Varenyky: è arrivato il “trojan a luci rosse”

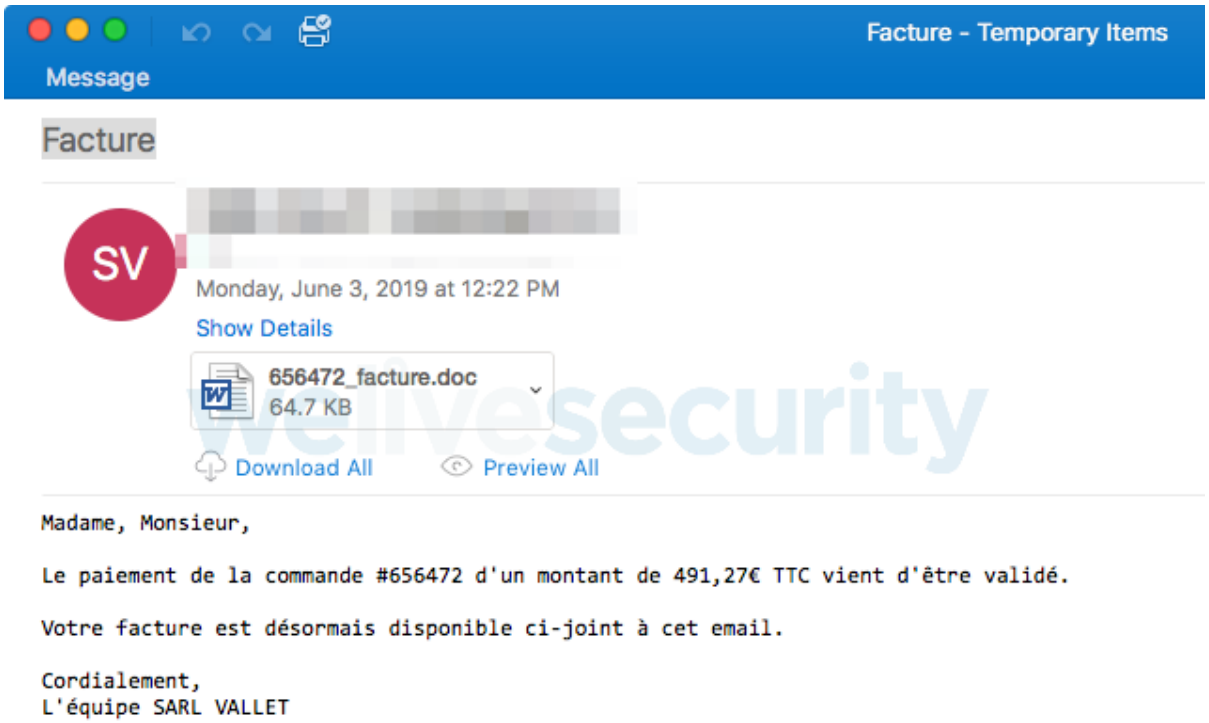
Ago 09, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS 0

Individuato in Francia, il malware controlla la navigazione della vittima e registra un video dallo schermo se visita un sito pornografico. Obiettivo estorsione?

L’inventiva dei cyber-criminali, in alcuni casi, è davvero ammirevole. Pur di spremere qualche euro alle loro vittime sono infatti capaci di inventarsi qualsiasi tipo di truffa e attacco, modificando le loro strategie in base alle esigenze del momento.

Il caso del trojan **Varenyky**, individuato dai ricercatori di **ESET**, è la dimostrazione di questa straordinaria capacità di fiutare un nuovo “affare”, puntando a estorcere denaro agli sventurati che ne finiscono vittima.

Come spiegano i ricercatori in un report pubblicato sul blog della società di sicurezza, Varenyky è comparso in Francia e viene distribuito attraverso una campagna di spam via email che cerca di attirare le potenziali vittime con classiche tecniche di phishing.

