# Microsoft al lavoro per risolvere 25 bug di Windows

Apr 03, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

---

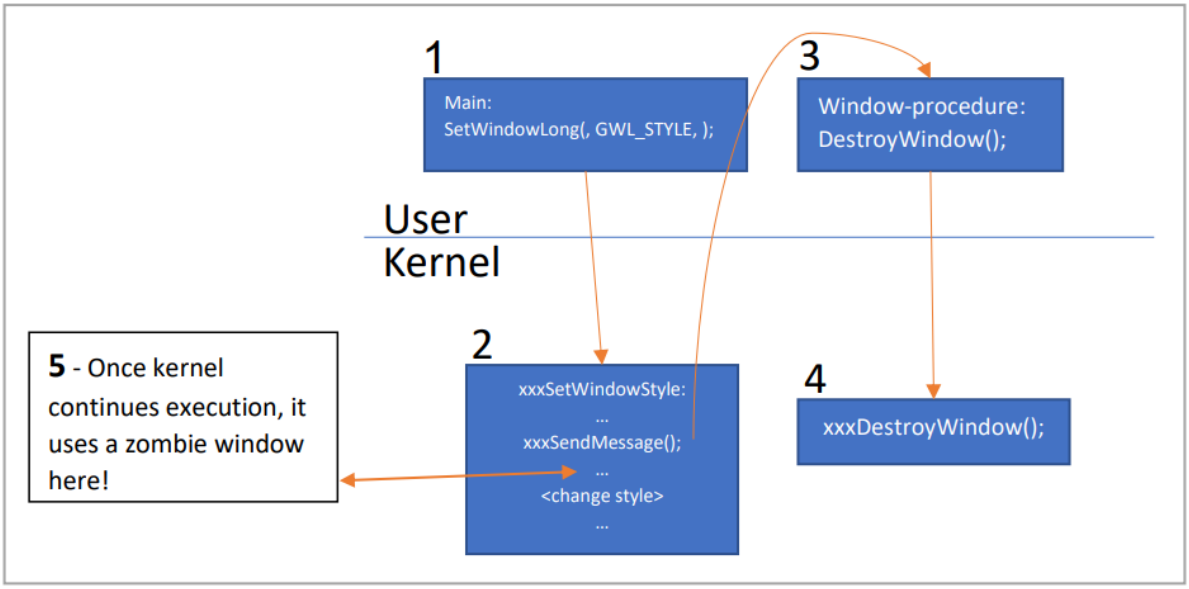
***Le falle di sicurezza sono collegate al famigerato WIN32K. Gli sviluppatori avrebbero già approntato le patch per le prime 11 falle di sicurezza.***

Tempo di straordinari per gli sviluppatori **Microsoft**, che si trovano a fronteggiare una raffica di vulnerabilità di **Windows** (sono la bellezza di 25) scoperte dal ricercatore di sicurezza israeliano **Gil Dabah**.

Il perno di tutta la vicenda è rappresentato da **WIN32K**, un componente di Windows dedicato alla gestione dell'interfaccia utente per le architetture a 32 bit di Windows.

Il componente, in circolazione da molto (troppo) tempo, è stato mantenuto nelle varie versioni di Windows (anche a 64 bit) per garantire la compatibilità con le vecchie applicazioni e interagisce tra interfaccia, driver e il Kernel.

Il problema, spiega Dabah nel suo report, è che l'uso di WIN32K richiede un ampio utilizzo di richiami (callback) dal livello Kernel a quello in modalità utente. Una procedura che, a partire dal 2010, ha evidenziato una serie di problemi e, in particolare, la possibilità di portare un attacco battezzato con il nome di **use-after-free o UAF**.




La tecnica fa leva su un errore nella gestione degli oggetti in memoria e consente, in pratica di eseguire comandi da parte di un utente non autenticato. **In altre parole: apre la strada alla compromissione della macchina**.

Negli ultimi 12 mesi, il ricercatore si è dedicato a questo problema e ha individuato le **25 vulnerabilità** (per alcune delle quali ha già pubblicato dei proof of concept su GitHub) che a settembre 2019 interessavano tutte le versioni di Windows, compresa l'ultima versione di Windows 10 al tempo disponibile.

Gli sviluppatori di Redmond, spiega Dabah, hanno cominciato a lavorare sui bug già dallo scorso novembre e ne avrebbero risolti 11. Il lavoro starebbe procedendo e lo stesso ricercatore ha dichiarato di essere impegnato a sviluppare un sistema di mitigazione più ampio delle singole patch.

Condividi l'articolo

---

Ti presento la botnet Vollgar: 2.000 attacchi al giorno negli ultimi 2 anni

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/04/03/microsoft-al-lavoro-per-risolvere-25-bug-di-windows-win32k/?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-al-lavoro-per-risolvere-25-bug-di-windows-win32k

---

# Ti presento la botnet Vollgar: 2.000 attacchi al giorno negli ultimi 2 anni

Apr 02, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

***Il malware si diffonde attraverso attacchi di brute forcing nei confronti dei database Microsoft SQL per installare backdoor e crypto-miner.***

Una gigantesca operazione di pirateria informatica che sarebbe cominciata nel maggio del 2018 e avrebbe colpito centinaia di migliaia di server. A descriverla nei dettagli sono i ricercatori di **Guardicore**, che in un dettagliato report pubblicato su Internet spiegano il modus operandi del malware **Vollgar**.

Si tratta di una classica botnet, che prende di mira i server **Microsoft SQL (MS-SQL)** con l'obiettivo di installare un crypto-miner (un software in grado di sfruttare la potenza di

calcolo dei server per generare crypto-valuta – ndr) sulla macchina colpita.

Vollgar, stando a quanto si legge nel report, utilizza una tecnica di attacco “mordi e fuggi”: i server vengono infatti infettati per un periodo limitato di tempo (circa due giorni) anche se in alcuni casi la presenza si prolunga fino a periodi di alcune settimane. Una parte di questi (circa il 10%) vengono infettati a più riprese.

