Pochi aggiornano e i pirati continuano a sfruttare la falla in Windows

Giu 11, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I cyber-criminali stanno sfruttando attivamente una vulnerabilità che in teoria è stata corretta a fine 2017. Ma i PC a rischio sono ancora tanti.

Difficile capire esattamente che cosa sia andato storto, ma a quanto dicono dalle parti di **Sophos** i pirati informatici stanno sfruttando per i loro attacchi un exploit che, almeno teoricamente, non dovrebbe più rappresentare un problema.

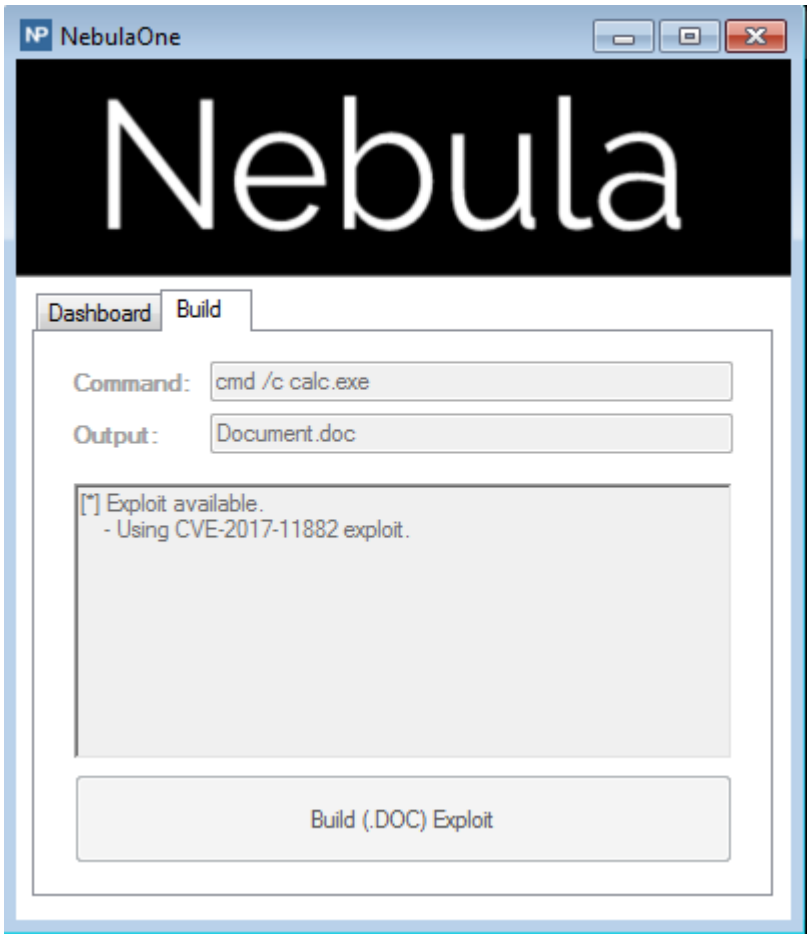
L'attacco, che sfrutta come vettore documenti allegati a messaggi di posta elettronica, fa leva su una vulnerabilità individuata tempo fa (CVE-2017-11882) e corretta con un aggiornamento di Windows nel novembre 2017.

Il bug, che interessa un componente di **Office** chiamato **Equation Editor**, aveva provocato un certo clamore. Il componente in quesitone, infatti, era stato "dimenticato" in tutti gli aggiornamenti precedenti e la versione integrata nel pacchetto software di Microsoft risaliva addirittura al 2000.

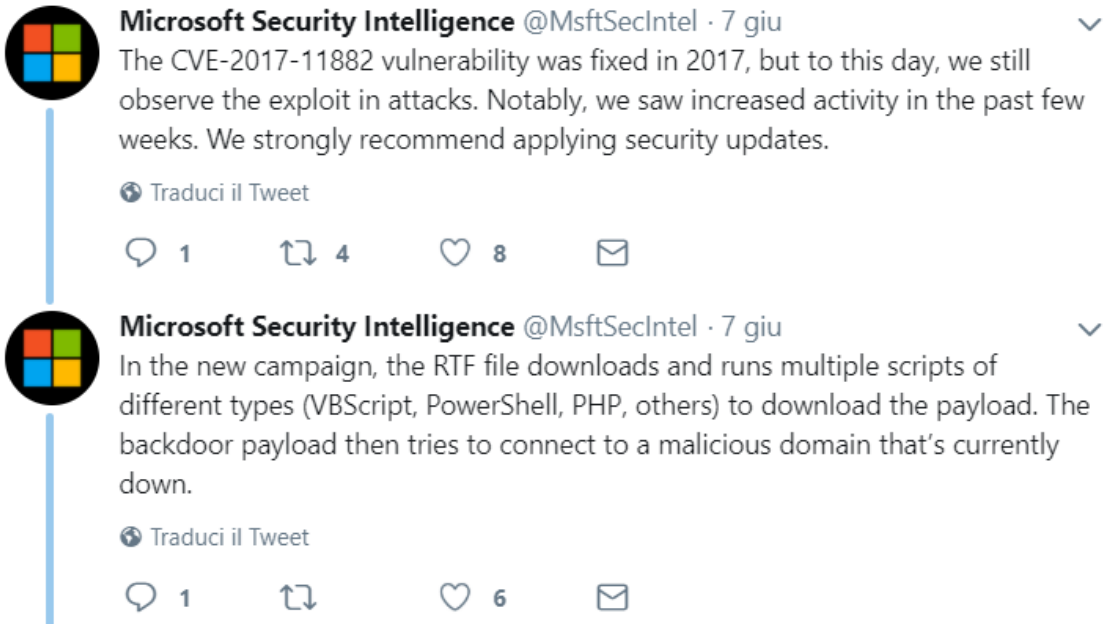
Come abbiamo raccontato in questo articolo, i pirati informatici hanno cominciato a sfruttarlo immediatamente dopo la notizia della sua esistenza, ma a quanto pare il suo utilizzo continua anche a più di 18 mesi di distanza.