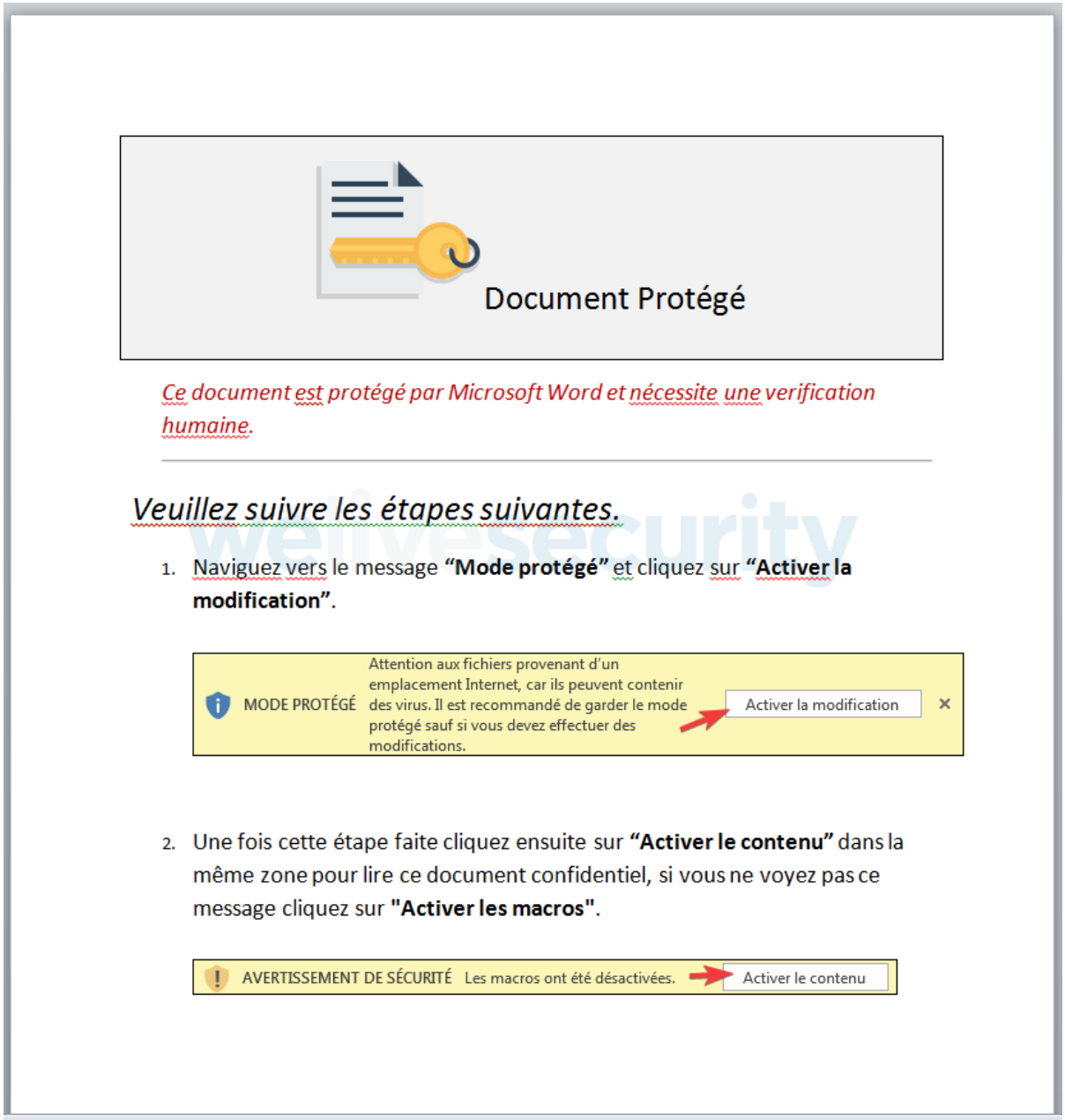


Nel dettaglio, il messaggio in francese fa riferimento a una presunta fattura da 491,27 euro ed è scritto con una certa cura.

Il trojan viene installato quando la vittima apre il documento **Word** allegato, che richiede la solita attivazione delle macro mascherata, in questo caso, come un sistema di verifica per superare la protezione del documento e consentirne l'apertura.

Gli autori del malware, inoltre, hanno introdotto un piccolo accorgimento per renderne più difficile l'individuazione da parte dei sistemi di scansione automatica. **Prima di avviare l'installazione, infatti, i comandi macro verificano le impostazioni di Word per controllare che sia impostato per la lingua francese**.

Nel caso in cui la lingua sia un'altra, o sia impostata sulle versioni pensate per altri paesi francofoni come Belgio o Canada, l'esecuzione del codice si blocca.



Un ulteriore controllo, questa volta relativo al layout di tastiera, viene effettuato all'inizio dell'esecuzione del codice del trojan.

La logica è semplice: quando il file finisce su un computer impostato con un'altra lingua (per esempio quelli usati dalle società di sicurezza per analizzare i file intercettati su Internet) il documento appare innocuo.

Le funzionalità di Varenyky comprendono moduli classici, come il furto delle credenziali di accesso ai servizi Internet, ma anche uno strumento piuttosto originale. Il trojan, infatti, esegue un monitoraggio della navigazione su Internet.

Obiettivo: individuare il momento in cui il proprietario del computer si collega a un sito con materiale pornografico.

Quando questo avviene (il malware verifica una serie di parole chiave) Varenyky attiva un sistema di registrazione dello schermo attraverso **FFmpeg**, che lo stesso trojan scarica e avvia. **Il video viene poi inviato al server Command and Control gestito dai pirati informatici**.

L'obiettivo, anche se i ricercatori di ESET usano il condizionale, è probabilmente quello di utilizzare il video per ricattare la vittima, minacciando di rendere pubblico il video nel caso in cui non paghi un riscatto.

Insomma: si tratterebbe di una nuova versione della **truffa a luci rosse**, di cui abbiamo parlato ampiamente in passato e che sembra aver fruttato centinaia di migliaia di dollari ai suoi autori.

Nel caso della truffa a luci rosse, però, il ricatto si basava su un bluff. Con Varenyky le cose vanno decisamente peggio, visto che in questo caso gli estortori avrebbero veramente tra le mani un video compromettente.

Condividi l'articolo

Il 5G è agli esordi ma ci sono già problemi di sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/09/varenyky-e-arrivato-il-trojan-a-luci-rosse/

Il 5G è agli esordi ma ci sono già problemi di sicurezza

Ago 08, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Il nuovo standard si trascina alcuni problemi ereditati dai suoi predecessori. Possibile mappare tutti i dispositivi e "sabotare" l'autonomia dei device IoT.

Mentre buona parte dell'opinione pubblica aspetta la nuova tecnologia 5G come la rivoluzione che trasformerà il nostro mondo in maniera radicale, dalle parti di Las Vegas emerge qualche dato preoccupante riguardo il livello di sicurezza garantito dalla nuova rete.

