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

Set 06, 2019 Marco Schiaffino In evidenza, Leaks, News, RSS, Vulnerabilità 0

Il database all'interno di un server accessibile a chiunque senza alcuna autenticazione. La parte più assurda: non si sa da dove arrivi.

La saga dei leak su Internet provocati da server "dimenticati" online senza alcuna protezione continua con un nuovo capitolo. Questa volta le vittime sono **419 milioni di utenti Facebook**, i cui numeri di telefono sono rimasti a disposizione di chiunque fino a ieri.

A individuare il server è stato **Sanyam Jain**, un ricercatore che fa parte della **GDI Foundation**. Come riporta in un articolo **TechCrunch**, che è stata contatta da Jain, buona parte degli utenti coinvolti (133 milioni) sono residenti negli Stati Uniti, 18 milioni nel Regno Unito e quasi 50 milioni in Vietnam.

Nel dettaglio, il database contiene per buona parte un elenco di numeri di telefono associati a utenti Facebook registrati attraverso il loro ID (il numero univoco che identifica ogni iscritto al social network – ndr) e di conseguenza facilmente individuabili.

Arrivare a nome e cognome dell'utente partendo dall'ID, infatti, è facilissimo. In alcuni casi, però, nei record del database sono riportati direttamente anche nome e nazionalità.

Il leak potrebbe avere conseguenze decisamente pesanti. Conoscendo il numero di telefono degli utenti, per lo più associato al profilo Facebook, un pirata informatico potrebbe infatti organizzare attacchi di phishing o utilizzare la tecnica del "SIM swapping" per violarne gli account.

Difficile capire da dove sia saltato fuori il database. Il ricercatore che l'ha scovato, infatti, non è riuscito a risalire al proprietario del server ed è riuscito a farlo mettere offline solo attraverso la società che si occupava dell'hosting.

Stando alle dichiarazioni di Facebook, dovrebbe risalire almeno a prima di un anno fa, quando Facebook ha modificato le sue policy sulla privacy cancellando la possibilità di utilizzare il numero di telefono per rintracciare i contatti su Facebook.

La vicenda, però, accende nuovamente i riflettori sul problema del controllo dei dati che vengono raccolti attraverso il social network di Mark Zuckerberg.

Come emerso nel caso **Cambridge Analytica**, appare evidente come le capacità di intervento della stessa Facebook sull'uso che viene fatto delle informazioni sugli utenti siano estremamente ridotte e si limitino, in buona sostanza, alla speranza che i

vari partner e clienti si attengano in maniera scrupolosa alle policy imposte dall’azienda californiana.

Condividi l’articolo

Il 50% degli smartphone Android vulnerabili a un attacco via SMS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/06/su-internet-i-numeri-di-telefono-di-419-milioni-di-utenti-facebook/

Il 50% degli smartphone Android vulnerabili a un attacco via SMS

Set 05, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La falla permette ai pirati di usare un messaggio OMA CP per alterare le impostazioni per la connessione e intercettare email e traffico Web.

Basta aprire l’SMS sbagliato per aprire la strada a un pirato

informatico che sarebbe in grado di intercettare tutti i nostri messaggi di posta elettronica e il traffico Internet.

La brutta sorpresa per gli utenti **Android** arriva da un report pubblicato da **Check Point**, che spiega i dettagli di una tecnica di attacco che interessa gli smartphone di alcuni dei maggiori produttori come **Samsung**, **Huawei**, **LG** e **Sony**.

Il vettore dell'attacco sono i messaggi **OMA CP** (Open Mobile Alliance Client Provisioning), uno standard utilizzato normalmente dagli operatori telefonici per inviare le impostazioni di rete ai nuovi dispositivi che si collegano al loro network.

Qual è il problema? Essenzialmente che gli smartphone dei produttori citati non utilizzano alcun sistema di autenticazione per la ricezione di questo tipo di messaggi (Samsung) o adottano un sistema che può essere facilmente aggirato.

Secondo i ricercatori, staremmo parlando di un numero di dispositivi vulnerabili che corrisponderebbe a circa il 50%

degli smartphone Android in circolazione.

