Estensioni per Chrome rimosse dallo store. Facevano “cookie stuffing”

Set 20, 2019 Marco Schiaffino Hacking, In evidenza, Malware, News, RSS 0

Bloccavano la pubblicità, ma all’interno del codice era nascosta una funzionalità che permetteva ai pirati informatici di lucrare sugli acquisti degli utenti.

Erano disponibili sul Web Store, ma dopo la segnalazione di un ricercatore di **AdGuard** le due estensioni malevole per **Chrome** sono state rimosse da **Google**.

Si trattava di due **ad-blocker**, cioè delle estensioni pensate per bloccare gli annunci pubblicitari nel corso della navigazione. **AdBlock** e **UBlock** (i nomi sono gli stessi di due estensioni piuttosto popolari) venivano proposte gratuitamente per il download, ma il loro scopo andava ben al di là di quanto dichiarato nella loro descrizione.

Una volta installate sul browser, le due estensioni bloccano effettivamente le pubblicità. Il loro codice, infatti, è basato su quello di AdBlock, l’estensione legittima che su Web Store risulta essere stata scaricata da più di 10 milioni di utenti.

Come spiegano i ricercatori nel loro report, però, la loro attività non si esaurisce qui. Le due estensioni, infatti, contattano periodicamente un server. Per circa 55 ore, spiegano dalle parti di AdGuard, le comunicazioni sono assolutamente normali.

Dopo questo periodo di tempo, però, le cose cambiano. Il server invia infatti una serie di comandi che vengono eseguiti dall'estensione e che hanno l'obiettivo di portare a termine un attacco che gli esperti chiamano **cookie stuffing**.

Il trucchetto funziona così: quando l'utente si collega a un particolare sito (nel report viene fatto l'esempio di teamviewer.com) l'estensione scarica e installa sul browser un particolare cookie che viene usato di solito come un sistema di riconoscimento per l'affiliazione a un sito di e-commerce. Si tratta di uno strumento che consente di retribuire chi collabora alla vendita di prodotti online.

In pratica, per rimanere all'esempio citato, se il visitatore

fa un acquisto sul sito il proprietario dell'estensione riceve una commissione da parte di TeamViewer come se avesse "favorito" l'acquisto.

Si tratta, in pratica, di una frode che sfrutta la navigazione degli inconsapevoli utenti per spillare denaro illegalmente alle aziende che vendono prodotti e servizi su Internet.

I ricercatori hanno individuato un elenco piuttosto nutrito di siti con cui scatta questo meccanismo e spiegano che si tratta solo di una piccola parte dell'elenco completo.

Le due estensioni, spiegano infine gli analisti, contengono anche delle funzionalità che hanno lo scopo di offuscare l'attività fraudolenta. **Se l'estensione rileva che è stata aperta una console per sviluppatori, ad esempio, sospende ogni attività illecita**.

Ora Google ha rimosso dal suo Web Store le due estensioni fraudolente. Resta il problema di chi le ha installate nel recente passato.

Condividi l'articolo

Quante vulnerabilità per i NAS! Sono 125 per 13 modelli

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/20/estensioni-per-chrome-rimosse-dallo-store-facevano-cookie-stuffing/

Quante vulnerabilità per i NAS! Sono 125 per 13 modelli

Set 19, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Un nuovo report mette in evidenza la presenza di falle di sicurezza spaventose nei modelli più diffusi per utenti privati e piccoli uffici.

Rientrano nella grande famiglia della **Internet of Things (IoT)** ma hanno caratteristiche tutte loro. I **NAS**, oltre a condividere la generalizzata vulnerabilità agli attacchi dei dispositivi IoT, pongono infatti anche un altro problema: al loro interno sono custoditi dati di ogni genere, anche quelli che definiremmo "sensibili".

La notizia (se così la possiamo chiamare) è che stando al report **SOHOpelessly Broken 2.0** pubblicato dai ricercatori di **ISE (Independent Security Evaluators)** questa particolare categoria di dispositivi è esposta ad attacchi di ogni genere.

Dal documento pubblicato su Internet, che riassume uno studio che ha preso in considerazione 13 modelli SOHO (Small Office – Home Office) tra i più diffusi, emergono la bellezza di **125 vulnerabilità** che mettono a rischio la riservatezza dei dati memorizzati nei dispositivi e la sicurezza stessa delle reti a cui sono collegati.