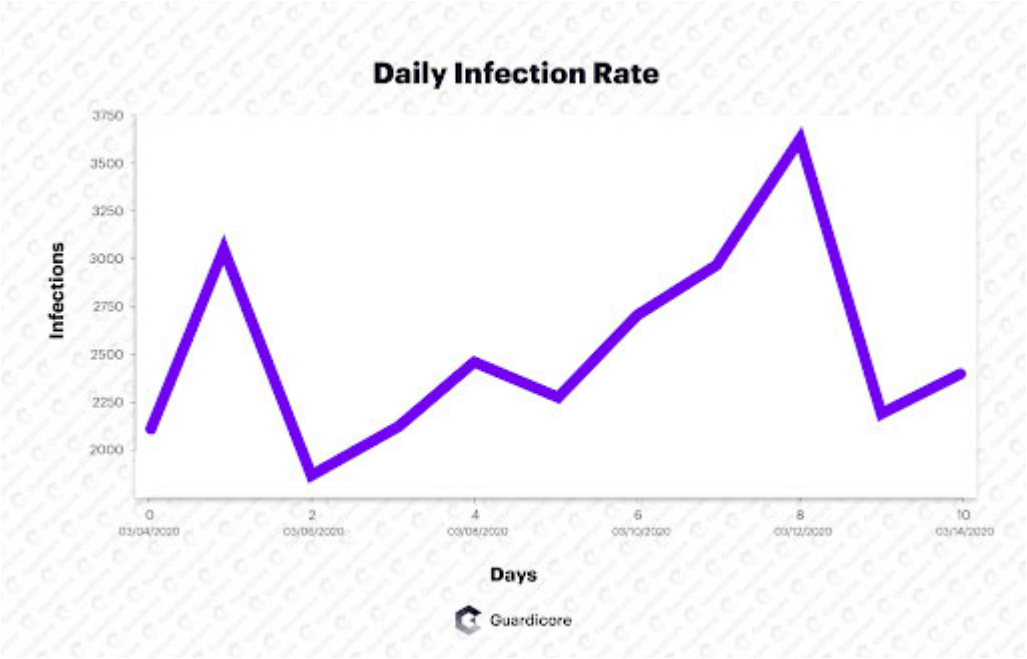



Una strategia che secondo i ricercatori può essere dovuta alla volontà di nascondere la presenza del malware il più a lungo possibile.

L’origine degli attacchi, secondo l’autrice dello studio **Ophir Harpaz**, sarebbe riconducibile a un centinaio di server, la maggior parte dei quali situati in Cina, che utilizzano tecniche di **brute forcing** per violare i database e iniettare da remoto i comandi che avviano l’installazione del miner.

Buona parte di questi server sarebbero comunque macchine compromesse dai pirati informatici, che le starebbero usando

per propagare l’attacco **a un ritmo che ha raggiunto ormai un numero di vittime che varia tra i 2.000 e i 3.000 al giorno**.




L’attribuzione a un gruppo cinese, però, sarebbe confermata da un altro elemento: l’interfaccia di controllo di uno dei server Command and Control (C&C) individuati da Guardicore, infatti, è in cinese.

**Le funzionalità del malware, spiega la ricercatrice, sono però molto più ampie rispetto alla semplice installazione di un crypto-miner**. La botnet, che sfrutta una doppia piattaforma di server C&C, mette infatti a disposizione dei cyber-criminali una serie di funzionalità tipiche dei classici trojan: dalla possibilità di accedere a microfoni e audio a funzioni di keylogging e cattura di schermate in remoto.




Insomma: la campagna di distribuzione del miner potrebbe essere solo la punta dell'iceberg di un'operazione più complessa, o una sorta di "fork" collegata a una classica azione di cyber-spionaggio.

La società di sicurezza ha pubblicato su **GitHub** uno script che consente di individuare Vollgar (scaricabile a questo indirizzo) per consentire agli amministratori di arginare la diffusione del malware che, al momento, sembra inarrestabile.

Condividi l'articolo

---

I veri problemi di Zoom: credenziali di Windows esposte

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/04/02/ti-presento-la-botnet-vollgar-2-000-attacchi-al-giorno-negli-ultimi-2-

anni/?utm_source=rss&utm_medium=rss&utm_campaign=ti-presento-la-botnet-vollgar-2-000-attacchi-al-giorno-negli-ultimi-2-anni

---

# I veri problemi di Zoom: credenziali di Windows esposte

Apr 01, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

---

***Sfruttando la chat della piattaforma di videoconferenza è possibile ottenere l'hash da cui ricavare nome utente e password dei partecipanti.***

Mentre sul Web si susseguono falsi allarmi riguardo eventuali violazioni della privacy da parte dell'ormai diffusissima piattaforma di videoconferenza Zoom (ne abbiamo parlato in questo articolo) cominciano a comparire segnalazioni decisamente più affidabili sui rischi correlati all'uso del sistema.