L’attacco, si legge nel report, può essere portato attraverso un modem GSM o un telefono in modalità modem. Ma non si tratta di un attacco che funziona automaticamente: è comunque necessario che la vittima apra il messaggio.

Un dettaglio tutto sommato poco rilevante, visto che di fronte a un messaggio confezionato in modo che sembri provenire dall’operatore è piuttosto difficile che il destinatario possa nutrire dei sospetti.

In alcuni casi (a seconda del produttore dello smartphone) è necessario conoscere l’IMSI del dispositivo (il numero univoco che identifica ogni smartphone – ndr) che si vuole colpire o utilizzare una tecnica più complessa che prevede l’invio di un messaggio OMA CP protetto da PIN e un successivo (o precedente) SMS con il PIN stesso. Quest’ultima procedura consente di avviare l’installazione anche se non si conosce l’IMSI del device.

Le conseguenze rischiano di essere devastanti. Attraverso i

messaggi OPA CP è infatti possibile modificare numerose impostazioni, tra cui il server per i messaggi **MMS** (se qualcuno ancora li usa) e l'homepage del browser, ma anche e soprattutto le impostazioni del proxy e quelle del mail server.

Insomma: inviando un semplice SMS i pirati potrebbero intercettare tutte le comunicazioni della vittima, aprendo la strada a ogni tipo di truffa e di ulteriore attacco.

Le patch per correggere la vulnerabilità stanno arrivando in ordine sparso. **Samsung** l'ha rilasciata a maggio e **LG** in luglio. **Huawei** l'ha programmata per i prossimi modelli mentre **Sony non sembra intenzionata a fare alcunché**. L'azienda, infatti, avrebbe semplicemente risposto che i suoi sistemi "corrispondono alle specifiche OMA CP. Contenti loro…

Condividi l'articolo

Kaspersky mette in sicurezza le Blockchain in-house

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/05/oma-cp-il-50-degli-smartphone-android-vulnerabili-a-un-attacco-via-sms/

Gli exploit per Android valgono più di quelli per iOS

Set 04, 2019 Marco Schiaffino In evidenza, Mercato, News, RSS, Scenario, Vulnerabilità 0

Zerodium cambia il suo prezzario: la società che "commercia" in exploit ora paga 2,5 milioni per le tecniche di attacco che prendono di mira Android.

Se vogliamo capire come si muovono i vari settori dell'economia guardiamo le quotazioni di **Wall Street**. Se vogliamo capire come si sta evolvendo il mondo della cyber-security nel settore smartphone, dobbiamo guardare il sito di **Zerodium**.

La società, definita comunemente come un "broker" di exploit per software e sistemi operativi, rappresenta infatti la migliore cartina tornasole per capire chi è al centro delle attenzioni (indesiderate) dei pirati informatici.

E a guardare l'aggiornamento pubblicato ieri via Twitter, Android ha scavalcato iOS nei desiderata di chi cerca un modo per fare breccia nei dispositivi mobile.

Zerodium, con una mossa a sorpresa, offre adesso la bellezza di **2,5 milioni di dollari** a chi fornisce un exploit per Android "full chain", cioè un attacco in grado di compromettere il dispositivo senza che sia necessaria alcuna interazione da parte della vittima.

Una cifra che supera quella offerta ai tempi (1,5 milioni) per le tecniche di jailbreak di iOS, che aveva surclassato quanto offerto da Apple nel suo programma di bug bounty e che supera anche quella per gli exploit "1 click" per l'iPhone, ferma a

1,5 milioni di dollari.

Ma cosa significa esattamente questo ribaltamento nella classifica? Android è diventato più sicuro di iOS? Non necessariamente.

Per leggere correttamente la questione è bene tenere presente il fatto che Zerodium non è un qualsiasi forum per hacker e pirati informatici, ma un'azienda (sigh!) che ha come interlocutori e clienti le società che mettono a punto strumenti di cyber-spionaggio che, almeno in teoria, dovrebbero finire nelle mani di **forze di polizia e servizi segreti**.

In questo specifico settore, a quanto pare, sarebbero comparsi numerosi exploit per iOS che avrebbero ormai saturato il mercato.