Le falle di sicurezza individuate dai ricercatori comprendono la possibilità di portare “classici” attacchi di **Cross-Site Scripting**, **Cross-Site Request Forgery** così come iniezioni di comandi e altre tecniche di attacco, che possono essere portate sia in remoto (purtroppo molto spesso) che dalla rete locale. **In sintesi, in seguito ai test i ricercatori sono riusciti a ottenere il controllo completo di 12 dispositivi su 13**.

La cosa più preoccupante è che in almeno in 5 modelli è possibile aggirare i sistemi di autenticazione per accedere all'interfaccia di configurazione e che in 7 dispositivi gli esperti sono riusciti a caricare file sfruttando vulnerabilità nel sistema di gestione degli upload. Per la cronaca, l'unico NAS a uscire "pulito" dai test è stato il **Synology DS218j**.

Buona parte delle vulnerabilità individuate sono già state corrette dai produttori. La procedura di disclosure, spiegano i ricercatori, non è però stata sempre facile. Alcuni dei produttori (**Drobo**, **Buffalo Americas**, e **Zioncom Holdings**) non hanno affatto risposto alle segnalazioni.

Dal report, in definitiva, emerge un elemento piuttosto interessante. Se abbiamo a cuore la sicurezza dei nostri sistemi, prima di verificare le caratteristiche di un dispositivo, dovremmo forse verificare che il produttore abbia un programma di bug bounty o partecipi a un programma collettivo.

In caso contrario potremmo ritrovarci tra le mani un dispositivo che potrebbe essere, sotto il profilo della cyber-security, un vero groviera.

Condividi l’articolo

Estensioni per Chrome rimosse dallo store. Facevano “cookie stuffing” Apocalisse privacy: dati sensibili di milioni di utenti sul Web

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/19/quante-vulnerabilita-per-i-nas-sono-125-per-13-modelli/

Apocalisse privacy: dati sensibili di milioni di

utenti sul Web

Set 18, 2019 Marco Schiaffino In evidenza, Leaks, News, Privacy, RSS, Vulnerabilità 0

In poche ore sono stati scoperti due leak di dimensioni spaventose. Online i dati sanitari di 24 milioni di persone e di milioni di clienti Lion Air.

Niente da fare: il vizietto di "perdere" dati sensibili su Internet sembra davvero difficile da cancellare. A dimostrare quanto il fenomeno sia ampio, in queste ore ci pensano due casi clamorosi riportati da numerosi esperti di sicurezza.

Il primo riguarda **Lion Air**, la più grande compagnia aerea privata indonesiana che avrebbe "perso" i dati personali di decine di milioni di passeggeri.

Stando a quanto riporta un ricercatore che su Twitter si fa chiamare **Under The Breach**, i dati sarebbero contenuti in due database collegati a Lion Air che circolano da almeno un mese nei forum specializzati nella compravendita di dati.

I due archivi sembrano provenire da **Malindo Air** e **Thai Lion Air** (entrambe di proprietà di Lion Air) e, secondo le prime ricostruzioni, potrebbero provenire (tanto per cambiare) da un **Bucket AWS** che sarebbe stato lasciato online senza alcuna protezione e di cui si è avuta notizia già ad agosto.

Non è chiaro, invece, quale tipo di informazioni siano contenuti nei database. Probabile però che ci siano dati sufficienti a consentire ai pirati informatici di sfruttarli per attacchi di phishing o truffe online.

Il secondo episodio riguarda invece il settore medico e, in particolare, alcuni server che contengono i dati sanitari di circa **24 milioni di persone**.

A lanciare l'allarme è stata la società di sicurezza **Greenbone**, che nel suo report spiega che i dati sensibili sono ospitati su dei server **PACS (Picture Archiving and Communication Systems)**, una tipologia di server utilizzata per memorizzare immagini ottenute attraverso analisi mediche come radiografie, risonanze magnetiche e simili.

Molti di questi, però, non hanno alcuna forma di protezione e vi si può accedere senza che sia necessario inserire delle credenziali.

