L’aggiornamento di agosto per Android è piuttosto “impegnativo”

Ago 06, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La tornata di update di sicurezza corregge più di 50 bug relativi al software e a componenti specifici di alcuni produttori hardware.

Sarà un’estate decisamente “calda” per gli sviluppatori che si occupano di aggiornare i sistemi Android per i vari produttori.

Il bollettino sulla sicurezza di Android pubblicato lo scorso 3 agosto da **Google** contiene la bellezza di 54 vulnerabilità ad altro rischio, tra cui un bug che può portare all’esecuzione di codice in remoto.

Si tratta della falla di sicurezza classificata come CVE-2020-0240 e che secondo i ricercatori di Google “potrebbe consentire a un utente malintenzionato remoto che utilizza un file appositamente predisposto di **eseguire codice arbitrario nel contesto di un processo senza privilegi**”.

La vulnerabilità riguarda l’**Android Framework**, il pacchetto di strumenti per sviluppatori che consente di realizzare applicazioni per il sistema operativo Google.

Le altre vulnerabilità a rischio elevato che riguardano quella che dalle parti di Google chiamano la “struttura” del sistema consentirebbero invece l’elevazione dei privilegi (CVE-2020-0238 e CVE-2020-0257); il furto di informazioni

sensibili (CVE-2020-0239, CVE-2020-0249 e CVE-2020-0258) e, infine, la possibilità di avviare un attacco Denial of Service (CVE-2020-0247).

Nel bollettino, però, è riportata un'altra vulnerabilità che potrebbe portare all'esecuzione di codice remoto. Si tratta di una falla di sicurezza in un componente (**dm-Verity**) di **AMLogic**, società produttrice di circuiti integrati.

L'elenco delle falle che interessano componenti di terze parti, però, è piuttosto nutrito e la parte del leone, manco a dirlo, la fa **Qualcomm**. Sono ben 31 i bug relativi a componenti della società statunitense che vengono segnalati nel bollettino.

Ora partirà il solito percorso a ostacoli che vedrà i vari produttori applicare le patch alle rispettive versioni del loro sistema Android.

Con la solita complicazione legata non solo ai tempi diversi per il rilascio di ogni aggiornamento, ma anche al fatto che le vulnerabilità relative a componenti specifici (che quindi non riguardano tutti i dispositivi in commercio) dovranno essere selezionate e applicate dai singoli produttori.

Condividi l'articolo

Allarme dell’FBI: aziende con Windows 7 a rischio attacchi hacker

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/08/06/laggiornamento-di-agosto-per-android-e-piuttosto-impegnativo/?utm_source=rss&utm_medium=rss&utm_campaign=laggiornamento-di-agosto-per-android-e-piuttosto-impegnativo

Allarme dell’FBI: aziende con Windows 7 a rischio attacchi hacker

Ago 05, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Il Bureau mette in guardia riguardo la possibilità che i cyber criminali prendano di mira le imprese che usano ancora il vecchio sistema operativo Microsoft.

I timori legati al livello di sicurezza di **Windows 7** dopo la cessazione del supporto da parte di **Microsoft** sono ancora di attualità. Dopo gli esperti di sicurezza, che hanno segnalato il problema in passato, adesso arriva anche l’FBI.

L’occasione è la pubblicazione di un documento rivolto all’industria privata, in cui gli esperti del Federal Bureau sollecitano le imprese ad aggiornare i loro sistemi alla nuova versione. Anche dopo il termine del 14 gennaio, che ha segnato il “fine vita” di Windows 7, molte aziende continuano infatti a usare macchine equipaggiate con la vecchia versione del sistema.

Le preoccupazioni dei federali vertono sulla facilità con cui i pirati informatici possono colpire i vecchi sistemi, soprattutto sfruttando le funzionalità di rete che hanno mostrato tutti i loro limiti in occasione di attacchi come quello di **WannaCry**.

In realtà il supporto, anche se limitato agli aggiornamenti di sicurezza, è disponibile per alcune licenze particolari che prevedono però una contropartita economica. Insomma: qualcosa che ben poche delle aziende che ancora utilizzano Windows 7 hanno probabilmente acquistato.

