrutture critiche. Questa volta, nel mirino dei pirati informatici finisce addirittura il sistema idrico di una città nella baia di Tampa in **Florida**.

La segnalazione proviene dall'ufficio dello sceriffo di **Oldsmar**, nella costa orientale degli Stati Uniti, che ha denunciato un attacco informatico ai danni delle infrastrutture che gestiscono le risorse idriche della contea.

Stando a quanto riportato, l'hacker avrebbe ottenuto l'accesso ai sistemi di gestione per modificare il livello di immissione di idrossido di sodio (quella che conosciamo come soda caustica) all'interno del sistema.

Il sabotatore avrebbe modificato le impostazioni per portare la quantità di soda caustica da 100 parti per milione a 11.100 parti per milione. **Una quantità tale da mettere a rischio la salute di tutti gli abitanti della zona**.

Se le motivazioni del gesto sono ancora sconosciute, le modalità riportano all'attenzione dell'opinione pubblica tutti i rischi legati all'adozione di modalità di lavoro remoto indotte dall'emergenza legata alla pandemia da **Covid 19**.

Il pirata informatico, infatti, avrebbe ottenuto l'accesso ai sistemi violando **TeamViewer**, il software di gestione dei computer in remoto che molte organizzazioni stanno utilizzando per consentire ai dipendenti di controllare a distanza i PC dei loro uffici.

L'attacco è avvenuto in un momento particolare: la città di Oldsmar, infatti, si trova non lontano da **Tampa Bay**, località in cui si è giocata la finale NFL. Proprio il **Superbowl** potrebbe essere stato uno dei fattori che ha indotto il cyber criminale a scegliere bersaglio e tempistica dell'attacco.

Condividi l'articolo

Nuovo attacco di phishing usa…. Il codice morse!

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2021/02/09/florida-un-pirata-attacca-il-sistema-idrico-per-avvelenare-la-citta/?utm_source=rss&utm_medium=rss&utm_campaign=florida-un-pirata-attacca-il-sistema-idrico-per-avvelenare-la-citta

Nuovo attacco di phishing usa…. Il codice morse!

Feb 08, 2021 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS 0

La tecnica adottata dai pirati punta ad aggirare i filtri che bloccano contenuti potenzialmente pericolosi sfruttando la codifica pensata per i telegrafi.

L'inventiva dei cyber criminali non ha limiti. L'ultimo caso, però, ha dell'incredibile: i pirati infatti stanno utilizzando il codice morse per portare attacchi di phishing agli utenti, aggirando così i sistemi di protezione delle caselle email.

Il caso, segnalato da **Bleeping Computer** in un articolo pubblicato poche ore fa, sembra essere l'ultima trovata per superare i filtri utilizzati dalle aziende per individuare e bloccare i messaggi di phishing e sfrutta una semplice email con un allegato in formato HTML.

Per trarre in inganno le loro vittime, i pirati utilizzano il vecchio trucco della doppia estensione. Il file, cioè, è nominato con una sintassi del tipo “**Documento.XLS.HTML**”.

Se la funzionalità di Windows che nasconde le estensioni per i tipi di file conosciuti è attiva, l’utente si troverà di fronte un file visualizzato come “**Documento.XLS**” e penserà di trovarsi di fronte a un file di Excel.

All’interno del file è presente uno script malevolo, il cui codice è però offuscato in una maniera molto particolare: attraverso il codice morse. Il contenuto viene convertito usando uno strumento specifico al momento dell’apertura.

Una volta decodificato e avviato, lo script visualizza una pagina Web in cui viene mostrato un falso documento Excel sullo sfondo e, in primo piano, un messaggio che informa la potenziale vittima che la sessione di **Office 365** sarebbe scaduta ed è richiesto l’inserimento della password.

Naturalmente il messaggio è falso e, se inserita, la password finisce direttamente sui sistemi dei pirati informatici che

possono così compromettere l’account della vittima.

I messaggi, secondo quanto riportano i colleghi di Bleeping Computer, utilizzerebbero una grande attenzione nel confezionare i messaggi, utilizzando i loghi delle aziende che intendono colpire e spacciando gli allegati come fatture destinate all’impresa stessa.