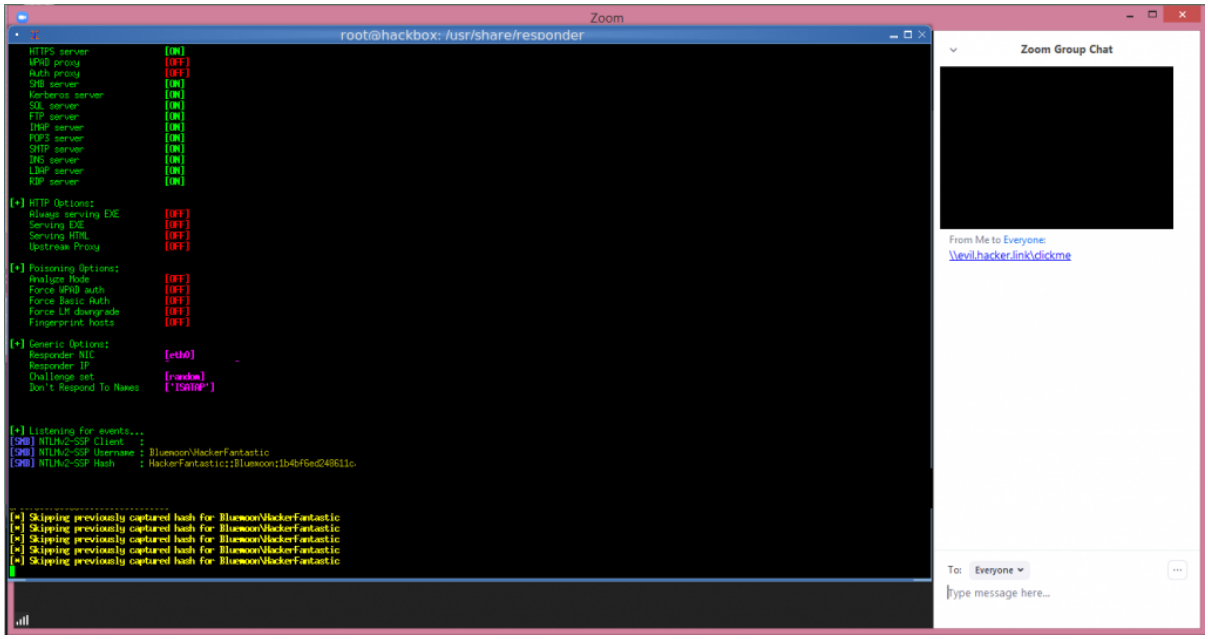
La più rilevante è stata individuata da un ricercatore di sicurezza che su Twitter si firma con il nome di @_g0dmode e che ha rivelato come Zoom possa essere usato per individuare le credenziali degli utenti Windows.

Il problema, in pratica, è che la chat di Zoom non distingue tra normali link Internet e UNC path, cioè ai percorsi che consentono di aprire file all'interno di una rete.

Sarebbe quindi possibile inserire in chat un percorso che, se

cliccato da uno dei partecipanti, avvierebbe una connessione attraverso il protocollo SMB, che invia l'hash delle credenziali dell'utente. **Con questa informazione, un pirata informatico potrebbe facilmente ottenere il nome utente e la password**.

Un problema non da poco, soprattutto in ambito aziendale. Tanto più che la violazione dell'hash, spiegano gli esperti, richiede una manciata di secondi attraverso l'utilizzo di strumenti come **Hashcat**.




Il problema ulteriore, evidenziato questa volta da **Matthew Hickey**, è che la stessa tecnica può essere usata per avviare l'esecuzione di un programma.

Per fortuna, una tale operazione attiverebbe il controllo **UAC**, chiedendo quindi una conferma all'utente. Considerata la situazione attuale, in cui molte persone stanno utilizzando strumenti di comunicazione e collaborazione in remoto con le quali non hanno una grande dimestichezza, il rischio rimane comunque elevato.

Insomma: se Zoom non rappresenta di per sé un pericolo per la privacy o la sicurezza, l'uso "disinvolto" della piattaforma può aprire la strada a forme di attacco a cui normalmente gli

utenti non sonno esposti e che, di conseguenza, possono rappresentare un problema non da poco, soprattutto se lo si utilizza per conversazioni “sensibili”.

Quest’ultimo tema è emerso per esempio in Gran Bretagna, quando il premier **Boris Johnson** ha pensato bene di condividere su **Twitter** l’immagine di una riunione di gabinetto via Zoom, facendo venire una crisi di nervi ai responsabili di sicurezza del Regno Unito.

> *This morning I chaired the first ever digital Cabinet.*
>
> *Our message to the public is: stay at home, protect the NHS, save lives. #StayHomeSaveLives pic.twitter.com/pgeRc3FHIp*
>
> *— Boris Johnson #StayHomeSaveLives (@BorisJohnson) March 31, 2020*

La piattaforma di videoconferenza, infatti, non dispone di un sistema di crittografica end to end e non sarebbe esattamente lo strumento più adatto per tenere meeting di questo livello. **Pubblicare la foto su Twitter, in cui si può vedere anche il codice di chiamata, non è poi un’idea particolarmente brillante**.

Per fortuna, riportano gli organi di stampa, la conferenza era protetta da password. Almeno quello…

Condividi l’articolo

---

Bufera su Zoom e Houseparty, ma non c’è niente di vero

---

## Articoli correlati

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/04/01/i-veri-problemi-di-zoom-credenziali-di-windows-esposte/?utm_source=rss&utm_medium=rss&utm_campaign=i-veri-problemi-di-zoom-credenziali-di-windows-esposte

---

# Bufera su Zoom e Houseparty, ma non c'è niente di vero

Mar 31, 2020 Marco Schiaffino In evidenza, News, Privacy, RSS, Scenario 0

---

***Presunte violazioni della privacy per Zoom. L'app di Epic accusata di rubare dati. Gli sviluppatori : "diamo 1 milione di dollari a chi ne fornisce la prova".***

La tempesta perfetta verificatasi in queste ore è stata generata dall'incrocio tra due fenomeni legati alla pandemia Covid-19: il boom delle piattaforme di videoconferenza e la crescita esponenziale di bufale in circolazione sul Web.

Il risultato è una raffica di allarmi (più o meno) ingiustificati che corrono su Internet e chat coinvolgendo due delle piattaforme più utilizzate in questi giorni per videoconferenze: **Zoom** e **Houseparty**.

Il caso di Houseparty, social network creato dal produttore di videogame **Epic**, è una classica bufala che è circolata via **Whatsapp** e **Twitter** in questi giorni e che accusa l'applicazione di contenere un malware in grado di rubare le

credenziali di vari servizi, dalla posta elettronica ai servizi di banking online.

Il tutto sembrerebbe essere partito dagli Stati Uniti, ma si è rapidamente diffuso anche in Italia, dove l'app sta avendo un certo successo tra chi la sua per fare videochiamate con amici e parenti in questo momento di isolamento.