Secondo i ricercatori Sophos, infatti, la vulnerabilità è la più utilizzata nei kit per la creazione di malware come

NebulaOne.



Non solo: a segnalare una crescita di questi attacchi è la stessa Microsoft, che in un tweet ha messo in guardia gli utenti riguardo la possibilità di ricevere messaggi che contengono documenti di Office modificati per sfruttare la vulnerabilità.



La falla in Equation Editor è particolarmente pericolosa. L'exploit che la sfrutta consente infatti di avviare l'esecuzione di codice sul sistema senza che sia necessaria alcuna interazione da parte dell'utente. **Insomma: basta aprire il documento per ritrovarsi il computer infetto**.

L'elemento curioso riguarda il fatto che molti computer, evidentemente, non abbiano installato correttamente l'aggiornamento che correggeva il bug.

Un problema che alcuni ricercatori hanno già segnalato in passato e che ha una causa molto semplice: sono poche le persone che controllano periodicamente lo stato degli aggiornamenti per verificare che non ne sia stato lasciato indietro qualcuno a causa di errori di varia natura.

Il suggerimento, piuttosto scontato, è quello di verificare che la cronologia degli aggiornamenti sia in ordine e che sia impostata per **scaricare gli aggiornamenti anche per gli altri prodotti Microsoft oltre al semplice sistema operativo**.

Condividi l'articolo

Traffico Internet europeo dirottato verso la Cina per due ore

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/06/11/pochi-aggiornano-e-i-pirati-continuano-a-sfruttare-la-falla-in-windows/

Traffico Internet europeo dirottato verso la Cina per due ore

Giu 10, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Scenario 0

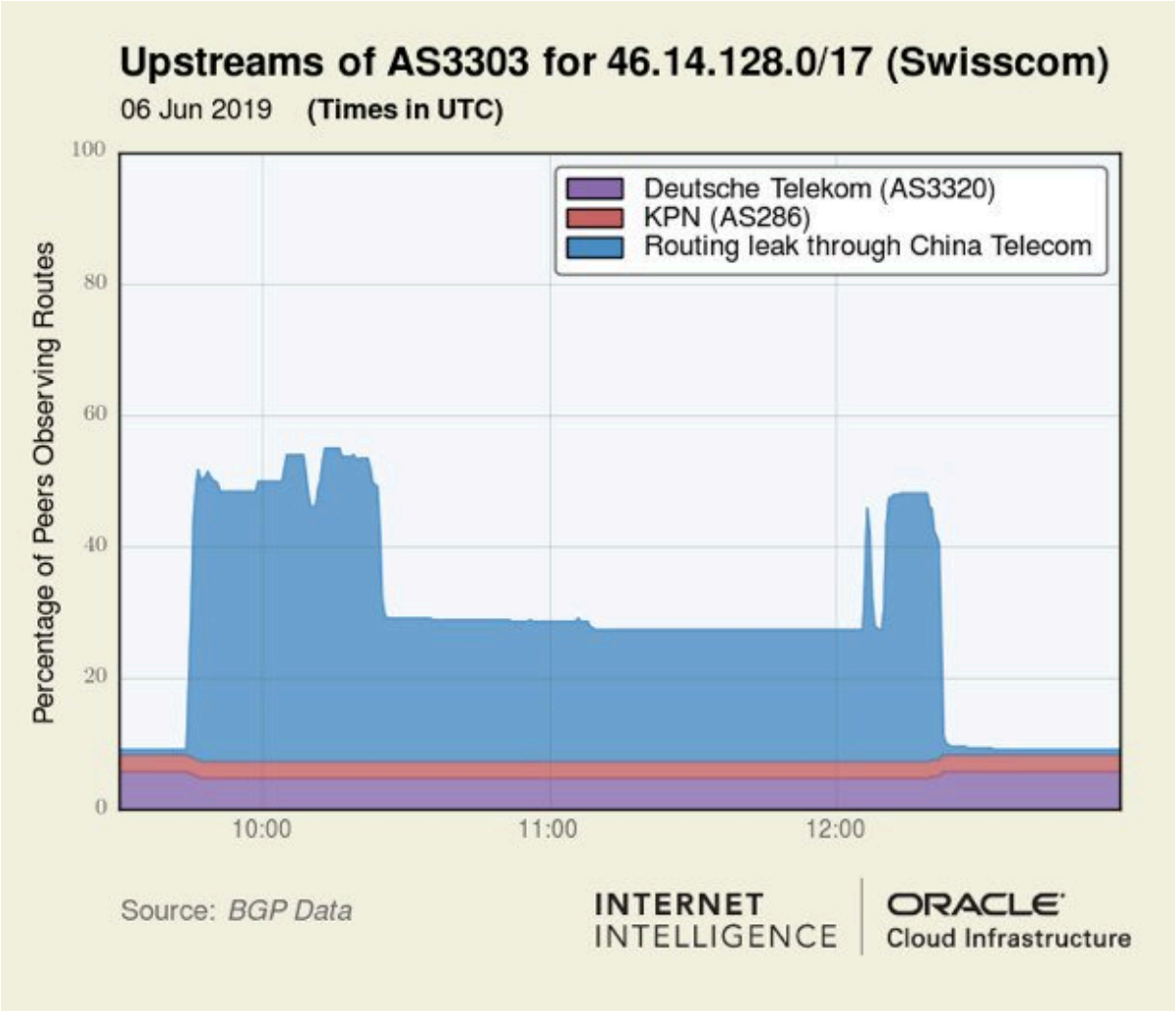
L'errore è stato generato da un centro svizzero, che ha inviato a China Telecom circa 70.000 route di provider europei provocando malfunzionamenti e disagi.

