Ecco Silex, il nuovo "giustiziere" che mette K.O. i dispositivi IoT

Giu 27, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario, Vulnerabilità 0

L'autore del malware utilizza exploit conosciuti per rendere inutilizzabili i dispositivi vulnerabili. L'obiettivo? Impedire che vengano compromessi dai pirati.

Gli allarmi delle società di sicurezza, le notizie riguardo la nascita di nuove botnet e addirittura l'interessamento di alcuni governi non sono serviti a molto: il settore della "Internet of Things" o **IoT** continua a essere uno dei più vulnerabili agli attacchi informatici.

In particolare, i dispositivi IoT rimangono i bersagli privilegiati per i cosiddetti **script kid**, cyber-criminali con limitate capacità tecniche che usano exploit conosciuti per compromettere i device e inserirli nelle loro botnet, più o meno come accade nel 2016 quando comparve il famigerato **Mirai**.

La soluzione del problema, però, appare lontana. I produttori di router, videocamere IP e dispositivi "smart" di ogni genere e tipo stanno facendo qualcosa, ma l'impegno è del tutto insufficiente. **In parte perché gli scivoloni continuano ad avvenire, in parte perché ci sono già in circolazione milioni di device vulnerabili, che continuano a rappresentare un problema di sicurezza**.

A cercare di arginare il problema ci stanno pensando le società di sicurezza, che sempre più spesso mettono a

disposizione strumenti specifici per proteggere i dispositivi IoT o, per lo meno, individuare quelli vulnerabili.

C’è però un altro fenomeno: la comparsa di quelli che potremmo chiamare **giustizieri IoT**. Si tratta di hacker (cosiddetti “grey hat”) che adottano una strategia che molti considerano discutibile, ma che ha una certa efficacia.

L’idea dei giustizieri, in pratica, è di colpire i dispositivi IoT usando malware simili a quelli dei pirati ma che hanno un obiettivo diverso: metterli fuori uso per impedire che i cyber-criminali li possano usare per i loro scopi.

L’ultimo a comparire è stato **Silex**, un worm emerso in questi giorni che sta facendo strage di dispositivi IoT sfruttando delle vulnerabilità conosciute.

Come si legge nell’analisi pubblicata da **Larry Cashdollar**, ricercatore di **Akamai**, Silex utilizza delle credenziali predefinite per garantirsi l’accesso ai device, dopodiché avvia la sua azione distruttiva.

Il malware esegue per prima cosa un’analisi del disco per individuare le partizioni e, immediatamente dopo, cancella i dati presenti in memoria sostituendoli con informazioni casuali. Nel codice del malware, l’autore (che si fa chiamare

Light) ha inserito un messaggio che spiega la logica dell'operazione.

I dispositivi colpiti da Silex possono tornare a funzionare se viene reinstallato il firmware. Operazione che, se eseguita correttamente e utilizzando una versione aggiornata permetterebbe, tra le altre cose di proteggere dagli attacchi il dispositivo, sempre che il produttore abbia rilasciato le patch adeguate.

Purtroppo molti utenti non hanno nemmeno idea di cosa sia un firmware e di come si possa aggiornare o reinstallare.

L'avventura di Light, però, sembra essere finita. Secondo quanto riporta **Bleeping Computer** citando come fonte **Ankit Anubhav**, ricercatore di **NewSky**, l'hacker avrebbe deciso di abbandonare la community legata al mondo IoT. La sua azione, infatti, avrebbe creato troppo clamore e l'autore di Silex avrebbe deciso di uscire di scena.

Condividi l'articolo

Gli attacchi via email continuano ad aumentare

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/27/ecco-silex-il-nuovo-giustiziere-che-mette-k-o-i-dispositivi-iot/

Gli attacchi via email continuano ad aumentare

Giu 26, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Il report di FireEye fotografa la tendenza del cyber-crimine. In aumento il phishing, l'uso di link "sicuri" e di servizi cloud di condivisione dei file.

Anche a distanza di anni, la posta elettronica è uno dei vettori di attacco più usati dai pirati informatici. A confermarlo è la nuova ricerca di **FireEye**, che nel suo **Email Threat Report** relativo al primo trimestre 2019 delinea le tendenze sulla base dell'analisi di **1.3 miliardi di email**.

Il primo dato che emerge dall'analisi, che conferma una tendenza rilevata nel corso degli ultimi anni, è quello dell'utilizzo del phishing come tecnica di attacco preferita da parte dei cyber-criminali. In termini numerici, l'incremento dell'uso di questa tecnica è del 17%.