Nella notifica, l’FBI sottolinea come i recenti attacchi (soprattutto quelli rivolti al settore sanitario, in cui i sistemi legacy sono purtroppo piuttosto diffusi) dimostrano che le spese per un aggiornamento (sia a livello software che hardware) sono comunque **minori dei danni che le aziende possono subire in caso di attacchi**.

I federali, inoltre, sottolineano un aspetto che spesso viene trascurato. Oltre a non ottenere gli aggiornamenti e le patch di sicurezza, i sistemi Microsoft per cui è terminato il supporto non ottengono nemmeno le nuove funzionalità sviluppate dal produttore.

Un “dettaglio”, questo, che può avere ulteriori conseguenze sulla sicurezza, spingendo gli amministratori IT a utilizzare strumenti software obsoleti per evitare problemi di compatibilità con Windows 7. **Insomma: il mancato aggiornamento rischia di innescare un “effetto domino” che mina alle fondamenta il livello di sicurezza delle aziende**.

Chissà se l’accorato appello dell’FBI, che mette sul piatto anche considerazioni di carattere geopolitico legate alla cosiddetta cyber-guerriglia, avrà qualche effetto.

Condividi l’articolo

Plugin in WordPress mette a rischio 150.000 siti Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/05/allarme-dellfbi-aziende-con-windows-7-a-rischio-attacchi-hacker/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-

dellfbi-aziende-con-windows-7-a-rischio-attacchi-hacker

Plugin in WordPress mette a rischio 150.000 siti Internet

Ago 04, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

---

l bug che interessano il plugin Newsletter consentirebbe ai pirati informatici di prendere il pieno controllo dei siti. Le tempistiche non hanno aiutato…

I plugin sono da sempre uno dei punti deboli della piattaforma CMS **WordPress** per la pubblicazione e la gestione di siti Internet. Ogni falla di sicurezza che viene scoperta in u n plugin, infatti, mette a rischio migliaia di siti Internet.

L'ultimo caso riguarda **Newsletter**, un popolare plugin che consente di gestire le comunicazioni tramite mail e che vanta più di 300.000 download dal repository ufficiale di WordPress.

Come spiegano i ricercatori di **Wordfence** in un report pubblicato ieri su Internet, la vicenda rischia di creare qualche grattacapo agli amministratori dei siti WordPress.

Le falle di sicurezza che interessano Newsletter, infatti, sonno state scoperte a breve distanza le une dalle altre e la segnalazione degli aggiornamenti potrebbe creare una certa confusione, soprattutto per chi si affida a controlli periodici.

Il primo bug, corretto con l'aggiornamento pubblicato il 13

luglio scorso, riguardava un classico Reflected XSS che è stato classificato con un livello di gravità media.

Quando i ricercatori di Wordfence hanno investigato sulla falla di sicurezza, però, ne hanno individuate altre due, ben più gravi.

Si tratta, nel dettaglio, di una vulnerabilità **Reflected XXS** e di un bug che consentirebbe una **PHP Object Injection**, il cui utilizzo consentirebbe di creare amministratori "nascosti" e inserire backdoor all'interno dei siti.

I ricercatori hanno segnalato le due vulnerabilità agli sviluppatori il 14 luglio e la nuova patch (la versione più recente oggi disponibile è la 4.8.3) è stata rilasciata il 17 luglio.

Questo incrocio di date sembra però aver creato un po' di confusione tra gli utenti. Secondo gli esperti di WordFence, infatti, solo la metà degli utilizzatori del plugin avrebbero aggiornato all'ultima versione. **In altre parole, ci sarebbero ancora 150.000 siti WordPress vulnerabili agli attacchi**.

Una situazione che, in qualche modo, i ricercatori avevano previsto e che hanno cercato di mitigare introducendo delle nuove regole firewall per il loro prodotto di sicurezza.

La speranza è che il nuovo sistema di aggiornamento automatico della piattaforma aiuti a risolvere la situazione rapidamente. In caso contrario, la vicenda legata a Newsletter rischia di rappresentare un problema piuttosto serio.