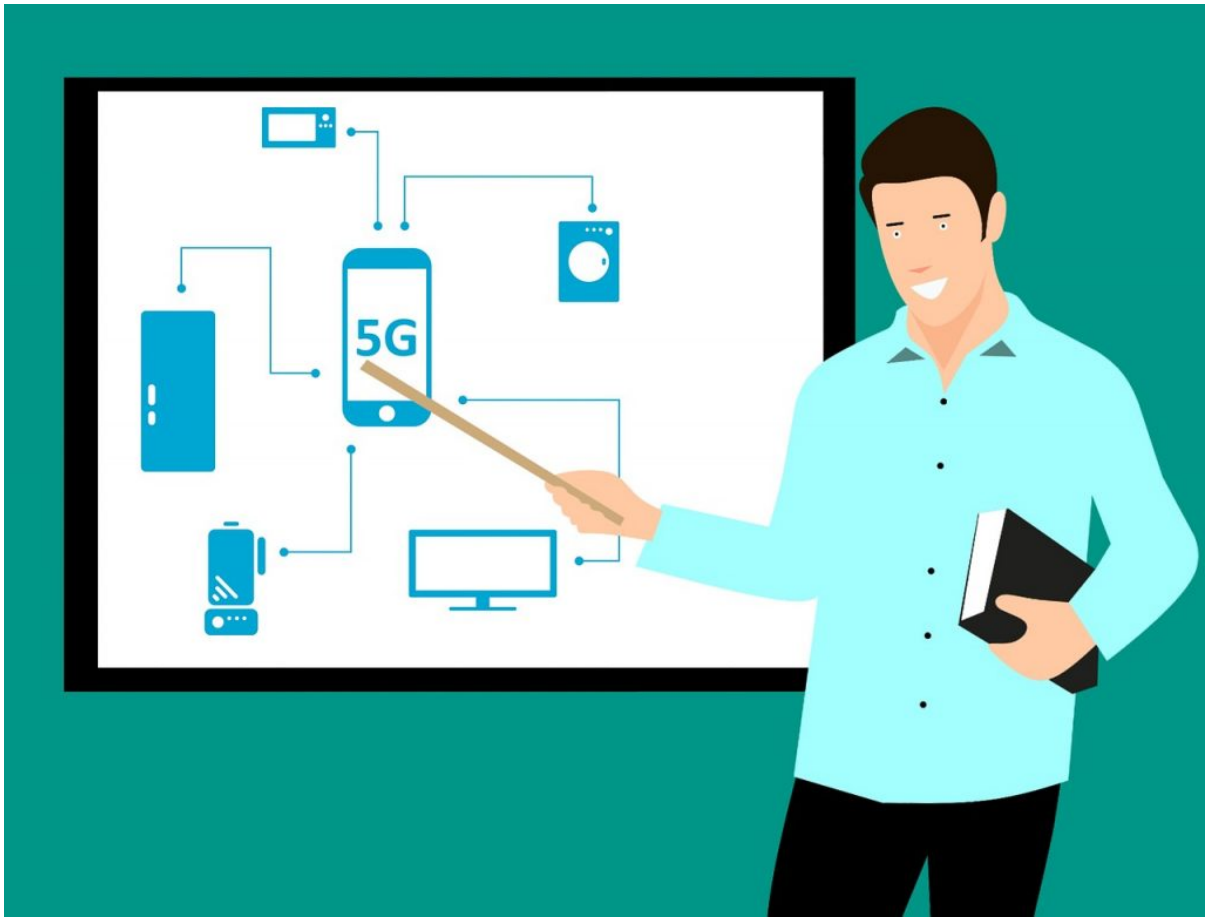
Nel corso del **Black Hat USA 2019**, infatti, i ricercatori di **Kaitiaki Labs** hanno esposto qualche "problemino" che il 5G si trascina come eredità dagli standard precedenti. A riportarlo è **Kaspersky**, in un articolo su uno dei suoi blog.

Il problema di fondo è che il protocollo prevede, come accadeva con 3G e 4G, che le trasmissioni vengono crittografate solo in una fase successiva al primo collegamento tra i dispositivi e la rete. Le prime informazioni trasmesse, quindi, sono in chiaro.

Solo che, con il protocollo 5G, questa debolezza diventa più rilevante. **Il nuovo protocollo, infatti, fonda la sua efficacia sulla capacità di offrire connessioni con**

caratteristiche diverse a seconda della tipologia di dispositivo o sulla specifica funzionalità a cui fa riferimento il traffico.

Detto in parole povere: al momento della connessione i dispositivi forniscono molte più informazioni rispetto a quanto facessero prima con i vecchi protocolli.



Risultato: pirati informatici e cyber-spioni possono sapere se il device è in grado di effettuare chiamate, inviare SMS, se gestisce comunicazioni tra veicoli (nel caso di automobili a guida autonoma), conoscere le frequenze che utilizza e i protocolli.

La tecnica, battezzata **MNmap** (Mobile Network mapping) permette in pratica di rilevare quale tipo di dispositivo si collega.

Non solo: analizzando i vari tipi di servizi attivi i ricercatori spiegano di essere in grado di ottenere molte altre informazioni dalle quali è possibile capire, per

esempio, se si ha a che fare con un iPhone o un Android, un modem o un dispositivo IoT.

Il tutto parte dal fatto che ci sono 5 produttori di hardware: **Intel**, **Huawei**, **Mediatek**, **Samsung** e **Qualcomm**. Ognuno di loro, per impostazione predefinita, utilizza alcune specifiche funzionalità. Mappandole è possibile capire quale modem viene usato e, di conseguenza, si riduce il campo a una lista di dispositivi. Incrociando questa informazione con i dati di cui sopra, individuare il dispositivo specifico diventa piuttosto facile.

Al di là di MNmap, i ricercatori sono riusciti anche a testare un attacco **Man in The Middle** (MiTM) che permetterebbe, in questo caso, di prendere di mira i dispositivi che utilizzano il 5G. Uno dei possibili obiettivi di un attacco del genere può essere quello di ridurre la banda disponibile inviando false informazioni alla rete, per esempio "strozzando" la connessione di un iPhone (normalmente 1Gbps) a soli 2Mbps.

Ma è possibile anche degradare l'autonomia dei dispositivi IoT. Uno degli sbandierati vantaggi del 5G, infatti, è la possibilità di gestire il funzionamento dei dispositivi in maniera "intelligente", facendo in modo che si attivino solo quando è necessario, arrivando a ottenere un'autonomia straordinaria, addirittura di 10 anni.

Un intervento attraverso un attacco MiTM potrebbe modificare i parametri per fare in modo che il device rimanga attivo e in costante ricerca di una connessione, riducendo l'autonomia a un quinto.

Tutti questi problemi sarebbero stati risolti con la release 14 dello standard 5G, che per il momento, però, non è stata implementata da nessun operatore sul mercato. Secondo i ricercatori potremo vedere le prime reti "sicure" solo dal prossimo anno e, per allora, chissà cos'altro sarà saltato fuori.