L'ennesimo cortocircuito nel sistema **Border Gateway Protocol (BGP)** ha provocato un "dirottamento" dei dati gestiti da alcuni provider europei verso la rete di **China Telecom**. Tutto è avvenuto nella mattinata del 6 giugno scorso.

Per due ore, spiegano dalle parti di **Oracle** in un report, migliaia di collegamenti sono stati gestiti dalla compagnia di telecomunicazioni cinese, che si è in pratica interposta anche in collegamenti tra macchine molto vicine tra loro. A essere

maggiormente coinvolti sono stati **Swisscom**, l'olandese **KPN**, e le francesi **Bouygues Telecom** e **Numericable-SFR**.

Difficile capire cosa sia successo esattamente. Il protocollo BGP, utilizzato per gestire l'instradamento dei dati sulle varie reti a livello mondiale, è infatti un sistema piuttosto delicato e tutt'altro che perfetto.



In passato si sono verificati casi simili, sui quali grava tuttora l'ombra del dubbio che non si sia trattato di semplici "incidenti", ma episodi di BGP hijacking, cioè un dirottamento deliberato delle connessioni.

Il caso più eclatante si è verificato nell'aprile del 2017 (ne abbiamo parlato in questo articolo) quando le transazioni di **Visa** e **Mastercard** hanno cominciato a transitare sui router di Rostelecom, una società di telecomunicazioni russa.

In quel caso, però, l’anomalia si era presentata per soli sette minuti. L’episodio del 6 giugno, invece, ha avuto una durata record: ben 2 ore nel corso delle quali i soggetti coinvolti hanno subito rallentamenti nelle connessioni ed errori a raffica che hanno impedito di raggiungere i server. Non solo: il dirottamento delle comunicazioni apre la strada, ovviamente, al sospetto di possibili intercettazioni dei dati trasmessi.

A quanto pare, il tutto sarebbe pertito da **Safe Host**, un data center svizzero che ha inviato le comunicazioni verso la Cina. Tutti i provider, spiegano gli esperti, utilizzano normalmente dei sistemi automatizzati per contenere situazioni del genere e fare in modo che il dirottamento venga bloccato in tempi rapidi. **Dalle parti di China Telecom, però, qualcosa non ha funzionato e tutte le connessioni sono state gestite dal provider cinese per la bellezza di 120 minuti**.

Condividi l’articolo

Germania: backdoor in 4 modelli di smartphone Android

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/10/traffico-internet-europeo-dirottato-verso-la-cina-per-due-ore/

Germania: backdoor in 4 modelli di smartphone Android

Giu 07, 2019 Marco Schiaffino In evidenza, Malware, News, RSS 1

Si tratta di telefoni di "fascia bassa" in vendita nel paese. Lo spyware è stato installato direttamente nel firmware dei dispositivi.

Prendere un malware a causa di qualche astuta tecnica cdi attacco può succedere. Ritrovarsi con una backdoor pre-installata su uno smartphone appena comprato, però, è qualcosa di decisamente più raro.

Secondo quanto riporta il **Bundesamt für Sicherheit in der Informationstechnik**, cioè l'ufficio federale per la sicurezza informatica tedesco, è quello che hanno sperimentato almeno 20.000 cittadini che hanno acquistato alcuni modelli di smartphone Android "low cost" nelle ultime settimane.

Non è la prima volta che succede una cosa del genere e, di solito, la causa è da ricercare in un attacco di tipo supply chain, che prende di mira gli sviluppatori di componenti utilizzati per la creazione dle firmware dei dispositivi.

Nel dettaglio, i telefoni infetti sono **Doogee BL7000**, **M-Horse Pure 1**, **Keecoo P11** e **VKworld Mix Plus**. Nel loro firmware è stato infatti rilevato **Andr/Xgen2-CY**, un trojan programmato per attivarsi all'accensione dello smartphone. Nel caso del VKworld Mix Plus, però, il malware sembra essere inattivo.



Il malware, spiegano in un report dalle parti di **Sophos**, è in grado di rubare numerose informazioni dal dispositivo.

Nel dettaglio, Andr/Xgen2-CY si preoccupa di registrare il numero di telefono, la posizione (sia l'indirizzo che le coordinate GPS), l'ID IMEI, la risoluzione dello schermo, il modello, produttore e versione del sistema operativo, le informazioni sul processore, il MAC adress, le dimensioni di RAM e ROM, della scheda SD, la nazione e la lingua usata dal proprietario del dispositivo e, infine, la società di telecomunicazioni che fornisce il servizio.

Ma queste, spiegano i ricercatori, sarebbero solo le operazioni preliminari che il trojan esegue prima di contattare il server Command and Control.

Una volta operativo, il malware consente ai pirati informatici di scaricare e installare applicazioni a loro piacimento, disinstallarle, eseguire comandi tramite shell e aprire qualsiasi indirizzo nel browser del telefono.

Il vero problema, però, è che secondo gli esperti non c'è modo di rimuovere il malware se non attraverso un aggiornamento del

firmware. **Peccato che una versione "pulita del firmware sia disponibile solo per il Keecoo P11**. I proprietari degli altri smartphone interessati hanno una sola possibilità: resettare tutto, spegnere lo smartphone e tenerlo in un cassetto fino a quando non arriverà un update anche per questi ultimi.

Condividi l'articolo

La sicurezza? Prima di tutto è una questione di cultura

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/07/germania-backdoor-in-4-modelli-di-smartphone-android/

Ti presento BlackSquid, il malware più aggressivo del momento

Giu 05, 2019 Marco Schiaffino In evidenza, Malware, Minacce, News, RSS 0

Per diffonderlo gli autori stanno utilizzando tutti gli

exploit più "feroci" comparsi negli ultimi mesi. Obiettivo: installare un miner per generare Monero.

Un motto latino recita "melius abundare quam deficere". Non sappiamo se i pirati informatici che hanno creato **BlackSquid** lo conoscano, ma il loro malware sembra decisamente ispirato a questa filosofia.