I ricercatori ne hanno fatto un censimento e ne hanno individuati numerosi nel Regno Unito, negli USA, Canada, Germania, Francia, Giappone, Russia e Svizzera.

Al loro interno ci sono circa **700 milioni di immagini organizzate in 24 milioni di record**, che potrebbero contenere anche informazioni sensibili come i nomi dei pazienti, il numero di previdenza sociale (per quanto riguarda gli Stati Uniti), date ed esiti degli esami, nomi di medici e tecnici di laboratorio.

Usiamo il condizionale perché i ricercatori di Greenbone specificano di non aver scaricato il contenuto del server ma

di essersi limitati a eseguire il conteggio dei file visibili. I prossimi che dovessero individuare i server in questione (o chi li ha già individuati) potrebbero però essere meno corretti.

Condividi l’articolo

Simjacker mette a rischio privacy e sicurezza di 1 miliardo di telefoni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/18/apocalisse-privacy-dati-sensibili-di-milioni-di-utenti-sul-web/

Simjacker mette a rischio privacy e sicurezza di 1 miliardo di telefoni

Set 17, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS, Vulnerabilità 0

La tecnica di attacco permette di colpire qualsiasi

modello di telefono sfruttando una vulnerabilità nel codice delle SIM. E viene usato da due anni…

Potremmo definirla una vulnerabilità "democratica", che colpisce sia gli smartphone **Android**, sia quelli con sistema **iOS**.

Stiamo parlando di **Simjacker**, la tecnica di attacco scoperta dai ricercatori di **AdaptiveMobile Security** e che interessa almeno **un miliardo di dispositivi** in tutto il mondo.

La chiave di tutto è **S@T Browser**, una funzionalità integrata nelle SIM dei telefoni e che viene normalmente utilizzata per visualizzarne il contenuto. Il problema è che S@T Browser può anche ricevere istruzioni attraverso semplici messaggi SMS che contengono istruzioni **SIM Toolkit (STK)**.

Come spiegano i ricercatori nella pagina Web dedicata a Simjacker, l'invio di questi comandi avviene in maniera del tutto "trasparente" per il proprietario del dispositivo. **In altre parole: la ricezione del messaggio non viene segnalata in alcun modo e consente, di conseguenza, di portare un attacco silenzioso e invisibile**.

Ma quali sono le azioni che si possono compiere attraverso l'invio di comandi con Simjacker? L'attacco individuato dai ricercatori è, in buona sostanza, un sistema per tenere sotto controllo la posizione della vittima.

Attraverso un semplice SMS, infatti, è possibile istruire la SIM per inviare una risposta con **la posizione rilevata dal GPS** (o l'identificativo della cella a cui il telefono è collegato se non è dotato di GPS) a un numero predefinito.

Secondo gli analisti di AdaptiveMobile Security, questo attacco è stato utilizzato per almeno due anni da quella che i ricercatori definiscono “una società specializzata nel cyber-spionaggio”.

Non ne fanno il nome, ma molti esperti di sicurezza hanno fatto notare che la descrizione corrisponde ad almeno un paio di aziende di spionaggio (per esempio **NSO Group**) specializzate nella fornitura di strumenti di controllo a governi (non sempre di specchiata democraticità) e forze di polizia.

L’uso dei comandi STK, però, apre potenzialmente la strada

anche ad altri tipi di attacchi che possono avere conseguenze decisamente più gravi.

Attraverso l'invio di SMS confezionati ad hoc sarebbe possibile, infatti, forzare la SIM a effettuare telefonate o ad aprire automaticamente pagine Web. Un pirata informatico, di conseguenza, potrebbe avviare a distanza una chiamata a un numero a pagamento per frodare la vittima.

La possibilità di "forzare" l'apertura di una pagina Web rappresenta invece un vettore di attacco formidabile per portare attacchi di phishing o colpire uno smartphone con un malware, sfruttando per esempio un exploit inserito nel codice della pagina stessa.

Insomma: gli scenari che si aprono sono devastanti e, almeno per il momento, non si vede quale possa essere la soluzione per correggere la vulnerabilità. **A peggiorare la situazione, poi, c'è il fatto che le SIM vulnerabili vengono stimate in circa 1 miliardo**.

