Un milione di utenti Android colpiti da finti mod per Minecraft

Nov 25, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

I pacchetti per il popolare videogioco erano disponibili su Google Play. Chi li ha installati si è trovato sommerso di pubblicità indesiderate.

Ancora **Google Play**, ancora applicazioni malevole che sfruttano le maglie larghe dello store ufficiale di Google. Questa volta a farne le spese sono gli appassionati di **Minecraft**, il videogioco per cui hanno fatto la comparsa numerosi pacchetti "mod" contenenti un malware.

I pacchetti in questione, di solito, integrano grafiche e modalità particolari di gioco che consentono di personalizzarlo. Stando a quanto si legge nel report pubblicato da **Kaspersky**, almeno 20 di questi mod contenevano del codice malevolo.

Nonostante una strategia piuttosto elementare, le applicazioni sono state scaricate da più di un milione di utenti, la maggior parte dei quali non ha nemmeno realizzato il fatto di aver installato un'app dannosa.

Al momento dell'installazione, infatti, i mod sembrano semplicemente non funzionare e la maggior parte delle vittime hanno semplicemente pensato di aver scaricato un software difettoso. Le recensioni delle app in questione, infatti, non sono particolarmente negative.

In realtà, le applicazioni sono perfettamente in grado di eseguire il compito per cui sono state progettate: sommergere di pubblicità indesiderata chi le ha installate.

In alcuni casi si tratta di pagine Web aperte (ogni due minuti!) tramite Chrome, ma i ricercatori di Kaspersky hanno individuato anche comportamenti più intrusivi come l'apertura di Google Play su determinate applicazioni o l'avvio della riproduzione di video tramite **YouTube**.

Inutile cercare di "pulire" il browser attraverso aggiornamenti o procedure di reset: l'unico sistema per fare piazza pulita di questo vero tsunami di inserzioni pubblicitarie è quello di rimuovere le app in questione, che

purtroppo non sono sempre facili da individuare.

La maggior parte dei mod contenenti codice malevolo sono state rimosse (nel report i ricercatori rilevano come ce ne siano ancora 5 disponibili) dopo le segnalazioni. SI spera che quelle sopravvissute seguano presto lo stesso destino.

Condividi l’articolo

Telsa Model X a rischio furto. Basta hackerare la chiave elettronica

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/25/un-milione-di-utenti-android-colpiti-da-finti-mod-per-minecraft/?utm_source=rss&utm_medium=rss&utm_campaign=un-milione-di-utenti-android-colpiti-da-finti-mod-per-minecraft

---

Telsa Model X a rischio furto. Basta hackerare la chiave elettronica

Nov 24, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità consente di sovrascrivere il firmware della chiave. Bastano pochi minuti per prendere il possesso del veicolo.

Altri guai per **Tesla** e, in particolare, per il suo **Model X**. A costringere l'azienda a rilasciare in fretta e furia un aggiornamento software è stato il ricercatore belga **Lennert Wouters**, che nella sua carriera è arrivato alla terza falla di sicurezza di Tesla individuata.

Come spiega in un report pubblicato su Internet, la vulnerabilità riguarda il sistema di aggiornamento del firmware, che consente di portare un attacco a breve o media distanza (fino a 30 metri) dalla chiave elettronica che controlla l'accesso all'auto.

La tecnica prevede una prima fase in cui il ladro deve riuscire ad attivare la chiave e sovrascrivere il firmware con una versione modificata, ottenendo così i comandi per aprire il veicolo.

Una volta ottenuto l'accesso, è possibile collegarsi al controller diagnostico ed eseguire il pairing con una chiave elettronica modificata.

[embedded content]

A rendere estremamente pericoloso il bug c'è anche il fatto che la tecnica di attacco non richiede l'uso di dispositivi o materiali particolarmente costosi: **bastano 200 euro per creare un kit che consente di rubare un'auto da 90.000 euro**.

La puntuale segnalazione a Tesla ha permesso agli sviluppatori dell'azienda di rilasciare un aggiornamento che corregge la vulnerabilità e inviarlo in modalità "push" a tutte le chiavi di Model X.