Condividi l’articolo

Double Dragon: il gruppo APT41 ha colpito anche l’Italia

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/08/il-5g-e-agli-esordi-ma-ci-sono-gia-problemi-di-sicurezza/

Double Dragon: il gruppo APT41 ha colpito anche l’Italia

Ago 07, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, Minacce, News, RSS, Scenario 0

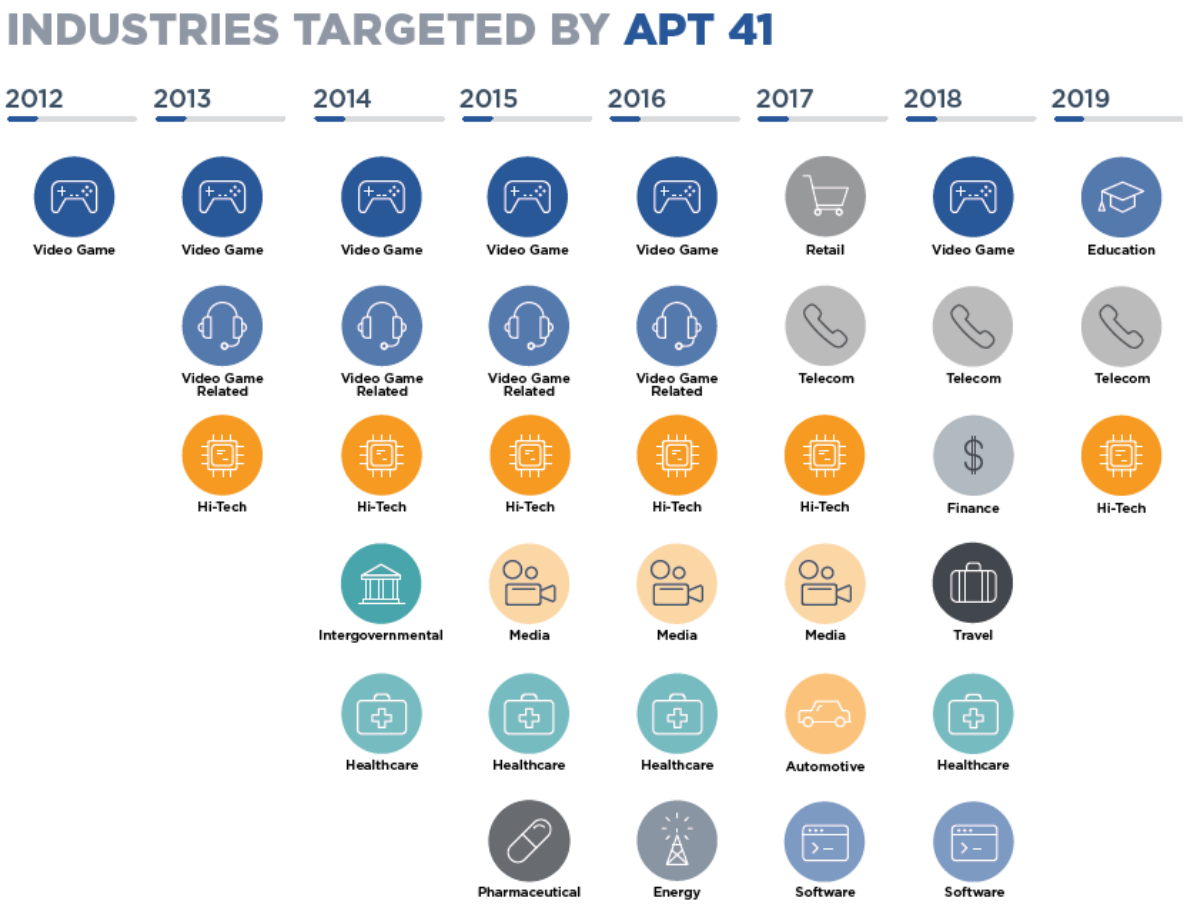
I pirati informatici cinesi usano strumenti sofisticati disponibili solo per gli “hacker di stato”, ma non disdegnano operazioni autonome per guadagnare denaro.

I ricercatori di **FireEye** lo hanno battezzato con il nome di **Double Dragon** o **APT41** ed è un gruppo che, secondo gli analisti, rappresenterebbe uno dei tanti soggetti che agiscono per conto del governo cinese nel settore del cyber-spionaggio.

Come spiegano nel loro report i ricercatori, però, APT41 ha caratteristiche piuttosto particolari e rappresenta un'anomalia rispetto ai gruppi di questo genere individuati in passato.

I gruppi **APT (Advanced Persistent Threat)** collegati al governo di Pechino, infatti, agiscono di solito seguendo rigorosamente gli ordini dei governi per cui lavorano e puntano esclusivamente allo spionaggio industriale.

Nel caso di APT41, che secondo quanto si legge nel report di FireEye sarebbe attivo almeno dal 2012, alle "normali" attività di spionaggio si alternano operazioni che hanno come obiettivo semplicemente il furto di denaro. **Insomma: saremmo di fronte a un "contractor" che in alcuni casi agisce in piena autonomia per finanziarsi**.