Naturalmente, come confermano i ricercatori di sicurezza che hanno analizzato l'app, non c'è nulla di vero. Il software non contiene funzioni malevole e non ha nemmeno vulnerabilità (o almeno vulnerabilità evidenti) che possano aprire la strada ad azioni di hacking.

Epic, che gestisce la piattaforma social, non ha preso bene quest'ondata di accuse e **ha offerto 1 milione di dollari a chi dovesse riuscire a provare che la sua app consente di hackerare i dispositivi degli utenti**.

> *We are investigating indications that the recent hacking rumors were spread by a paid commercial smear campaign to harm Houseparty. We are offering a $1,000,000 bounty for the*

> *first individual to provide proof of such a campaign to bounty@houseparty.com.*
>
> *— Houseparty (@houseparty)* ***March 31, 2020***

In precedenza, sul Web sono comparse denunce riguardanti Zoom, l'altra piattaforma per videoconferenze che in questo momento sta registrando una crescita esponenziale di utilizzatori. Le accuse di violazione della privacy lanciate da **Doc Searls** sul suo blog negli ultimi giorni, però, non sembrano avere grande fondamento.

Searls sostiene, in pratica, che Zoom abbia accesso a ogni tipo di informazione (anche quelle trasmesse in videoconferenza) e che le rivenda a società esterne che le utilizzerebbero con finalità di marketing.

Le condizioni d'uso della piattaforma, però, non contengono quanto riportato dal ricercatore (anzi, sembrano negare in qualsiasi modo che Zoom abbia accesso a informazioni registrate dalle videoconferenze) e gli articoli di Searls non contengono prove tecniche che confermino un uso improprio.

**Security Info** ha contattato Zoom per avere un commento, ma per il momento non abbiamo ancora ricevuto risposta.

Nel frattempo la piattaforma sta effettivamente vivendo qualche problema che, nella maggior parte dei casi, è dovuto semplicemente a un uso improprio o troppo "disinvolto" da parte dei suoi utenti.

A segnalarlo è l'**FBI**, che ha emesso un avviso per sensibilizzare gli utenti nei confronti dei **rischi di intrusioni nelle videoconferenze**. Il problema, però, non riguarda una vulnerabilità della piattaforma, ma la scarsa confidenza con il mezzo che hanno molti degli utilizzatori, che organizzano videoconferenze pubbliche e spesso condividono il link per parteciparvi anche sui social network.

**Il caso citato a esempio è quello di una classe di un liceo, la cui lezione in videoconferenza è stata interrotta da un individuo che, proferendo bestemmie, avrebbe anche rivelato pubblicamente l'indirizzo di residenza dell'insegnante**.

Si moltiplicano, però, i tentativi da parte dei pirati informatici di sfruttare la popolarità di Zoom per distribuire malware. La tecnica è quella di proporre il download di una versione infetta dell'applicazione su siti "alternativi".

La raccomandazione, piuttosto banale per la verità, è quindi quella di scaricare l'installer di Zoom solo dal sito ufficiale.

Condividi l'articolo

---

Gruppi hacker sconosciuti all'attacco dei dispositivi DrayTek

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/03/31/bufera-su-zoom-e-houseparty-ma-non-ce-niente-di-vero/?utm_source=rss&utm_medium=rss&utm_campaign=bufera-su-zoom-e-houseparty-ma-non-ce-niente-di-vero

---

# Gruppi hacker sconosciuti

# all’attacco dei dispositivi DrayTek

Mar 30, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

---

***I due gruppi APT stanno sfruttando delle vulnerabilità zero-day dei dispositivi per registrare tutto il traffico di rete delle aziende che li usano.***

Due vulnerabilità zero-day utilizzate dai pirati informatici per intercettare il traffico delle aziende. La denuncia arriva da **Qihoo 360** e riguarda alcuni dispositivi di **DrayTek** che i cyber-criminali starebbero prendendo di mira in una campagna di spionaggio avviata lo scorso dicembre.

Come si legge nel post pubblicato sul blog ufficiale della società di sicurezza cinese, a sfruttare le falle di sicurezza sarebbero due distinti gruppi hacker.

Il primo, che i ricercatori chiamano semplicemente **Attack Group A**, si è concentrato su una falla di sicurezza estremamente complessa da sfruttare, che in pratica utilizza come vettore di attacco un tentativo di login attraverso un pacchetto di dati crittografati che vengono inviati nel campo relativo allo username.

**Quando il pacchetto viene ricevuto, viene decodificato ed eseguito, consentendo ai pirati di prendere il controllo del router DrayTek Vigor**.

L’obiettivo dei pirati, spiegano i ricercatori, non è quello di sfruttare il dispositivo per scopi “normali”, come l’esecuzione di attacchi DDoS. **Il gruppo, invece, dirotta il traffico e lo registra**. Si tratterebbe, quindi, di una vera e

propria attività di spionaggio.




Dall’analisi delle porte monitorate (21; 25; 110 e 143) i ricercatori hanno dedotto che gli hacker sono interessati alle trasmissioni di mail e alle comunicazioni tramite protocollo FTP.

Si tratta di comunicazioni che avvengono senza protezione crittografica e che, di conseguenza, permetterebbero ai pirati informatici di appropriarsi facilmente delle credenziali di accesso ai vari servizi.

L’attività di quello che è stato battezzato **Attack Group B**, invece, è meno sofisticata e sfrutta una vulnerabilità che era emersa su alcuni forum specializzati a fine gennaio. La tecnica consente, in pratica, di creare delle backdoor sui router DrayTek.

Entrambe le vulnerabilità sono state corrette nello scorso febbraio, quando DrayTek ha rilasciato la nuova versione del

firmware per i suoi dispositivi.

La buona notizia è che il livello di aggiornamento a livello globale è piuttosto avanzato: solo 100.000 dei 978.000 dispositivi rilevati online attraverso **Shodan** utilizzano una versione del firmware vulnerabile agli attacchi.