Nel report dedicato a Simjacker, i ricercatori si rivolgono infatti direttamente agli operatori telefonici (gli stessi che hanno lasciato un software obsoleto e pericoloso sulle loro SIM) suggerendo di mettere in atto policy che siano in grado di filtrare i messaggi per bloccare quelli potenzialmente dannosi.

Condividi l'articolo

Esperti di sicurezza arrestati per effrazione. "Stavamo lavorando"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/17/simjacker-mette-a-rischio-privacy-e-sicurezza-di-1-miliardo-di-telefoni/

Esperti di sicurezza arrestati per effrazione. “Stavamo lavorando”

Set 16, 2019 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario 1

I due pen-tester, assoldati per mettere alla prova i sistemi di sicurezza, si sono introdotti in un edificio della Corte di Giustizia in Iowa.

Non c’è alcun dubbio: la vicenda riportata dal **Des Moines Register** lo scorso venerdì dovrebbe essere inserita sotto il titolo “Inconvenienti del mestieri che non dovrebbero capitare”.

Gli sfortunati protagonisti della vicenda sono **Gary Demercurio** e **Justin Wynn**, due esperti di sicurezza della società **Coalfire** specializzati in penetration testing, cioè nella valutazione del livello di sicurezza dei sistemi informatici.

Un’attività che professionisti di questo genere svolgono, in buona sostanza, portando veri e propri attacchi ai sistemi dei clienti che li hanno assunti.

Come viene riportato nell'articolo del giornale locale, i due pen-tester sono stati arrestati mercoledì scorso per essersi introdotti all'interno del **Tribunale della contea di Dallas (Iowa)** utilizzando "numerosi strumenti di scasso".

Già al momento dell'arresto, si legge, i due si sono giustificati spiegando di essere stati ingaggiati proprio dall'autorità giudiziaria e di aver compiuto l'effrazione nell'ambito della loro attività professionale.

Il ricorso a violazioni "fisiche" degli spazi delle aziende che commissionano attività di penetration testing è tutt'altro che raro. Anzi: in molti casi si tratta di un aspetto fondamentale nella valutazione complessiva dei sistemi di sicurezza e protezione dei dati. **La Corte della contea di Dallas, a quanto pare, non è di questa opinione**.

Secondo quanto si legge in un comunicato ufficiale, le autorità avrebbero sì confermato di aver ingaggiato Coalfire per mettere alla prova i loro sistemi di sicurezza informatica, ma avrebbero specificato di **non aver mai inteso**

che l’attività degli esperti di sicurezza potesse comprendere attacchi “fisici” alle strutture del tribunale.

Ora Demercurio e Wynn si trovano in una situazione decisamente spinosa. Secondo quanto riporta **The Register**, un portavoce di Coalfire avrebbe rassicurato sulla correttezza delle procedure seguite dalla società di sicurezza nel corso di tutte le sue attività di penetration testing.

Tuttavia, l’azienda ha specificato di non ritenere opportuno fornire ulteriori dettagli sulla vicenda specifica, sia per non violare il rapporto di riservatezza con il cliente, sia a causa del fatto che c’è un’indagine in corso.

Condividi l’articolo

Il gruppo cinese Thrip prende di mira i sistemi satellitari

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/16/pen-tester-esperti-di-sicurezza-arrestati-per-effrazione-stavamo-lavorando/

Il gruppo cinese Thrip prende di mira i sistemi satellitari

Set 13, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS, Scenario 0

Gli hacker al soldo di Pechino agiscono tenendo un basso profilo ma puntano a obiettivi di alto livello. Gli esperti: "forse puntano a sabotare i sistemi satellitari".

In gergo sono chiamati **APT (Advanced Persistent Threat)** e rappresentano la punta di diamante dei servizi segreti nella cyber-guerrilla. Tra i più pericolosi (e attivi) ci sono quelli collegati al governo di **Pechino**, i cui obiettivi spaziano tra lo spionaggio industriale e l'acquisizione di informazioni di inteligence.

Il nuovo report di **Symantec**, pubblicato sul blog della società di sicurezza informatica, accende i riflettori su **Thrip**, un gruppo APT attivo da tempo (i ricercatori l'hanno individuato per la prima volta nel giugno del 2018) e che negli ultimi tempi ha intensificato la sua attività.