Condividi l’articolo

Attacco hacker a Twitter: individuati i responsabili

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/04/plugin-in-wordpress-mette-a-rischio-150-000-siti-internet/?utm_source=rss&utm_medium=rss&utm_campaign=plugin-in-wordpress-mette-a-rischio-150-000-siti-internet

---

Attacco hacker a Twitter: individuati i responsabili

Ago 03, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, Phishing, RSS 0

La “mente” è un diciassettenne che avrebbe aggirato le protezini con una semplice telefonata. I truffatori traditi da una serie di errori incredibili.

Si è parlato della possibilità di un coinvolgimento di gruppi hacker collegati a governi stranieri e di professionisti del cyber crimine. Niente di tutto questo: dietro all’attacco che ha permesso di hackerare decine di profili **Twitter** di celebrità c’è la mano di un 17enne originario della Florida.

La ricostruzione della vicenda, resa possibile dai documenti giudiziari pubblicati dalla procura del distretto della California, rende l’idea di come una simile “impresa” non richieda grandi mezzi o conoscenze specifiche. Anzi: tutto sarebbe cominciato con una semplice telefonata che avrebbe permesso all’hacker di aggirare il sistema di autenticazione a doppio fattore usato per proteggere gli account degli amministratori Twitter.

Tutto comincia il 15 luglio, quando l’hacker diciassettenne originario di Tampa (Florida) ma residente in California, contatta telefonicamente alcuni operatori di Twitter utilizzando classiche tecniche di ingegneria sociale per farsi fornire le credenziali di accesso al backend del social network.

Il trucchetto funziona e l’autore dell’attacco ottiene, attraverso una serie di ulteriori attacchi portati tra le pieghe dei sistemi di Twitter, un accesso pressoché libero a tutti gli account.

A questo punto, il pirata informatico si è preoccupato di procurarsi dei complici e lo ha fatto contattando alcuni utenti che frequentavano un canale dedicato all’hacking su **Discord**, offrendo loro anche delle dimostrazioni delle sue possibilità di accesso.

Nel dettaglio, **Kirk#5270** (il suo nickname su Discord) ha convinto uno dei suoi futuri complici (**Rolex#0373**,

identificato con il 22enne **Nima Fazeli**) alterando il suo profilo Twitter.

Dopo aver reclutato un terzo membro della gang, il britannico **Mason Sheppard**, il gruppo sarebbe passato all'azione sfruttando l'accesso ai sistemi per violare circa 130 account Twitter, per 45 dei quali avrebbero avviato il reset della password.

Il loro obiettivo, come abbiamo spiegato in un articolo precedente, era quello di mettere in atto una classica truffa "give away", utilizzando gli account Twitter di celebrità per indurre le potenziali vittime a trasferire Bitcoin sui loro conti.

Lo stratagemma avrebbe permesso loro di raccogliere la bellezza di 117.000 dollari in poche ore. Il bottino, però, avrebbe potuto essere più ricco. Secondo quanto dichiarato da **Coinbase**, una delle più celebri piattaforme per il commercio di criptovalute, nelle tasche dei truffatori avrebbero potuto finire altri **280.000 dollari**. A impedirlo, è stato il tempestivo blocco dei conti utilizzati per la truffa.

A tradire gli hacker sarebbe stato un uso troppo "disinvolto" dei social media e di alcuni forum, che ha permesso all'FBI di incrociare i dati e risalire all'identità dei truffatori. In particolare, Fazeli si è tradito utilizzando lo stesso

nickname sia in Discord, sia sul forum di **OGUsers**.

Non solo, il truffatore avrebbe usato per i suoi conti su Coinbase gli stessi indirizzi email utilizzati per registrarsi sul forum e violare un account Twitter. **Nella registrazione a Coinbase avrebbe confermato la procedura caricando un'immagine della sua carta d'identità**.

E ancora: lo stesso Fazeli avrebbe usato la sua connessione domestica per connettersi sia a Discord, sia ai conti su Coinbase.

Errori simili sarebbero ascrivibili anche a Mason Sheppard, che avrebbe utilizzato un conto Coinbase connesso alla truffa per acquistare un videogioco. **Conto che aveva registrato, peraltro, utilizzando la sua vera patente come documento di riconoscimento**.

Insomma: da quanto emerge leggendo i documenti della Procura, gli hacker che hanno messo a segno il "colpo dell'anno" non sarebbero propriamente dei geni.

