La botnet Prometei usa ancora EternalBlue… davvero?

Lug 24, 2020 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario, Vulnerabilità 0

Campagna di attacchi cryptojacking ai danni dei sistemi Windows. I pirati usano la solita, vecchia, vulnerabilità di Server Message Block.

Abbiamo qualche speranza di vincere la battaglia contro il cyber crimine? A guardare la cronaca recente, sembrerebbe proprio di no.

Tra le news della giornata, infatti, spicca una campagna di attacchi che punta a installare strumenti di cryptojacking sui sistemi Windows. L'exploit usato? Tenetevi forte: è **EternalBlue**.

La vulnerabilità, che prende di mira il **Server Message Block**, è emersa nel 2017 e **Microsoft** ha distribuito aggiornamenti mirati (anche per i sistemi operativi non più supportati) per bloccarla. Niente da fare: la sciatteria nella gestione degli aggiornamenti è evidentemente ben superiore a qualsiasi sforzo che la community della cyber security possa mettere in campo.

Il risultato è che, a tre anni distanza, ci ritroviamo con un malware in grado di sfruttare l'exploit per installare un miner che sfrutta la potenza di calcolo delle macchine infette per generare **Monero**.

La botnet in questione, battezzata con il nome di **Prometei**, utilizza in realtà un malware estremamente complesso, che secondo i ricercatori del gruppo **Talos** di **Cisco** sfrutta anche tecniche di brute forcing sui sistemi remote desktop per

ottenere accesso ai sistemi.

Si tratterebbe, come si legge nel report pubblicato dal team di analisti, di un malware modulare che i pirati stanno utilizzando dallo scorso marzo, ma che sarebbe riuscito a “volare sotto i radar” fino a oggi.

I ricercatori, inoltre, sottolineano come il malware sia distribuito su due “filoni”: uno rivolto al mining di cripto-valuta, l’altro specializzato nell’infiltrazione dei sistemi attraverso tecniche di diffusione che sfruttano, tra le altre cose, una versione modificata di **Mimikatz.** Secondo gli esperti di Talos, però, non c’è dubbio che il tutto sia gestito dallo stesso soggetto.

Oltre a sfruttare la potenza di calcolo delle macchine compromesse per generare MOnero, Prometei sarebbe però in grado di agire come una backdoor, consentendo al suo autore di sottrarre informazioni dalle macchine compromesse e inviarle a un server Command and Control sfruttando sistemi di comunicazione offuscati attraverso l’uso del circuito **Tor**.

Insomma: il quadro è quello di un malware estremamente evoluto che si avvantaggia, a tre anni di distanza, di una vulnerabilità conosciuta e per la quale esistono patch e

aggiornamenti.

Condividi l’articolo

Attacco Meow fa strage di database esposti. È un vigilante?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/24/la-botnet-prometei-usa-ancora-eternalblue-davvero/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-prometei-usa-ancora-eternalblue-davvero

---

Attacco Meow fa strage di database esposti. È un vigilante?

Lug 23, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, News, RSS, Scenario 0

Qualcuno sta sistematicamente violando e cancellando il contenuto dei database ElasticSearch e MongoDB lasciati esposti su Internet.

Il primo caso individuato da **Bob Diachenko** è stato quello del

database di **UFO VPN**, un server che la società di “sicurezza” aveva esposto su Internet senza alcuna protezione e di cui ci siamo occupati in questo articolo giusto qualche giorno fa.

Quando i ricercatori hanno cominciato a investigare, però, hanno scoperto che l’autore degli attacchi **Meow** aveva colpito più di 1.000 database, cancellandone completamente il contenuto.

I bersagli hanno tutti le stesse caratteristiche: database **ElasticSearch** (sono 987 quelli colpiti) e **MongoDB** (70 vittime) i cui amministratori non hanno previsto un sistema di autenticazione per accedervi. Insomma: si tratta dei classici server “dimenticati” in rete come accade sempre più spesso.

Il bizzarro nome assegnato all’attacco (Meow) è dovuto all’abitudine dello sconosciuto hacker di sovrascrivere o cancellare i file contenuti nel database senza lasciare alcuna richiesta di riscatto o rivendicazione. Semplicemente, i file sono sostituiti con altri che contengono nel loro nome la parola “meow”.