Per diffondere BlackSquid, infatti, i cyber-criminali hanno deciso di utilizzare la bellezza di otto diversi exploit, scegliendoli tra quelli più efficaci in circolazione.

Come spiegano i ricercatori di Trend Micro in questo report, la collezione comprende **EternalBlue** (lo stesso usato da **WannaCry** – ndr); **DoublePulsar**; gli exploit per tre vulnerabilità note (CVE-2014-6287, CVE-2017-12615 e CVE-2017-8464) oltre a tre exploit per **ThinkPHP**.

I vettori di attacco sono tre: siti Internet infetti, tecniche di attacco dirette ai server Web e unità rimuovibili come dischi esterni e chiavette USB. Grazie a EternalBlue e DoublePulsare, però, è in grado di propagarsi all'interno delle reti locali.

```
v5 = GetTickCount();
IP1 = v5 * (sub_3F5165() + 3) % 0xDF;
switch ( IP1 )
{
  case 0u:
    IP1 = 180;
    break;
  case 0xAu:
    IP1 = 11;
    break;
  case 0x7Fu:
    IP1 = 60;
    break;
  case 0xACu:
    IP1 = 173;
    break;
  case 0xA9u:
    IP1 = 170;
    break;
  default:
    break;
}
allocate_mem(&RANDOM_IPADDR, 0, 50);
v6 = GetTickCount();
IP4 = v6 * (sub_3F5165() + 3) % 255;
v8 = GetTickCount();
IP3 = v8 * (sub_3F5165() + 3) % 255;
v10 = GetTickCount();
v11 = sub_3F5165();
wsprintfA(&RANDOM_IPADDR, "%d.%d.%d.%d", IP1, v10 * (v11 + 3) % 0xFF, IP3, IP4);// Random IP Address
WSAStartup(0x202u, &WSAData);
name.sa_family = 2;
*&name.sa_data[2] = inet_addr(&RANDOM_IPADDR);
```

La versione individuata dagli analisti contiene un payload che installa **XMRig**, un miner piuttosto conosciuto che consente di sfruttare la potenza di calcolo del computer compromesso per generare **Monero**, la cripto-valuta preferita dai cyber-criminali.

Secondo i ricercatori, però, l'impianto generale del malware consentirebbe di modificare il payload piuttosto facilmente, modificandone quindi le funzionalità.

A preoccupare è anche il fatto che BlackSquid utilizza una serie di tecniche di evasione che gli consentono di "accorgersi" della eventuale presenza di una sandbox del tipo di quelle utilizzate dai ricercatori di sicurezza per analizzare i malware.

Tra le curiosità segnalate dagli esperti di Trend Micro c'è anche il fatto che uno degli exploit contiene un errore. **I pirati hanno infatti inserito nel codice la lettera "I" al posto di "1"**. L'errore, però, non compromette l'efficacia degli altri 7 exploit.

Condividi l'articolo

Il threat hunting è la risposta alle minacce alle grandi aziende

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/05/ti-presento-blacksquid-il-malware-piu-aggressivo-del-momento/

Il threat hunting è la risposta alle minacce alle grandi aziende

Giu 05, 2019 Giancarlo Calzetta Approfondimenti, In evidenza, Mercato, Prodotto, RSS 2

Panda Security è un'azienda che negli ultimi anni si è trasformata profondamente, passando dalla soluzione di sicurezza endpoint per la quale era famosa anche nel segmento consumer molto tempo fa, fino a uno stravolgimento totale del proprio modello di business che l'ha portata a offrire **sicurezza in cloud e una soluzione di threat hunting** "puro".

"Rincorrere le minacce note" – dice Juan Santamaría, Ceo di Panda Security – "è una perdita di tempo perché le soluzioni endpoint sono ormai in grado di rintracciarle senza problemi. I casi di infezione da malware 'tradizionale' scalati al nostro servizio clienti sono nell'ordine della singola infezione ogni due settimane. La vera sfida è quella di riconoscere e fermare le minacce sconosciute, quelle che superano i primi strati di difesa e agiscono sulla rete interna."



La piattaforma delegata a svolgere questo complicato compito si chiama Orion ed è **indirizzata principalmente alle grandi aziende,** settore al quale Panda guarda con molto interesse per la propria crescita.
“Al momento” – afferma Santamaria – “il nostro fatturato arriva solo per il 15% dalle aziende di grandi dimensioni, ma contiamo di portarlo al 40 nei prossimi tre anni”.

Per integrarsi con i sistemi informatici tipici delle enterprise, Orion **può interfacciarsi con sistemi di servizi gestiti e SOC**. “È già disponibile” – conferma il CEO – “un set di API che andremo a espandere nei prossimi mesi, rendendolo più ampio già da giugno per poi andare a svilupparne di ‘specifici’ per piattaforme di analisi e automazione come ServiceNow e simili.”

La filosofia alla base della piattaforma di sicurezza è quella, sempre più diffusa ormai, della zero trust: **non viene eseguito nulla che non abbia una reputazione nota**. Su questo, agisce comunque un motore di controllo che blocca tutti quei processi, anche autorizzati, che inanellano una serie di

azioni sospette. Una analisi comportamentale che ancora risulta essere lo strumento più efficace contro gli attacchi fileless.

In Italia, Panda Security sta crescendo molto bene, tanto da convincere il management spagnolo a mandare l'ex country manager italiano a "colonizzare" il mercato americano.

"Negli USA" – ci dice Gianluca Busco Arrè, Vice President of Sales and Operations North America – "c'è un'ampia fetta di mercato attualmente scoperta, rappresentata da quelle aziende di medie dimensioni che non possono permettersi le soluzioni 'top di gamma' di threat hunting, ma hanno comunque un budget per la sicurezza informatica molto interessante. Noi andremo ad aggredire quel segmento con un prodotto, Orion, dalle grandi prestazioni a un prezzo abbordabile".