Insomma: investigatori e agenti segreti avrebbero a disposizione tutto quello che gli serve per violare le protezioni dell'iPhone e sarebbero al momento più interessati ad avere strumenti più efficaci per i dispositivi con il sistema di Google.

Una conferma di questo trend arriva anche dalla recente scoperta di una rete di siti Internet contenenti numerosi exploit per iOS (ne abbiamo parlato in questo articolo) che, secondo fonti contattate da Forbes, sarebbero stati

controllati dai servizi segreti cinesi con lo scopo di compromettere i dispositivi della minoranza Uiguri nella provincia dello Xinjiang.

Anche se nello stesso articolo di Forbes si specifica che i siti contenevano anche strumenti per attaccare Android e Windows, la presenza di un arsenale così ampio per iOS è decisamente una novità.

Condividi l'articolo

USBAnywhere: raffica di bug nei server Supermicro

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/04/gli-exploit-per-android-valgono-piu-di-quelli-per-ios/

USBAnywhere: raffica di bug nei server Supermicro

Set 03, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le falle di sicurezza permettono di violare i sistemi di autenticazione e montare un’unità USB virtuale in remoto sui sistemi.

La virtualizzazione è un’arma a doppio taglio. Soprattutto quando si parla della possibilità di virtualizzare un’unità o un dispositivo USB attraverso un servizio remoto. A scoprirlo, in queste ore è **Supermicro**, i cui server basati su piattaforma **X9**, **X10** e **X11** risultano essere vulnerabili a un attacco remoto che sfrutta una serie di falle di sicurezza nei **Baseboard Management Controller (BMC)** utilizzati per la loro gestione in remoto.

Come si legge nel report pubblicato da **Eclypsium**, il fulcro del problema risiede proprio nei BMC utilizzati sui server Supermicro, che mettono a disposizione un sistema per utilizzare dispositivi USB virtuali attraverso un protocollo accessibile attraverso la porta TCP 623.

Secondo i ricercatori, infatti, il sistema che gestisce l’accesso in remoto ha almeno quattro problemi. Il primo riguarda **la possibilità di accedere attraverso username e**

password in chiaro, il secondo ha invece a che fare con la gestione del traffico, che in buona parte non è protetto da crittografia.

Come se non bastasse, c'è il fatto che il sistema crittografico utilizza **un algoritmo debole (RC4)** e una chiave predefinita integrata nel firmware del BMC. Il quarto e ultimo punto (ma questo riguarda solo i server su piattaforma X10 e X11) riguarda un bug che consente, in pratica, di aggirare il sistema di autenticazione.

Insomma: secondo i ricercatori di Eclypsium, un pirata informatico avrebbe gioco facile a individuare un server i cui servizi BMC sono accessibili in remoto (**nel report si spiega che su Internet ce ne sarebbero più di 47.000**) e "montare" un qualsiasi dispositivo USB virtuale per poi utilizzarlo per installare malware o assumere il controllo della macchina.

[embedded content]

Gli aggiornamenti del firmware per le piattaforme Supermicro interessate sono già disponibili sul sito del produttore, ma i ricercatori indicano nel documento anche alcune tecniche di mitigazione che permettono di ridurre il rischio di un attacco.

Prima tra tutte quella di evitare di esporre direttamente su Internet l'accesso ai BMC, che rappresenta in ogni caso un potenziale fattore di rischio.

Condividi l'articolo

Gli exploit per Android valgono più di quelli per iOS Ecco i siti che hanno fatto strage di dispositivi iOS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/03/usbanywhere-raffica-di-bug-nei-server-supermicro/

Ecco i siti che hanno fatto strage di dispositivi iOS

Set 02, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS, Vulnerabilità 0

Le pagine Web contengono 14 exploit per il sistema mobile di Apple e installano un trojan. "Siti visitati da migliaia di utenti negli ultimi 3 anni".

Quando si parla di sicurezza per smartphone, tra utenti **Android** e **iOS** volano invariabilmente gli stracci e, normalmente, i fan del sistema operativo **Google** devono sorbirsi gli sfottò di chi pensa di avere tra le mani un dispositivo nettamente più affidabile.