Il fenomeno dei server insicuri “abbandonati” su Internet è emerso ormai da qualche anno e, secondo gli esperti di sicurezza, è uno degli effetti collaterali dell’adozione dei sistemi virtuali, che consentono di clonare un server e metterlo online con estrema facilità e, con la stessa facilità, dimenticarsene.

Il problema è che, in molti casi, i database in questione contengono informazioni sensibili di utenti e i pirati

informatici ci vanno a nozze. I casi di furti di informazioni e di estorsioni che hanno sfruttato la sciatteria degli amministratori IT sono ormai incalcolabili.

L’autore di Meow sembra aver deciso di portare avanti una sorta di “campagna di educazione” utilizzando un sistema automatico che non punta a rubare dati o a estorcere denaro, ma semplicemente “punire” gli admin distratti.

E, tutto sommato, un po’ di simpatia finisce anche per suscitarla. D’altra parte, chi non ama i gattini?

Condividi l’articolo

Il controllo degli accessi? Con l’intelligenza artificiale è più sicuro

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/23/attacco-meow-fa-strage-di-database-esposti-e-un-vigilante/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-meow-fa-strage-di-database-esposti-e-un-vigilante

---

Il controllo degli accessi? Con l’intelligenza

artificiale è più sicuro

Lug 22, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

Le nuove tecnologie CyberArk Impact Live introducono sistemi di analisi avanzata per garantire un controllo rigoroso basato sulla filosofia "Zero Trust".

Il connubio tra intelligenza artificiale e cyber security non è certo una novità. L'uso dell'AI per proteggere i servizi e le infrastrutture IT delle aziende, però, è interessato da un progetto di evoluzione che sembra non volersi arrestare.

La nuova applicazione, introdotta da **CyberArk**, riguarda il controllo degli accessi e punta a "irrobustire" i sistemi di privileged access management dell'azienda.

La tecnologia, implementata grazie all'acquisizione di **Idaptive**, è stata battezzata con il nome di **CyberArk Impact Live** e poggia su due pilastri: l'introduzione di nuove tecnologie per l'autenticazione multi-fattore e un sistema di controllo basato, appunto, sull'intelligenza artificiale.

La soluzione sfrutta tecnologie di machine learning per realizzare una profilazione di base di ogni utente, utilizzando degli elementi contestuali come la geolocalizzazione e la tempistica degli accessi, il network e il sistema utilizzato.

Su questa base, a ogni accesso viene assegnato un “livello di rischio” che consente di definire le policy per reagire a eventuali attività pericolose, attraverso un’analisi che mette a fuoco il contesto e l’intento dell’accesso a servizi e risorse.

Il metodo, spiegano dalle parti di CyberArk, mira a coniugare il massimo livello di sicurezza con una elevata qualità dell’esperienza utente, soprattutto in una fase in cui i processi di digital transformation e l’affermazione dello smart working stanno amplificando il fenomeno dell’utilizzo di servizi in remoto e su piattaforma cloud, estremamente vulnerabili ad attacchi basati sulla violazione dei sistemi di autenticazione.

Condividi l’articolo

Attacco Meow fa strage di database esposti. È un vigilante? Microsoft dice basta ai protocolli TLS obsoleti in Office 365

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/22/il-controllo-degli-accessi-con-lintelligenza-artificiale-e-piu-sicuro/?utm_source=rss&utm_medium=rss&utm_campaign=il-controllo-degli-accessi-con-lintelligenza-artificiale-e-piu-sicuro

Microsoft dice basta ai protocolli TLS obsoleti in Office 365

Lug 22, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Tecnologia 0

Dal prossimo 15 ottobre TLS 1.0 e 1.1 non saranno più supportati. L'azienda di Redmond aveva sospeso il blocco a causa della pandemia da Covid-19.

Con la riapertura delle aziende e la conseguente possibilità per gli amministratori IT di intervenire sui sistemi, **Microsoft** ha deciso di revocare la sospensione della messa al

bando dei protocolli **TLS 1.0** e **1.1** originariamente prevista per giugno.