Condividi l’articolo

Il gruppo Lazarus mette nel mirino i ricercatori di cyber security

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/08/nuovo-attacco-di-phishing-usa-il-codice-morse/?utm_source=rss&utm_medium=rss&utm_campaign=nuovo-attacco-di-phishing-usa-il-codice-morse

---

Il gruppo Lazarus mette nel mirino i ricercatori di cyber security

Feb 05, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

I pirati legati al governo della Corea del Nord stanno attaccando gli esperti di sicurezza utilizzando exploit zero-day di Chrome e Internet Explorer.

Sembra essere la nuova tendenza tra i pirati informatici: prendere di mira gli esperti di sicurezza per rubare strumenti di hacking e informazioni riservate che gli consentano di affinare o ampliare le loro tecniche di attacco.

A darsi un gran da fare in questo senso sembra essere il gruppo **Lazarus**. I pirati del gruppo APT, considerato molto "vicino" al governo della Corea del Nord, avrebbero portato una serie di attacchi indirizzati a ricercatori che operano nella cyber security sfruttando una serie di exploit Zero-day.

Il primo, individuato da **Microsoft** che lo ha descritto in un report pubblicato su Internet, fa leva su una vulnerabilità (CVE-2021-21148) nelle versioni di Chrome per **Windows**, **Linux** e **macOS**. SI tratta di un bug nel **motore V8 JavaScript** del browser di **Google**.

I pirati lo sfrutterebbero attraverso complesse tecniche di social engineering, che prevedono l'instaurazione di un "rapporto di fiducia" con le potenziali vittime attraverso contatti sui social network, per poi inviare link malevoli che permettono di portare l'attacco. **Google ha corretto il bug con l'aggiornamento alla versione 88.0.4324.150 del browser, già disponibile**.

L’exploit basato su Internet Explorer è invece stato segnalato da **ENKI**. La società di sicurezza sud-coreana ha descritto le caratteristiche dello zero-day in un report (a meno che non conosciate il coreano serve Google Translator per leggerlo) in cui i ricercatori spiegano che l’attacco sfrutta come vettore un file in formato **MIME HTML**.

La sua apertura, in Windows, avvia automaticamente **Internet Explorer** (sì, c’è ancora) nel quale è presente un bug zero-day che consente l’esecuzione di codice in remoto.

Anche in questo caso, stando a quanto si legge, la tecnica è sfruttata dal gruppo Lazarus per colpire ricercatori di sicurezza e compromettere i loro dispositivi.

Dalle parti di Microsoft sembra stiano ancora lavorando all’aggiornamento che consentirà di correggere la vulnerabilità.

Condividi l’articolo

La botnet Matryosh sfrutta i dispositivi Android per portare attacchi DDoS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/05/il-gruppo-lazarus-mette-nel-mirino-i-ricercatori-di-cyber-security/?utm_source=rss&utm_medium=rss&utm_campaign=il-gruppo-lazarus-mette-nel-mirino-i-ricercatori-di-cyber-security

---

La botnet Matryosh sfrutta i dispositivi Android per portare attacchi DDoS

Feb 04, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware punta a prendere il controllo degli smartphone per utilizzarli nelle operazioni di sabotaggio di siti Internet e servizi online.

Tra le nuove declinazioni dei malware per dispositivi mobili c’è anche quella legata agli attacchi DDoS. Per il momento rimangono eventi episodici, ma la comparsa di **Maytrosh** potrebbe rappresentare l’indizio di un cambio di strategia da parte dei cyber criminali.

La botnet, che prende di mira i dispositivi Android, è stata individuata dai ricercatori di **Netlab**, la divisione dedicata alla sicurezza a livello di networking di **Qihoo 360**.

La scelta del nome, che si ispira alle matrioske, è dovuta alle caratteristiche tecniche del malware che i pirati informatici utilizzano per compromettere i dispositivi che poi sfruttano per portare i loro attacchi.

Maytrosh utilizza un vettore di attacco piuttosto comune: quel **Android Debug Bridge (ADB)** che ha già causato parecchi guai al sistema operativo di Google e che molti produttori sembrano ostinarsi a mantenere attivo (ed esposto su Internet) sulla porta 5555.