Un atteggiamento che, a ben vedere, qualche giustificazione ce l'ha. Le cronache, infatti, parlano chiaro: se i sistemi Android subiscono un bombardamento continuo da parte di malware di ogni genere, per iOS di solito le uniche minacce arrivano da spyware ultra-professionali utilizzati da servizi segreti e governi.

A smantellare questa rappresentazione dei fatti, però, ci ha

pensato la stessa Google. Gli esperti di sicurezza di Mountain View hanno infatti individuato un gruppo di pirati informatici che da almeno tre anni prende di mira i dispositivi Apple utilizzando alcuni siti Internet in grado di scardinare i sistemi di sicurezza di iOS.

A spiegare i dettagli è **Ian Beer**, membro dell'ormai celebre **Project Zero** di Google, che in un report pubblicato su Internet spiega che i cyber-criminali potevano contare su un arsenale decisamente nutrito.

Come spiega il ricercatore, sui siti in questione sono stati individuati 5 catene di exploit che usavano ben 14 vulnerabilità per violare i sistemi di chi visitava i siti infetti senza che fosse necessaria alcuna ulteriore interazione da parte degli utenti.

Il primo sito sarebbe comparso nel 2016 e, secondo il ricercatore, sulle pagine infette sarebbero finite diverse migliaia di utenti iOS. COl tempo, i pirati avrebbero aggiornato le loro modalità di attacco aggiungendo vulnerabilità per le nuove versioni di iOS.

Buona parte delle vulnerabilità sfruttate dagli exploit (Beer ha individuato 5 diverse "catene" utilizzate per gli attacchi) sarebbero già state corrette da Apple. **In un caso, però, i pirati informatici utilizzerebbero uno zero-day che Apple avrebbe corretto nell'ultimo aggiornamento di iOS**.

L’obiettivo degli attacchi era quello di installare quello che viene definito un “impianto”, cioè un trojan in grado di rubare informazioni di vario genere dal dispositivo.

È stato battezzato con il nome di **Teardown** ed è in grado di rubare file, trasmettere i contenuti dei messaggi inviati con varie applicazioni come **Whatsapp** e **Telegram**, oltre a fornire informazioni sulla posizione della vittima attraverso il sistema di localizzazione GPS.

Insomma: qualcosa di molto simile ai software-spia professionali. In questo caso, però, non veniva usato per attacchi mirati, ma utilizzato per colpire “a pioggia” gli utenti Apple. Un precedente che ci obbliga a rivedere gli scenari per come siamo abituati a considerarli.

Condividi l’articolo

Oltre il 50% delle richieste di Incident Response avviene troppo tardi

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/02/ecco-i-siti-che-hanno-fatto-strage-di-dispositivi-ios/

Google estende il bug bounty alle app più popolari su Google Play

Ago 30, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario 0

L'azienda ha deciso di dare un giro di vite e retribuire i ricercatori che trovano bug nelle applicazioni Android con più di 100 milioni di installazioni.

Il rapporto tra gestori degli store per applicazioni mobili e sviluppatori, nel settore della sicurezza, sono sempre stati piuttosto conflittuali. In sintesi, li si potrebbe definire così: il ruolo dei gestori, di solito, è quello del "cane da guardia": se l'app non è sicura, viene buttata fuori dallo store.

Un'impostazione che siamo abituati a considerare logica e che scarica tutta la responsabilità di individuare eventuali vulnerabilità ai produttori di app.

Ora sembra che le cose stiano cambiando, per lo meno per quanto riguarda il mondo **Android**. La notizia, infatti, è che **Google** avrebbe deciso di avviare un programma di **bug bounty** che "premia" i ricercatori che individuano falle di sicurezza nelle applicazioni più popolari, individuate come quelle che hanno più di **100 milioni di download sul suo Google Play**.

L'annuncio dell'iniziativa, pubblicato su questa pagina Internet, cambia radicalmente lo scenario ed estende la responsabilità di Google a un ambito che fino a questo momento veniva considerato completamente estraneo.