La sospensione era stata decisa per evitare di creare problemi alle aziende, che a causa della pandemia da **Covid-19** si trovavano costrette a gestire i sistemi in remoto e a fronteggiare notevoli difficoltà anche a lavorare con partner e fornitori.

A partire dal prossimo 15 ottobre, quindi, per utilizzare Office 365 sarà necessario usare **TLS 1.2**. I vecchi protocolli di crittografia, infatti, sono considerati vetusti e insicuri.

Il passaggio rischia di essere complesso, soprattutto perché gli amministratori spesso non hanno nemmeno una mappatura affidabile dei servizi che utilizzano i vecchi protocolli.

Per questo motivo, Microsoft ha rilasciato una documentazione per gestire il passaggio e uno (serve un account Microsoft per scaricarlo da questo indirizzo) per aiutare i tecnici a identificare i servizi e i dispositivi che usano TLS 1.0 e 1.1.

In particolare, dalle parti di Microsoft suggeriscono di eseguire una analisi del traffico e una scansione completa dei dispositivi, oltre a una serie di test per verificare l'impatto della disabilitazione dei protocolli obsoleti.

I vecchi protocolli, come annunciato nell'ormai lontano ottobre 2018, verranno abbandonati anche su tutti i browser più diffusi proprio nel corso di quest'anno. **Apple**, **Mozilla**, **Google** e **Microsoft** hanno però modificato le date di questo passaggio proprio a causa delle difficoltà causate dalla pandemia di Covid-19.

Gli utenti, in ogni caso, avranno la possibilità di abilitare i vecchi protocolli sui loro browser. Una possibilità, questa, che rappresenta una sorta di "salvagente" per chi si trovasse comunque in difficoltà nell'aggiornamento di servizi essenziali.

I siti Internet che usano ancora TLS 1.0 1.1, secondo le stime più recenti (marzo 2020) sarebbero una minoranza. Solo 850.000 su circa 1,7 miliardi di siti complessivi nel World Wide Web.

Condividi l'articolo

Il controllo degli accessi? Con l'intelligenza artificiale è più sicuro Attacchi ai bancomat sfruttano porzioni di codice originale del sistema

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/22/microsoft-dice-basta-ai-protocolli-tls-obsoleti-in-office-365/?utm_source=rss&utm_medium=rss&utm_campaign=microso

ft-dice-basta-ai-protocolli-tls-obsoleti-in-office-365

Attacchi ai bancomat sfruttano porzioni di codice originale del sistema

Lug 21, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, Prodotto, RSS, Vulnerabilità 0

L'allarme arriva da Diebold Nixford. I pirati userebbero una tecnica che gli permette di svuotare i bancomat collegandosi alla porta USB.

In gergo viene chiamato "jackpotting" ed è un attacco che permette di forzare i bancomat a erogare denaro direttamente nelle mani dei pirati informatici. Secondo **Diebold Nixdorf**, uno dei maggiori produttori di bancomat, il fenomeno sarebbe in aumento grazie a una tecnica estremamente efficace.

Come si legge nel report pubblicato dall'azienda, gli attacchi si starebbero verificando in alcuni paesi europei, in cui i criminali starebbero usando degli speciali dispositivi che collegano al bancomat per alterarne il funzionamento.

Dal punto di vista fisico, la tecnica prevede per prima cosa la rimozione del pannello frontale per ottenere l'accesso al collegamento tra l'erogatore di denaro (**CMD-V4**) e il bancomat. Si tratta di un semplice cavo USB, che i pirati collegano al loro dispositivo.

A questo punto, i criminali hanno la possibilità di svuotare letteralmente l'erogatore. Secondo quanto ricostruito dai tecnici di Diebold Nixford, **il dispositivo sfrutterebbe almeno in parte lo stesso codice del software integrato nel bancomat**.

Non è chiaro, però, come i pirati abbiano avuto accesso al codice. Nell'alert, l'azienda fa riferimento a un attacco offline (evidentemente un eufemismo per indicare un furto con scasso) che avrebbe portato al furto di un hard disk privo di crittografia.

Non si tratta però dell'unica tecnica usata dai pirati informatici per colpire i bancomat. **In alcune varianti, spiegano gli esperti, il collegamento prevede l'uso del cavo di rete**.

