Attacco a un server MDM per diffondere un malware per Android

Mag 04, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L'azione mirata ha permesso ai pirati di prendere il controllo del sistema di Mobile Device Management e distribuire il trojan Cerberus.

L'adozione di sistemi di **Mobile Device Management (MDM)** rappresentano uno strumento fondamentale attraverso il quale le aziende possono garantire un adeguato livello di sicurezza sui dispositivi mobili dei loro dipendenti, prevedendo la distribuzione centralizzata di aggiornamenti e il controllo dei software di protezione.

Come ogni sistema centralizzato, però, MDM rappresenta un bersaglio ideale per i pirati informatici, che potrebbero sfruttarlo per colpire con facilità un elevato numero di dispositivi sfruttando un canale privilegiato.

Fino a oggi, però, questa era solo un'ipotesi. Ora non più. Come spiegano i ricercatori di **Check Point**, il primo caso di violazione di un sistema MDM è stato compiuto da un gruppo di pirati informatici che hanno sfruttato la tecnica per diffondere **Cerberus**, un trojan per smartphone **Android**.

Nel loro report, gli analisti della società di sicurezza ricostruiscono la vicenda partendo dal rilevamento di una inusuale diffusione del malware che ha insospettito da subito gli esperti.

L’azienda colpita, di cui non indicano il nome, ha infatti subito un attacco che ha portato in pochissimo tempo all’infezione del 75% dei dispositivi mobili aziendali.

Un fenomeno che ha fatto pensare a due ipotesi: l’utilizzo di un malware in grado di diffondersi attraverso una sorta di “movimento laterale” all’interno della rete mobile dell’azienda o, appunto, la compromissione del sistema MDM.

L’azienda interessata ha confermato la seconda ipotesi, senza fornire però maggiori dettagli sulle modalità con cui i cyber-criminali avrebbero preso il controllo del sistema.

Anche se derivato da un malware originariamente specializzato nel furto delle credenziali dei servizi bancari, Cerberus è un classico trojan programmato per sottrarre informazioni personali e, in particolare, le credenziali di accesso a servizi, gli SMS e il registro delle chiamate.

L’obiettivo dei pirati informatici, quindi, era presumibilmente quello di avviare una campagna di spionaggio in grande stile ai danni dell’impresa colpita.

Condividi l’articolo

Boom di attacchi ai collegamenti in remoto RDP

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/04/attacco-a-un-server-mdm-per-diffondere-un-malware-per-android/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-a-un-server-mdm-per-diffondere-un-malware-per-android

---

Boom di attacchi ai collegamenti in remoto RDP

Apr 30, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS, Scenario 0

L'allarme di Kaspersky: con la quarantena da Covid sono aumentati esponenzialmente gli attacchi di brute forcing ai sistemi Remote Desktop.

Altro che tregua: se alcuni gruppi di cyber-criminali hanno annunciato una sorta di "sospensione delle attività" durante la pandemia che sta attraversando il pianeta, altri stanno approfittando della situazione sottoponendo i sistemi delle aziende a veri e propri bombardamenti.

Il bersaglio preferito, spiegano dalle parti di **Kaspersky**, sono i collegamenti **Remote Desktop**, che molte aziende hanno dovuto attivare in fretta e furia per consentire ai loro dipendenti di continuare a lavorare da casa.

Stando ai rilevamenti della società di sicurezza, gli attacchi basati su tecniche di brute forcing rivolti ai servizi **RDP (Remote Desktop Protocol)** hanno registrato una clamorosa impennata nel momento stesso in cui molti paesi hanno avviato il lockdown delle attività, invitando le imprese ad adottare formule di smart working quando possibile.

Il servizio RDP è lo standard **Microsoft** per le connessioni da remoto e utilizza, di solito, un sistema di autenticazione basato esclusivamente su username e password. L'adozione di attacchi di brute forcing, di conseguenza, rappresenta la tecnica più semplice per violare gli account.