I cyber-spioni che fanno riferimento a Thrip rappresentano una categoria particolarmente £"rognosa" per gli esperti di sicurezza. Come spiegano i ricercatori nel report dell'anno scorso, gli hacker utilizzano tecniche di attacco che sfruttano normali strumenti di amministrazione, che lasciano ben poche tracce e gli consentono di agire mantenendo un basso profilo che rende più difficile la loro individuazione.

In passato, Thrip ha preso di mira principalmente aziende di telecomunicazioni, società operanti nel settore della difesa e anche aziende che gestiscono operativamente i sistemi satellitari. Un dettaglio, quest'ultimo, che aveva suscitato anche un certo allarme legato alla possibilità che il reale obiettivo dei pirati informatici fosse quello di portare a termine operazioni di sabotaggio in grado di mettere K.O. le reti satellitari.

La nuova analisi si concentra proprio su questo aspetto. **Thrip, infatti, avrebbe continuato a mantenere nel centro del mirino proprio le società coinvolte nella gestione delle trasmissioni via satellite e, in particolare, i dipartimenti che si occupano della gestione operativa dei satelliti stessi**.

Una scoperta che, specificano dalle parti di Symantec, è stata possibile solo grazie all'uso della tecnologia **Targeted Attack Analytics (TAA)**, che utilizza sistemi di intelligenza artificiale per individuare attacchi che, con gli strumenti tradizionali, rischierebbero di passare inosservati.

Gli attacchi più recenti, gli ultimi dei quali risalgono al luglio 2019, hanno fornito ai ricercatori anche degli elementi ulteriori che permettono di inquadrare meglio l'attività del gruppo.

Tra gli strumenti adottati, infatti, c'è una nuova backdoor (battezzata con il nome di **Sagerunex**) che gli hacker utilizzano per garantirsi la persistenza di acceso ai sistemi compromessi.

L'analisi del codice di Sagerunex avrebbe evidenziato, si legge nel report, notevoli similitudini con uno strumento simile che gli esperti conoscono con il nome di **Evora** e che è

stato utilizzato in passato da un altro gruppo di cyber-spioni: **Billbug**.

Insomma: secondo gli esperti di Symantec, l'attività di Thrip si inserirebbe in una più ampia campagna di spionaggio condotta da diversi gruppi ma orchestrata da un'unica mano. Con tutta probabilità, quella di Pechino.

Condividi l'articolo

Ryuk: ransomware e furto di documenti in un colpo solo?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/13/il-gruppo-cinese-thrip-prende-di-mira-il-sud-est-asiatico/

Ryuk: ransomware e furto di documenti in un colpo solo?

Set 12, 2019 Marco Schiaffino In evidenza, Malware, Minacce, News 0

Un nuovo malware derivato dal ransomware setaccia i

file presenti sul computer alla ricerca di documenti confidenziali da rubare.

Le strategie adottate dai cyber-criminali nelle loro azioni sono spesso "spezzettate" in diverse fasi. Non è raro, per esempio, che a un primo attacco ne seguano altri, portati attraverso ulteriori moduli dello stesso malware o nuovi strumenti di attacco che vengono installati sfruttando l'accesso al sistema.

È quello che gli appassionati di videogiochi chiamerebbero una "combo", cioè una successione di mosse che ottimizzano il danno. Il caso più classico è quello di un attacco tramite un trojan che ruba informazioni al quale segue l'installazione di un ransomware (acquistato ad hoc sul mercato nero) una volta che il computer infetto è stato "spolpato" a sufficienza.

Il caso di **Ryuk**, però, rappresenta un'anomalia. Come spiega **Bleeping Computer** in un articolo, gli autori del ransomware sembrano aver fatto il percorso inverso.

I ricercatori di **MalwareHunterTeam**, infatti, avrebbero individuato un malware programmato per rubare documenti che sembra essere stato sviluppato a partire dal codice di Ryuk e pensato per agire in contemporanea con il ransomware.

Come spiegano gli analisti, si tratta di un "info stealer" che passa al setaccio tutti i file memorizzati all'interno del computer cercando in particolare file **Word** ed **Excel**, di cui analizza le caratteristiche per verificare che si tratti effettivamente di documenti di testo o fogli di calcolo.