Dalle parti di Diebold Nixford raccomandano, in ogni caso, di predisporre tutti i controlli e implementare le impostazioni che permettono di mitigare il rischio di un attacco, tra cui l'uso di funzioni avanzate di protezione crittografica e, tanto per cambiare, l'aggiornamento periodico del firmware utilizzato.

Condividi l’articolo

VPN (in)sicure: i dati degli utenti su un server esposto su Internet

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/21/attacchi-ai-bancomat-sfruttano-porzioni-di-codice-originale-del-sistema/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-ai-bancomat-sfruttano-porzioni-di-codice-originale-del-sistema

---

Hacker russi attaccano i centri di ricerca sul vaccino per il Covid-19

Lug 17, 2020 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, News, RSS 0

La denuncia di NSA e dell’agenzia di intelligence britannica. Gli attacchi proverrebbero dal solito gruppo APT29, meglio conosciuto come Cozy Bear.

Si tratterebbe di una vera campagna di cyber-spionaggio in grande stile, che avrebbe preso di mira numerosi istituti e

aziende farmaceutiche occidentali che sono impegnate nella ricerca di un vaccino per il **Covid-19**.

Protagonista, una vecchia conoscenza degli esperti di sicurezza informatica: il gruppo **APT 29** (altrimenti conosciuto come **Cozy Bear**) che nel 2016 si è guadagnato una fama notevole per aver hackerato i server del Partito Democratico.

La denuncia arriva dai servizi di intelligence di USA e Regno Unito, che hanno pubblicato un report in cui viene descritta l'attività dei pirati informatici. Cozy Bear, che secondo il britannico **National Cyber Security Centre** sarebbero "al 95% responsabili degli attacchi" è considerato un gruppo collegato ai servizi segreti **FSB**.

Secondo gli analisti inglesi, gli attacchi sarebbero stati portati attraverso l'uso di exploit conosciuti ma piuttosto recenti, come quelli che affliggono alcuni servizi VPN e i sistemi **Citrix**, con l'obiettivo di installare sui sistemi delle aziende coinvolte delle backdoor in grado di sottrarre informazioni sensibili.

I malware utilizzati sarebbero due, battezzati con i nomi di **WellMess** e **WellMail**. Entrambi vengono descritti come "leggeri" ma consentono di eseguire comandi attraverso server Command

and Control e caricare e scaricare file sulle macchine infette.

WellMess, in particolare, utilizzerebbe un sistema di comunicazione con l'esterno in grado di sfruttare i protocolli HTTP, TLS e DNS per le sue operazioni.

In alcuni casi, lo stadio iniziale dell'attacco sfrutterebbe un downloader chiamato **SoreFang**. Si tratta, spiegano gli autori del report, di un malware che prende di mira i dispositivi del produttore cinese **Sangfor** e che sarebbe stato utilizzato in altri attacchi che gli analisti attribuiscono però a cyber criminali "comuni".

A margine della pubblicazione del rapporto, le autorità hanno stigmatizzato gli attacchi che "prendono di mira chi sta portando avanti un'attività vitale per combattere la pandemia da Cornovairus".

Condividi l'articolo

Apocalisse Twitter: la truffa dei VIP frutta 100.000 dollari in poche ore

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/17/hacker-russi-attaccano-i-centri-di-ricerca-sul-vaccino-per-il-covid-19/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-russi-attaccano-i-centri-di-ricerca-sul-vaccino-per-il-covid-19

Apocalisse Twitter: la truffa dei VIP frutta 100.000 dollari in poche ore

Lug 16, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, Phishing, RSS 0

Presi di mira gli account di Elon Musk, Bill Gates, Barack Obama e altre celebrità. I pirati potrebbero avere un complice all'interno del social network.

Una clamorosa violazione dei sistemi di **Twitter** ha permesso a un gruppo di pirati informatici di prendere il controllo di un numero imprecisato di account verificati di personaggi di primo piano per mettere a segno **una truffa su scala globale che ha fruttato centinaia di migliaia di dollari**.

Mentre scriviamo, dalle parti di Twitter stanno ancora cercando di capire che cosa sia successo esattamente, ma il quadro che emerge per il momento fa pensare a un lavoro dall'interno, attraverso la compromissione di un account di un impiegato o la sua complicità.