Una tecnica che, per la verità, era già ampiamente utilizzata dai pirati informatici per avere accesso ai network aziendali. In particolare nelle strategie adottate per diffondere ransomware.

Come difendersi? Gli esperti consigliano l'utilizzo di VPN e una particolare attenzione nella gestione delle impostazioni dei firewall, prevedendo la chiusura della porta 3389 se il servizio non viene utilizzato.

La soluzione adottata da alcuni amministratori IT di

modificare la porta utilizzata per RDP è invece completamente inutile. Strumenti come **Shodan** permettono tranquillamente di rilevarne la presenza anche su una porta diversa.

Condividi l’articolo

Cresce il lavoro da casa: i pirati fanno festa

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/30/boom-di-attacchi-ai-collegamenti-in-remoto-rdp/?utm_source=rss&utm_medium=rss&utm_campaign=boom-di-attacchi-ai-collegamenti-in-remoto-rdp

---

Cresce il lavoro da casa: i pirati fanno festa

Apr 29, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

I cyber-criminali stanno approfittando dello “smart working forzato” in tempi di coronavirus per portare attacchi ai network aziendali.

Dopo gli allarmi, arrivano le conferme. Il boom del lavoro in

remoto provocato dall’isolamento forzato per contrastare la pandemia di coronavirus si è trasformato in un’occasione che i pirati informatici stanno sfruttando attivamente.

A spiegarlo è **Nate Warfield**, senior security program manager di **Microsoft**, che nel corso del **Security Analyst Summit** (in edizione virtuale) ha segnalato come i cyber criminali stiano moltiplicando i loro sfrozi per sfruttare a tempo di record qualsiasi vulnerabilità utile per colpire quelli che, a tutti gli effetti, sono diventati i nuovi anelli deboli nella sicurezza aziendale.

Il tema è quello della vulnerabilità delle reti domestiche, che nella nuova situazione si sono trasformate in un’estensione del network aziendale, senza però avere le caratteristiche di sicurezza e la possibilità di controllo e monitoraggio delle normali reti locali.

All’improvviso, spiega Warfield, la sicurezza del network aziendale sconta tutti i limiti di router antiquati, , Smart TV e dispositivi IoT di qualsiasi genere. **Tutti device che, in un ambito professionale, di solito non sono presenti e che**

rappresentano fattori di rischio assolutamente fuori controllo.

Non che la situazione a livello di infrastrutture più strettamente aziendali vada molto meglio. Con il divieto di circolazione, molti amministratori IT non possono infatti avere accesso fisico ai dispositivi aziendali (per esempio per resettare un server) e sono costretti a lavorare solo in remoto.

Uno dei risultati, fa notare l'esperto, è che da una ricerca di Shodan risultano essere online almeno 126.000 macchine in cui non è stata applicata la patch per correggere la falla **SMB Ghost** rilasciata da Microsoft lo scorso 12 marzo.

Dall'altro lato, i pirati informatici si stanno muovendo sempre più rapidamente, sfruttando le condizioni precarie in cui si trovano le aziende. Uno dei casi citati da Warfield è quello della vulnerabilità di **Citrix Netscaler** (ne abbiamo parlato in questo articolo) che i cyber-criminali sarebbero riusciti a sfruttare con strumenti automatici nel giro di un paio di giorni.

Nel nuovo scenario, attacchi come questi possono contare su una posizione di vantaggio che rischia di mettere in seria crisi l'attività dei responsabili della cyber security.

Condividi l'articolo

Il ransomware Shade abbandona il campo. I pirati rilasciano le password

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/04/29/cresce-il-lavoro-da-casa-i-pirati-fanno-festa/?utm_source=rss&utm_medium=rss&utm_campaign=cresce-il-lavoro-da-casa-i-pirati-fanno-festa

Il ransomware Shade abbandona il campo. I pirati rilasciano le password

Apr 28, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I cyber-criminali pubblicano più di 750.000 password per decodificare i file colpiti dal malware. Esperti al lavoro per sviluppare il tool di decrittazione.