Condividi l'articolo

Da Windows a Linux: TrickBot si evolve

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/03/attacco-hacker-a-twitter-individuati-i-responsabili/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-hacker-a-twitter-individuati-i-responsabili

Da Windows a Linux: TrickBot si evolve

Ago 03, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La nuova versione del trojan è stata battezzata con il nome di Anchor_Linux e consente di prendere il totale controllo delle macchine infette.

È uno dei "pesi massimi" tra i malware e sembra non avere nessuna intenzione di cedere il suo trono. Anzi: a quanto pare gli autori di **TrickBot** hanno deciso di espandere il campo d'azione del loro trojan per colpire anche le macchine con sistemi **Linux**.

A segnalare questa "invasione di campo" sono i ricercatori di **Intezer**, che hanno individuato un esemplare di malware collegato a TrickBot e in grado di colpire i computer Linux.

Come spiegano tutti i ricercatori che lo hanno analizzato, Anchor_Linux non è una versione derivata dal trojan vero e proprio. Il legame, infatti, è più complesso.

Gli autori di TrickBot, per diffondere e controllare il loro malware, utilizzano infatti una piattaforma chiamata **Anchor**, che sfrutta DNS per inviare comandi alle macchine infette.

Anchor_Linux sarebbe quindi una versione per Linux di Anchor, che al suo interno contiene anche una copia di TrickBot per Windows.

Il malware agisce come una classica backdoor e sfrutta i

collegamenti sulla LAN per infettare ulteriori macchine (sia Linux che Windows) utilizzando principalmente alcuni exploit basati su **Server Message Block**.

Insomma: siamo di fronte a un vero e proprio ecosistema che consente ai pirati informatici di diffondere i loro trojan sui due sistemi, aprendo la strada a qualsiasi genere di attività.

La versatilità di TrickBot e di Anchor_Linux consente infatti ai cyber criminali di rubare credenziali di accesso, documenti e installare qualsiasi tipo di ulteriore malware.

Tra questi, per esempio, i ricercatori evidenziano due ransomware (**Ryuk** e **Conti**) che vengono utilizzati come "payload finale" negli attacchi portati attraverso la piattaforma Anchor e anche strumenti pensati per compromettere i sistemi di pagamento POS attraverso campagne di lungo periodo.

Proprio la presenza di un installer del trojan per Windows, secondo gli esperti, indicherebbe che questa evoluzione di TrickBot non punterebbe tanto ad ampliare il campo di azione del malware per compromettere le macchine Linux, quanto per

creare una “testa di ponte” che consenta di attaccare i sistemi Microsoft, che rimangono il principale obiettivo dei pirati.

Condividi l’articolo

Attacco hacker a Twitter: individuati i responsabili Ti presento Doki: la backdoor per sistemi virtuali su Linux

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/03/da-windows-a-linux-trickbot-si-evolve/?utm_source=rss&utm_medium=rss&utm_campaign=da-windows-a-linux-trickbot-si-evolve

---

Ti presento Doki: la backdoor per sistemi virtuali su Linux

Lug 31, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware colpisce i server Docker e usa una serie di tecniche basate su blockchain per comunicare con i server Command and Control.

Una nuova minaccia, l’ennesima, prende di mira i servizi

virtualizzati su piattaforma cloud e il bersaglio sono ancora una volta i server **Docker**, utilizzati dalle aziende per l'implementazione di servizi virtualizzati "autonomi".

Doki, individuato dai ricercatori di **Intezer**, è una backdoor che consente ai pirati informatici di compromettere i server Linux su cui "girano" i container Docker. A differenza di altri malware che in passato hanno preso di mira questo tipo di piattaforma, che si limitavano a installare dei miner per generare criptovaluta, Doki consente ai pirati informatici un campo di azione maggiore.

La backdoor consente infatti di eseguire qualsiasi tipo di codice sulla macchina infetta e apre la possibilità, di conseguenza, che i cyber criminali installino qualsiasi tipo di payload ulteriore.

Come spiegano gli analisti nel report, gli attacchi vengono portati attraverso un sistema di scansione che individua i server Docker con impostazioni "deboli", in particolare a livello di API, che i pirati sfruttano per violare il sistema.