La tendenza è quella di prendere di mira popolari servizi Internet, con l'obiettivo di rubare le credenziali delle potenziali vittime. Tra i servizi più gettonati ci sono quelli **Microsoft**, con circa il 30% di tutti i rilevamenti, seguita da **OneDrive**, **Apple**, **PayPal** e **Amazon**.

A segnare un aumento considerevole (+26%) è anche l'uso del protocollo HTTPS per gli attacchi basati sull'uso di url malevole. Qui la logica fa leva sul falso senso di sicurezza collegato al fatto che i collegamenti utilizzano un protocollo "sicuro".

Tra le novità c'è l'utilizzo di piattaforme cloud per il file sharing utilizzate per distribuire malware. I pirati utilizzano servizi noti come **WeTransfer**, **Google Drive** e **OneDrive**. Il primato in questo settore è però di **Dropbox**, considerato da molti come uno strumento "normale" per condividere file e documenti.

Non rallenta, infine, il fenomeno della BEC **(Business Email Compromise)** che prevede l'uso di attacchi mirati e tecniche di

social engineering attraverso i quali i pirati informatici impersonificano dirigenti delle aziende per disporre trasferimenti di denaro che finiscono nelle tasche dei cyber-criminali.

In questo settore, i ricercatori FireEye hanno individuato due nuove varianti rispetto allo schema “classico” di cui abbiamo parlato anche in passato.

La prima è **rivolta all’ufficio paghe di un’organizzazione** con un’email contenente una richiesta di modifica dei dati personali di un dirigente, come i dati bancari, con l’obiettivo di trasferire la retribuzione di un dirigente verso un conto di terzi.

La seconda, invece, colpisce il dipartimento che segue la contabilità dei fornitori dove gli attaccanti impersonano, tramite email, **un fornitore di fiducia** per reindirizzare un pagamento fraudolento verso un conto di terzi.

“Gli attaccanti stanno facendo i loro compiti. Stiamo assistendo a nuove varianti degli attacchi di

impersonificazione che mirano a nuovi contatti e nuovi dipartimenti all'interno delle organizzazioni" commenta **Ken Bagnall, Vice President of Email Security di FireEye**. "Il pericolo è che queste nuove vittime potrebbero non essere preparate o possedere le conoscenze necessarie per identificare un attacco. Sfortunatamente, una volta scoperta l'attività fraudolenta, l'organizzazione vittima ritiene di aver pagato una fattura legittima, anziché aver effettuato la transazione direttamente sul conto dell'attaccante".

Condividi l'articolo

Compagnie telefoniche hackerate per spiare gli utenti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/26/gli-attacchi-via-email-continuano-ad-aumentare/

Compagnie telefoniche hackerate per spiare gli utenti

Giu 25, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS 0

I pirati hanno infiltrato i sistemi per spiare le comunicazioni degli utenti. Nel mirino politici, esponenti di governo in almeno 30 paesi diversi. Sotto accusa la Cina.

Si tratterebbe di un’operazione di spionaggio estremamente vasta e articolata, che avrebbe preso di mira almeno una dozzina di compagnie telefoniche in più di 30 paesi nel mondo. A denunciare quella che è stata battezzata **Operation Soft Cell** è la società di sicurezza israeliana **Cybereason**.

Nel post pubblicato sul blog ufficiale della società di sicurezza i ricercatori spiegano che gli attacchi sarebbero partiti nel **2017** e avrebbero interessato almeno una decina di compagnie di telefonia mobile.

Nel report non viene fatto alcun nome, ma gli autori lasciano intendere che si tratti di grandi operatori attivi in occidente, che sarebbero stati presi di mira a opera di un gruppo hacker che i ricercatori ritengono lavorare per conto del **governo cinese**.

A indirizzare i sospetti verso Pechino, in particolare, sono gli strumenti utilizzati per compromettere i sistemi delle società di telecomunicazioni, che comprenderebbero una versione modificata di **China Chopper**, una web shell utilizzata in passato dal gruppo **APT 10**.

APT 10, conosciuto anche come **Stone Panda**, è uno dei gruppi di "hacker di stato" più attivi e temuti, che in passato ha fatto parlare di sé per una serie di attacchi clamorosi ai danni di aziende e organizzazioni governative negli anni passati.