Condividi l'articolo

Ti presento BlackSquid, il malware più aggressivo del momento
Da Sophos un controllo centralizzato che dialoga con tutti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/05/il-threat-hunting-e-la-risposta-alle-minacce-alle-grandi-aziende/

Gli USA e i sospetti sulle VPN: “c’è pericolo di spionaggio”

Giu 03, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

La Homeland Security ritiene che i servizi VPN proposti da soggetti esteri possano sorvegliare o spiare gli impiegati federali, ma non c’è nessuna policy per impedirlo.

La paranoia per la possibilità che paesi stranieri possano spiare i cittadini statunitensi non è un’esclusiva di **Donald Trump**. Anche alcuni membri del senato degli Stati Uniti sembrano terribilmente preoccupati dal rischio legato al cyber-spionaggio da parte di potenze straniere.

Nel mirino dei politici, questa volta, sono finiti i servizi **VPN** proposti sui vari market per dispositivi mobili. A interessarsene, nel dettaglio, sono **Ron Wyden** e **Marco Rubio**, che con una lettera inviata lo scorso 7 febbraio hanno chiesto maggiori informazioni sul tema al direttore del CISA (Cybersecurity and Infrastructure Security Agency) **Chris Krebs**.

Il direttore dell’agenzia, che fa parte del Dipartimento della Homeland Security, ha risposto ai senatori lo scorso 22 maggio, tratteggiando uno scenario in cui esprime tutta la “preoccupazione” degli esperti governativi in merito.

A quanto si legge nella lettera, l’allerta rossa nei confronti dei servizi VPN (ma anche dei semplici proxy) dipenderebbe dal rischio legato alla possibilità che vengano sfruttati dai

servizi di spionaggio stranieri per controllare la navigazione e le comunicazioni degli utenti.



Nella missiva (che si può leggere su questa pagina Web) il direttore del CISA sottolinea la funzione “strategica” delle VPN, citando per esempio la recente legge promulgata dal governo russo che sottoporrebbe i gestori di VPN allo stesso regime degli Internet Provider, in particolare per quanto riguarda l’applicazione della censura sul Web in territorio russo.

Quello che si scopre, però, è che il governo degli Stati Uniti, al momento, non ha una policy chiara in merito. **Krebs, infatti, spiega che “non ci sono policy complessive o whitelist che impediscano agli impiegati governativi di installare applicazioni VPN sui dispositivi”**.

Insomma: qualsiasi impiegato o contractor del governo USA; al momento, può installare una VPN di terze parti sul suo dispositivo, facendo transitare tutti i dati su server controllati da chissà chi.

E considerato che i servizi VPN in circolazione, come abbiamo raccontato in questo articolo, sono per la maggior parte gestiti da operatori cinesi, si comincia a capire da dove derivino le preoccupazioni dei senatori che hanno contattato il direttore del CISA.

Se a tutto questo si aggiunge il fatto che buona parte dei servizi (soprattutto per Android) sono tutt'altro che sicuri, il quadro è completo.

Ora resta da capire quali possano essere le conseguenze di questo carteggio. **In un paese che ormai ha la piena consapevolezza del fatto che tutte le comunicazioni sono controllate, spiate e sorvegliate dal suo stesso governo, pensare di mettere un freno per legge all'uso di VPN potrebbe scatenare una protesta diffusa da parte di tutti i difensori dei diritti civili**. In tempi come questi, però, non è detto che lo spauracchio degli hacker cinesi possa consentire anche questo.

Condividi l'articolo

Attacco massiccio a Docker. I pirati usano Shodan per colpire gli host

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/03/gli-usa-e-i-sospetti-sulle-vpn-ce-pericolo-di-spionaggio/

Attacco massiccio a Docker. I pirati usano Shodan per colpire gli host

Mag 31, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

La campagna punta a distribuire container al cui interno è nascosto un miner per generare cripto-valuta. Colpiti almeno 10.000 server.

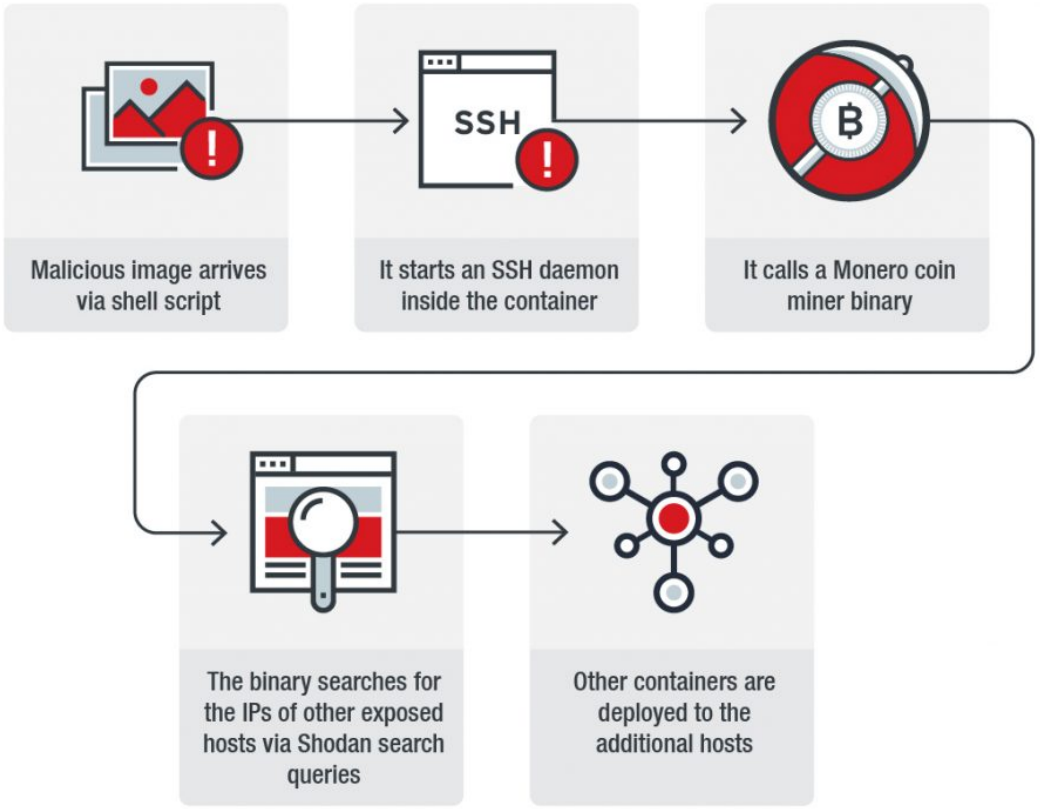
Una vera emergenza che avrebbe coinvolto migliaia di host **Docker** e che gli esperti di sicurezza stentano a contenere. L'attacco individuato da **Trend Micro**, che ne ha pubblicato i dettagli in questo report, ha caratteristiche che lo collocano a metà tra una botnet e un worm.