La mossa, a ben vedere, a una sua logica che si sviluppa a partire da tre considerazioni. Primo: un attacco che colpisce milioni di utenti Android rischia di danneggiare la reputazione di Google molto più di quanto possa danneggiare lo sviluppatore.

Secondo: l'idea per cui un'applicazione molto popolare ha necessariamente alle spalle una società molto strutturata e quindi in grado di gestire un proprio progetto di bug bounty

(come **Facebook** e soci) si può considerare ormai un’illusione.

Ci sono casi, come quello di **CamScanner** di cui abbiamo parlato un paio di giorni fa, in cui sviluppatori relativamente piccoli riescono a pescare il jolly e ottenere un notevole numero di installazioni. D’altra parte, secondo Google ci sarebbero in circolazione più di 2,5 miliardi di dispositivi Android. Per avere milioni di utenti non serve essere **Mark Zuckerberg**.

In definitiva possiamo dire che si tratti di una buona notizia. Chissà che non possa influenzare anche altri produttori (difficile che accada con Apple) e che l’iniziativa di Google non possa cambiare qualcosa e avviare la nascita di un sistema di bug bounty “solidale” nel settore dei produttori di software.

Condividi l’articolo

Oltre il 50% delle richieste di Incident Response avviene troppo tardi Il trojan TrickBot ora smantella l’autenticazione via SMS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/30/google-estende-il-bug-bounty-alle-app-piu-popolari-su-google-play/

Il trojan TrickBot ora smantella l'autenticazione via SMS

Ago 29, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS 0

Un nuovo modulo ruba le informazioni che consentono ai pirati di ingannare gli operatori telefonici ed eseguire un attacco "SIM swapping".

L'autenticazione a due fattori (**Two Factor Authentication o 2FA**) è uno strumento per proteggere in maniera più "robusta" i nostri account. Pensare che l'uso di un sistema 2FA ci metta completamente al sicuro dal furto dell'account, però, è un errore. Se ci troviamo ad avere a che fare con il trojan **TrickBot**, poi, potremmo pagare caro un eventuale eccesso di fiducia.

TrickBot è un malware in circolazione da tempo (ne abbiamo parlato l'ultima volta in questo articolo) che prende di mira in particolare gli account dei servizi di home banking. Un vero flagello, che è stato mitigato solo dalla diffusione (appunto) dell'autenticazione a due fattori.

I pirati informatici che utilizzano TrickBot, però, hanno cominciato a darsi da fare per trovare il modo di scardinare i sistemi 2FA e, in particolare, quelli che utilizzano l'invio di codici via SMS, utilizzati normalmente dai sistemi di home banking.

La tecnica più efficace in questo senso si chiama SIM swapping (ne abbiamo parlato in questo articolo) e prevede, in pratica, di contattare l'operatore telefonico della vittima per

chiedere una nuova SIM e la disattivazione di quella vecchia.

In questo modo i cyber-criminali potranno ricevere il codice di autenticazione sulla nuova SIM e aggirare il sistema di protezione a due fattori.

L'ostacolo che hanno di fronte i pirati è quello di dover impersonare il legittimo proprietario della SIM. In alcuni casi lo fanno sfruttando la complicità di impiegati infedeli delle compagnie telefoniche. **Nel caso di TrickBot, invece, i pirati puntano direttamente ai servizi di assistenza**.

Il problema (dal loro punto di vista) è che le compagnie telefoniche statunitensi utilizzano un PIN che i clienti devono usare per identificarsi quando contattano i servizi di assistenza. Per poter richiedere una nuova SIM, quindi, serve conoscere il PIN.

Ecco quindi che gli autori di TrickBot hanno pensato bene di inserire nel loro malware un modulo che gli permette di portare un attacco di phishing per ottenere il prezioso PIN.

Come spiegano i ricercatori di **Secureworks** in un report pubblicato su Internet, nei primi giorni di agosto il trojan è stato riprogrammato per monitorare i collegamenti ad alcuni operatori telefonici (**Verizon Wireless**, **T-Mobile** e **Sprint**) e iniettare codice HTML e JavaScript nel browser dei computer infetti in modo che nelle pagine di login degli operatori appaia un campo aggiuntivo: quello del PIN.