Dopo sei anni di (dis)onorevole attività, il ransomware **Shade** (conosciuto anche come **Troldesh**) abbandona le scene. Il malware, comparso nel 2014, ha imperversato soprattutto nell'est Europa e il suo "pensionamento" è stato annunciato dagli stessi cyber-criminali con una comunicazione su **GitHub**.

Shade è un classico crypto-ransomware, che codifica con un algoritmo di crittografia i documenti presenti sul computer della vittima e richiede un riscatto per ottenere la chiave che consente il recupero dei file.

Nel messaggio, si legge che gli autori di Shade hanno cessato la loro attività di diffusione del ransomware nel 2019, ma adesso hanno deciso di rendere pubblico su un repository

GitHub sia il loro software per la decrittazione dei file, sia un database con oltre 750.000 password.

L’obiettivo, spiegano, è quello di consentire alle società di sicurezza di sviluppare un software più facile da utilizzare rispetto al loro tool di decrittazione, che possa essere distribuito alle vittime del ransomware (quelle che non hanno pagato il riscatto) per recuperare i loro dati.

In realtà, nel corso degli anni sono comparsi numerosi tool per la decodifica dei file colpiti da Shade, ma lo sviluppo di nuove versioni del ransomware aveva reso comunque problematico offrire uno strumento efficace per tutti.

Ora, contando sulla disponibilità del software utilizzato dai pirati e, soprattutto, delle password, gli esperti di sicurezza possono creare lo strumento “definitivo” per la decodifica.

Nessuna spiegazione da parte dei pirati riguardo le motivazioni che li hanno indotti a cessare la loro attività. **È possibile, però, che i cyber-criminali stiano semplicemente preparando un altro malware e che questa “uscita di scena” sia solo una strategia per ottenere credibilità agli occhi dell’opinione pubblica**.

Il rilascio delle password o degli strumenti di decodifica al termine di una campagna di attacchi ransomware, infatti, non è

un evento insolito.

I pirati informatici, in questo modo, dimostrano che il loro ransomware consente effettivamente di recuperare di dati (cosa che non sempre accade) e dimostrano anche una sorta di “etica” nel rimediare ai danni fatti nei confronti di chi non ha voluto cedere all’estorsione.

Tanto più che i pirati informatici specializzati in ransomware puntano ormai a portare attacchi mirati nei confronti delle aziende, che garantiscono guadagni maggiori. È possibile che anche gli autori di SHade abbiano deciso di cambiare specializzazione.

Condividi l’articolo

Attacchi attraverso uno zero-day ai firewall Sophos

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/28/il-ransomware-shade-abbandona-il-campo-i-pirati-rilasciano-le-password/?utm_source=rss&utm_medium=rss&utm_campaign=il-ransomware-shade-abbandona-il-campo-i-pirati-rilasciano-le-password

---

Falla in Microsoft Teams: l’account si ruba con una GIF

Apr 27, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La tecnica permette di sottrarre i dati dell’account utente attraverso una catena di azioni che sfruttano una vulnerabilità nell’autenticazione.

Non solo Zoom. Con il boom delle videoconferenze e dello smart working l’attenzione dei ricercatori di sicurezza si sta concentrando sulle piattaforme di comunicazione e collaborazione. Tra questi, un ruolo di primo piano, soprattutto a livello aziendale, l’ha **Microsoft Teams**.

La notizia della presenza di una vulnerabilità nella piattaforma di chat, videoconferenza e collaborazione basata su **Skype for Business** rappresenta quindi una pessima notizia per le aziende.

A individuare il problema sono stati i ricercatori di **CyberArk**, che in un (dettagliatissimo) report pubblicato sul blog ufficiale della società di sicurezza spiega come sia possibile sottrarre un account Microsoft Teams utilizzando una semplice immagine in formato **GIF**.

La possibilità di un attacco deriva da due fattori. Il primo è la modalità con cui vengono gestite le immagini e la loro visualizzazione in Teams. **Il secondo risiede nel sistema di autenticazione di Teams, che sfrutta un sistema di due token che vengono scambiati con i server Microsoft**.