Docker è una piattaforma che permette di creare dei "pacchetti" (container) che contengono applicazioni in grado di girare su cloud come se fossero su una macchina virtuale, ma senza che sia necessaria la presenza di un intero sistema operativo per supportarle. La piattaforma è popolarissima e sfrutta una rete di Hub da cui è possibile scaricare e installare i container.

Nel dettaglio, i cyber-criminali individuati da Trend Micro prendono di mira gli host Docker che hanno API esposte su Internet attraverso la porta 2375 per violarne i sistemi di sicurezza tramite una tecnica di **brute forcing**.

Una volta ottenuto l'accesso, utilizzano uno script (ubu.sh) per caricare l'immagine infetta del container. Al suo interno sono presenti alcuni script aggiuntivi utilizzati dai pirati per installare il payload e diffondere ulteriormente i

container infetti.



Per quanto riguarda il payload, si tratta di un classico miner in grado di sfruttare la potenza di calcolo del server per generare cripto-valuta (il solito **Monero**) che viene depositata sui conti dei pirati informatici. La scelta di Monero non è casuale.

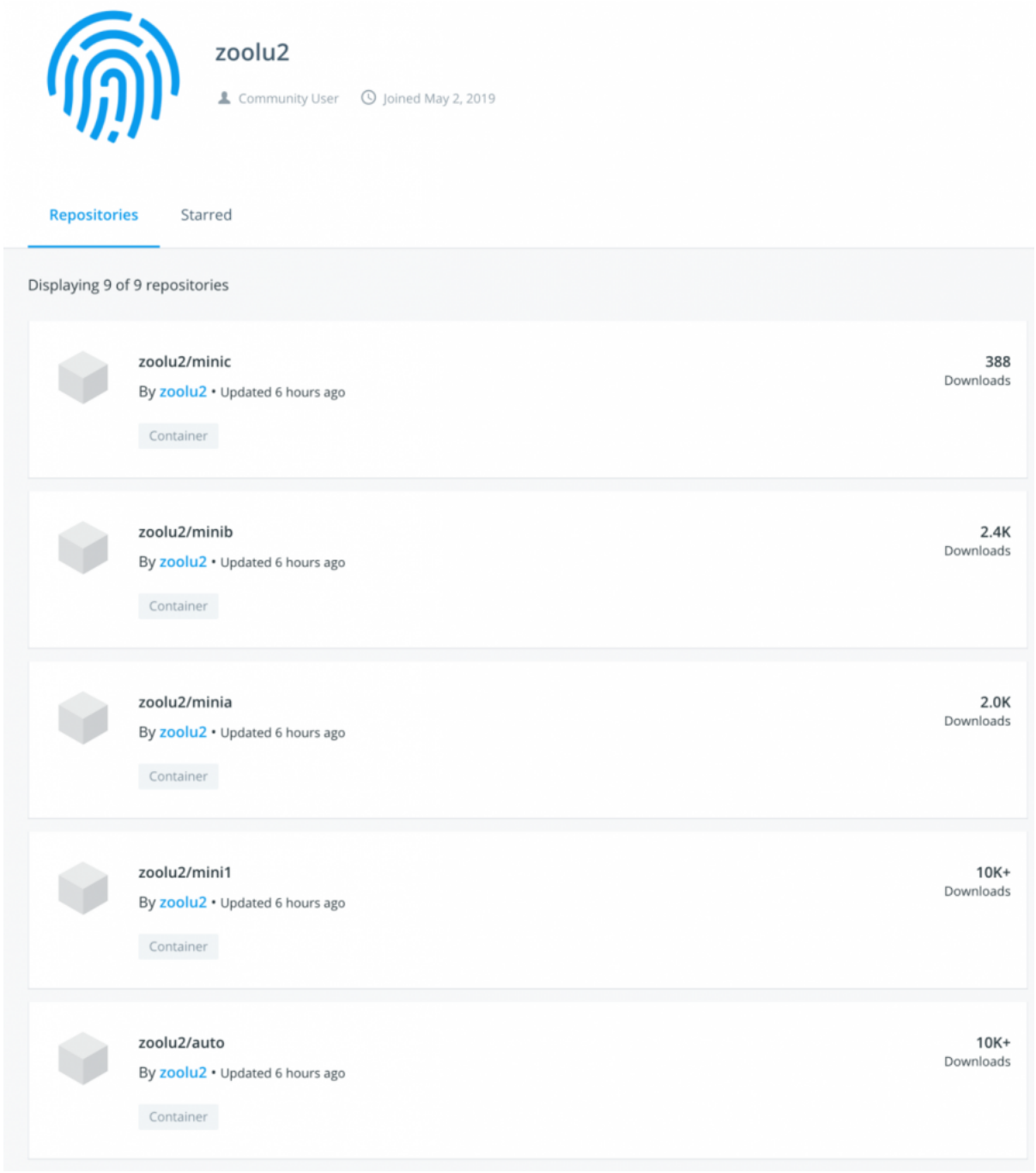
Oltre a garantire un livello di anonimato superiore a quello di altre monete virtuali, Monero ha un'altra caratteristica utile ai cyber-criminali: mentre i miner di altre cripto-valute (per esempio Bitcoin) sono ottimizzati per l'uso con i processori grafici che eseguono calcolo parallelo, quelli di Monero offrono le migliori prestazioni con le normali CPU.