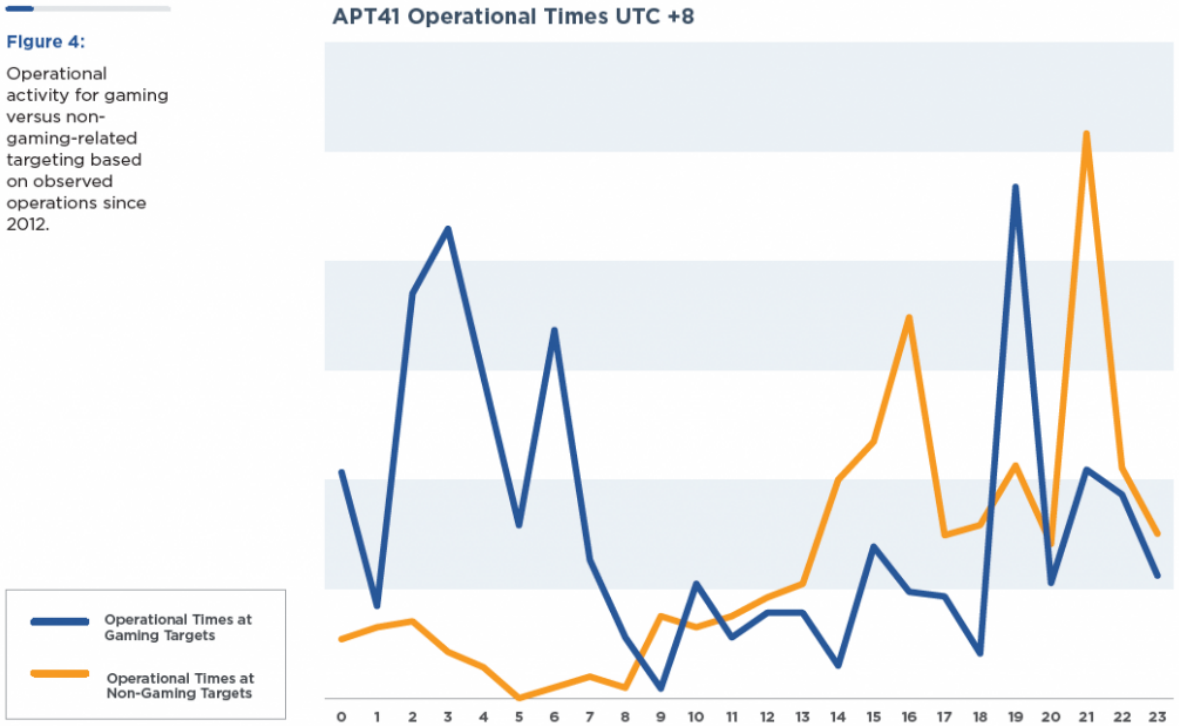


Tanto più che, guardando alle attività del gruppo, sembrerebbe che i pirati informatici che lo compongono si siano fatti le ossa attraverso azioni di comune cyber-crimine ai danni di

società nel settore dei videogiochi per passare solo in seguito alle operazioni di spionaggio.

Non solo: da quando lo spionaggio è diventata la loro attività principale, sembra che i pirati conducano le altre operazioni in quello che possiamo definire il loro "tempo libero".

L'analisi condotta dai ricercatori di FireEye, infatti, dimostra come le due tipologie di attacco vengano condotte in momenti diversi della giornata.



Se gli attacchi portati al settore dei videogiochi sembrano essere ispirati alla semplice logica dell'opportunismo (con l'utilizzo occasionale di **ransomware**) le azioni di spionaggio ricostruite dagli analisti corrispondono alla perfezione con le strategie seguite normalmente dai gruppi APT al soldo di Pechino.

Da quando la Cina ha avviato il suo programma economico **Made in China 2025**, che punta sulla crescita di settori come la farmaceutica e l'Hi-Tech, tutte le operazioni di spionaggio attribuite a gruppi cinesi hanno riguardato, in maniera diretta o indiretta, questi ambiti produttivi.

Non solo: nel caso dell'Italia, per esempio, gli esperti hanno registrato un aumento delle attività di spionaggio in seguito alla firma dell'accordo economico collegato alla cosiddetta **nuova via della seta**. Un effetto collaterale che si spiegherebbe con l'intenzione del governo di Pechino di acquisire intelligence per poter contrattare al meglio gli accordi con il nostro paese.

Sotto questo profilo, APT41 ricalca il copione alla perfezione. Il gruppo avrebbe colpito in Francia, India, Italia, Giappone, Myanmar, Paesi Bassi, Singapore, Corea del Sud, Sudafrica, Svizzera, Thailandia, Turchia, Regno Unito, Stati Uniti e Hong Kong.

Obiettivi: case farmaceutiche, settore ospedaliero, società del comparto tecnologico ed energetico, delle telecomunicazioni e in alcuni casi anche agenzie di stampa.

Tra le strategie adottate dai pirati, anche quella degli attacchi "supply chain", in cui i cyber-spioni hanno colpito produttori di software per inserire nei loro prodotti i malware che gli hanno permesso poi di compromettere i reali bersagli.

Table 1. Supply chain compromises.

Date	Compromised Entities	FireEye Attribution Assessment
December 2014	Online games distributed by a Southeast Asian video game distributor • Path of Exile • League of Legends • FIFA Online 3	Possibly APT41 or a close affiliate
March 2017	CCleaner Utility	Unconfirmed APT41
July 2017	Netsarang software packages (aka ShadowPad)	Confirmed APT41
June 2018 - November 2018	ASUS Live Update utility (aka ShadowHammer)	Stage 1 unconfirmed APT41 Reported Stage 2 confirmed APT41
July 2018	Southeast Asian video game distributor Infestation PointBlank	Confirmed APT41

Una tecnica che APT41 ha adottato con estrema cautela, prevedendo un sistema che gli consentisse di attivare i payload soltanto sui sistemi che volevano colpire, evitando così il rischio di esporsi troppo ed essere individuati.

Per farlo, gli hacker di Pechino hanno utilizzato il numero di serie dei dischi fissi o il MAC address per individuare con la massima precisione le macchine su cui si sarebbe dovuto attivare il loro malware.

Tra gli attacchi supply chain attribuiti ad APT41 c'è anche quello ai danni degli utenti di **Ccleaner** avvenuto nel 2017, di cui abbiamo parlato ampiamente in questi articoli (1–2–3) e che ha potenzialmente messo a rischio più di **1,6 milioni di computer**.

Tutte le operazioni del gruppo, in ogni caso, dimostrano straordinarie capacità tecniche e una dotazione di strumenti di spionaggio che normali cyber-criminali possono solo sognarsi, a partire per esempio dalla disponibilità di certificati digitali che gli consentono di aggirare i normali sistemi di controllo.