Riassumendo: quando un’immagine viene inviata in Teams, è memorizzata sui server Microsoft e per guardarla è necessario

che il software si autentichi. I token utilizzati per l’autenticazione, che vengono generati volta per volta, possono essere però intercettati da chi gestisce dei sottodomini di teams.microsoft.com.

La domanda, qui, sorge spontanea: è possibile che un pirata informatico ottenga il controllo di un sottodominio del genere? Secondo i ricercatori di CyberArk, sì. In particolare, gli analisti della società di sicurezza ne hanno potuti individuati rapidamente due: **aadsync-test.teams.microsoft.com** e **data-dev.teams.microsoft.com**.

Come funzionerebbe quindi l’attacco? Lo schema qui sotto lo spiega bene.

Dopo essersi assicurato il controllo di un sottodominio adeguato, il pirata informatico non deve fare altro che inviare un messaggio con una GIF creata ad hoc che gli consente di recuperare i token di autenticazione e rubare l’accesso all’account della vittima.

A questo punto, può usare l’account rubato per inviare il messaggio ad altri utenti all’interno dell’azienda e sottrarre così tutti i messaggi e i dati scambiati con Microsoft Teams.

Il tutto avverrebbe senza alcun segnale che possa far pensare a una violazione e avrebbe quindi un impatto devastante.

La vulnerabilità, comunicata tempestivamente a Redmond, è stata corretta con un aggiornamento del software e adesso il rischio di un furto di account tramite l'invio di immagini. Tutta la vicenda, però, rappresenta un ulteriore indizio di quanto i sistemi di comunicazione e collaborazione siano vulnerabili ad attacchi esterni.

Condividi l'articolo

Allarme dell'NSA sulla diffusione delle Web Shell

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/27/falla-in-microsoft-teams-laccount-si-ruba-con-una-gif/?utm_source=rss&utm_medium=rss&utm_campaign=falla-in-microsoft-teams-laccount-si-ruba-con-una-gif

---

Allarme dell'NSA sulla diffusione delle Web Shell

Apr 24, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

L’agenzia statunitense ha registrato un aumento nell’infiltrazione dei server di rete. Sarebbero migliaia quelli compromessi.

Nuovo capitolo legato al “nuovo ruolo” che si stanno ritagliando i servizi segreti statunitensi nel panorama della sicurezza. Dopo aver reso disponibili i loro strumenti di analisi alla comunità dei ricercatori, dalle parti dell’**NSA** sembrano decisi a darsi da fare per contribuire al contrasto del cyber crimine anche diffondendo segnalazioni.

L’allarme lanciato dagli 007 Made in USA riguarda in particolare l’utilizzo, da parte dei pirati informatici, delle cosiddette **Web Shell** (particolari script che agiscono come backdoor – ndr) per garantirsi un controllo di lungo periodo sui network compromessi.

Nel loro comunicato, spiegano che gli script sono sempre più utilizzati da gruppi di cyber-criminali e che la situazione ha raggiunto livelli tali da richiedere una reazione da parte di tutti i soggetti che gestiscono sistemi informatici.

Lo strumento messo a loro disposizione è un paper di 17 pagine (scaricabile a questo indirizzo) e una serie di software che gli stessi esperti della NSA hanno raccolto su un repository di GitHub accessibile a chiunque.

Nel paper pubblicato, vengono anche segnalate una serie di vulnerabilità utilizzate dai pirati informatici per diffondere le loro backdoor. Falle di sicurezza che fanno riferimento a piattaforma e software molto diffusi, come **Microsoft SharePoint**, **WordPress** e alcuni applicativi **Citrix**.

Insomma: il nuovo corso dell'NSA in cui l'agenzia di sicurezza nazionale abbandona il suo ruolo di "battitore libero" nella cyber security per adottare quello di responsabile partner delle società di sicurezza prosegue. Anche se tra gli addetti ai lavori rimane qualche (giustificata) diffidenza nei confronti della svolta.