Come fanno notare gli analisti, il nuovo modulo dedicato al furto del PIN è stato inserito in tutte le installazioni di TrickBot. Questo significa che è attivo su tutti i computer già infettati dal gruppo di pirati informatici che utilizza il trojan.

Considerato che il malware è in circolazione dal 2016, stiamo parlando di un numero presumibilmente consistente di computer.

Al di là del nuovo modulo, la minaccia di TrickBot è rilevante anche per un altro motivo. I pirati informatici che gestiscono la botnet, infatti, utilizzano da tempo la formula del "malware as a service" e permettono ad altri cyber-criminali di sfruttare i PC infettati con TrickBot per installare ulteriore malware.

Una formula, questa, sempre più popolare nei bassifondi del Web e che mette a rischio un numero impressionante di persone che, oltre a finire vittima del pericolosissimo trojan , potrebbero trovarsi ad avere anche a che fare con altri attacchi, compresi i ransomware.

Dal punto di vista di chi gestisce i servizi di home banking, invece, l'intera vicenda dovrebbe servire come monito. I

sistemi 2FA basati sui codici inviati via SMS stanno infatti mostrando tutti iloro limiti da (troppo) tempo. Forse è il caso di passare oltre.

Condividi l’articolo

App per Android con il trojan dentro. L’hanno scaricata in 100 milioni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/29/il-trojan-trickbot-ora-smantella-lautenticazione-via-sms/

App per Android con il trojan dentro. L’hanno scaricata in 100 milioni

Ago 28, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS 0

CamScanner era disponibile da tempo su Google Play. L’ultimo aggiornamento ha però aggiunto un modulo in

grado di scaricare e installare malware.

Sarebbero la bellezza di 100 milioni gli utenti che hanno scaricato un'applicazione per Android chiamata **CamScanner** che contiene un dropper in grado di infettare i l dispositivo con trojan e malware di vario genere.

Un colpo fenomenale dei pirati informatici? La (ennesima) dimostrazione del fatto che **Google Play** è un colabrodo in termini di sicurezza?

La verità è che dalle parti di **Google** dovrebbero appendere un bel cartello con scritto "Vietato rilassarsi". Soprattutto quando si parla di applicazioni per **Android** e di **Google Play**, lo store ufficiale che troppo spesso ha proposto agli utenti app contenenti malware e funzionalità dannose di vario genere.

Il monito ha una logica che affonda le radici nella cronaca più o meno recente e che impone agli esperti di sicurezza di Google di non limitarsi a controllare le app quando vengono proposte la prima volta sullo store, ma controllarle costantemente a ogni aggiornamento.

Molto spesso, infatti, i pirati informatici utilizzano una tattica in due passaggi: prima caricano sullo store un'app assolutamente innocua e poi, quando hanno ottenuto un numero sufficiente di download, rilasciano un aggiornamento che aggiunge le funzionalità dannose.

Come spiegano i ricercatori di **Kaspersky** in questo report, il caso di CamScanner rientra esattamente in questa categoria.

L’app, in una prima fase, prevedeva semplicemente un sistema di pubblicità e acquisti in-app. Funzionalità piuttosto comuni per le applicazioni gratuite, che usano queste funzionalità per incassare i loro guadagni.

Le cose però sono cambiate quando nell’app è stata aggiunta una libreria con funzioni di pubblicità che contiene un modulo (**Trojan-Dropper.AndroidOS.Necro.n**) con funzionalità di dropper.

Il nuovo componente, in pratica, è in grado di installare una ulteriore applicazione “nascosta” all’interno dell’installer di CamScanner. Il malware in questione, secondo i ricercatori, ha due funzionalità dannose: **visualizza pubblicità estremamente intrusive e forza la sottoscrizione a servizi a pagamento**. Inutile dire che la seconda rischia di esser decisamente più pericolosa della prima.

La società di sicurezza ha analizzato il codice dell’app in seguito alla comparsa di una serie di commenti negativi sullo store di Google. Una volta individuato il modulo dannoso, ha segnalato il problema è l’app è stata prontamente rimossa.