Una vulnerabilità che può essere corretta con un semplice intervento sulle impostazioni in molti smartphone, ma che in

molti dispositivi rimane fuori dalla portata degli utenti.

A ispirare la scelta del nome è il fatto che la botnet utilizza un sistema di server command and control che utilizzano **TOR** (il circuito di navigazione anonima gestito dal basso – ndr) per offuscare le loro comunicazioni.

L'obiettivo dei pirati informatici, secondo quanto spiegano i ricercatori nel loro report, sarebbe quello di usare i dispositivi controllati a distanza per portare attacchi DDoS. **Una strategia che di solito impiega più frequentemente i PC, ma che risulta essere efficace anche con i dispositivi mobili**.

Con un ulteriore danno per le vittime: il traffico legato agli attacchi rischia infatti di intaccare la quantità disponibile nel contratto. Insomma: oltre a partecipare inconsapevolmente a un'attività malevola, le vittime di Matryosh rischiano anche di veder evaporare i gigabyte di traffico garantiti dal loro contratto.

Condividi l'articolo

Kobalos mette nel mirino i supercomputer e i sistemi degli ISP

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/04/la-botnet-matryosh-sfrutta-i-dispositivi-android-per-portare-attacchi-ddos/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-matryosh-sfrutta-i-dispositivi-android-per-portare-attacchi-ddos

Kobalos mette nel mirino i supercomputer e i sistemi degli ISP

Feb 03, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware per sistemi Linux è piccolo, versatile e… cattivo. Secondo i ricercatori sarebbe in grado di colpire anche altre piattaforme.

I ricercatori di **ESET**, che lo hanno individuato per primo, lo hanno battezzato con il nome di **Kobalos**, che nella mitologia greca indica una sorta di piccolo fauno.

Le ragioni all'origine della scelta del nome si capiscono leggendo il report pubblicato dagli analisti che hanno "sezionato" il malware: si tratta infatti di un software di piccole dimensioni ma estremamente pestifero, che starebbe procurando non pochi grattacapi nel settore IT.

Il trojan, la cui presenza può essere rilevata scansionando i sistemi sulla porta TCP 55201 per verificare la presenza di servizi **SSH (Secure Shell)**, sarebbe programmato per sottrarre le credenziali dei sistemi che colpisce.

Sul vettore di attacco utilizzato dai pirati per diffonderlo, però, non ci sono al momento indizi rilevanti. In pratica i ricercatori sanno che esiste, ma non hanno la minima idea di come venga distribuito.

Dall’analisi eseguita da ESET, il malware avrebbe colpito numerosi Internet Service Provider in Asia, **reti gestite da diverse università e supercomputer in Europa**, mentre negli USA i casi individuati riguarderebbero (ancora una volta) società di sicurezza e agenzie governative.

Immagine: ESET

Da un punto di vista tecnico, Kobalos si distingue per una spiccata versatilità, che consente ai pirati di comunicare con la backdoor attraverso diversi canali. **Il malware, inoltre, sembrerebbe essere in grado di adattarsi ad altre piattaforme oltre a Linux, tra cui Solaris e (forse) Windows**.

Una volta installato, il malware è anche in grado di agire come proxy o come server command and control e questo, secondo i ricercatori, garantirebbe alla botnet un livello di resilienza estremamente alto, **In altre parole, anche se i server principali venissero “abbattuti”, i cyber criminali potrebbero adattare qualsiasi macchina infetta per sostituirli**.

Immagine: ESET

Nessun indizio, infine, sugli obiettivi degli autori di Kobalos. Il malware potrebbe puntare a rubare informazioni riservate, installare crypto-miner o usare le macchine per qualsiasi altro scopo.

Insomma: poche certezze e tante preoccupazioni per un malware che, a dispetto delle piccole dimensioni del codice che lo compone, sembra avere un livello di complessità (ed efficacia) molto elevato.