Condividi l’articolo

I pirati adesso vanno a caccia dei file ENV

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/24/telsa-model-x-a-rischio-furto-basta-hackerare-la-chiave-elettronica/?utm_source=rss&utm_medium=rss&utm_campaign=telsa-model-x-a-rischio-furto-basta-hackerare-la-chiave-elettronica

---

I pirati adesso vanno a caccia dei file ENV

Nov 23, 2020 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS, Scenario 0

Gli esperti hanno individuato botnet dedicate che eseguono una scansione continua per rilevare i file. Obiettivo: rubare le impostazioni dei server.

Si apre un nuovo fronte nella partita sulla cyber security, che questa volta coinvolge piattaforme come **Docker**, **Node.js**, **Symfony**, e **Django**. I cyber criminali, infatti, sembrano averle prese di mira attraverso un’attività continua di scansione online.

A lanciare l’allarme sono numerose società di sicurezza, tra cui **Bad Packets** e **Greynoise**. Entrambe, infatti, hanno individuato attività di scansione che punta specificatamente a individuare la presenza di **file ENV** accessibili online.

Si tratta di particolari file che vengono utilizzati dagli sviluppatori per memorizzare informazioni “sensibili” come **token di accesso alle API, credenziali dei database e simili**. File che, normalmente, dovrebbero essere conservati in cartelle protette ma che spesso (troppo spesso) rimangono esposti. Questo tipo di attività, in realtà, va avanti da tempo.

Negli ultimi mesi, però, ha subito un’accelerazione. Negli ultimi tre anni sarebbero stati individuati più di 2.800 indirizzi IP unici utilizzati per questo tipo di scansione.

Secondo gli esperti, l’obiettivo dei pirati informatici è quello di individuare i file ENV accessibili, scaricarli ed estrarre le informazioni che contengono per utilizzarle poi in vari tipi di attacchi.

L’accesso ai servizi cloud tramite API, per esempio, permetterebbe loro di abusare del software in questione, ma

anche le altre informazioni (in molti casi credenziali di accesso) consentirebbero loro di **infiltrare le reti aziendali con estrema facilità**.

L’appello, rivolto agli sviluppatori e agli amministratori IT, è naturalmente quello di avviare procedure e policy per la verifica del livello di sicurezza nella gestione di questi file, che ormai rappresentano un obiettivo privilegiato per i cyber criminali.

Condividi l’articolo

Falla in Facebook Messenger consentiva di spiare a distanza un utente

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/23/i-pirati-adesso-vanno-a-caccia-dei-file-env/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-adesso-vanno-a-caccia-dei-file-env

---

Falla in Facebook Messenger consentiva di spiare a

distanza un utente

Nov 20, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug nella versione Android consentiva di chiamare un utente e attivare il microfono prima che questo rispondesse.

Una falla di sicurezza in **Facebook Messenger** per **Android** avrebbe permesso di trasformare il telefono della vittima in una perfetta "cimice" per spiare conversazioni a distanza.

A individuare la vulnerabilità è stata **Natalie Silvanovich**, ricercatrice del team **Project Zero** di **Google**, che ha segnalato il bug incassando una ricompensa di 60.000 dollari.

La tecnica individuata consentiva, in pratica, di "ingannare" l'app di messaggistica facendole credere che il destinatario di una chiamata avesse risposto, avviando quindi la trasmissione audio.

Per ottenere il risultato sarebbe sufficiente avviare una chiamata al dispositivo della vittima e, mentre il telefono squilla, inviare un particolare comando tramite un messaggio **SDP** (Session Description Protocol).

Il comando in questione (**SdpUpdate**) impatta sul protocollo **WebRTC** utilizzato sull’app Messenger per Android per gestire le chiamate audio e video. Nel dettaglio, il messaggio avvia la conversazione anche se il destinatario della chiamata non ha ancora risposto.