Nella sua ricerca, il malware utilizza la stessa tecnica del ransomware, utilizzando una black list che gli permette di ottimizzare la sua attività evitando le cartelle di sistema o quelle che contengono software come "Intel", "Windows", "Mozilla" e simili.

Gli autori del malware, inoltre, sembrano avere le idee

abbastanza chiare su quello che vogliono trovare. I file individuati vengono infatti analizzati alla ricerca di alcune parole chiave come “marketwired”, “10-Q”, “fraud”, “hack”, “tank”, “defence”, “military”, “checking”, “classified”, “secret”, “clandestine”, undercover”, “federal”.

L’impressione, insomma, è che siano particolarmente interessati a documenti riservati (soprattutto in ambito militare e di intelligence) o collegati al settore finanziario.

Non solo: la ricerca comprende anche una serie di nomi propri (come Emma, Liam, Olivia, Noah) che secondo i colleghi di Bleeping Computer corrispondono ai nomi più usati negli Stati Uniti per i neonati nel 2018 secondo una statistica del dipartimento della Social Security statunitense.

L’ipotesi è che i pirati informatici intendano usare questo filtro per trovare informazioni riguardanti neonati per usare queste informazioni in una frode fiscale di cui abbiamo già parlato tempo fa. **I documenti considerati “interessanti” vengono inviati a un server FTP controllato dai pirati**.

Da un punto di vista operativo, è difficile capire quale possa essere l’esatta strategia dei pirati. Quello che è certo è che il malware è pensato per lavorare su un computer in cui è già presente il ransomware Ryuk. Tra i file da ignorare, infatti, compaiono anche **RyukReadMe.txt** (il documento creato dal ransomware per chiedere il riscatto) e tutti i file con estensione.**RYK**.

Molto probabilmente si tratta di una sorta di modulo aggiuntivo pensato per operare in contemporanea e presumibilmente prima che il ransomware proceda alla codifica dei file.

Condividi l’articolo

Falla nei load balancer BIG-IP di F5 Networks. Aziende a rischio attacco

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/12/ryuk-ransomware-e-furto-di-documenti-in-un-colpo-solo/

Falla nei load balancer BIG-IP di F5 Networks. Aziende a rischio attacco

Set 11, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

La vulnerabilità mette a rischio i sistemi informatici di banche, enti pubblici e grandi aziende. Gli esperti di F-Secure: "cambiate la configurazione".

Un bug a livello di codice espone migliaia di aziende ed enti pubblici a un possibile attacco da parte dei pirati informatici.

L'allarme arriva da **F-Secure**, che in un report pubblicato su Internet segnala il rischio che i cyber-criminali possano sfruttare la vulnerabilità come "testa di ponte" per portare attacchi alle infrastrutture informatiche che utilizzano i dispositivi **BIG-IP** di **F5 Networks**.

BIG-IP è un **load balancer**, cioè un dispositivo che ha il compito di gestire il traffico di rete per garantirne il corretto funzionamento ed evitare blocchi provocati dalla congestione delle reti. Device come questi sono utilizzati normalmente da organizzazioni governative, banche e grandi corporation.

Secondo quanto riporta **Christoffer Jerkeby**, il ricercatore di F-Secure che ha individuato il problema, la falla si annida nel linguaggio di programmazione Tcl, usato per scrivere le iRules di BIG-IP, cioè la funzione dedicata all'indirizzamento del traffico in entrata.

Nel dettaglio, il problema riguarda un’errata configurazione che consentirebbe a un attaccante di iniettare comandi che gli consentirebbero di intercettare e manipolare il traffico Web o colpire altri bersagli all’interno delle reti e gli stessi utenti che accedono ai servizi.

Secondo Jerkeby, la gravità della falla di sicurezza è amplificata dal fatto che qualsiasi azione di questo tipo non viene registrata a livello di log, rendendo così un eventuale attacco molto difficile da individuare o ricostruire.

“Questa problematica di configurazione è davvero grave perché un attaccante può entrare furtivamente, raggiungere una gran varietà di obiettivi, e poi coprire le sue tracce. Inoltre, molte organizzazioni non sono preparate per trovare e risolvere problematiche che sono sepolte in profondità nella supply chain software, il che porta a un più grande problema per la sicurezza” spiega Jerkeby. “Finché non sai cosa cercare, è difficile prevedere che si sta verificando questo problema, e ancora più difficile affrontarlo in un attacco

reale.”