Condividi l’articolo

---

Il malware arriva per posta… in una chiavetta USB!

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/03/30/gruppi-hacker-sconosciuti-allattacco-dei-dispositivi-draytek/?utm_source=rss&utm_medium=rss&utm_campaign=gruppi-hacker-sconosciuti-allattacco-dei-dispositivi-draytek

---

# Il malware arriva per posta… in una chiavetta USB!

Mar 27, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

***Il bizzarro attacco ha preso di mira una struttura***

***sanitaria negli Stati Uniti. La memoria USB era in realtà un dispositivo in grado di infettare il PC.***

L’uso di memorie USB contenenti malware come vettore d’attacco non è una novità assoluta. In passato la cronaca ha infatti registrato numerosi casi in cui i cyber-criminali hanno adottato questa tecnica, per esempio “seminando” chiavette infette all’interno di parcheggi o ingressi degli edifici.

Il caso riportato da **Trustwave**, però, si distingue nettamente sia per il livello di sofisticazione dell’attacco sotto il profilo tecnico, sia per lo stratagemma adottato per recapitare la chiavetta.

Come si legge nel report pubblicato sul blog ufficiale della società di sicurezza, l’attacco ha preso di mira una struttura sanitaria statunitense e ha utilizzato, come vettore, un pacchetto recapitato negli uffici dell’ospedale.

Il plico, confezionato con un credibilissimo involucro marchiato **Best Buy**, conteneva una lettera in cui si annunciava l’accredito di una gift card del valore di 50 dollari. La chiave USB inclusa nel pacchetto, spiegava la lettera, conteneva l’elenco degli articoli acquistabili con il buono regalo.

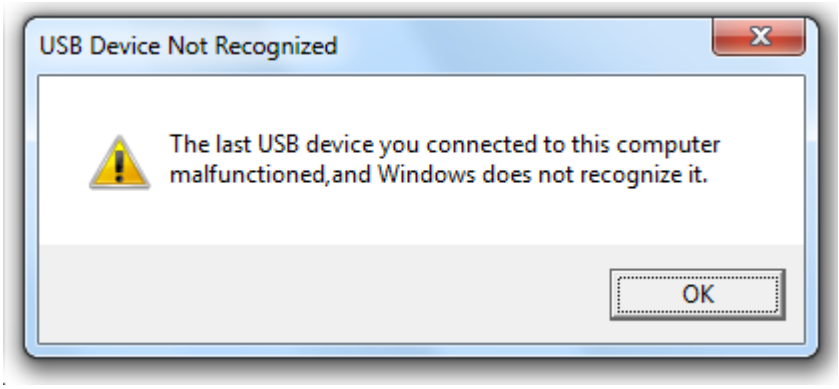



La chiavetta, però, non era una semplice memoria USB. Si trattava invece di un dispositivo chiamato **BadUSB Leonardo USB ATMEGA32U4**, in vendita per pochi dollari sul Web.

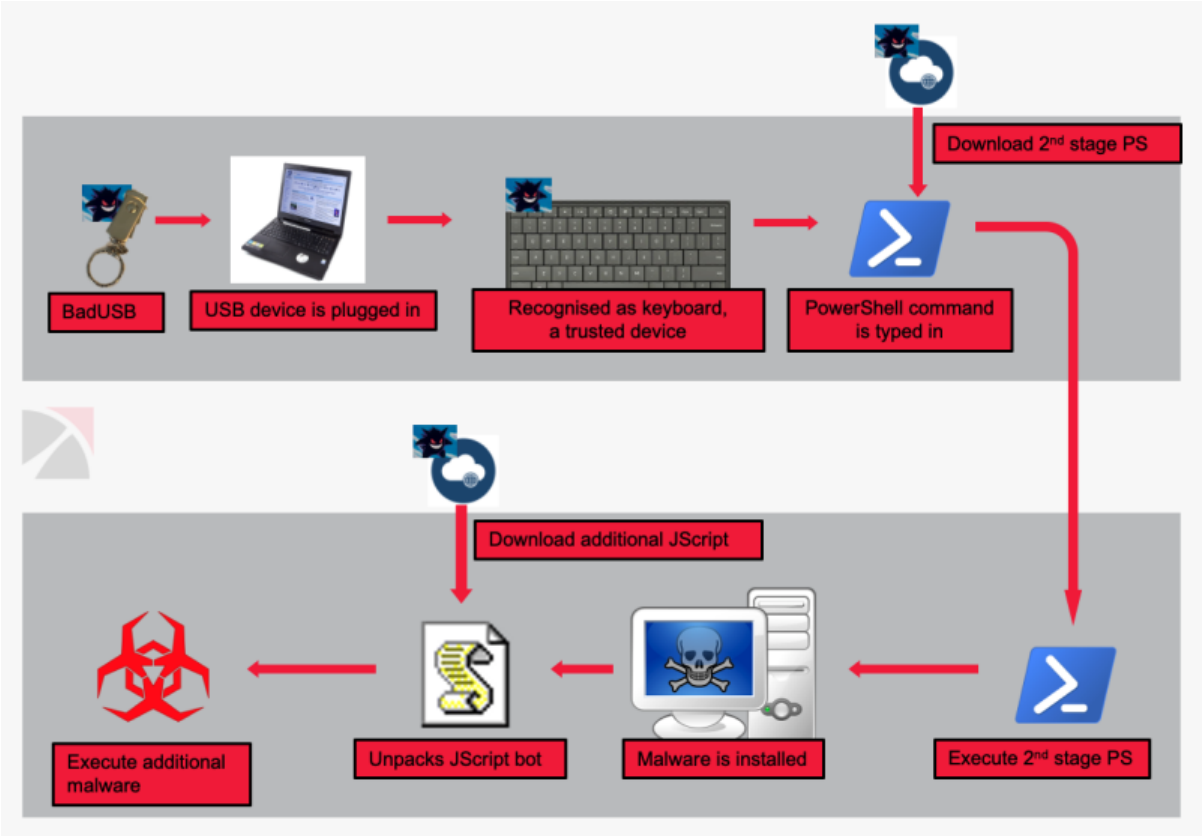
**Si tratta di un dispositivo del tutto simile a una memoria rimuovibile, che contiene in realtà un microcontroller Arduino programmato per simulare una tastiera USB**.