Condividi l’articolo

La botnet Matryosh sfrutta i dispositivi Android per portare attacchi DDoS Ti presento Cedar: gli hacker libanesi che hanno violato centinaia di server

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/03/kobalos-mette-nel-mirino-i-supercomputer-e-i-sistemi-degli-isp/?utm_source=rss&utm_medium=rss&utm_campaign=kobalos-mette-nel-mirino-i-supercomputer-e-i-sistemi-degli-isp

---

Ti presento Cedar: gli hacker libanesi che hanno violato centinaia di server

Feb 02, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il gruppo APT legato al governo di Beirut avrebbe compromesso più di 250 server nel corso dell'ultimo anno usando due diversi malware in una versione aggiornata.

Non solo le grandi potenze: anche paesi che siamo normalmente abituati a considerare "outsider" possono dire la loro nel campo della guerriglia informatica. In questo caso, a farlo è il **Libano**.

Un report pubblicato da **ClearSky Security** chiarisce i contorni della vicenda: protagonisti i pirati informatici del gruppo **Cedar**, che secondo i ricercatori della società di sicurezza avrebbero creato nuove varianti di due malware.

Il primo, che i ricercatori definiscono come una web shell, è

stato battezzato con il nome di **Caterpillar**, mentre il secondo (**Explosive RAT**) sarebbe un classico trojan che consente di rubare informazioni dal computer compromesso e controllarlo a distanza.

I due malware sarebbero stati utilizzati per colpire dei bersagli negli USA, nel Regno Unito; in Egitto; Giordania; Israele e nei territori sotto il controllo dell'Autorità Palestinese. **In tutto 250 vittime, che il gruppo di pirati informatici sarebbero riusciti a infiltrare nel corso degli ultimi 12 mesi**.

Secondo i ricercatori, la nuova ondata di attacchi portata da Cedar si avvantaggerebbe di alcuni aggiornamenti nei due malware.

Per quanto riguarda Explosive RAT, gli hacker avrebbero sfruttato una serie di exploit basati su nuove vulnerabilità (come quelle che affliggono i sistemi **Oracle**) e avrebbero dotato il malware di una serie di nuove caratteristiche che variano da tecniche di offuscamento all'uso di sistemi di comunicazione crittografati.

Caterpillar, che sarebbe una variante derivata da una web shell open source chiamata **ASPXspy**, verrebbe invece utilizzato per sottrarre informazioni sensibili dai sistemi colpiti, come le credenziali per l'accesso alle funzionalità di amministrazione.

Da un punto di vista complessivo, in realtà, gli attacchi portati dal gruppo Cedar sembrano aver sfruttato **una serie di vulnerabilità ben conosciute** e il successo dei pirati informatici nell'infiltrarsi nei sistemi colpiti è da ascrivere più alle colpe di un mancato aggiornamento di software e sistemi operativi che a un'effettiva efficacia dei malware.

Condividi l'articolo

Falle nei sistemi IT/OT industriali di Fuji

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/02/ti-presento-cedar-gli-hacker-libanesi-che-hanno-violato-centinaia-di-server/?utm_source=rss&utm_medium=rss&utm_campaign=ti-presento-cedar-gli-hacker-libanesi-che-hanno-violato-centinaia-di-server

---

Falle nei sistemi IT/OT industriali di Fuji

Feb 01, 2021 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le vulnerabilità consentono ai pirati informatici di avviare l'esecuzione di codice in remoto. A rischio gli tutti gli impianti industriali che sfruttano la piattaforma.

Altri guai per il mondo dell'industria 4.0 e, questa volta, a farne le spese sono i sistemi sviluppati da Fuji. Nel dettaglio, a soffrire di una vulnerabilità che consentirebbe di portare cyber attacchi ai sistemi di gestione IT/OT sarebbero **Tellus Lite V-Simulator** e **V-Server Lite**.

I due prodotti fanno parte della piattaforma Fuji che consente di monitorare i sistemi industriali e raccogliere dati in tempo reale per gestire la produzione attraverso un'interfaccia che la mette in comunicazione con i PLC e altri dispositivi all'interno delle linee produttive.

Secondo quanto riportato dagli stessi sviluppatori in un advisory di sicurezza, i bug dei software Fuji possono essere sfruttati senza che sia necessario avere grandi competenze tecniche, una caratteristica che li rende particolarmente "sensibili" ai fini della protezione dei sistemi industriali che utilizzano la piattaforma.