Difficile capire cosa sia effettivamente successo. Un’ipotesi

è che lo stesso sviluppatore sia rimasto vittima di un attacco che ha permesso ai pirati di inserire il dropper in quello che, a questo punto, sarebbe un classico attacco **supply chain**.

Quale che sia il retroscena, il fatto che l'applicazione fosse installata su 100 milioni di dispositivi rende questa vicenda uno dei più clamorosi attacchi ai sistemi Android.

Condividi l'articolo

Pasticcio Apple su iOS: patch per correggere l'ultimo aggiornamento

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/28/camscanner-app-per-android-con-il-trojan-dentro-lhanno-scaricata-in-100-milioni/

Pasticcio Apple su iOS: patch per correggere l'ultimo aggiornamento

Ago 27, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Grande confusione dalle parti di Cupertino. L'update per iOS aveva cancellato una patch che correggeva una grave falla di sicurezza. Ora hanno rimediato.

Patch, altra patch e contro-patch: dalle parti di **Cupertino** si sonno trovati costretti a distribuire un nuovo aggiornamento per iOS. Un "fuori programma" causato da un pasticcio clamoroso degli sviluppatori.

Al centro della vicenda c'è una vulnerabilità (CVE-2019-8605) che consente, in pratica, il jailbreak di iPhone e iPad. Sfruttandola, sarebbe possibile installare applicazioni al di fuori del (rigidissimo) recinto predisposto da Apple per i suoi dispositivi.

La falla di sicurezza, che in pratica permette di eseguire codice a livello kernel di iOS, era stata scovata da **Ned Wialliamson**, del solito **Project Zero di Google**. Apple, ricevuta la segnalazione aveva predisposto la patch e l'aveva inserita nell'aggiornamento alla versione 12.3.

In seguito, però, qualcosa è andato storto. **Con i rilascio**

della versione successiva (12.4) del sistema operativo per i suoi dispositivi mobile, gli sviluppatori hanno fatto qualche pasticcio.

La nuova versione, che conteneva un fix per bloccare gli attacchi tramite iMessage, ha in pratica cancellato la patch precedente. **Risultato: i dispositivi con la versione 12.4 sono di nuovo vulnerabili alla falla che consente il jailbreak di iOS**.

Ieri Apple ha dovuto quindi pubblicare un nuovo aggiornamento (12.4.1) che reintroduce la patch già distribuita precedentemente, eliminando così il rischio che qualcuno sfrutti la vulnerabilità per distribuire malware per iPhone e iPad.

Condividi l'articolo

I pirati sfruttano nuove falle nei server Webmin. E non solo…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/27/pasticcio-apple-su-ios-patch-per-correggere-lultimo-aggiornamento/

I pirati sfruttano nuove

falle nei server Webmin. E non solo…

Ago 26, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 1

Attacchi a ripetizione ai servizi di controllo remoto. I cyber-criminali stanno prendendo di mira anche le VPN di FortiGate e Pulse Secure.

Il bello del mondo della sicurezza informatica è che ci sono dei meccanismi che funzionano sempre nello stesso modo. Uno di questi riguarda il fatto che dopo una conferenza internazionale in cui vengono rese pubbliche vulnerabilità e nuove tecniche di attacco, i pirati informatici iniziano a sfruttarle a tempo di record.

Questo mese, di conferenze ce ne sono state due. Oltre al **Def Con** di Las Vegas, si è tenuto infatti anche il **Black Hat USA 2019**. In entrambi, inutile dirlo, sono emerse numerose tematiche e una grandinata di vulnerabilità.

Naturalmente sono state tutte (o quasi) comunicate in modo "responsabile" affinché produttori e sviluppatori potessero mettere mano ai codici per correggere le falle di sicurezza rese pubbliche. **Ma come sappiamo, tra la disponibilità di un aggiornamento e la sua effettiva implementazione ne passa un po'**.

I pirati informatici lo sanno benissimo e nello scorso week-end hanno cominciato a darsi da fare, prendendo di mira in particolare tre prodotti utilizzati a livello enterprise: il

sistema di controllo remoto **Webmin** e le VPN **FortiGate** e **Pulse Secure**.