Ma quale può essere il reale impatto di un simile attacco? In buona sostanza dipende dal contesto. Se la vittima per esempio ha disattivato la suoneria, potrebbe non accorgersi della chiamata e la tecnica consentirebbe, a questo punto, di monitorare l’ambiente in cui si trova proprio come un microfono spia.

La segnalazione della ricercatrice è stata immediatamente

presa in carico dagli sviluppatori di **Menlo Park** che hanno sfornato la patch a tempo di record, rispettando ampiamente il termine di 90 giorni fissato da Natalie Silvanovich.

La ricercatrice, su Twitter, ha annunciato di aver devoluto i 60.000 dollari ricevuti da Facebook a **GiveWell**, un'organizzazione no-profit che si occupa di aiutare persone bisognose.

Condividi l'articolo

Le previsioni sulla cyber security per il 2021

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/20/falla-in-facebook-messenger-consentiva-di-spiare-a-distanza-un-utente/?utm_source=rss&utm_medium=rss&utm_campaign=falla-in-facebook-messenger-consentiva-di-spiare-a-distanza-un-utente

---

Le previsioni sulla cyber security per il 2021

Nov 19, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Ecco quali saranno le dinamiche nella sicurezza informatica nel prossimo anno secondo gli esperti di sicurezza di WatchGuard.

Ci avviciniamo alla fine di questo (poco memorabile) 2020 e, come da tradizione, è il momento di fare bilanci e previsioni. Il primo pronostico sui temi della cyber security arriva da **WatchGuard**, che ha individuato 10 temi "caldi" per il 2021.

L'automazione porterà a una crescita delle campagne di spear phishing

Nel 2021, secondo gli autori del report, i pirati informatici sfrutteranno i **nuovi strumenti di automazione** per semplificare gli aspetti manuali della creazione delle campagne di spear phishing (gli attacchi mirati a singole persone – ndr) ed estrarre dati precisi e specifici delle vittime dalle reti dei social media e dalle pagine web aziendali, il che porterà ad un **aumento notevole del volume di email di spear phishing** che potranno inviare contemporaneamente. La speranza, però, è che siano meno sofisticate e più facili da individuare rispetto a quelle tradizionali generate manualmente. Molti di questi attacchi di spear phishing automatizzati faranno leva sui timori relativi alla pandemia da Covid-19.

I provider di hosting cloud prenderanno provvedimenti contro gli abusi informatici

Il 2021 sarà l'anno in cui i provider di hosting cloud come **Amazon**, **Google** e **Microsoft** inizieranno finalmente a **reprimere il phishing** e altre attività malevole che sfruttano i loro servizi. I cyber criminali ultimamente hanno utilizzato campagne di phishing con mail che rimandano a form falsificati su domini che appaiono legittimi, ma sono in realtà controllati dai pirati. Nel 2021, WatchGuard prevede che i provider di hosting cloud inizieranno a reprimere pesantemente il phishing e altre truffe, implementando strumenti automatizzati che individuano portali di autenticazione falsificati.

Gli hacker infesteranno le reti domestiche con i worm

Il lavoro da remoto rimarrà una costante anche nel 2021. Di conseguenza, i criminali informatici cambieranno strategia sferrando attacchi mirati ai dipendenti in smart working. Gli hacker spesso includono moduli di funzionalità worm nel loro malware, per spostarsi lateralmente verso altri dispositivi su una rete. Sfrutteranno così le reti domestiche poco protette come mezzo per accedere ai dispositivi endpoint aziendali.

Smart charger e “homebrew” apriranno la strada a violazioni di smart car

È da un po’ di tempo che non si verifica una grossa violazione alle smart car. Nel 2021, WatchGuard ritiene che il trend possa riavviarsi prendendo di mira gli smart charger. Nel prossimo anno è probabile che ricercatori di sicurezza e/o hacker identificheranno e dimostreranno una grave vulnerabilità in un charger per smart car. Ciò potrebbe permettere di interrompere l’uso della smart car impedendone la ricarica, o persino portare a un attacco malware che impedisca all’auto di caricarsi fino a quando non si paga il riscatto.