Per individuare i potenziali bersagli e portare l'attacco, gli autori di Doki utilizzano una botnet basata su **ngrok** (un servizio di reverse proxy – ndr) individuata tempo fa dagli esperti di sicurezza.

Lo schema di attacco prevede, una volta eseguito l’accesso al server, la creazione di nuovi container che i pirati caricano da un repository pubblico. I container in quesitone, infatti, non contengono direttamente il codice malevolo, ma permettono l’esecuzione di **Curl**, che i criminali sfruttano per i loro scopi.

Uno degli elementi più interessanti evidenziati dai ricercatori di Intezer, però, è il fatto che Doki utilizza un particolare sistema di comunicazione con i server Command and Control, che sfrutta la blockhain di **Dogecoin**, una criptovaluta lanciata nel 2014.

Insomma: utilizzando una botnet basata su reverse Proxy, container apparentemente legittimi e un sistema di comunicazione che sfrutta una tecnica di offuscamento innovativa, Doki rappresenta una minaccia estremamente difficile da rilevare.

Non solo: secondo i ricercatori, che hanno eseguito dei test usando **Virus Total**, al momento solo 24 motori antivirus su 60 sono in grado di individuare il malware.

Il metodo più efficace per bloccarne la diffusione, in ogni caso, è quello di eseguire una corretta configurazione dei server Docker, avendo cura in particolare di non esporre le API a collegamenti esterni.

Condividi l’articolo

SkyArk: uno strumento open per individuare falle in AWS e Azure

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/31/ti-presento-doki-la-backdoor-per-sistemi-virtuali-su-linux/?utm_source=rss&utm_medium=rss&utm_campaign=ti-presento-doki-la-backdoor-per-sistemi-virtuali-su-linux

---

SkyArk: uno strumento open per individuare falle in AWS e Azure

Lug 30, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Tecnologia, Vulnerabilità 0

Lo ha sviluppato CyberArk e permette di individuare eventuali account con configurazioni che mettono a rischio i sistemi su piattaforma cloud.

Si chiama **SkyArk** ed è un nuovo strumento pensato per contrastare il fenomeno delle violazioni a livello di piattaforme cloud. A metterlo a disposizione gratuitamente per chiunque lo voglia utilizzare è **CyberArk**, società di sicurezza specializzata nel **Privileged Access Management**.

Il tema, spiegano i ricercatori CyberArk in un post sul blog ufficiale dell'azienda, è quello degli "amministratori fantasma" o **Shadow Admin**. Si tratta di quegli account che hanno privilegi di amministrazione a causa di errate configurazioni. In altre parole: utenti a cui vengono concessi poteri troppo ampi e che rappresentano un rischio per la sicurezza dei sistemi.

In molti casi, infatti, questi account passano del tutto inosservati agli occhi degli stessi amministratori IT e, soprattutto, non vengono difesi adeguatamente.

Secondo i ricercatori di CyberArk, l'origine del problema è da identificare nei sistemi di permessi utilizzati da servizi cloud come **AWS** e **Azure**, che hanno un livello tale di complessità che gli amministratori faticano ancora a gestire.

SkyArk, che è stato rilasciato come progetto "aperto" su **GitHub**, è un tool pensato proprio per arginare questo fenomeno. È composto da due moduli (uno per ognuna delle due piattaforme) e consente di eseguire una scansione dei sistemi e individuare tutti gli Shadow Admin presenti sui sistemi.

L’obiettivo, in pratica, è quello di mettere a disposizione di tutte le aziende uno strumento (gratuito) che gli consenta di migliorare il livello di sicurezza e porre un freno al fenomeno degli “epic fail” nella gestione dei servizi cloud, che negli ultimi tempi stanno creando parecchi grattacapi agli esperti di sicurezza.

Il tutto in attesa che gli addetti IT riescano a prendere maggiore dimestichezza con i sistemi ultra-flessibili delle piattaforme cloud e si decidano, finalmente, a utilizzare strumenti specializzati per la gestione degli accessi.