Il modus operandi dei pirati informatici, in ogni caso, lascia pochi dubbi sul fatto di trovarsi di fronte a dei professionisti. Dopo aver compromesso un server esposto su Internet, infatti, i cyber-spioni hanno eseguito un classico "movimento laterale" all'interno della rete utilizzando strumenti come **Mimikatz**, per poi procedere all'installazione di backdoor nei punti sensibili e all'esfiltrazione dei dati attraverso delle **VPN installate direttamente sui sistemi compromessi**.

Per evitare di essere individuati, gli hacker hanno utilizzato una tecnica di attacchi "a ondate", alternando periodi di inattività per cercare di rimanere sotto i radar degli amministratori IT, che infatti non si sono accorti di nulla per lungo tempo.

In buona sostanza, i pirati avrebbero avuto accesso a centinaia di gigabyte di dati, con informazioni sulle

comunicazioni di tutti i clienti delle compagnie telefoniche. Secondo quanto ricostruito dai ricercatori, gli hacker non avrebbero però rubato informazioni di carattere finanziario, come numeri di carte di credito o simili.

La loro attenzione si sarebbe concentrata piuttosto sulle informazioni riguardanti gli spostamenti e le comunicazioni di 20-30 persone. **Si tratterebbe di politici, esponenti di governo e delle forze di polizia**.

Insomma: il quadro generale è quello di una classica operazione di spionaggio, che per modalità e ampiezza ha però del clamoroso.

Tutta la vicenda, poi, emerge proprio nel mezzo della prolungata crisi tra USA e Cina culminata con il bando di **Huawei**, finito sulla "lista nera" dell'amministrazione **Trump** proprio per i timori legati alla possibilità che il governo di Pechino sfrutti le infrastrutture dell'azienda cinese per le sue attività di spionaggio.

Condividi l'articolo

Le app per smartphone sono piene di falle di sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/25/compagnie-telefoniche-hackerate-per-spiare-gli-utenti/

Le app per smartphone sono piene di falle di sicurezza

Giu 24, 2019 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Vulnerabilità 0

Prima di installare una nuova app pensiamoci bene. Ci sono buone probabilità che apra una voragine a livello di sicurezza.

La strada per avere app sicure sui nostri dispositivi mobile è ancora lunga e accidentata. A confermarlo, oltre alla cronaca, è una ricerca pubblicata da **Positive Technologies** che mette in fila una serie di dati piuttosto inquietanti.

Partiamo dal dato più generico: secondo gli autori dello studio, che hanno analizzato in profondità 17 applicazioni per dispositivi mobile, **ci sono falle ad alto rischio nel 43% delle applicazioni Android e nell 38% di quelle per iOS**.

I problemi relativi alla sicurezza sono di varia natura, ma il più comune è quello relativo a una carenza di sicurezza nella gestione dei dati memorizzati, tra cui il più rilevante riguarda la pessima abitudine di registrare i PIN di accesso sul dispositivo al posto che sui server.

Anche la sicurezza nelle connessioni non raggiunge livelli eccelsi. **Nel report si spiega che il 38% delle app per Android e il 22% di quelle per iOS utilizzano connessioni che non soddisfano criteri di sicurezza**.

Le carenze sono rilevanti anche in altri ambiti, come la protezione dagli attacchi di Brute Forcing o l'attenzione per evitare di memorizzare informazioni sensibili nel codice delle app.

A livello di gravità, però, c’è di molto peggio. L’uso degli **snapshots**, cioè la registrazione dello stato di un’applicazione che viene normalmente eseguita quando l’utente passa a un’altra app, viene gestito in maniera piuttosto approssimativa dalla maggior parte degli sviluppatori.

In particolare, nel 65% dei casi nessuno si preoccupa di escludere informazioni sensibili (come il numero di carta di credito) da queste “immagini”.

E fin qui ci siamo occupati solo del “lato client”. Quando si passa alla gestione dei dati “lato server”, le cose non vanno molto meglio.

I maggiori problemi sono rappresentati dalle vulnerabilità **cross-site scripting (XSS)**, seguite dagli errori nelle configurazioni dei server stessi, che in molti casi consentono di rubare informazioni utili per sottrarre le credenziali di accesso ai servizi.

Insomma, gli sviluppatori delle app mobile, secondo gli esperti di Positive Technologies, hanno ancora parecchia strada da fare per imparare a sviluppare applicazioni che corrispondano al concetto di “secure by design”.