Condividi l'articolo

Rapporto Cisco: cloud e automazione sono le sfide della security

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/24/allarme-dellnsa-sulla-diffusione-delle-web-shell/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-dellnsa-sulla-diffusione-delle-web-shell

---

Rapporto Cisco: cloud e automazione sono le sfide della security

Apr 24, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 1

L'indagine del colosso statunitense mette in luce le priorità delle aziende in tema di sicurezza informatica. Dalle esigenze alle strategie di difesa: ecco il quadro che emerge.

Si parla in continuazione del mutato panorama in ambito cyber security, della sua rilevanza a livello aziendale e dei cambiamenti avvenuti sia a livello di minacce, sia a livello di approccio da parte di chi queste minacce deve affrontare.

Più raramente, però, si ha l'occasione di verificare tutto questo sul campo, attraverso i feedback di chi si occupa tutti i giorni di sicurezza. Il report di **Cisco**, intitolato **2020 CISO Benchmark Study**, rappresenta da questo punto di vista uno strumento per avere una mappatura di ciò che sta accadendo a livello di cyber security attraverso la lente degli esperti

del settore.

Lo studio, oltre a confermare alcuni elementi di ciò che sta accadendo nel settore, accende anche i riflettori sulle differenze tra l'Italia e il resto del mondo, evidenziando un livello di percezione decisamente diverso nel nostro paese rispetto ad altre realtà.

A partire, per esempio, dal tema dell'omologazione degli strumenti di difesa. Un problema che riguarda sempre più aziende, che per proteggere i loro sistemi IT arrivano a utilizzare soluzioni specifiche di differenti produttori (fino a 20) che rendono estremamente complessa la loro gestione.

Un fenomeno che, secondo gli analisti di Cisco, è alla base di quello che hanno battezzato come "cybersecurity fatigue", cioè la rinuncia a stare al passo con le minacce e i criminali informatici.

Un problema che, nel nostro paese, sembra incidere meno che altrove, visto che viene indicato solo dal 29% degli intervistati contro il 42% del campione estero. Il tema, secondo gli esperti di Cisco, non è però da sottovalutare.

"Per supportare il percorso di trasformazione digitale che sta affrontando gran parte delle aziende, i CISO stanno dando

sempre più importanza all’adozione di tecnologie di sicurezza per ridurre l’esposizione alle minacce informatiche. Spesso, molte di queste soluzioni non sono integrate, creando così una sostanziale complessità nella gestione del loro ambienti di sicurezza,” spiega **Steve Martino**, **Senior Vice President and Chief Information Security Officer di Cisco**. “Per risolvere tale problema, i professionisti della sicurezza devono continuare verso il consolidamento dei vendor, aumentando al contempo la fiducia nella sicurezza e nell’automazione nel cloud per rafforzare il loro livello di sicurezza e ridurre il rischio di violazioni”.

Ma quali sono gli ambiti in cui le aziende incontrano le maggiori difficoltà? Secondo la ricerca, uno dei temi più spinosi riguardala protezione dei dispositivi mobile e personali, che per il 52% degli intervistati (il 32% in Italia) continuano a rappresentare un problema.

Percepito come problematica anche **la gestione dei datacenter**, con il 41% delle aziende intervistate (il 23% in Italia) che ritiene estremamente difficile proteggerli, mentre il 39% (il 25% in Italia) dichiara di avere difficoltà nel garantire l’integrità delle applicazioni.

Altra criticità sarebbe rappresentata dal **cloud pubblico**, con il 52% (il 30% in Italia) che ritiene tale attività molto o estremamente difficile, e il 50% (il 36% in Italia) secondo il quale l’infrastruttura cloud privata è stata una delle principali sfide in termini di sicurezza.

Insomma: a guardare i dati, sembrerebbe che nel nostro paese ci sia una percezione decisamente diversa. Il dubbio, inutile negarlo, è che più che un minore livello di criticità, ci sia un’inferiore consapevolezza dei rischi e, in definitiva, una minore sensibilità sul tema.