Condividi l’articolo

Infrastrutture critiche a rischio: il bug è nelle VPN

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/30/skyark-uno-strumento-gratuito-per-individuare-falle-negli-account-aws-e-azure/?utm_source=rss&utm_medium=rss&utm_campaign=skyark-uno-strumento-gratuito-per-individuare-falle-negli-account-aws-e-azure

Infrastrutture critiche a rischio: il bug è nelle VPN

Lug 29, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Le falle di sicurezza nei sistemi di controllo in remoto mettono a rischio i sistemi industriali. L'allarme lanciato dagli esperti del settore.

Aumentano le preoccupazioni per la possibilità di attacchi informatici ai danni dei sistemi industriali e, in particolare, alle infrastrutture che gestiscono servizi critici come energia, erogazione dell'acqua e trasporti.

Gli allarmi più recenti fanno riferimento alle falle di sicurezza che interessano i sistemi di controllo remoto e, in particolare, le VPN (Virtual Private Network) utilizzate per accedere ai sistemi che gestiscono le infrastrutture.

Secondo quanto riporta il **Claroty Research Team** in un report pubblicato sul blog ufficiale della società di sicurezza specializzata in analisi dei sistemi IT/OT, nelle ultime settimane sono emerse una serie di vulnerabilità che suscitano serie preoccupazioni riguardo alla possibilità di futuri

attacchi.

IL primo squillo ha riguardato una vulnerabilità (CVE-2020-14511) relativa ai router **Moxa** della serie **EDR-G902** ed **EDR-G903**. A seguire, sono arrivati indizi sulle falle di sicurezza dei prodotti di **Secomea** e **HMS Networks**.

Insomma: stiamo parlando di dispositivi e sistemi che vengono utilizzati per gestire i collegamenti in remoto di infrastrutture complesse dedicate alla gestione di impianti industriali.

Le vulnerabilità scoperte da **Sharon Brizinov** e **Tal Keren** consentirebbero, in pratica, di sfruttare una connessione remota per avviare l'esecuzione di codice sui dispositivi.

La collezione di bug individuati dai ricercatori comprende alcune falle di sicurezza che potrebbero essere sfruttate utilizzando come vettore di attacco una semplice mail.

Qualcosa di estremamente preoccupante, come il **Proof of Concept** (PoC) pubblicato in video che dimostra ocme sia possibile sviluppare uno strumento di compromissione che funziona con una semplicità disarmante.
[embedded content]

Claroty Demo Video of Secomea GateManager CVE-2020-14500 Exploit from BleepingComputer.com on Vimeo.

In conclusione, il tema della vulnerabilità delle infrastrutture critiche a eventuali attacchi informatici dimostra di essere più caldo che mai. E il fatto che i punti deboli siano presenti proprio nei sistemi di collegamento in remoto rappresenta un fattore ulteriore di preoccupazione.

Condividi l’articolo

SkyArk: uno strumento open per individuare falle in AWS e Azure Allarme QSnatch: il malware ha colpito più di 60.000 NAS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/29/infrastrutture-critiche-a-rischio-il-bug-e-nelle-vpn/?utm_source=rss&utm_medium=rss&utm_campaign=infrastrutture-critiche-a-rischio-il-bug-e-nelle-vpn

---

Allarme QSnatch: il malware ha colpito più di 60.000 NAS

Lug 28, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La botnet prende di mira i dispositivi QNAP per installare una backdoor che consente ai pirati di accedere a qualsiasi contenuto memorizzato.

L'allarme arriva direttamente dalla statunitense **CISA** (Cybersecurity and Infrastructure Security Agency) e dalla britannica **NCSC** (National Cyber Security Centre). Lo spauracchio del momento è invece **QSnatch**, un malware comparso nell'ormai lontano 2014 e che prende di mira i NAS marchiati **QNAP**.

Secondo gli analisti delle due agenzie, negli ultimi mesi QSnatch avrebbe incrementato la sua attività, raggiungendo una diffusione davvero notevole. Se nell'ottobre del 2019 erano stati individuati 7.000 dispositivi infetti, a metà di giugno sono diventati più di 62.000. I bersagli, rappresentati per lo

più da aziende, sono concentrati nell’Europa occidentale e negli Sti Uniti.