Ma quali sono le dimensioni del problema? **Il ricercatore, nel corso della sua analisi, ha individuato più di 300,000 implementazioni BIG-IP attive su internet**. Circa il 60 percento delle istanze di BIG-IP che ha trovato erano negli Stati Uniti. Difficile però capire quanti siano a rischio attacco.

“A meno che un’organizzazione non abbia svolto un’indagine approfondita su questa tecnologia, esiste una forte probabilità che abbia questo problema” afferma Jerkeby. “Anche qualcuno incredibilmente ben informato sulla sicurezza che lavora in un’azienda con risorse adeguate può commettere questo errore. Pertanto, diffondere la consapevolezza del problema è molto importante se vogliamo aiutare le organizzazioni a proteggersi meglio da un potenziale scenario di violazione”.

Il rischio è che i pirati informatici sfruttino l’occasione utilizzando un sistema di scansione di massa di Internet per identificare e colpire le istanze vulnerabili della tecnologia. Il consiglio, quindi, è di indagare da subito per verificare la presenza della vulnerabilità.

Jerkeby ha contribuito a sviluppare alcuni strumenti gratuiti e open source che le organizzazioni possono utilizzare per identificare configurazioni non sicure nelle loro implementazioni BIG-IP. Ma secondo il ricercatore, non esiste una soluzione rapida per problemi di sicurezza come questi, quindi spetta alle singole organizzazioni affrontare il problema.

“L’aspetto positivo di questo tipo di problema di sicurezza è che non tutti quelli che usano il prodotto saranno interessati. **Ma il rovescio della medaglia è che il problema non può essere risolto con una patch o un aggiornamento del software del fornitore, quindi spetta alle organizzazioni fare**

il lavoro per verificare se hanno questo problema e, se lo trovano, risolverlo” spiega. “Ecco perché è importante che chiunque usi BIG-IP agisca subito”.

Condividi l’articolo

Il trojan Stealth Falcon sfrutta le funzioni di Windows Update

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/11/falla-nei-load-balancer-big-ip-di-f5-networks-aziende-a-rischio-attacco/

Il trojan Stealth Falcon sfrutta le funzioni di Windows Update

Set 10, 2019 Marco Schiaffino In evidenza, Malware, Minacce, News, RSS 0

La nuova versione del malware utilizza il servizio BITS per comunicare con il server Command and Control aggirando firewall e antivirus.

È in circolazione da almeno 7 anni, ma non smette di

evolversi. Stiamo parlando di **Stealth Falcon**, un trojan comparso nel 2012 che oggi utilizza nuove tecniche di comunicazione in grado di renderne ancora più difficile l'individuazione.

Stealth Falcon è un classico strumento di cyber-spionaggio ed è stato utilizzato in passato per colpire dissidenti politici nell'area mediorientale.

Secondo **Citizen Lab**, che già nel 2016 ha pubblicato un'inchiesta sulla vicenda legata a un attacco che aveva preso di mira il giornalista **Rori Donaghy**, si tratterebbe di uno strumento utilizzato dai servizi segreti degli **Emirati Arabi Uniti**.

Un collegamento confermato anche da un'altra inchiesta, questa volta pubblicata da **Reuters** nel gennaio di quest'anno, che anche se usa un altro nome (**Project Raven**) sembra riferirsi allo stesso gruppo di cyber-spioni, composto da **ex-agenti della NSA** reclutati dal governo degli Emirati Arabi Uniti.

Un background che spiegherebbe il livello di sofisticazione del malware, che in un report di **ESET** viene definito come un malware che dimostra un "approccio sistematico alla raccolta di dati, la loro esfiltrazione, alla possibilità di aggiungere ulteriori strumenti e aggiornare la sua configurazione".

I comandi a disposizione dei cyber-spioni sono piuttosto elementari. Il vero elemento su cui si concentra l'attenzione dei ricercatori di ESET, però, è la tecnica usata da Stealth Falcon per comunicare con i server Command and Control.