Chi le utilizza, invece, dovrebbe semplicemente tenere presente che queste falle dovrebbero far scattare un campanello di allarme **ogni volta che un’applicazione sul nostro smartphone ci chiede l’accesso a informazioni in qualche modo sensibili**. Forse, prima di concedere il permesso, è meglio pensarci due volte.

Condividi l’articolo

Online gli strumenti per hackerare le scuole

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/24/le-app-per-smartphone-sono-piene-di-falle-di-sicurezza/

Attacco agli MSP per colpire i loro clienti con un ransomware

Giu 21, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati informatici hanno violato i sistemi di tre Managed Service Provider e hanno usato il controllo in remoto per diffondere il malware.

L'allarme è partito ieri su **Reddit**, in una sezione dedicata agli MSP. Nonostante la "normale" confusione del sito, la vicenda ricostruita (e tutt'altro che conclusa) ha del clamoroso. Un gruppo di pirati informatici sarebbe infatti riuscito a colpire un numero imprecisato di aziende utilizzando come vettore di attacco tre **Managed Service Provider**.

I MSP sono soggetti che forniscono servizi di vario genere (tra cui quelli di sicurezza) attraverso un sistema di abbonamento e che utilizzano sistemi di controllo remoto per la gestione delle infrastrutture dei clienti.

Un sistema che permette di centralizzare il controllo di tutti gli aspetti legati all'IT e che (normalmente) garantisce un maggior livello di sicurezza ed efficienza rispetto a una gestione tradizionale. **Questa volta, però, le cose sono andate decisamente male e gli stessi MSP sono diventati il "cavallo di troia" che ha permesso gli attacchi**.

La segnalazione è arrivata da **Kyle Hanslovan**, CEO di **Huntress Lab**. Secondo Hanslovan, i cyber-criminali avrebbero come prima cosa utilizzato dei sistemi di **Remote Desktop Endpoints** per violare i sistemi di almeno tre MSP.

Dopo aver ottenuto i privilegi di amministratori e aver disattivato i software antivirus, avrebbero rubato le credenziali per gli account di **Webroot SecureAnywhere**, il software di sicurezza Webroot che sfrutta un sistema di controllo centralizzato con numerose funzioni di controllo remoto. **Tra queste, la possibilità di scaricare e installare applicazioni sui computer su cui è in funzione**.

Proprio questa funzionalità sarebbe la "testa di ponte" usata in seguito per **attaccare i clienti degli MSP, distribuendo sui loro computer un ransomware**.

Il malware si chiama **Sodinokibi** ed è comparso per la prima volta lo scorso aprile. Si tratta di un classico crypto-ransomware, che dopo aver codificato i file presenti sulla macchina infetta, chiede un riscatto in Bitcoin minacciando un aumaneto del denaro richiesto se il pagamento non viene effettuato entro 2 giorni.

Ora la partita si sta giocando su due piani: da una parte l’impegno per sbloccare i computer colpiti dal ransomware, dall’altra gli sforzi per arginare gli attacchi portati attraverso Webroot SecureAnywhere.

Sotto quest’ultimo aspetto, la società di sicurezza ha preso le sue contromisure inviando un’email a tutti i suoi utenti **e forzando l’implementazione del sistema di autenticazione a due fattori (2FA) per l’accesso**. Il sistema 2FA in Webroot è infatti disponibile, ma non è attivato come impostazione predefinita. Lo stratagemma, si spera, dovrebbe bloccare l’attività dei pirata.

Condividi l’articolo

Nuovo crypto-miner usa Cron per assicurarsi la persistenza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/21/attacco-agli-msp-per-colpire-i-loro-clienti-con-un-ransomware/

Nuovo crypto-miner usa Cron per assicurarsi la

persistenza

Giu 20, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware prende di mira i Web Server su piattaforma Linux per sfruttare le risorse di sistema allo scopo di generare cripto-moneta. Se rimosso, si reinstalla da solo.

La partita a scacchi tra pirati informatici e amministratori dei server Web continua senza sosta. Dopo l'ondata di **crypto-miner** registrata negli ultimi mesi, infatti, tutti i responsabili IT hanno preso contromisure per mettere in sicurezza i loro sistemi implementando, in particolare, sistemi di monitoraggio del consumo di risorse per individuare eventuali componenti sospetti e disattivarli.