Tutto è cominciato nella giornata di ieri, quando i profili Twitter di numerose celebrità hanno cominciato a postare dei messaggi che annunciavano campagne di "donazione di Bitcoin. Tra gli account compromessi quello di **Barack Obama**; **Elon Musk; Bill Gates**; **Jeff Bezos** e il rapper **Kanye West**. I pirati, però, hanno colpito anche i profili di aziende come **Apple**, **Uber** e **Coinbase**.

I tweet riportavano, con poche varianti, un annuncio con il classico schema della truffa “give away”, già utilizzata in passato dai cyber criminali utilizzando falsi account. Lo schema è semplice: annunciare una donazione in Bitcoin da parte di un personaggio famoso (e ricco) chiedendo a chi vuole ricevere il “regalo” di inviare una somma in Bitcoin su uno specifico conto, con la promessa che ne riceverà il doppio.

Una truffa che, apparentemente, è piuttosto infantile, ma che in passato ha già permesso ai truffatori di intascare notevoli somme sfruttando questo schema.

In questo caso, il suo impatto rischia però di essere molto più forte, visto che i pirati non hanno dovuto creare dei falsi account, ma hanno usato quelli autentici.

Le prime stime parlano di circa **120.000 dollari inviati al conto Bitcoin principale**, anche se potrebbero essercene altri. Il fatto che Twitter abbia rimosso i post no appena è stato

evidente quello che stava succedendo ostacola anche una ricostruzione della campagna nel suo complesso.

Quello che è certo, è che oltre agli inviti "diretti", i pirati hanno usato anche un sito dedicato (ora offline) che proponeva uno schema simile sfruttando il tema della pandemia da Covid-19 come esca.

Analizzando le transazioni sul conto Bitcoin principale, in ogni caso, emerge come la maggior parte dei versamenti siano di entità davvero modesta, intorno a 1 dollaro per trasferimento. **Molto probabilmente si tratta di utenti che hanno voluto mettere alla prova il meccanismo ma che hanno comunque permesso ai pirati di incassare una discreta somma**.

Dalle parti di Twitter, invece, hanno il loro bel da fare per capire come sia stato possibile tutto questo. L'unica certezza è che l'attacco è partito dall'interno, attraverso l'account di amministrazione di un impiegato del social network.

Buona parte degli account utilizzati per la truffa usavano il sistema di autenticazione a due fattori, che sarebbe stato disattivato utilizzando il pannello di amministrazione interno. Non solo: gli indirizzi email sono stati modificati per impedire ai legittimi proprietari di accedervi.

Stando a quanto pubblicato dall'azienda di **Jack Dorsey,** una delle ipotesi è che i cyber criminali abbiano preso di mira gli impiegati di Twitter utilizzando tecniche di phishing e social engineering.

Non mancano, però, opinioni diverse. “Dopo un’iniziale ipotesi che si trattasse di un’attività di social engineering perpetrata da un insider, sembra che questo hack esterno sia riuscito grazie in realtà a metodi più ‘tradizionali’ e cioè comprando la collaborazione di un interno per accedere al tool di gestione che ha così consentito il takeover di account di

alto profilo” ha commentato **David Higgins**, EMEA technical director **CyberArk**.

“In ogni caso, conferma che gli hacker mirano sempre a impossessarsi degli accessi e dei diritti privilegiati degli insider. In alcuni casi, ciò avviene attraverso il takeover dell’identità, ma è possibile che in questa istanza si tratti di un malicious insider all’opera” conclude Higgins.

Quale che sia la verità, si tratta di un colpo clamoroso e l’utilizzo malevolo degli account VIP potrebbe anche essere solo la punta dell’iceberg di una violazione ben più profonda dei sistemi di Twitter. Ne sapremo di più, probabilmente, nei prossimi giorni.

Condividi l’articolo

SigRed: il bug in Windows Server rimasto nascosto per 17 anni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/16/apocalisse-twitter-la-truffa-dei-vip-frutta-100-000-dollari-in-poche-ore/?utm_source=rss&utm_medium=rss&utm_campaign=apocalisse-twitter-la-truffa-dei-vip-frutta-100-000-dollari-in-poche-ore

---

SigRed: il bug in Windows Server rimasto nascosto per 17 anni

Lug 15, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità potrebbe essere sfruttata per creare un worm in grado di propagarsi autonomamente attraverso le reti locali.