La vera "chicca" in questo attacco però riguarda il sistema di diffusione scelto dagli hacker. Il modulo a cui è affidato questo compito utilizza infatti **Shodan** (un motore di ricerca

in grado di individuare i dispositivi collegati a Internet – ndr) per localizzare nuove potenziali vittime e avviare l'attacco.

Gli indirizzi IP degli host vulnerabili vengono inseriti in un file di testo (**iplist.txt**) e poi verificati uno per uno. Se al loro interno viene rilevato un miner già attivo, gli indirizzi vengono cancellati. In caso contrario parte l'attacco. **Insomma: in questo modo i container infetti si diffondono autonomamente**.

I ricercatori di Trend Micro hanno individuato l'attacco quando hanno analizzato un container "comparso" su un loro honeypot (i server usati dalle società di sicurezza come "falsi bersagli" per i malware) che proveniva da un Docker Hub chiamato **zoolu2**.



Sarebbe proprio questo, secondo i ricercatori, il repository all'origine dell'attacco. Ma da quanto va avanti? Dalle loro analisi risulta che le immagini sono state caricate nel mese di maggio, ma nel report sottolineano come i container siano stati più volte aggiornati ed è probabile, di conseguenza, che l'attacco sia iniziato prima.

Ora l'account di zoolu2 è stato disattivato, così come gli account Shodan usati per le ricerche e un altro account Docker (**Pavlov32**) che aveva le stesse caratteristiche di zoolu2. A quanto pare, però, una delle immagini container infette

sarebbe stata già scaricata più di 10.000 volte.

Il suggerimento degli esperti di sicurezza per gli utenti è quello di controllare le impostazioni per verificare che container e API non siano raggiungibili dall'esterno, implementando sistemi di autenticazione per impedire intrusioni come queste.

Condividi l'articolo

Rivoluzione GitHub: ecco gli aggiornamenti automatici per i pacchetti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/31/attacco-massiccio-a-docker-i-pirati-usano-shodan-per-colpire-gli-host/

Rivoluzione GitHub: ecco gli aggiornamenti automatici per i pacchetti

Mag 30, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia, Vulnerabilità 0

Il nuovo Dependabot permette agli sviluppatori di ricevere un avviso quando è disponibile un update per le "dipendenze" utilizzate nel progetto.

È la classica rivoluzione "nascosta", di cui buona parte dell'opinione pubblica non verrà mai a conoscenza. La nuova funzione proposta da **GitHub**, però, potrebbe avere un impatto davvero significativo in termini di sicurezza su tutto il mondo dell'informatica.

Il sistema automatizzato per gli aggiornamenti di sicurezza **Dependabot** introdotto dal servizio di hosting per i progetti software rappresenta infatti un enorme passo avanti che potrebbe ridurre in maniera decisiva la superficie di attacco a disposizione dei pirati informatici.

Per capirne il potenziale impatto, bisogna partire da una prima considerazione. Nello scenario attuale, qualsiasi sviluppatore lavora, in buona parte, come un assemblatore che utilizza singoli "pacchetti" sviluppati da altri programmatori.

Ogni software, quindi, contiene al suo interno decine di componenti (le cosiddette "dipendenze") a cui sono affidati compiti specifici, che vengono utilizzati anche da altri programmi.



La prima conseguenza di questo sistema è che ogni volta che compare una vulnerabilità in uno dei pacchetti, questa si ripercuote quasi invariabilmente su tutti i progetti che lo utilizzano come dipendenza. **In pratica, una falla di sicurezza in un singolo pacchetto può potenzialmente generare una vulnerabilità in decine di software**.

Il secondo problema, invece, riguarda la filiera di aggiornamento. In una situazione simile, infatti, la catena degli update diventa molto più complicata. Quello che succede, in molti casi, è che quando viene individuata una falla, l'autore realizzi tempestivamente l'aggiornamento che la corregge, ma tutti gli sviluppatori che usano il suo codice non implementino il suo update, o lo facciano con molto ritardo.

Un ritardo che, in molti casi, è anche dovuto a problemi molto pratici, come i dubbi sulla compatibilità della nuova versione nell'impianto generale dei loro software.

Con la nuova funzionalità di GitHub, tutti questi problemi potranno essere risolti. Il nuovo sistema prevede infatti una

procedura in modalità “pull”. Quando è disponibile un aggiornamento di sicurezza per un pacchetto, tutti gli sviluppatori che lo utilizzano nei loro progetti ricevono un alert che gli consente di scaricare l’update.

Non solo: ogni sviluppatore riceve anche tutta la documentazione, compresa una valutazione di compatibilità generata automaticamente grazie a Dependabot, uno strumento sviluppato da una società specializzata che GitHub (dal 2018 controllata da Microsoft) ha acquisito solo una settimana fa.

In definitiva, quello a cui siamo di fronte è una piccola grande rivoluzione che potrebbe avere conseguenze estremamente positive nel prossimo futuro. Incrociamo le dita.

Condividi l’articolo

Attacco massiccio a Docker. I pirati usano Shodan per colpire gli host L’esercito cinese punta ad abbandonare Windows

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/30/rivoluzione-github-ecco-gli-aggiornamenti-automatici-per-i-pacchetti/

L’esercito cinese punta ad

abbandonare Windows

Mag 29, 2019 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario, Tecnologia 0

Troppo alto il rischio di attacchi da parte dei servizi segreti USA. In preparazione un sistema operativo completamente "Made in China".