La chiavetta, in pratica, era programmata per iniettare un comando PowerShell che avvia il download di un payload che viene installato sul computer a cui è collegata la chiavetta.

Per allontanare qualsiasi sospetto, lo script visualizza un messaggio di errore relativo a un presunto malfunzionamento della memoria USB. Insomma: l'obiettivo è quello di far credere alla vittima che la chiavetta sia semplicemente difettosa.




La realtà, però, è molto diversa. IL malware, infatti, agisce dietro le quinte per scaricare il terzo stadio del payload, attraverso una procedura che usa sistemi di crittografia per oscurare le comunicazioni con il server Command and Control.




Una volta operativo, il torjan invia una serie di informazioni al server C&C, tra cui le informazioni sull'utente, il livello di privilegi di cui gode, la versione del sistema operativo e delle eventuali installazioni di **Microsoft Office** e di prodotti **Adobe**. Da questo momento in poi, i pirati informatici hanno assoluta libertà d'azione e possono inviare qualsiasi tipo di comando tramite la backdoor installata.

Per la cronaca, almeno in questo caso, il destinatario del pacchetto si è insospettito di fronte a questo bizzarro stratagemma e non ha collegato la chiave USB al suo computer, avvisando i responsabili cyber security dell'azienda.

Condividi l'articolo

---

Cyber-spionaggio: attacco in grande stile del gruppo cinese APT41

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/03/27/il-malware-arriva-per-posta-in-una-chiavetta-usb/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-arriva-per-posta-in-una-chiavetta-usb

---

# Cyber-spionaggio: attacco in grande stile del gruppo cinese APT41

Mar 26, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

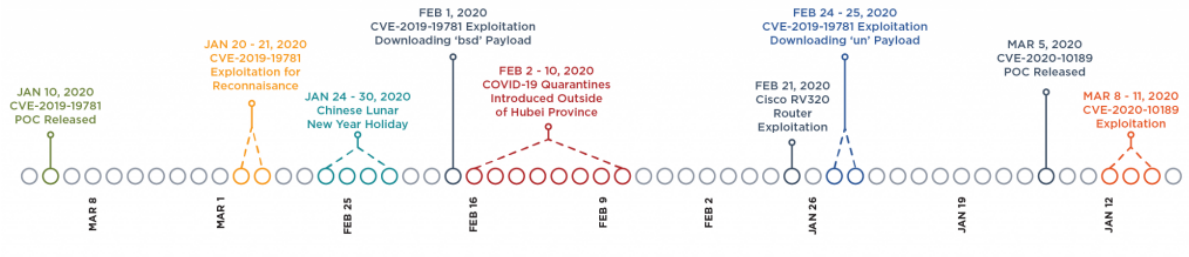
---

***I pirati hanno sfruttato vulnerabilità nei sistemi Cisco, Citrix e Zoho. Nel mirino aziende che operano in un gran numero di settori diversi.***

Quando si parla di gruppi **APT (Advanced Persistent Threat)** di solito è in relazione ad attacchi mirati piuttosto limitati. Questa volta, però, ci troviamo di fronte a un'eccezione.

Secondo quanto riporta **FireEye**, infatti, uno dei più noti gruppi di hacker legati al governo di Pechino avrebbe condotto una campagna di attacchi che avrebbe preso di mira decine di imprese attive nel settore energetico, finanziario, manifatturiero, dell'informazione, dei trasporti e dei servizi.

Come si legge nel report pubblicato dai ricercatori, protagonista di questo cambio di strategia è **APT41**, un gruppo ben conosciuto dagli esperti di sicurezza. Secondo gli autori del rapporto, tra il 20 gennaio e l'11 marzo di quest'anno (in concomitanza con la diffusione dell'epidemia **Covid-19**) i pirati avrebbero attaccato bersagli in Australia, Canada, Danimarca, Finlandia, Francia, India, **Italia**, Giappone, Malesia, Messico, Filippine, Polonia, Qatar, Arabia Saudita, Singapore, Svezia, Svizzera, Emirati Arabi Uniti, Regno Unito e USA.




Gli attacchi hanno sfruttato una serie di vulnerabilità conosciute in diversi sistemi molto diffusi. La prima (CVE-2019-19781) interessa i sistemi **Citrix** e, secondo i ricercatori, sarebbe stata sfruttata per cercare di installare una backdoor all'interno dei sistemi che i pirati informatici avrebbero accuratamente selezionato.

Più nebulosi, invece, i contorni di un attacco che avrebbe preso di mira un router RV320 di **Cisco**. Gli analisti in questo caso si muovono nel campo delle ipotesi, la più accreditata delle quali tira in ballo l'uso di un modulo **Metasploit** che sfrutta due falle di sicurezza (CVE-2019-1653 e CVE-2019-1652) emerse l'anno scorso.

Lo strumento più pericoloso, però, è stato adottato dai pirati nel corso di questo mese, quando APT41 ha cominciato a sfruttare un exploit comparso per una vulnerabilità **zero-day** (CVE-2020-10189) che affligge **Zoho ManageEngine Desktop Central**.

Insomma: sembra proprio che i pirati al soldo del governo di Pechino abbiano avviato un’offensiva senza precedenti, che sta approfittando anche di una situazione particolare legata alla pandemia coronavirus. Il suggerimento, ovvio, è di non abbassare la guardia.