Nei panni di **Microsoft**, chiunque deciderebbe di costruire un monumento a **Sagi Tzaik**. Il ricercatore di **Check Point**, infatti, è riuscito a scovare un bug di quelli che avrebbero potuto causare grossi problemi a tutte le infrastrutture IT basate su **Windows Server**.

La vulnerabilità (CVE-2020-1350) battezzata con il nome di **SigRed**, affligge Microsoft Windows DNS, il componente dedicato al **Domain Name System** dei sistemi operativi Microsoft.

Nel report pubblicato da Check Point, la vulnerabilità riguarda la possibilità che le query DNS inviate a un server provochino un buffer overflow, consentendo in pratica a un pirata informatico di eseguire codice in remoto con privilegi di sistema. **In altre parole, uno scenario da incubo che ha indotto i ricercatori ad assegnare un punteggio di 10 su 10 alla gravità di SigRed**.

[embedded content]

Il bug può essere sfruttato dall'esterno, semplicemente

attirando un utente su un sito malevolo che può provocare un crash (o l'esecuzione di codice) sul server che gestisce il DNS.

L'aggiornamento che corregge SigRed è stato distribuito da Microsoft nella tornata di update di luglio 2020 ed è quindi disponibile per chiunque. Nel loro report, però, i ricercatori di Check Point non escludono che la vulnerabilità sia già stata sfruttata in passato.

Anche perché, secondo quanto emerge dalle analisi, il codice che consente questo exploit sarebbe presente nei sistemi Windows da ben 17 anni.

Ora la vicenda è arrivata al suo "lieto fine" e si spera che gli aggiornamenti vengano eseguiti prima che qualcuno possa sfruttare SigRed per portare un attacco. SI accettano scommesse…

Condividi l'articolo

Vulnerabilità critica in SAP: 40.000 aziende a rischio per RECON

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/15/sigred-il-bug-in-windows-server-rimasto-nascosto-per-17-anni/?utm_source=rss&utm_medium=rss&utm_campaign=sigred-il-bug-in-windows-server-rimasto-nascosto-per-17-anni

---

Vulnerabilità critica in SAP: 40.000 aziende a rischio per RECON

Lug 14, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Si chiama RECON e consentirebbe a un pirata informatico di prendere il controllo completo dei sistemi. Gli esperti: "rischio elevatissimo".

Allarme rosso per una vulnerabilità nei sistemi **SAP** che potrebbe avere conseguenze devastanti. La falla di sicurezza, segnalata dalla stessa azienda in concomitanza con il rilascio degli aggiornamenti di luglio, interesserebbe **40.000 aziende**.

Il bug (CVE-2020-6287) è stato battezzato con il nome di **RECON** (Remotely Exploitable Code On NetWeaver) e permetterebbe a un pirata informatico di avere accesso pressoché completo ai sistemi ERP degli utenti SAP vulnerabili. Non stupisce, quindi, che il livello di pericolosità sia stato indicato come massimo, con uno score di 10 su 10.

A preoccupare, soprattutto, è il fatto che un attacco a segno consentirebbe a un cyber criminale di accedere (e potenzialmente cancellare o modificare) informazioni particolarmente sensibili, come quelle relative al settore finanziario e amministrativo. **Insomma: un'ondata di attacchi che dovesse sfruttare RECON potrebbe risolversi in un vero disastro**.

La vulnerabilità riguarda le versioni di **SAP NetWeaver Java** dalla 7.30 alla 7.50 e permetterebbe l'esecuzione di codice in remoto sui sistemi aziendali.

Il report di sicurezza pubblicato da **Onapsis** non fornisce particolari dettagli tecnici e si concentra, piuttosto, sul possibile impatto della vulnerabilità. Fortunatamente non risulta alcun PoC (Proof of Concept) o exploit in grado di sfruttare il bug.