Potremmo anche assistere a casi di “homebrew” (installazione di software non autorizzato) da parte di appassionati esperti di tecnologia che amano bypassare i controlli di sicurezza per sbloccare tutta la potenza dei loro “gioielli tecnologici”. Oltre a interferire con la possibilità di installare successivi aggiornamenti di sicurezza forniti dal produttore, queste operazioni potrebbero aprire la strada a possibili attacchi informatici da parte dei pirati.

Gli utenti si ribelleranno chiedendo di regolamentare la privacy degli smart device

Gli smart device sono diventati pervasivi nelle nostre vite. Assistenti digitali come **Alexa**, **Google Assistant** e **Siri** guardano e ascoltano tutto ciò che accade nelle nostre case. Alcuni dispositivi indossabili (wearable) tracciano e rilevano parametri di salute critici, come la frequenza con cui ci muoviamo, il nostro battito cardiaco, il nostro ECG e ora anche i nostri livelli di ossigeno nel sangue. Se si aggiungono all'equazione gli algoritmi di machine learning (ML) che le aziende tecnologiche impiegano per correlare i big data degli utenti, il tutto dipinge un quadro decisamente lesivo della privacy. Nel 2021 WatchGuard prevede che questa consapevolezza cresca e che gli utenti inizieranno a richiedere ai legislatori di regolamentare le aziende produttrici di dispositivi IoT affinché proteggano la loro privacy e i loro dati.

Con l'aumento dello smart working gli attaccanti colpiranno VPN e RDP

Mentre molte aziende in passato utilizzavano poco soluzioni **RDP (Remote Desktop Protocol)** e **VPN (Virtual Private Network)**, questi servizi con lo smart working diffuso sono diventati i pilastri per consentire ai dipendenti di accedere ai dati e ai servizi aziendali al di fuori del tradizionale perimetro di rete. Nel 2021, WatchGuard prevede che gli attacchi informatici contro **RDP, VPN e server di connessione remota** raddoppieranno mediante l'uso di credenziali rubate, exploit e un'attività brute-force vecchio stile.

Gli attaccanti individueranno lacune di sicurezza negli endpoint legacy

Una parte significativa delle aziende si affida ancora a vecchi sistemi operativi per svariate ragioni. Gli hacker lo sanno e cercano il modo per trarne vantaggio. È ironico che l'aumento del lavoro da remoto coincida con lo stesso anno in cui Microsoft ha interrotto il supporto esteso di alcune delle versioni più popolari di Windows, come 7 e server 2008. Nel 2021, gli esperti della società di sicurezza si aspettano che i criminali informatici cerchino una falla di sicurezza significativa in **Windows 7** nella speranza di sfruttare endpoint legacy su cui gli utenti a casa non possono facilmente applicare patch.

Ogni servizio senza MFA subirà una violazione

Nessun servizio su Internet è al sicuro dalle intrusioni informatiche se non utilizza **l'autenticazione a più fattori (MFA)**. Sul dark web e nei numerosi forum clandestini sono disponibili miliardi di nomi utente e password frutto di varie violazioni di dati e se ne aggiungono milioni ogni giorno. Il rischio è che l'aumento di attacchi automatizzati rivolti alle procedure di autenticazione porti a un aumento esponenziale

delle violazioni.

I truffatori sfrutteranno la paura della pandemia durante il 2021

Gli esperti di tecniche di social engineering sanno che gli esseri umani prendono decisioni guidate dallo stato d'animo e dall'impulsività. Con la seconda ondata di **Coronavirus**, le persone rimarranno probabilmente in uno stato generale di disagio e soggetti a una forte componente emotiva per tutto il 2021. Aspettiamoci di vedere molte campagne di phishing e di social engineering che sfrutteranno la paura e il senso di incertezza dovuti alla pandemia e alla situazione economica.