Sfruttando le falle di sicurezza (CVE-2021-22637; CVE-2021-22655; CVE-2021-22653; CVE-2021-22639 e CVE-2021-22641) sarebbe possibile, a quanto si legge, a**vviare l'esecuzione di codice sui dispositivi con gli stessi privilegi dell'applicazione vulnerabile**.

Il problema, inoltre, riguarda il fatto che un attacco permetterebbe anche di dissimulare le operazioni in corso, nascondendo ciò che sta succedendo agli amministratori di sistema. **Insomma: l’attacco sarebbe completamente invisibile**.

Una tipologia di attacco, quindi, che considerato il settore particolarmente “delicato” in cui vengono usati i sistemi Fuji potrebbe portare a malfunzionamenti blocchi ed eventi potenzialmente pericolosi anche sotto un profilo “fisico”.

La soluzione passa per un aggiornamento che l’azienda produttrice ha già reso disponibile per entrambi i prodotti. Inutile dire che gli sviluppatori (cui ci uniamo volentieri) sollecitano tutti gli utilizzatori della piattaforma a installare il prima possibile le patch.

Condividi l’articolo

Allarme per la nuova variante dell’attacco NAT Slipstream

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/01/falle-nei-sistemi-it-ot-industriali-di-fuji/?utm_source=rss&utm_medium=rss&utm_campaign=falle-nei-sistemi-it-ot-industriali-di-fuji

---

Allarme per la nuova variante dell'attacco NAT Slipstream

Gen 29, 2021 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La nuova versione della tecnica di attacco consente di individuare dall'esterno l'indirizzo IP di tutti i dispositivi interni alla rete locale.

Torna l'incubo **NAT Slipstream**, in una nuova versione riveduta e corretta che potrebbe creare ancora maggiori rischi. La vulnerabilità originale, scoperta nel novembre dello scorso anno, aveva messo in allarme i ricercatori e ha costretto gli sviluppatori di browser (e gli amministratori IT) a prendere le contromisure indispensabili per bloccarne l'utilizzo.

A lanciare l'allarme sulla nuova versione sono stati due ricercatori di **Armis**, che hanno reso pubblico il loro studio

sul blog ufficiale della società di sicurezza.

Ben Seri e **Gregory Vishnepolsky**, in pratica, hanno trovato il modo di sfruttare NAT Slipstream per ottenere informazioni più dettagliate (e ampie) rispetto a quanto fosse possibile fare con la tecnica originale.

Ma di cosa si tratta in pratica? La funzione **NAT (Network Address Translation)** è disponibile nella maggior parte dei router e ha la funzione di ridurre il numero di indirizzi IP esposti verso l'esterno.

Il sistema, in pratica, reindirizza il traffico Internet facendo in modo che ogni dispositivo connesso "esca" dalla rete locale utilizzando l'indirizzo IP del router. **In questo modo, un eventuale pirata informatico non ha la possibilità di conoscere l'esatto indirizzo del device**.

La tecnica di NAT Slipstream prevede l'utilizzo di Javascript malevoli che consentono di inviare delle risposte generate con criteri particolari per aggirare il NAT. Gli script in questione possono essere caricati su un sito Internet e l'attacco si avvia quando un utente visita le pagine in questione.

[embedded content]

L'attacco sfrutta l'Application Layer Gateway (ALG) **H.323**, un protocollo VoIP le cui caratteristiche consentono di portare l'attacco NAT Slipstream sfruttando un maggior numero di porte rispetto alla versione originale. Come spiegano i ricercatori, infatti, è possibile usare connessioni **WebRTC TURN** verso qualsiasi porta e questo consente di colpire anche altri ALG come quello **FTP** o **IRC**.

La reazione degli sviluppatori di browser non si è fatta aspettare. Tutti i più diffusi software per la navigazione (**Firefox, Chrome, Safari ed Edge**) hanno provveduto a bloccare le connessioni sulle porte TCP incriminate (69, 137, 161,

1719, 1720, 1723 e 6566) per “disinnescare” la tecnica di attacco.

Condividi l’articolo

Smantellata la botnet Emotet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/29/allarme-per-la-nuova-variante-dellattacco-nat-slipstream/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-per-la-nuova-variante-dellattacco-nat-slipstream