La risposta dei cyber-criminali, però, non si è fatta attendere. Come spiega **Luke Leal**, un ricercatore di **Sucuri**, i pirati stanno utilizzando nuove tecniche per assicurare la persistenza dei loro miner in modo che possano continuare il loro lavoro anche se qualcuno interviene per rimuoverli.

Il caso analizzato da Leal nel suo report spiega bene le tecniche utilizzate. Il vettore di attacco è un file bash, chiamato **cr2.sh**, che una volta eseguito avvia la procedura di infezione seguendo una precisa procedura. Per prima cosa, il malware si preoccupa di controllare l'eventuale presenza di una serie di processi tra cui **Xmrig** e **CryptoNight**.

Se sono presenti, li termina. La logica, che non rappresenta una novità e di cui abbiamo parlato già in precedenza, è quella di fare piazza pulita di eventuali miner installati da altri cyber-criminali.

Una volta ripulita la macchina dalla presenza di concorrenti indesiderati, avvia il collegamento a un server predefinito da cui scarica il miner sotto forma di un file che viene memorizzato come **/tmp/php**. In seguito scarica dallo stesso server il file di configurazione che permette l'esecuzione dello script.

Una volta che il processo è caricato in memoria, i due file utilizzati per avviare il processo vengono cancellati allo scopo di nascondere le tracce dell'infezione.

Il vero tocco di classe, però, è la tecnica utilizzata per garantire la persistenza del processo. Lo script, infatti, usa **Cron** (un job scheduler utilizzato in ambiente Unix – ndr) per controllare ogni minuto se il processo è attivo. **Nel caso in cui sia stato eliminato, il cronjob avvia il download del file cr2.sh e riavvia l'intero processo**.

In questo modo, ogni sforzo per eliminare in via definitiva il crypto-miner dal Web Server è destinato a fallire. Almeno fino a quando l'amministratore non controllerà la coda di Cron e si accorgerà della presenza del job in questione.

Condividi l’articolo

Falla critica in Firefox. Aggiornare subito!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/20/nuovo-crypto-miner-usa-cron-per-assicurarsi-la-persistenza/

Falla nel kernel: sistemi Linux a rischio attacco DoS

Giu 18, 2019 Marco Schiaffino Emergenze, In evidenza, News, RSS, Vulnerabilità 0

TCP SACK PANIC permette di portare un attacco in remoto che porta al blocco del sistema a livello kernel. Allarme per i server aziendali e i sistemi cloud.

L’hanno battezzata **TCP SACK PANIC** ed è una falla nella gestione del protocollo di connessione che potrebbe causare parecchi guai in ambiti aziendali e (soprattutto) nei sistemi cloud, per la maggioranza affidati a sistemi Linux.

I tre bug (CVE-2019-11477, CVE-2019-11478 e CVE-2019-11479) interessano il kernel e di conseguenza coinvolge **tutte le**

distro Linux e le piattaforme derivate (per esempio quella **Amazon** di **AWS**) basate sul sistema open source. Lo scenario, spiegano i ricercatori, è quello di un attacco remoto che potrebbe mettere in un attimo K.O. i sistemi.

Ma di cosa stiamo parlando esattamente? SACK (Selective Acknowledgements) è un meccanismo che permette di **ottimizzare la trasmissione dei pacchetti nelle connessioni TCP** (Transmission Control Protocol) utilizzate normalmente per le comunicazioni su Internet.

Il protocollo TCP, tra le sue caratteristiche, ha quella di prevedere un sistema di verifica dell'integrità delle comunicazioni. In pratica, se una parte dei pacchetti inviati non raggiunge il destinatario, questi frammenti vengono ritrasmessi.

Normalmente, in caso di perdita di una parte dei dati, la trasmissione viene ripetuta integralmente a partire dal primo segmento mancante.

Come viene spiegato esaurientemente in questo report di **Red Hat**, SACK permette di **individuare con precisione i pacchetti andati persi nella trasmissione** e fare in modo che solo quelli effettivamente mancanti debbano essere trasmessi di nuovo. Come risultato, l'utilizzo di SACK consente di effettuare le comunicazioni con una maggiore efficienza e velocità.

Quello che i ricercatori hanno scoperto, è come sia possibile utilizzare una trasmissione TCP per mandare in “cortocircuito” il sistema semplicemente sovraccaricando il **Socket Buffer (SKB)** che nei sistemi Linux si occupa di gestire le code di frammenti nei collegamenti TCP.