Dopo Huawei, che ha lasciato intendere di avere in cantiere un sistema operativo per smartphone in grado di rimpiazzare Android, è il turno dell'Esercito Popolare di Liberazione, che sembra voler abbandonare Windows per sviluppare un proprio sistema "sganciato" dalle aziende statunitensi.

La guerra commerciale tra Washington e Pechino, questa volta, c'entra fino a un certo punto. Certo, il fatto che le tensioni tra i due paesi siano aumentate ha certamente il suo peso, ma a determinare i vertici militari a seguire questa strada sarebbero ragionamenti molto più pratici.

Nel dettaglio, dalle parti di Pechino sono perfettamente consapevoli del fatto che i servizi segreti USA hanno a disposizione un formidabile arsenale per lo spionaggio informatico.

Le rivelazioni di **Edward Snowden**, così come la vicenda legata ai tool pubblicati dagli **Shadow Brokers**, hanno chiarito al mondo che NSA e CIA hanno la possibilità di violare qualsiasi dispositivo. **Che si tratti di Windows, Linux, sistemi mobile o smart TV, gli 007 statunitensi hanno sempre lo strumento giusto per portare attacchi devastanti**.

Di qui la nuova strategia, che prevederebbe una migrazione verso un sistema operativo "fatto in casa" che sarebbe inattaccabile anche dagli esperti hacker al servizio di

Washington.



Secondo quanto riporta in un articolo **Epoch Times**, l'operazione sarebbe stata affidata a un **Internet Security Information Leadership Group**, che avrebbe il compito di guidare la transizione.

Il nuovo soggetto risponderebbe direttamente al **Comitato Centrale del Partito Comunista Cinese** e non è escluso, si legge nell'articolo, che il progetto non vada a coprire anche altri ambiti, come i sistemi di controllo a livello industriale che oggi sono affidati a **SCADA**.

Tornando al sistema operativo "militare", secondo quanto è trapelato non sarebbe nemmeno basato su Unix, che i militari cinesi considerano vulnerabile quanto Windows. **L'ipotesi, quindi, è quella di qualche cosa di completamente nuovo e diverso, che metterebbe i rivali statunitensi nella situazione di dover affrontare un sistema ignoto**.

Insomma, sembra proprio che la geopolitica e le tensioni internazionali stiano portando a una frammentazione a livello

tecnologico, come già segnalato quando è emersa la notizia che la **Russia** di **Vladimir Putin** starebbe lavorando a una "Internet locale" in grado di funzionare anche in caso di isolamento dalle infrastrutture internazionali.

Per il momento tutto questo sembra interessare livelli militari e governativi. Se la tendenza dovesse contagiare anche il settore consumer, però, potremmo trovarci di fronte a una situazione inedita. Con quali ripercussioni, lo capiremo col tempo.

Condividi l'articolo

Kaspersky punta sulle startup. Una gara per selezionare i migliori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/29/lesercito-cinese-punta-ad-abbandonare-windows/

Protezione cloud: l'obiettivo è controllare i container

Mag 23, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

Dopo gli attacchi che colpiscono la filiera DevOps gli esperti prendono le contromisure. Trend Micro: "Ecco come proteggiamo le applicazioni cloud".

Tecnicamente si chiamano attacchi **supply chain**, cioè attacchi che prendono di mira gli sviluppatori per andare a colpire la vittima designata (o più vittime) che utilizza i componenti software infetti.

Con l'esplosione del cloud, questa tecnica di attacco è diventata non solo più popolare tra i pirati informatici, ma anche più insidiosa. Il sistema che utilizza i container per implementare funzionalità attraverso "pacchetti" già pronti offre infatti un formidabile vettore di attacco per i cyber-criminali.

La cronaca recente conferma la tendenza: gli ultimi attacchi a **Docker** (ne abbiamo parlato in questo articolo) e le vulnerabilità scoperte in **Kubernetes** (in questo articolo) ne sono la conferma più evidente.

Non stupisce, quindi, che le società di sicurezza abbiano puntato i riflettori su questo aspetto della sicurezza su cloud, attivando procedure di controllo per garantire l'integrità dei container ed evitare che possano trasformarsi in un fattore di rischio.



Ora sembra che questo aspetto stia vivendo una fase di ulteriore evoluzione. A proporla è **Trend Micro**, che ha annunciato una serie di nuove funzionalità che puntano a trasformare il controllo dei container, fino a oggi eseguito a livello runtime, in un sistema di monitoraggio che copre tutto il ciclo di vita **DevOps**.

Nel dettaglio, spiegano dalle parti di Trend Micro, i nuovi strumenti comprendono un controllo dell'immagine dei container nella pipeline di creazione software, attraverso una scansione pre-registro che permette di individuare in anticipo le vulnerabilità e i malware, consentendo di individuare eventuali minacce future.

Non solo: il sistema **Deep Security** a cui è affidata l'analisi controlla anche password e chiavi private per verificarne la conformità e analizza tutti i movimenti di traffico laterali e orizzontali tra i container e i livelli della piattaforma.

Tutto questo, ci tengono a specificare gli esperti della società di sicurezza con sede a Tokyo, attraverso **un sistema completamente automatizzato**, sfruttando un ambiente che consente di utilizzare qualsiasi command shell per eseguire API.

Insomma, la strada per espandere alla cloud il concetto di “sicurezza come processo” è aperta. Ora aspettiamo di vederne l’impatto in un settore che negli ultimi tempi ha dimostrato di soffrire più degli altri le indesiderate “attenzioni” dei cyber-criminali.

Please follow and like us:



SandboxEscaper colpisce ancora: altro zero-day per Windows

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/23/protezione-cloud-lobiettivo-e-controllare-i-container/