Alla luce dello studio di FireEye, APT41 sarebbe uno dei pochi gruppi di pirati informatici che ha la possibilità di utilizzare strumenti avanzati come quelli usati normalmente per lo spionaggio anche in "normali" cyber-attacchi. Tradotto per il settore della sicurezza informatica: un incubo.

Condividi l'articolo

QualPwn: come ti infetto lo smartphone Android dal Wi-Fi

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/07/double-dragon-apt41-il-gruppo-di-spionaggio-cinese-ha-colpito-anche-litalia/

QualPwn: come ti infetto lo smartphone Android dal Wi-Fi

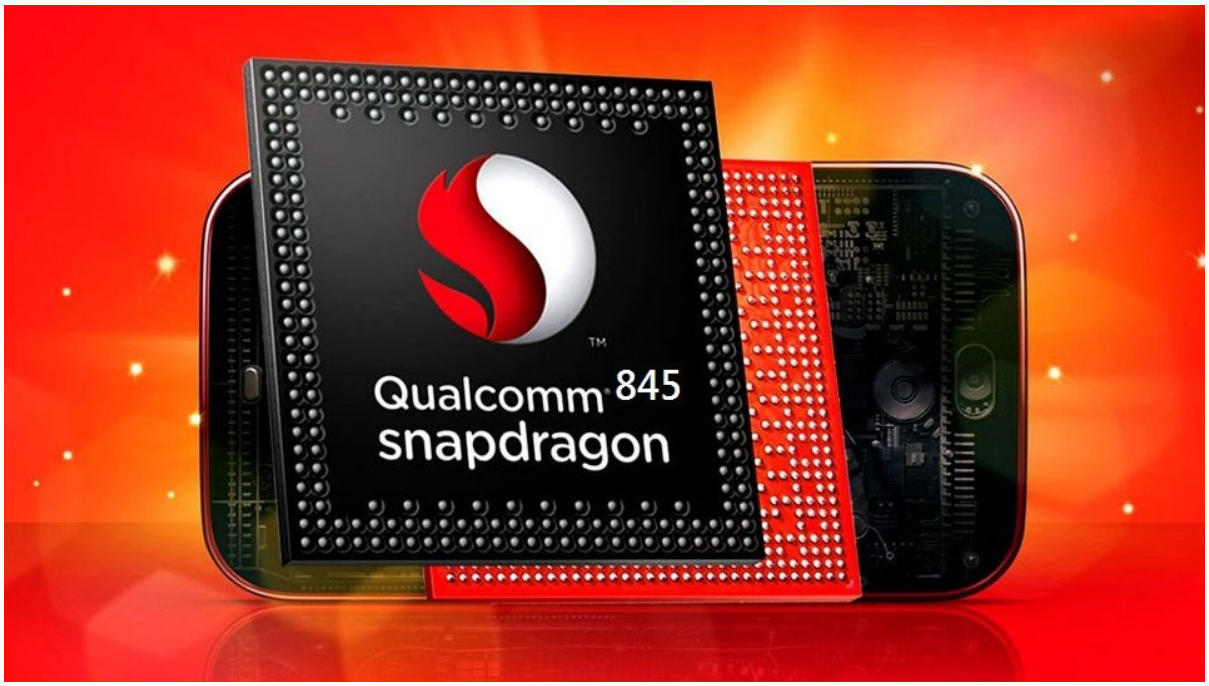
Ago 06, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'uso combinato di due vulnerabilità permette di prendere il controllo di qualsiasi dispositivo Android equipaggiato con chip Qualcomm.

È stato battezzata **QualPwn** ed è probabilmente la tecnica di attacco più devastante mai messa a punto per colpire i dispositivi **Android**. L'anello debole della catena, in questo caso, sono i chip **Qualcomm Snapdragon**. Più precisamente, il componente dedicato al collegamento Wi-Fi.

Le falle di sicurezza, individuate dai ricercatori del **Tencent's Blade team** (qui la pagina Internet dedicata) permettono in pratica di violare qualsiasi sistema Android semplicemente attraverso l'invio di dati via Wi-Fi.

Nel dettaglio, la prima vulnerabilità (CVE-2019-10540) affligge il firmware equipaggiato sul controller Wi-Fi dei chip Qualcomm e consente di provocare un buffer overflow semplicemente inviando dei pacchetti che contengono il codice malevolo, che viene eseguito dal controller.



Già da sola, questa falla di sicurezza consentirebbe di installare un malware o uno spyware sul dispositivo senza che sia necessaria alcuna interazione da parte della vittima. L'unica condizione necessaria è che il pirata informatico sia collegato alla stessa rete Wi-Fi.

Le cose peggiorano, però, se i cyber-criminali utilizzano una seconda vulnerabilità (CVE-2019-10538) che permette di eseguire un passaggio fondamentale dal controller Wi-Fi al kernel Linux del chip Qualcomm. **In questo caso, infatti, sarebbero in grado di prendere il completo controllo del sistema**.

Ma quali sono i dispositivi vulnerabili? I ricercatori del Tencent's Blade team spiegano di aver testato l'attacco soltanto sui **Google Pixel2 e Pixel3**. A loro giudizio, però, dovrebbe funzionare su qualsiasi smartphone o tablet che equipaggia **Snapdragon 835 e 845**.

Ora il problema riguarda gli aggiornamenti. Per i dispositivi Google e (si spera) per buona parte dei maggiori produttori non c'è nessun problema, visto che Qualcomm ha reso disponibili gli aggiornamenti per il suo kernel già lo scorso giugno. **Rimane il problema di tutti quei dispositivi che, per**

motivi di età, non ricevono più aggiornamenti.

Se a questo aggiungiamo l’esercito di utenti che continua stolidamente a ignorare gli aggiornamenti, il rischio è che là fuori ci siano milioni di dispositivi Android a rischio attacco. La buona notizia è che, almeno per il momento, non è circolato alcun exploit pronto da usare. Incrociamo le dita…

Condividi l’articolo

Il 90% degli iPhone vulnerabili a un attacco via iMessage

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/06/qualpwn-come-ti-infetto-lo-smartphone-android-dal-wi-fi/

Il 90% degli iPhone vulnerabili a un attacco via iMessage

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

La vulnerabilità è emersa in questi giorni e corretta con iOS 12.4. Sono pochissimi, però, gli utenti Apple che hanno aggiornato il sistema operativo.