Per farlo, un pirata dovrebbe avviare una connessione TCP in cui le dimensioni dei segmenti (**Maximum Segment Size o MSS**) siano impostate al valore minimo (48 byte) e trasmettere una sequenza particolare di pacchetti SACK al bersaglio.

La procedura, secondo quanto riportano gli sviluppatori, innescherebbe il blocco del Socket Buffer e, a cascata, dell’intero sistema operativo.

Gli aggiornamenti del kernel sono già disponibili e (si spera) in corso di aggiornamento per tutte le macchine interessate.

Condividi l’articolo

Symantec subisce un attacco a un suo lab australiano Più di 900.000 utenti colpiti da malware diffusi da video giochi contraffatti

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/06/18/falla-nel-kernel-sistemi-linux-a-rischio-attacco-dos/

Attacco alle app Web per il sequenziamento del DNA

Giu 17, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I pirati sfruttano una falla nelle applicazioni. L'origine dell'attacco in Iran, ma i ricercatori hanno dubbi sugli obiettivi e identità degli attaccanti.

Un attacco coordinato che sta prendendo di mira da giorni alcune **applicazioni Web per il sequenziamento del DNA**. A denunciarlo è **Ankit Anubhav**, che attraverso il suo profilo Twitter ha segnalato l'inizio degli attacchi lo scorso 12 giugno.

I pirati informatici si stanno concentrando su **dnaLIMS**, un'applicazione utilizzata da università e organizzazioni di vario genere per contribuire all'analisi e il sequenziamento del DNA.

Gli attacchi, spiega Anubhav, sfruttano una vulnerabilità

(CVE-2017-6526) scoperta nel 2017, che lo sviluppatore dell'applicazione non ha però corretto.

La falla di sicurezza consentirebbe, nel dettaglio, di impiantare delle shell che consentono di controllare in remoto il Web Server su cui gira dnaLIMS.

Difficile, però, capire quale sia il reale obiettivo dei pirati informatici. **Secondo i ricercatori, l'origine degli attacchi sarebbe in Iran, un indizio che farebbe pensare immediatamente a un'azione collegata al governo di Teheran**.

Oltre alla "normale" cautela nell'attribuzione degli attacchi informatici, però, in questo caso a suggerire di non saltare a conclusioni affrettate contribuiscono anche altri elementi.

Per esempio il fatto che non sia ancora chiaro quali siano i reali obiettivi dei pirati informatici. **Se il primo pensiero è quello che possano puntare a rubare i dati processati sui server, non è escluso che abbiano come scopo "solo" quello di poter infettare le macchine per altri obiettivi, come quello di reclutare i dispositivi in una botnet o installare miner per la generazione di cripto-valuta**.

Tanto più che gli indirizzi IP individuati dai ricercatori come origine dell'attacco sono stati utilizzati in passato per

operazioni decisamente più “prosaiche”, che hanno preso di mira dei router **Zyxel** e installazioni di **Apache Struts** sfruttando bug piuttosto conosciuti.

Insomma: l’impressione è che più che a un gruppo di hacker al soldo del governo iraniano, ci si trovi di fronte a quelli che gli esperti di sicurezza chiamano **script kiddie**, cioè principianti che usano codice che sfrutta vulnerabilità conosciute e che, in realtà, non hanno livelli di professionalità degni di nota.

Il problema, però, rimane e c’è da chiedersi se gli sviluppatori di dnaLIMS non si decideranno infine a distribuire una patch per correggere la vulnerabilità sfruttata dai pirati.

Condividi l’articolo

Triplicato l’interesse dei bambini per i siti di ecommerce

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/17/attacco-alle-app-web-per-il-sequenziamento-del-dna/

Falla in IOS XE permette di

prendere il controllo dei dispositivi Cisco

Giu 14, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug è stato corretto ed è disponibile un aggiornamento specifico. Router e switch vulnerabili possono essere riconfigurati in remoto o controllati a distanza.

Tecnicamente l'attacco viene chiamato **cross-site request forgery (CSRF)** e consiste nell'inserimento di un collegamento malevolo che, una volta attivato con un clic dall'utente, avvia operazioni indesiderate.

In questo caso, però, il rischio di un attacco del genere non riguarda un sito Internet qualsiasi, ma l'interfaccia grafica Web per la gestione dei sistemi **Internetworking Operating System (IOS)** di **Cisco**, cui è affidata la gestione di router e switch della società statunitense.