Al posto di usare una "semplice" backdoor, il malware sfrutta infatti il servizio **BITS** (**Background Intelligent Transfer Service**) di Windows. Si tratta di una funzionalità utilizzata principalmente per gli aggiornamenti del sistema operativo e di alcuni software, oltre che dai programmi di messaggistica.

BITS è progettato per ottimizzare il trasferimento dei dati, consentendo di spostare grandi quantità di informazioni senza congestionare la rete. **Le comunicazioni di Stealth Falcon, quindi, hanno una buona probabilità di passare inosservate, anche quando il trojan trasmette al server C&C grandi quantità di dati**.

Non solo: considerando la funzione "normale" di BITS, le comunicazioni di questo servizio sono di solito autorizzate automaticamente dal firewall. Il trasferimento, inoltre, viene ripreso automaticamente anche in caso di blocco temporaneo

della rete, riavvio della macchina o disconnessione dell’utente.

Insomma: si tratta in buona sostanza di un canale preferenziale con caratteristiche perfette per garantire l’efficacia delle comunicazioni verso il server controllato dai pirati informatici.

Oltre all’utilizzo di BITS, Stealth Falcon si distingue anche per un’altra particolarità. Prima dell’avvio del payload principale, infatti, il malware importa una gran quantità di dati dal sistema infetto, che poi non utilizza.

Secondo i ricercatori di ESET potrebbe rappresentare una tecnica di evasione, che punta a “confondere” eventuali sistemi antivirus.

Condividi l’articolo

Toyota vittima di una truffa via email. Rubati 37 milioni di dollari

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/10/il-trojan-stealth-falcon-sfrutta-le-funzioni-di-windows-update/

Toyota vittima di una truffa via email. Rubati 37 milioni di dollari

Set 09, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS 0

L'azienda giapponese avrebbe subito un attacco attraverso un account email compromesso. Una conseguenza dell'attacco dello scorso marzo?

La vittima è di quelle eccellenti. A finire vittima dell'ennesima truffa milionaria è stata infatti una succursale europea di **Toyota**, l'azienda giapponese conosciuta per lo più per la sua attività nel settore automotive.

Stando alle (scarse) informazioni divulgate dalla dirigenza di Toyota, la frode sarebbe una classica **BEC (Business Email Compromise)** portata ai danni della sua sussidiaria europea.

Lo schema BEC, di cui abbiamo parlato ampiamente anche in questo articolo, sfrutta una strategia piuttosto semplice. Tutto comincia con la compromissione di un account di posta elettronica di un dirigente o di un responsabile amministrativo dell'azienda.

L'indirizzo di posta elettronica viene utilizzato dai pirati informatici per dirottare i pagamenti dell'azienda sui conti controllati dai cyber-criminali. Normalmente questo avviene inviando ordini di pagamento verso reali fornitori in cui le coordinate bancarie sono modificate ad arte.

In alcune varianti, però, gli esperti di sicurezza hanno visto anche prendere di mira gli uffici delle amministrazioni per

modificare direttamente gli estremi di pagamento dei dipendenti e fare in modo che gli stipendi siano accreditati su conti correnti diversi.

Secondo un recente report dell'FBI, le truffe BEC nel 2018 avrebbero fruttato ai cyber-criminali più di 1,2 miliardi di dollari.

Nel caso specifico, il laconico comunicato di Toyota non offre alcuno spunto che permetta di ricostruire gli esatti contorni della vicenda. L'unico dettaglio fornito riguarda la somma sottratta: **4 miliardi di yen (poco più di 37 milioni di dollari)** che l'azienda prevede di dover iscrivere come perdita a bilancio.

La truffa potrebbe essere la conseguenza diretta dell'attacco informatico che lo scorso marzo ha preso di mira i sistemi informatici di Toyota. In quel caso si era parlato solo della possibilità che gli hacker avessero messo le mani sui dati di **3 milioni di clienti**.

Non è escluso, però, che l'attacco abbia permesso ai criminali

di ottenere le informazioni che gli hanno permesso di portare a termine la truffa.

Condividi l’articolo

Su Internet i numeri di telefono di 419 milioni di utenti Facebook

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/09/toyota-vittima-di-una-truffa-via-email-rubati-37-milioni-di-dollari/