Condividi l’articolo

---

Il malware arriva per posta… in una chiavetta USB! TrickMo aggira l’autenticazione a due fattori con un’app Android

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/03/26/cyber-spionaggio-attacco-in-grande-stile-del-gruppo-cinese-apt41/?utm_source=rss&utm_medium=rss&utm_campaign=cyber-spionaggio-attacco-in-grande-stile-del-gruppo-cinese-apt41

---

# TrickMo aggira l’autenticazione a due fattori con un’app Android

Mar 25, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

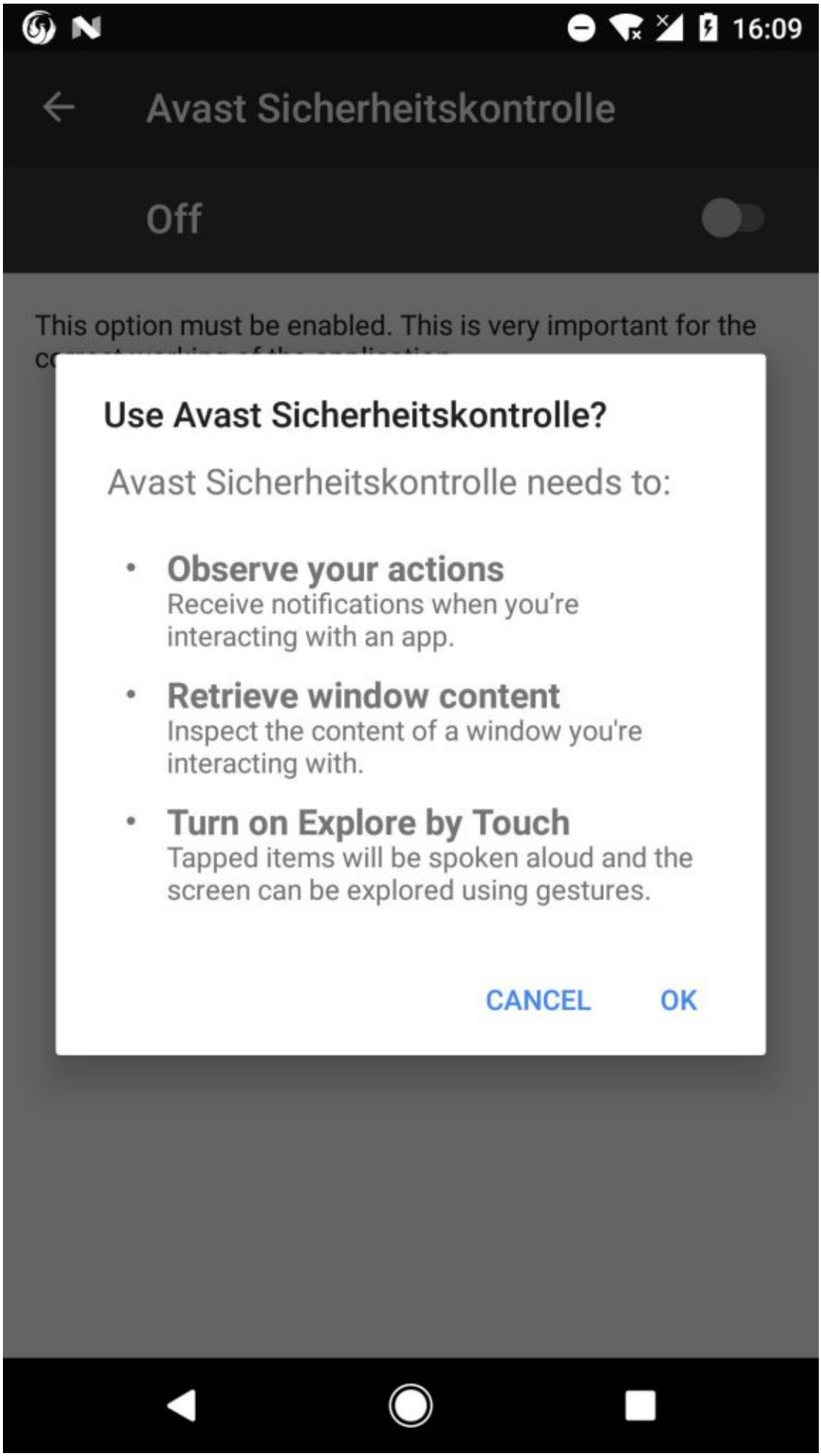
***Gli autori di TrickBot hanno diffuso un malware per smartphone che inoltra loro i codici di autenticazione. Sotto attacco la Germania.***

Per il momento si stanno concentrando sugli utenti tedeschi, ma la nuova campagna di attacchi degli autori di **TrickBot** potrebbe espandersi presto ad altre nazioni. I pirati informatici, specializzati nel furto di credenziali bancarie, stanno infatti sperimentando un metodo per **violare gli account che utilizzano sistemi di autenticazione a due fattori**.

Lo strumento che hanno scelto è un malware per Android, che i ricercatori di IBM hanno battezzato con il nome di **TrickMo**. Nel loro report, gli analisti del team **X-Force** spiegano che gli esemplari individuati fino a questo momento sarebbero delle versioni in via di sviluppo.

L'app verrebbe distribuita alle vittime del loro trojan TrickBot e avrebbe l'obiettivo di "collaborare" con il malware per consentire ai cyber-criminali di aggirare i sistemi di autenticazione che sfruttano, per esempio, l'invio di codici tramite SMS.

TrickMo, che viene proposto come uno strumento di sicurezza apparentemente offerto dall'istituto di credito di cui è cliente la vittima (ma ne esiste anche una versione che finge di essere un prodotto di **Avast**) si installa sullo smartphone e adotta una serie di accorgimenti che gli permettono di impedire la sua rimozione.


16:09
Avast Sicherheitskontrolle
Off
This option must be enabled. This is very important for the
Use Avast Sicherheitskontrolle?
Avast Sicherheitskontrolle needs to:
Observe your actions
Receive notifications when you're interacting with an app.
Retrieve window content
Inspect the content of a window you're interacting with.
Turn on Explore by Touch
Tapped items will be spoken aloud and the screen can be explored using gestures.
CANCEL
OK

Il malware, inoltre, integra funzionalità che gli consentono di catturare schermate, rubare informazioni personali e avviare una procedura di auto-distruzione.