Sembrava si trattasse di una vulnerabilità facilmente arginabile. Le falle di sicurezza che interessano **iOS** (CVE-2019-8624 e CVE-2019-8646) si stanno invece dimostrando più problematiche di quanto si potesse pensare. Colpa degli utenti, che a quanto pare non ne hanno colto la pericolosità.

Se sfruttate, le due vulnerabilità permettono di violare la sandbox di **iMessage** e, di conseguenza, accedere ai file memorizzati sul dispositivo. Tutto questo senza che sia necessaria alcune interazione da parte della vittima.

Insomma: quello a cui siamo di fronte è un exploit che scardina alle fondamenta il sistema di sicurezza di iPhone e iPad, che si basa proprio sui sistemi sandbox.

La filosofia di base di iOS, infatti, è quella di avvantaggiarsi di una struttura a "compartimenti stagni" che impedisce alle app di interagire con altri dati presenti sul dispositivo. Le vulnerabilità in questione smantellano questa impostazione.

A peggiorare la situazione c'è il fatto che il codice per sfruttare l'exploit è già comparso su Internet e, di conseguenza, chiunque abbia tra le mani un Mac e il numero di telefono della potenziale vittima può utilizzarlo tranquillamente per sottrargli informazioni o documenti senza che questi possa accorgersene.



Le vulnerabilità, segnalate ad Apple dal solito **Project Zero di Google**, sono state corrette con la nuova versione del sistema operativo mobile Apple, pubblicato lo scorso 22 luglio. Ma gli aggiornamenti vanno a rilento.

Secondo quanto riporta **Liarna La Porta** in un post sul blog della società di sicurezza **Wandera**, al 1 agosto (dieci giorni dopo la pubblicazione dell'aggiornamento) **iOS 12.4 è stato installato soltanto sul 9,6% dei dispositivi Apple monitorati dai ricercatori**.

Un dato preoccupante, anche perché il campione analizzato riguarda dispositivi aziendali. Quelli per cui, si spera, dovrebbero essere previste policy rigorose per quanto riguarda gli aggiornamenti di sicurezza. **Il dato per quanto riguarda il mondo consumer, quindi, potrebbe anche essere peggiore**.

Paradossalmente, la causa di questa inerzia da parte degli utenti è probabilmente dovuta alla cieca fiducia nel fatto che iPhone abbia un sistema di sicurezza a prova di bomba. Il che potrebbe anche essere (quasi) vero, ma solo quando parliamo di un sistema aggiornato.

Condividi l’articolo

SystemBC: il malware per nascondere il malware

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/05/il-90-degli-iphone-vulnerabili-a-un-attacco-via-imessage/

SystemBC: il malware per nascondere il malware

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

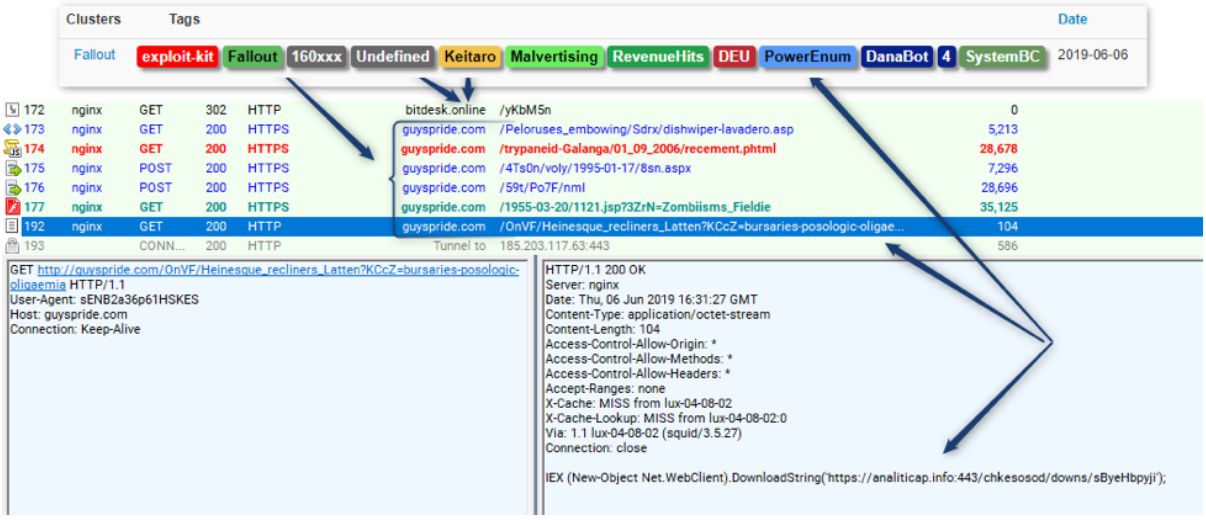
Il virus installa sui PC infetti un proxy che permette di nascondere il traffico Internet di altri software dannosi per impedirne il rilevamento.

I pirati informatici più scaltri utilizzano spesso strumenti per offuscare le comunicazioni dei malware che utilizzano. Il motivo è piuttosto ovvio: la presenza di comunicazioni sospette è infatti uno degli indizi che i software di sicurezza utilizzano per individuare la presenza di software dannoso.

Di solito strumenti di questo tipo sono inclusi nei malware più complessi, spesso dotati di una struttura modulare, e non sono molto diffusi.

Da oggi, però, sembra che tutti i cyber-criminali possano contare su un formidabile strumento di offuscamento. Si chiama **SystemBC** ed è un malware autonomo, che ha la funzione specifica di "supportare" altri programmi nocivi.