Gli attacchi prenderanno di mira i bambini per arrivare ai genitori

Secondo gli autori del report, potremmo anche assistere ad attacchi mirati di phishing nel 2021 con una svolta particolare. Mentre gli attacchi di spear phishing prendono di

mira normalmente i dipendenti, questi nuovi attacchi potrebbero prendere di mira i membri della famiglia del dipendente stesso. Se il criminale riesce a inserire il proprio malware sulla rete domestica, ha maggiori possibilità di arrivare al tuo computer aziendale. Meglio, spiegano gli esperti di WatchGuard, separare il computer aziendale dagli altri dispositivi connessi sulla rete domestica. Una VPN potrebbe non essere sufficiente per proteggersi da un'infezione locale.

Condividi l'articolo

Le password più usate continuano a essere un disastro

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/19/le-previsioni-sulla-cyber-security-per-il-2021/?utm_source=rss&utm_medium=rss&utm_campaign=le-previsioni-sulla-cyber-security-per-il-2021

Le password più usate continuano a essere un disastro

Nov 18, 2020 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Scenario 0

La ricerca di NordPass è impietosa: nel 2020 la maggior parte degli utenti utilizza password banali che i pirati impiegano una manciata di secondi a violare.

Può sembrare assurdo, ma all'alba del 2020 c'è ancora chi usa password come "123456" e… "password". A rilevarlo è una ricerca di **NordPass**, che ha passato al setaccio 275.699.516 parole di accesso in vendita sul Dark Web analizzando quali siano quelle più utilizzate a livello globale.

Un metodo abbastanza affidabile per valutare come gli utenti scelgono le loro password, visto che i database in questione provengono normalmente da data breach subiti da vari servizi Internet e rappresentano quindi un campione "neutro" degli account utilizzati.

Il risultato dello studio, consultabile a questo indirizzo Internet, è davvero sconsolante. **Al primo posto, infatti, si conferma il classico "123456", seguito da "123456789". La prima "new entry" è al terzo posto ed è "picture1"**.

Qualcosa di più complesso rispetto alla prima e seconda piazza (violabili in meno di un secondo con un software di brute forcing) ma che comunque non richiederebbe più di 3 ore per essere scardinata.

E se al quarto posto si conferma la classica “password”, un ingresso in classifica interessante si registra invece alla decima posizione, dove fa il suo ingresso in classifica “senha”.

La cosa, però, non deve stupire più di tanto: “senha” è infatti l’equivalente in portoghese di “password” e la sua comparsa in questa vera e propria galleria degli orrori è probabilmente dovuta al fatto che il database utilizzato come riferimento per la ricerca si è arricchito negli ultimi mesi di molti account sottratti da server brasiliani.

Da un punto di vista statistico, i ricercatori di NordPass fanno notare come solo il 44% delle password analizzate possano essere considerate “uniche”.

Singolare il caso della password “jobandtalent”, che i ricercatori considerano piuttosto resiliente agli attacchi di brute forcing (tempo stimato per la sua violazione **3 anni**) ma che sarebbe stata usata da **34.512** account tra quelli analizzati.

In redazione siamo però riusciti a spiegare il mistero piuttosto rapidamente: **Jobandtalent** è un’azienda che si occupa di lavoro interinale con sede a Madrid, che nel 2019 ha subito

un data breach che ha portato alla compromissione di 11 milioni di account, probabilmente finiti nel database analizzato da NordPass.

Ai 34.512 utenti che hanno pensato bene di usare come password il nome del sito, inviamo un amorevole (e virtuale) buffetto sulla guancia.

Condividi l’articolo

Le previsioni sulla cyber security per il 2021 Microsoft introduce i suoi chip per la sicurezza su tutte le CPU

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/18/le-password-piu-usate-continuano-a-essere-un-disastro/?utm_source=rss&utm_medium=rss&utm_campaign=le-password-piu-usate-continuano-a-essere-un-disastro

---

Microsoft introduce i suoi chip per la sicurezza su tutte le CPU

Nov 17, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

Il chip Pluton verrà inserito nei processori Intel, AMD e Qualcomm. Obiettivo: introdurre la protezione hardware per Windows 10.

Un passo avanti verso un migliore livello di sicurezza nei sistemi Windows. Il fulcro dell'innovazione introdotta da Microsoft si chiama **Pluton** ed è un chip della famiglia **Trusted Platform Modules (TPM)** pensato per implementare funzioni di sicurezza a livello hardware.