Come accade sempre in questi casi, adesso si apre una corsa contro il tempo per l'aggiornamento dei sistemi, che in questo caso pone problemi notevoli. Quando si parla di SAP, infatti, ci si riferisce a servizi considerati "critici" e che devono essere sempre disponibili.

L'update di software di questo genere, di solito, richiede qualche tempo per le verifiche di compatibilità che gli amministratori IT richiedono per garantire la business continuity.

Insomma: tutta la vicenda mette gli operatori del settore di fronte a un dilemma: forzare l'aggiornamento sperando che vada tutto bene o esporsi al rischio di un attacco? Gli esperti

consigliano caldamente di bruciare i tempi almeno per quelle aziende che hanno sistemi esposti su Internet (stimati in circa 2.500) che corrono i rischi maggiori.

Condividi l’articolo

ServHelper raddoppia: oltre alla backdoor installa un miner

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/14/vulnerabilita-critica-in-sap-40-000-aziende-a-rischio-recon/?utm_source=rss&utm_medium=rss&utm_campaign=vulnerabilita-critica-in-sap-40-000-aziende-a-rischio-recon

---

ServHelper raddoppia: oltre alla backdoor installa un miner

Lug 13, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

La nuova versione del trojan integra un generatore di

cripto-valuta che viene installato sul sistema infetto in un ambiente virtuale.

Perché limitarsi a rubare informazioni quando, nel frattempo, si può anche raggranellare qualche dollaro usando i sistemi infetti per generare cripto-valuta?

L'idea è venuta a **TA505**, un gruppo di pirati informatici specializzato in attacchi ad aziende operanti nel settore finanziario e commerciale. La nuova versione del loro **ServHelper**, un trojan che finora hanno utilizzato semplicemente per garantirsi l'accesso ai sistemi delle loro vittime, integra infatti un miner che viene installato automaticamente al momento dell'attacco.

Come si legge nel dettagliatissimo report pubblicato da **G Data**, si tratta di un malware estremamente complesso, che sfrutta numerose tecniche di offuscamento e una serie di procedure per evitare di essere rilevato da eventuali sandbox.

Il vettore di attacco usato dai pirati, spiegano i ricercatori, è normalmente un messaggio di posta elettronica che contiene un file **NSIS** (Nullsoft Scriptable Install System) la cui apertura avvia la procedura d'infezione.

Il malware, per prima cosa, si preoccupa di verificare di non trovarsi in una sandbox virtuale. Per farlo, verifica in prima battuta la presenza di un file (**C:\aaa_TouchMeNot_.txt**) presente nelle istanze virtualizzate di Windows.

Solo a questo punto, il programma decodifica il modulo principale ServHelper e ne avvia l'esecuzione. Anche in questa seconda fase, però, viene eseguita una seconda verifica.

Questa volta il malware esegue un controllo di sistema attraverso **System Management BIOS** per ottenere informazioni sulle dimensioni della ROM e verificare che ammonti almeno a 2 MB.

Dal momento che non è presente alcuna ROM nei sistemi virtualizzati, a giudizio dei ricercatori l'operazione mira a verificare la presenza di indizi che indichino la presenza di un ambiente virtuale.

Se i controlli vanno a buon fine, ServHelper viene installato e, da questo momento, agisce come un servizio di controllo remoto, consentendo agli autori del malware un accesso completo al sistema.

Il modulo aggiuntivo, che i ricercatori hanno battezzato con il nome di **LoudMiner** a causa del fatto che fa un uso intensivo delle risorse di sistema, sfrutta una tecnica di offuscamento basata sulla virtualizzazione. Una volta installato nssm.exe (Non-Sucking Service Manager), uno strumento gratuito che consente di gestire I servizi su sistemi Windows, avvia una sessione di **VirtualBox** al cui interno "gira" il miner.

Risultato: oltre ad avere un accesso completo al sistema, i pirati di TA505 hanno da subito una rendita fissa sfruttando la potenza di calcolo dei sistemi compromessi.

Condividi l’articolo

Tsunami: il software di sicurezza targato Google diventa open

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/13/servhelper-raddoppia-oltre-alla-backdoor-installa-un-miner/?utm_source=rss&utm_medium=rss&utm_campaign=servhelper-raddoppia-oltre-alla-backdoor-installa-un-miner