Dallo studio, però, emergono anche alcuni dati rassicuranti per il nostro paese. Il primo riguarda l’adozione di sistemi di autenticazione multi-fattore. Secondo quanto registrato nella ricerca, il 38% delle aziende italiane utilizzerebbe un approccio **Zero Trust** basato su MFA per l’accesso alle reti, contro il 27% a livello globale.

Anche il numero di attacchi subiti a causa di vulnerabilità non corrette (46% delle aziende a livello globale, 30% in Italia) lascerebbe pensare a una situazione che, per una volta, colloca il nostro paese in una posizione migliore rispetto ad altre realtà.

La tendenza nel settore, però, conferma l’attenzione degli esperti al tema dell’automazione nei sistemi di sicurezza, in cui l’adozione di strumenti di intelligenza artificiale e machine learning rappresenta una priorità assoluta.

Soprattutto per quanto riguarda la protezione dei servizi cloud, che vengono percepiti come un fattore abilitante ma richiedono strumenti specifici per garantirne la sicurezza.

Condividi l’articolo

Allarme dell’NSA sulla diffusione delle Web Shell Pasticcio sulle falle di sicurezza per IBM: online 4 zero-day

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/24/rapporto-cisco-cloud-e-automazione-sono-le-sfide-della-security/?utm_source=rss&utm_medium=rss&utm_campaign=rapporto-cisco-cloud-e-automazione-sono-le-sfide-della-security

---

Pasticcio sulle falle di sicurezza per IBM: online 4 zero-day

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

L’azienda ha ignorato per errore la segnalazione di un

ricercatore. Ora i dettagli delle falle di sicurezza sono stati pubblicati.

In un primo momento qualcuno ha pensato che dalle parti di **IBM** avessero deciso di sposare la classica scusa usata in passato da altri colossi dell'informatica per sminuire l'impatto di una falla di sicurezza, ricorrendo al mantra "non è una vulnerabilità, è una feature".

In realtà quello che è successo dalle parti di IBM è un classico pasticcio dovuto a una serie di errori di comunicazione, che hanno però portato a una situazione decisamente spinosa. Qualcosa di simile a ciò che è accaduto a **Microsoft** qualche tempo fa.

Protagonista della vicenda è **Pedro Ribeiro**, direttore del settore di ricerca di **Agile Information Security**. Il ricercatore ha individuato una serie di quattro vulnerabilità all'interno di **IBM Data Risk Manager (IDRM)**, un tool che la società mette a disposizione dei suoi utenti per individuare e analizzare eventuali rischi nella gestione dei dati.

Le falle di sicurezza, nel dettaglio, riguarderebbero un sistema per aggirare l'autenticazione, un bug che consente l'iniezione di comandi, la presenza di una password predefinita e una vulnerabilità che consente di forzare il download di un file.

Vulnerabilità decisamente gravi, che se sfruttate (singolarmente o in sequenza) permetterebbero di portare attacchi ai sistemi che usano IDRM.

Quando Ribeiro ha contattato IBM per segnalare le falle (senza peraltro pretendere alcun compenso sulla base del programma bug bounty dell'azienda) si è sentito però rispondere che le vulnerabilità non venivano considerate perché riguardavano un prodotto "opzionale" dedicato al supporto dei sistemi IBM.

Una cantonata clamorosa, che il ricercatore ha sottolineato spiegando che le vulnerabilità in questione posso portare alla compromissione di tutti i sistemi collegati a IDRM.

A fronte della bizzara risposta dell'azienda, Ribeiro ha però deciso di rendere pubbliche le vulnerabilità, pubblicando anche dei proof of concept per sfruttarle. Solo a questo punto, dalle parti di IBM si sono resi conto dell'errore e si sono attivati per correggere gli zero-day individuati dal ricercatore.

Al momento, gli sviluppatori IBM hanno corretto due delle vulnerabilità e starebbero lavorando a quelle rimanenti.