Dal punto di vista dell'architettura, Pluton mira a eliminare il rischio legato al trasferimento dei dati tra il processore principale e i chip TPM, emerso più volte nei mesi scorsi.

Come? Semplice: Pluton sarà integrato direttamente nella CPU, eliminando così il rischio che lo scambio di dati (tipicamente legato a funzioni crittografiche) possa essere intercettato.

Per introdurre un ulteriore elemento di sicurezza, dalle parti di Microsoft hanno anche sviluppato un particolare sistema di aggiornamento del firmware, che prevede l'utilizzo della piattaforma cloud.

Tra le varie forme di attacco dirette ai chip TPM, infatti, quello di un "inquinamento" del firmware è uno ttra quelli considerati più efficaci. La procedura prevista da Microsoft dovrebbe "blindare" il software di controllo in modo da evitare il rischio di alterazioni.

La procedura di aggiornamento sarà integrata con Windows Update per garantire che il firmware sia sempre aggiornato all’ultima versione.

Prima di avviare l’implementazione di Pluton per i normali PC, l’azienda di Satya Nadella ha testato il chip TPM su **Xbox** e **Azure Sphere**, affinandone la tecnologia e le procedure di update.

Nel post pubblicato su Internet dalla stessa azienda viene dato grande risalto al valore della partnership con i tre produttori coinvolti (**Intel**, **AMD** e **Qualcomm**) che garantirà a Microsoft di “coprire” praticamente tutto il mercato dei processori.

Condividi l’articolo

Raffica di data breach: rubate le informazioni di milioni di utenti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/17/microsoft-introduce-i-suoi-chip-per-la-sicurezza-su-tutte-le-cpu/?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-introduce-i-suoi-chip-per-la-sicurezza-su-tutte-le-cpu

---

Raffica di data breach: rubate le informazioni di milioni di utenti

Nov 16, 2020 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Intrusione, Leaks, News, RSS 0

Le vittime sono Pluto TV, 123RF e Vertafore. In tutto i pirati informatici hanno messo le mani su dati riguardanti più di 40 milioni di persone.

Una settimana che si apre all'insegna dei data breach e che conferma la crescita esponenziale degli attacchi informatici alle aziende.

La cronaca di questo lunedì comprende infatti tre violazioni "di peso", che avranno certamente ripercussioni sulle aziende che le hanno subite e sugli sventurati utenti.

La prima riguarda il servizio **Pluto TV**, un servizio di streaming che vanta 28 milioni di utenti registrati. Secondo quanto riporta **Bleeping Computer** in un articolo, l'azienda avrebbe subito un furto di dati e i database sottratti sarebbero ora in vendita sul mercato nero.

Stando a quanto risulta ai colleghi di Bleeping Computer, i dati sarebbero di due anni fa, ma i 3,2 milioni di indirizzi email riportati corrisponderebbero a quelli di utenti effettivamente registrati al servizio.

Le informazioni contenute nell'archivio comprendono le generalità degli utenti, l'indirizzo di posta elettronica, la password (protetta da hashing), l'indirizzo IP, il tipo di dispositivo utilizzato e la loro data di nascita.

L'attacco a **123RF**, popolare stock di immagini, risalirebbe invece allo scorso marzo, ma anche in questo caso il database con 8,3 milioni di record avrebbe fatto la sua comparsa solo negli ultimi giorni.

In questo caso la situazione è più grave. Non solo perché l'archivio contiene un maggior numero di informazioni (come il numero di telefono degli utenti coinvolti e il loro indirizzo di residenza), ma anche perché le password sono "protette" da **un hashing con algoritmo MD5**, noto per essere vulnerabile a tecniche di brute forcing basate su collisione.

Più recente, invece, l'attacco subito da **Vertafore**, azienda specializzata nello sviluppo di software per il settore assicurativo. Stando a quanto dichiarato dalla società stessa, la violazione dei suoi sistemi risalirebbe a un periodo compreso tra marzo e agosto di quest'anno.