> *"This week's attacks against Webmin, Pulse Secure, and Fortinet FortiGate are some of the worst this year, not because of volume, but because of the sensitive nature of the systems they target."https://t.co/nVZTXQ6FW2*
>
> *— Bad Packets Report (@bad_packets) August 25, 2019*

Webmin è uno strumento di gestione che permette di controllare in remoto sistemi Linux e Unix, diventato protagonista al Def Con quando il ricercatore turco **Özkan Mustafa Akkuş** ha svelato al mondo che nel programma si nasconde una backdoor.

Akkuş, nel dettaglio, ha spiegato che la backdoor è stata inserita nel programma in seguito a un attacco che ha preso di mira direttamente il pacchetto di installazione del programma e che è passata inosservata per più di un anno.

La vulnerabilità (CVE-2019-15107) in realtà è presente solo nella versione di Webmin disponibile su **SourceForge**, mentre quella su GitHub è "pulita". L'ipotesi, quindi, è che in qualche modo i cyber-criminali siano riusciti a infettare il repository o direttamente i sistemi dello sviluppatore.

Quale che sia l'origine, la backdoor rappresenta una vera voragine nella piattaforma: consente infatti di avviare esecuzione di codice in remoto senza alcun bisogno di autenticazione. Il problema è stato risolto nella versione v1.930 di Webmin, rilasciata la scorsa settimana.

I pirati non hanno perso tempo e hanno cominciato a sfruttare la vulnerabilità in maniera intensiva. Anche se gli esperti specificano che gli attacchi non destano preoccupazioni (almeno per ora dal punto di vista quantitativo, questa tipologia di attacchi rischia di essere estremamente distruttiva.

Per quanto riguarda le VPN, invece, le dritte per gli attacchi sono arrivate dal Black Hat USA 2019, nel corso del quale il tema delle vulnerabilità nelle **Virtual Private Network** ha avuto ampio risalto.

Sebbene nel corso del talk dedicato siano emerse falle di sicurezza in un gran numero di prodotti enterprise, a partire dallo scorso venerdì gli esperti hanno rilevato attacchi che hanno preso di mira soltanto due prodotti.

Il motivo? Per la VPN di FortiGate e per Pulse Secure sono disponibili dei Proof of Concept pubblicati in questo post su Internet. **Insomma: i cyber-criminali, in questo caso, hanno già tutto quello che gli serve per portare l'attacco**.

La vulnerabilità consente, in pratica, di colpire i dispositivi che utilizzano la VPN accedendo ai file di autenticazioni per ottenere le password.

Teoricamente, gli attacchi dovrebbero avere ben poche possibilità di andare a segno. Entrambe le vulnerabilità (CVE-2019-11510 per Pulse Secure e CVE-2018-13379 per FortiGate) sono state infatti corrette con il rilascio di patch, rispettivamente, in aprile e in maggio.

> *14,528 Pulse Secure VPN servers vulnerable to CVE-2019-11510.*
>
> *2,535 organizations affected including government agencies, universities, and numerous Fortune 500 companies.*
>
> *We've shared our findings with @USCERT_gov and other CERT teams around the world.https://t.co/lXcedIyQSB*
>
> *— Bad Packets Report (@bad_packets) August 25, 2019*

Peccato che gli amministratori IT delle aziende che utilizzano i due prodotti non siano evidentemente molto reattivi in tema di aggiornamenti. **Nel caso di Pulse Secure, secondo i ricercatori ci sarebbero ben 14.500 installazioni vulnerabili**

su un totale di 42.000.

Per capire la rilevanza del problema, Pulse Secure viene utilizzato da numerosi enti pubblici (tra cui università e istituti di ricerca) e dall'esercito USA.

Condividi l'articolo

Pasticcio Apple su iOS: patch per correggere l'ultimo aggiornamento Torna la botnet Emotet. Gli esperti: "i server sono di nuovo attivi"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/26/i-pirati-sfruttano-nuove-falle-nei-server-webmin-e-non-solo/