La vulnerabilità (CVE-2019-1904) è stata classificata con un livello di gravità di **8.8 su 10** e permetterebbe a un pirata informatico di portare un attacco remoto che gli consentirebbe, in pratica, di prendere il controllo del dispositivo.

L’assenza di un sistema di protezione nei confronti degli attacchi CSRF garantirebbe infatti al cyber-criminale un livello di interazione con il sistema con gli stessi privilegi dell’utente. Nel caso in questo abbia i permessi di amministratore, potrebbe quindi riconfigurare completamente il dispositivo.

Nel loro report, i ricercatori di Cisco spiegano che il bug interessa tutti i dispositivi che girano su **IOS XE** in cui è abilitata la funzionalità **HTTP Server** e che non esistono soluzioni tecniche o modifiche alle configurazioni per correggere il bug. **L’unica soluzione è quella di applicare la patch sviluppata dall’azienda**.

La falla non interesserebbe invece **Cisco IOS Software**, **Cisco IOS XR Software** e **Cisco NX-OS Software**. In ogni caso Cisco ha messo a disposizione uno strumento gratuito accessibile via Internet per verificare se il proprio sistema è vulnerabile.

Condividi l’articolo

Attacco DDoS a Telegram mette in crisi il servizio

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/06/14/falla-in-ios-xe-permette-di-prendere-il-controllo-dei-dispositivi-cisco/

Have I Been Pwned pronto per crescere

Giu 12, 2019 Marco Schiaffino In evidenza, Leaks, News, RSS, Scenario 0

Il fondatore Troy Hunt annuncia l'intenzione di avviare una collaborazione commerciale per far diventare "adulta" la sua creatura.

Quando **Troy Hunt** diede il via al progetto **Have I Been Pwned** (era il 2013) non aveva idea che il tema degli account compromessi potesse crescere ai livelli che ha raggiunto in questi ultimi mesi. Tanto meno che nel suo database finissero miliardi di record.

Lo spiega lo stesso fondatore, che in un lungo post pubblicato sul suo blog, annuncia la sua intenzione di fare un "salto di qualità" con il suo progetto.

Have I Been Pwned (HIBP per gli amici) è essenzialmente un enorme database che contiene un elenco indicizzato degli

account che sono stati compromessi negli ultimi anni e che i visitatori possono consultare (con modalità diverse a seconda se lo facciano gratuitamente o tramite un pagamento di una quota) per verificare se qualcuno dei loro account è stato violato.

Al suo interno, in buona sostanza, ci sono tutti i dati comparsi negli anni sui vari forum hacker o market del **Dark Web**. Quelli che i pirati informatici possono comprare o "procurarsi" per portare attacchi.

Fino a oggi HIBP ha mantenuto una dimensione piuttosto "artigianale" e il primo passo di una sorta di industrializzazione del servizio si è vista con l'avvio della collaborazione con **Mozilla** e il suo **Firefox Monitor** (ne abbiamo parlato in questo articolo) che ha consentito di allargare la platea di utenti del servizio.

Ora le cose starebbero per cambiare e il motivo, per lo meno come lo illustra Hunt, riguarda proprio il modello di gestione di HIBP in rapporto alla mole di dati e di lavoro che richiede.

Il servizio, scrive Hunt, a oggi è in grado di controllare quasi **8 miliardi di credenziali rubate**, con 3 milioni di utenti che hanno sottoscritto il servizio di notifica e una media di 150.000 visitatori giornalieri, che raggiungono però picchi di 10 milioni quando si verifica qualche grosso attacco. **Ecco: tutto questo fino a oggi è stato gestito da un team composto da… una persona. Troy Hunt**.

Di fronte alla costante crescita di richieste e di interesse, il ricercatore si è di conseguenza deciso a cercare un partner per garantire la sopravvivenza di HIBP. Nelle sue intenzioni, il servizio dovrebbe comunque mantenere alcuni punti fermi tra cui la possibilità di fare ricerche gratuite e di ampliare costantemente sia il database di riferimento, sia gli strumenti a disposizione.

Il **Progetto Svalbard**, nome scelto per omaggiare il più grande repository nell'artico, dovrebbe permettere a Troy Hunt di individuare il partner più adatto per raggiungere l'obiettivo. Non resta che aspettare.

Condividi l'articolo

Pochi aggiornano e i pirati continuano a sfruttare la falla in Windows

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/12/have-i-been-pwnd-pronto-per-crescere/