Il bottino finito nelle mani dei pirati, in questo caso, comprende i dati delle patenti di 27 milioni di cittadini residenti nello stato del Texas. Informazioni che i pirati potranno usare per portare attacchi di phishing o sfruttare per mettere in atto truffe di qualsiasi genere.

Condividi l'articolo

Il malware ModPipe mette nel mirino i POS dei ristoranti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/16/raffica-di-data-breach-rubate-le-informazioni-di-milioni-di-utenti/?utm_source=rss&utm_medium=rss&utm_campaign=raffica-di-data-breach-rubate-le-informazioni-di-milioni-di-utenti

---

Il malware ModPipe mette nel mirino i POS dei ristoranti

Nov 16, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati informatici attaccano un software Oracle ampiamente utilizzato per la gestione dei pagamenti digitali nel settore della ristorazione.

Anche in periodo di pandemia, i ristoranti rimangono evidentemente un bersaglio particolarmente appetitoso per i pirati informatici. A prenderli di mira, in queste settimane, è un gruppo di cyber criminali che sfrutta un trojan studiato specificatamente per rubare i dati delle carte di credito dai sistemi **POS** usati nel settore della ristorazione e dell'ospitalità.

Il malware utilizzato dai pirati chiama **ModPipe** e, secondo quanto si legge in un rapporto pubblicato dai ricercatori di **ESET**, è pensato per colpire un software in particolare: **Oracle Micros Restaurant Enterprise Series 3700**.

ModPipe, secondo gli esperti della società di sicurezza, è un

malware estremamente complesso, dotato di una struttura modulare che consente ai suoi autori di aggiornarne caratteristiche e funzionalità con estrema facilità. Sulla sua efficacia, però, non ci sono certezze.

Fonte immagine: ESET

Il malware è certamente in grado di accedere a numerose informazioni "collaterali", come alcune impostazioni del sistema, i nomi dei clienti e la cronologia delle operazioni. Per farlo, utilizza un modulo chiamato **GetMicInfo**, che consente di decrittare le password di accesso al database partendo dal registro di Windows.

Lo stratagemma, spiegano gli autori del report, denota una conoscenza approfondita del funzionamento del software Oracle, che potrebbe affondare le sue radici in un data breach subito dall'azienda nel 2016.

Stando all'analisi effettuata da ESET, per quel che si conosce finora ModPipe non permetterebbe di sottrarre le informazioni più "sensibili", quelle cioè riguardanti i dati delle carte di credito utilizzate per i pagamenti.

Per ottenere queste informazioni, infatti, i pirati dovrebbero essere in grado di scardinare il sistema di crittografia che utilizza la passphrase locale per proteggere i dati. L'esistenza di un modulo che consenta di decodificare queste informazioni non è confermata, ma i ricercatori non la escludono a priori.

Difficile non condividere la posizione degli esperti ESET: chi realizzerebbe infatti un malware del genere se non avesse la possibilità di estrapolare i dati che gli servono per sfruttare l'attacco?

Condividi l'articolo

Raffica di data breach: rubate le informazioni di milioni di utenti Attacchi DNS poisoning sfruttano un bug di Linux del 2008

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/16/il-malware-modpipe-mette-nel-mirino-i-pos-dei-ristoranti/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-modpipe-mette-nel-mirino-i-pos-dei-ristoranti

---

Attacchi DNS poisoning sfruttano un bug di Linux del 2008

Nov 13, 2020 Marco Schiaffino In evidenza, News, Vulnerabilità 0

La vulnerabilità era considerata "risolta" ma è emersa una nuova tecnica che consente di dirottare il traffico sfruttando tecniche di DNS cache poisoning.

A 12 anni di distanza, gli sviluppatori si sono trovati a dover rimettere mano alle modalità con cui vengono gestite le richieste DNS sui server Linux. Obiettivo: bloccare una nuova tecnica che permetterebbe di "inquinare" la cache DNS e dirottare il traffico degli utenti.