Il pezzo forte, però, è rappresentato dalla sua capacità di intercettare gli SMS (TrickMo si registra come applicazione predefinita per l'invio e la ricezione dei messaggi) e **sottrarre i codici dalle applicazioni per la generazione delle password monouso utilizzate come secondo fattore di autenticazione**.

La tecnica utilizzata è quella di sfruttare i servizi di accessibilità di Android, che rappresentano ormai lo strumento prediletto dai pirati informatici per garantire agibilità ai loro malware.

Come spiegano i ricercatori IBM, il trojan comunica con i server Command and Control attraverso due canali diversi: una connessione tramite protocollo http e un sistema che utilizza **SMS crittografati**. Questo secondo vettore viene utilizzato, in particolare, per dirottare i codici ricevuti via SMS.

Condividi l'articolo

---

Cyber-spionaggio: attacco in grande stile del gruppo cinese APT41 Crescono gli strumenti di hacking per colpire il settore ICS

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/03/25/trickmo-aggira-lautenticazione-a-due-fattori-con-unapp-android/?utm_source=rss&utm_medium=rss&utm_campaign=trickmo-

aggira-lautenticazione-a-due-fattori-con-unapp-android

---

# Falla in Citrix interessa 80.000 aziende. E per ora niente patch…

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

---

***La vulnerabilità consente di avviare l'esecuzione di codice in remoto, non ha ancora una soluzione ed è arrivata a ridosso delle vacanze natalizie.***

Non sarà la proverbiale "tempesta perfetta", ma ci somiglia parecchio. L'annuncio di **Citrix**, affidato a un security advisor pubblicato lo scorso 17 dicembre, ha probabilmente rovinato le vacanze di Natale a parecchi amministratori IT.

La vulnerabilità (CVE-2019-19781) individuata da **Mikhail Klyuchnikov** di **Positive Technologies** interessa **Citrix Application Delivery Controller (ADC)** e, stando a quanto si legge nel report, permetterebbe di avviare l'esecuzione di codice in remoto sui sistemi gestiti con la piattaforma di virtualizzazione.

L'attacco portato attraverso un eventuale exploit richiederebbe un solo minuto e avrebbe possibili conseguenze tali da aver meritato una valutazione di rischio massima (10/10).

Nel dettaglio, la vulnerabilità consentirebbe a un pirata

informatico di ottenere l'accesso diretto alla rete, senza che sia necessaria alcuna procedura di autenticazione. Secondo la stima di Klyuchnikov, i sistemi vulnerabili sarebbero più di 80.000, distribuiti in 158 paesi diversi. **Solo in Italia ci sarebbero più di 1.300 installazioni a rischio**.




**Una bella rogna, a cui si aggiunge il fatto che la società non ha ancora sviluppato un aggiornamento del firmware che consenta di correggere la falla di sicurezza**.

Dalle parti di Citrix hanno però indicato una serie di operazioni che permettono di mitigare il rischio di attacchi (le istruzioni sono disponibili in questa pagina Web) in attesa che sia disponibile l'aggiornamento.

Nella scheda riassuntiva pubblicata sul blog di Positive Technologies, il ricercatore precisa che la vulnerabilità sarebbe presente da 5 anni e mezzo e che sono quindi coinvolte anche le versioni precedenti di ADC, conosciute come **NetScaler ADC**, **Citrix Gateway** o **NetScaler Gateway**.

Condividi l'articolo

---

Falla zero-day in Dropbox. Per ora c'è solo una patch provvisoria

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2019/12/27/falla-in-citrix-interessa-80-000-aziende-e-per-ora-niente-patch/

# Falla zero-day in Dropbox. Per ora c’è solo una patch provvisoria



Dic 23, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

***La vulnerabilità consente di elevare i privilegi a livello di sistema. In attesa di una soluzione definitiva, è disponibile una micro-patch.***

Una nuova vulnerabilità in **Dropbox** sta creando qualche grattacapo ai responsabili della sicurezza. Al contrario di quanto si potrebbe pensare, però, la falla non riguarda la

condivisione dei file o la protezione dei dati degli utenti, ma mette a rischio l'integrità di **Windows**.

Come spiega **Decoder** sul suo blog, il problema si annida nel sistema di aggiornamento di Dropbox, che nella versione Windows del client viene installato come servizio con privilegi di sistema, cioè quelli più elevati possibili.

Ciò che hanno scoperto i ricercatori, è che il componente memorizza i file di log in una cartella nella quale può mettere mano qualsiasi utente. Sfruttando questa possibilità e le operazioni pianificate per l'avvio di *dropboxupdate*, i ricercatori sono riusciti a mettere a punto un exploit che consente di **avviare un eseguibile con privilegi di sistema**.

[embedded content]

Una vera manna per i pirati informatici, che potrebbero sfruttare la tecnica per eseguire qualsiasi cosa su un computer che ha un'installazione standard di Dropbox.

**A peggiorare la situazione c'è il fatto che dalle parti di Dropbox non hanno ancora rilasciato un aggiornamento per risolvere il problema, nonostante la segnalazione da parte di Decoder si stata inviata lo scorso 18 settembre**.

Scaduto il termine di 90 giorni indicato dalla società di sicurezza, i ricercatori hanno pubblicato i dettagli della vulnerabilità e, come risultato, tutti i PC su cui "gira" Dropbox potrebbero finire nel mirino di attacchi basati sulla tecnica esposta.

L'unico argine, per il momento, è rappresentato da **una micro-patch** messa a punto dalla piattaforma 0Patch. Si tratta comunque di una soluzione provvisoria, utile per mitigare il rischio in attesa di una soluzione definitiva da parte di Dropbox.

Condividi l'articolo

Emotet fa strage in Germania. Francoforte bloccata per 24 ore

## Articoli correlati

## Altro in questa categoria

https://www.securityinfo.it/2019/12/23/falla-zero-day-in-dropbox-per-ora-ce-solo-una-patch-provvisoria/