Nel rapporto pubblicato su Internet, gli esperti della CISA spiegano quali siano le caratteristiche del malware, che è composto da più moduli. Uno di questi visualizza una versione “alterata” della pagina di login, che consente ai pirati informatici di sottrarre le credenziali di accesso e prendere così il controllo del dispositivo.

QSnatch, però, integra anche altre funzionalità, tra cui una **backdoor SSH** che consente ai pirati informatici di eseguire codice in remoto sul dispositivo. In altre parole: una volta installato il malware, i cyber criminali possono aggiungere qualsiasi funzionalità desiderino.

QSnatch integra in ogni caso una funzione che consente di esfiltrare dati verso il server che lo controlla, trasformando il malware in u perfetto strumento per il furto di informazioni sensibili.

Il report, anche se non contiene alcun riferimento a possibili attribuzioni degli attacchi. Un’anomalia, in tempi in cui qualsiasi attività cyber viene normalmente collegata all’attività di gruppi hacker collegati a governi e servizi

segreti stranieri. In questo caso, forse, a fare impressione sono bastati numeri.

Condividi l’articolo

Hacker attacca la botnet Emotet. Payload sostituito con immagini GIF

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/28/allarme-qsnatch-il-malware-ha-colpito-piu-di-60-000-nas/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-qsnatch-il-malware-ha-colpito-piu-di-60-000-nas

---

Hacker attacca la botnet Emotet. Payload sostituito con immagini GIF

Lug 27, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 0

Il vigilante sta facendo letteralmente a pezzi la rete di computer controllati dai pirati informatici

sostituendo il malware con immagini animate.

Contrattempo imprevisto per i pirati informatici che gestiscono la temibile botnet **Emotet**. Una delle più pericolose e coriacee botnet in circolazione sta subendo un attacco devastante da parte di un vigilante che sembra intenzionato a metterla K.O.

Tutto è cominciato lo scorso 21 luglio, quando il gruppo **Cryptolaemus** (un team di hacker etici che sta da tempo contrastando la diffusione di Emotet) ha rilevato una curiosa azione di sabotaggio diretta alla botnet.

Emotet, in realtà, era sparita dalla circolazione per quasi cinque mesi ed è tornata a far parlare di sé la scorsa settimana. I cyber criminali che la gestiscono sono ben conosciuti nell'ambiente della cyber security, ma la loro fama non è dovuta a grandi capacità tecniche. Tutt'altro.

La botnet Emotet, piuttosto, è da sempre considerata una sorta di gigante dai piedi d'argilla. I pirati che diffondono il malware, infatti, utilizzano uno schema di diffusione che prevede l'uso di messaggi di posta elettronica che contengono allegati malevoli.

Lo schema d'infezione, però, si appoggia su una rete di siti Web compromessi (su piattaforma **WordPress**) che vengono usati come "contenitori" per il payload che viene scaricato al momento dell'infezione.

È proprio il sistema di controllo di questi siti Internet che rappresenta il punto debole della botnet Emotet. I pirati, infatti, per controllarli utilizzano delle **Web Shell** open source piuttosto elementari. **Di più: secondo gli hacker di Cryptolaemus, usano sempre la stessa password**.

Il misterioso vigilante, a quanto pare, avrebbe scoperto la password e avrebbe cominciato a sabotare sistematicamente tutti i siti che i cyber criminali usano come rete di supporto

per distribuire il malware, sostituendo l’eseguibile che contiene il malware con delle innocue GIF animate.

Come riporta ZDNet in un articolo, questa azione avrebbe innescato una sorta di “gara” tra il vigilante (che ora sta usando una GIF di **HackerMan**) e i pirati informatici, che starebbero cercando di ripristinare la loro rete. Nonostante gli sforzi dei criminali, al momento la botnet funzionerebbe a un quarto delle sue abituali capacità.

Nessun indizio, invece, riguardo l’identità del misterioso vigilante. Non è escluso, però, che si tratti di un pirata informatico parte di un gruppo rivale, che abbia come unico obiettivo quello di liberare “fette di mercato” su Internet.

Condividi l’articolo

La botnet Prometei usa ancora EternalBlue… davvero?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/27/hacker-attacca-la-botnet-emotet-payload-sostituito-con-immagini-gif/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-attacca-la-botnet-emotet-payload-sostituito-con-immagini-gif