Condividi l'articolo

Rapporto Cisco: cloud e automazione sono le sfide della security Clamoroso zero-day permette di attaccare iOS attraverso Mail

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/24/pasticcio-sulle-falle-di-sicurezza-per-ibm-online-4-zero-day/?utm_source=rss&utm_medium=rss&utm_campaign=pasticcio-sulle-falle-di-sicurezza-per-ibm-online-4-zero-day

---

Clamoroso zero-day permette di attaccare iOS attraverso Mail

Apr 23, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

La vulnerabilità permette di compromettere l'iPhone con un attacco "zero click". I pirati la stanno usando da almeno due anni.

Grossi guai per gli utenti **iPhone**. Le rivelazioni dei ricercatori di **ZecOps** accendono infatti i riflettori su una clamorosa vulnerabilità zero-day nell'applicazione **Mail** di iOS che consentono attacchi in grado di installare un malware senza che sia necessaria alcuna interazione da parte dell'utente.

La scoperta è avvenuta in seguito all'analisi di una serie di "anomalie" che i ricercatori di ZecOps hanno individuato sui dispositivi di alcuni utenti di alto profilo.

La tecnica utilizzata sfrutterebbe come vettore di attacco semplici messaggi email, il cui contenuto porterebbe a un consumo di memoria RAM tale da permettere una scrittura di dati **Out-Of-Bounds**. La responsabilità, spiegano i ricercatori, è da attribuire a una vulnerabilità della libreria **MIME**.

Dalle parti di ZecOps, però, hanno individuato un'ulteriore falla di sicurezza (nello specifico un **heap overflow**) che consente di ottenere lo stesso effetto.

Le vulnerabilità riguardano sicuramente i sistemi iOS distribuita a partire dalla versione 6 (rilasciato nel 2012), anche se lo studio non esclude che anche le versioni precedenti alla 6 possano essere vulnerabili.

L'attacco si attiva al momento della ricezione dell'email, prima ancora che il contenuto del messaggio sia scaricato completamente. L'unico sintomo visibile sarebbe un rallentamento dell'applicazione di posta e, nel caso di iOS 12, un eventuale crash della stessa.

Nel caso in cui l’attacco dovesse fallire, l’indizio sarebbe invece il fatto che il messaggio di posta elettronica risulterebbe essere privo di contenuto.

Ma qual è il risultato finale dell’attacco? **In realtà l’exploit consente semplicemente di compromettere la stessa applicazione di posta, che opera all’interno di una sandbox**. In altre parole: attraverso questa tecnica è possibile copiare, cancellare un messaggio e (forse) inviarne uno. **L’attacco, da solo, non permette quindi ci compromettere l’intero dispositivo**.

Per ampliare la portata dell’attacco, questo dovrebbe essere combinato a un altro zero-day (di cui non si ha notizia) che consenta di estenderlo al resto del sistema operativo.

Nel loro report, i ricercatori spiegano che entrambe le

tecniche sarebbero utilizzate da tempo da un gruppo che ritengono possa lavorare per conto di un'organizzazione governativa. **Il primo attacco verificato di questo tipo, spiegano, risalirebbe addirittura al gennaio 2018**.

A rendere ancora più insidioso questo tipo di attacco, c'è il fatto che le email utilizzate per colpire i dispositivi, per lo meno nei casi individuati dai ricercatori, sono state cancellate dai mail server, nascondendo così le tracce dell'attività malevola.

La ricostruzione presentata nel report evidenzia che i pirati informatici che stanno portando attacchi ai dispositivi iOS starebbero utilizzando attivamente la seconda vulnerabilità individuata (heap overflow) mentre la prima tecnica di attacco sarebbe stata utilizzata "per errore".

Quello che è certo, invece, è che l'exploit non richiede l'uso di una catena che coinvolge entrambe le falle di sicurezza: la tecnica di heap overflow è sufficiente per compromettere l'applicazione.

Dalle parti di Apple stanno lavorando alle patch per correggere le vulnerabilità, al momento inserite soltanto in una versione beta di iOS 13.4.5.