Il problema, emerso nel 2008, riguarda la possibilità che un pirata informatico possa interferire con la catena di comunicazione dei server **DNS (Domain Name Server)** attraverso una tecnica di brute forcing.

I server DNS, spesso paragonati agli “elenchi del telefono” del Web, hanno il compito di convertire il dominio richiesto da un dispositivo (per esempio www.securityinfo.it) nell’indirizzo IP corrispondente al server che ospita (in questo caso 88.198.117.84).

Il loro funzionamento, però, non è lineare come si potrebbe immaginare. Esistono vari livelli di DNS, distribuiti gerarchicamente in una sorta di “piramide” per consentire di rispondere a tutte le richieste. Nella catena, i server DNS gerarchicamente superiori forniscono le informazioni a quelli inferiori (DNS resolver) che le memorizzano in una cache per poi fornirli ai dispositivi che li richiedono.

Un attacco DNS Poisoning, in pratica, punta a iniettare nella cache di un DNS resolver un’informazione sbagliata, che dirotta il traffico diretto a un sito su indirizzo IP diverso, normalmente controllato dai cyber criminali.

Per farlo, i pirati utilizzano tecniche di spoofing dell’indirizzo IP con lo scopo di impersonare un server DNS legittimo e inviare delle false risposte che vengono memorizzate nel DNS resolver.

Immagine: Varonis

Le misure di prevenzione di questo attacco adottate originariamente prevedevano l’uso di un identificativo (ID) a 16 bit che avrebbe dovuto permettere di verificare la provenienza delle informazioni. Nel 2008, però, il ricercatore **Dan Kaminsky** scoprì una tecnica per aggirare questa verifica.

Il numero di possibili ID, infatti, era limitato a 65.536 possibili combinazioni. Un numero tutto sommato basso e che consentiva di eseguire una sorta di brute forcing. Nel

dettaglio, la tecnica prevedeva di inviare una serie di false risposte, ognuna indicando un differente sottodominio (1.secuirtyinfo.it; 2. secuirtyinfo.it; 3.secuirtyinfo.it; etc.). In questo modo, un pirata avrebbe potuto identificare l'ID corretto e portare a termine l'attacco.

Per correggere la vulnerabilità, gli sviluppatori hanno introdotto un ulteriore elemento di selezione: abbandonare l'uso esclusivo della porta 53 per la ricezione delle risposte DNS e adottare invece l'uso di una porta casuale tra le 65.536 possibili. In questo modo un attacco come quello ipotizzato da Kaminsky avrebbe richiesto miliardi di tentativi.

Un gruppo di ricercatori universitari, però, hanno trovato un modo per "resuscitare" la tecnica. Nel loro report spiegano che la nuova modalità di attacco sfrutta una particolarità legata al modo in cui Linux gestisce le comunicazioni su protocollo **ICMP**.

Per evitare un sovraccarico sui server, Linux infatti limita il numero di risposte alle richieste di altri server, consentendone solo 1.000 al secondo.

Ii dettaglio su cui fa leva la tecnica messa a punto dai ricercatori è che una risposta inviata a una porta sbagliata ridurrà di uno il conteggio delle possibili comunicazioni, mentre quella inviata alla porta corretta non influenza il conteggio.

In altre parole, se i pirati inviano 1.000 risposte al secondo, possono eseguire una sorta di scansione delle porte per scoprire qual è quella giusta e, a questo punto, portare un attacco con il metodo indicato da Kaminsky.

La contromossa per disinnescare questo tipo di attacco, immediatamente implementata, è comunque semplice: **modificare le impostazioni che definiscono il limite di comunicazioni ICMP**.

Con questa modifica, i server adottano un limite casuale che varia tra 500 e 2.000, in modo da non offrire un punto di riferimento che consenta di individuare la porta corretta a cui inviare le risposte.

Condividi l’articolo

Microsoft: “basta con i sistemi di autenticazione che sfruttano il telefono”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/13/attacchi-dns-poisoning-sfruttano-un-bug-di-linux-del-2008/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-dns-poisoning-sfruttano-un-bug-di-linux-del-2008