Difficile capire perché gli sviluppatori Apple abbiano scelto questa strada, visto che la pubblicazione della patch, anche se in versione beta, equivale a rendere pubblica la vulnerabilità.

La disponibilità dell'aggiornamento in beta, però, spiega la decisione di ZecOps di rendere pubblici i dettagli prima del rilascio della patch definitiva. Mantenere la consueta riservatezza in un'ottica di responsible disclosure, a questo punto, non avrebbe avuto senso.

Il consiglio, di conseguenza, è di non utilizzare Mail fino a quando non verrà rilasciata la versione definitiva di iOS

13.4.5. In un periodo di lockdown, in ogni caso, non è un grande sacrificio.

Condividi l’articolo

Il malware arriva nelle librerie di sviluppo Ruby

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/23/clamoroso-zero-day-permette-di-attaccare-ios-attraverso-mail/?utm_source=rss&utm_medium=rss&utm_campaign=clamoroso-zero-day-permette-di-attaccare-ios-attraverso-mail

---

Il malware arriva nelle librerie di sviluppo Ruby

Apr 21, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L’attacco ha sfruttato i pacchetti di sviluppo del linguaggio di programmazione open source per diffondersi. Obiettivo: rubare Bitcoin.

Un complicato attacco **supply chain** che ha permesso di diffondere con straordinaria efficacia un malware che ha come

obiettivo il furto di Bitcoin. È questa, in sintesi, l'operazione individuata da **ReversingLabs**, illustrata in un report pubblicato lo scorso 16 aprile.

A finire nel mirino dei pirati, spiega l'autore del rapporto **Tomislav Maljic**, è **Ruby**, un linguaggio di programmazione open source piuttosto popolare.

Nel dettaglio, i cyber-criminali hanno sfruttato come vettore di attacco **RubyGems**, un pacchetto software dedicato agli sviluppatori che usano Ruby e che mette a disposizione degli utenti un repository con le "gemme", cioè componenti software (sono circa 158.000) che possono essere utilizzati liberamente.

La tecnica utilizzata dai pirati è stata piuttosto banale: si sono affidati cioè alla tattica del **typo-squatting**, la pubblicazione di file con nomi simili a librerie molto popolari che, in questo modo, vengono scaricate dagli utenti.

L'operazione è stata porta avanti attraverso due account controllati dai pirati che hanno portato al download di migliaia di componenti infetti all'interno del repository.

L'attacco portato dai pirati, però, potrebbe non avere una grande efficacia. Lo schema di attacco, per funzionare, richiede infatti che quella specifica libreria infetta sia scaricata da uno sviluppatore che lavora in ambiente Windows.

Non solo: il codice malevolo inserito nelle librerie, che viene avviato attraverso una complessa catena di operazione che consentono di eseguire il malware senza alcuna interazione da parte dell'utente, prevede semplicemente **l'accesso ai dati contenuti nella clipboard** e la loro sostituzione con un indirizzo di un wallet Bitcoin controllato dai pirati.

In altre parole: il payload finale prevede, per essere efficace, che la vittima stia eseguendo una transazione in Bitcoin che può essere alterata dall'attacco. Quello che gli anglosassoni definirebbero un "long shot" e che, francamente, ha ben poche possibilità di andare a segno.

La vicenda, però, riaccende i riflettori sui rischi legati agli attacchi supply chain, soprattutto quando coinvolgono le filiere di sviluppo software. Per capirne la caratura, è sufficiente considerare che RubyGem, secondo quanto viene riportato sul sito, può vantare **49 miliardi di download**.

Insomma: il tema degli attacchi supply chain è più attuale che mai e rappresenta un fattore di rischio enorme a livello globale.

Condividi l'articolo

Nuova campagna di truffe per i buoni spesa gratuiti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/21/il-malware-arriva-nelle-librerie-di-sviluppo-ruby/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-arriva-nelle-librerie-di-sviluppo-ruby