Come spiegano i ricercatori di **Proofpoint** in questo report, SystemBC installa sul computer infetto un proxy SOCKS5 che consente di occultare il traffico di qualsiasi "collega" installato sullo stesso computer.

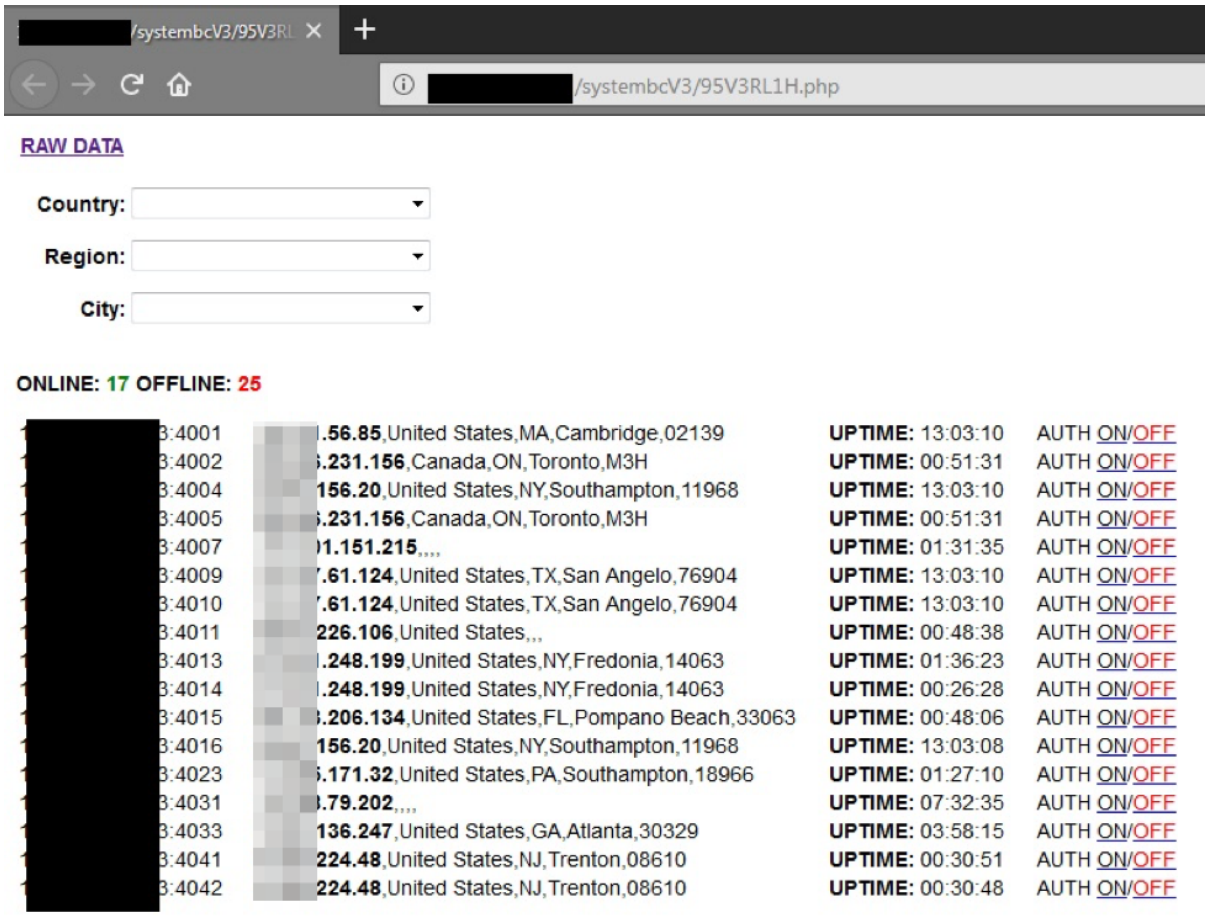


Gli esperti di sicurezza lo hanno individuato per la prima volta lo scorso 6 giugno, mentre analizzavano una campagna di attacchi portata attraverso un Exploit Kit e che aveva come obiettivo principale la diffusione del ransomware **Maze**.

Nelle settimane successive, però, dalle parti di Proofpoint hanno incrociato SystemBC più volte in occasione di attacchi portati da altri gruppi di cyber-criminali, ad esempio per diffondere il trojan bancario **Danabot**. La conclusione dei ricercatori è che il malware sia venduto nei bassifondi del Web come strumento di copertura.

Intuizione confermata quando i ricercatori hanno trovato un "annuncio pubblicitario" che, oltre alla descrizione di

SystemBC, conteneva anche degli screenshot del sistema di controllo.



SystemBC utilizza **un sistema di crittografia XOR a 40 byte** per proteggere informazioni come l'indirizzo del server Command and Control e dei DNS utilizzati, evitando di conservare questi dati su un file, ma iniettandoli nella memoria del computer per renderne più difficile il rilevamento.

Tutte le comunicazioni in entrata e in uscita sono protette attraverso una chiave crittografica **RC4**, utilizzando una particolare procedura che rende più complicata l'individuazione della trasmissione dati.

Insomma, come sottolinea Proofpoint, con SystemBC ci troviamo di fronte a un'ulteriore evoluzione di quella filosofia di "cyber-crimine collaborativo" che negli ultimi anni sembra vivere una crescita esponenziale.

Condividi l'articolo

Raffica di attacchi ransomware ai NAS

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/08/02/systembc-il-malware-per-nascondere-il-malware/

Raffica di attacchi ransomware ai NAS

Ago 01, 2019 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Intrusione, Malware, News, RSS 1

I pirati stanno usando tecniche di Brute Forcing per accedere ai dispositivi. I dati al loro interno vengono crittografati e viene chiesto un riscatto in Bitcoin.

L'allarme è partito da **Sinology**, ma non lasciamoci ingannare: l'ondata di attacchi segnalata dal produttore taiwanese non interessa solo i **NAS** del produttore con sede a Taipei, ma anche prodotti di altre aziende.

Quello a cui si sta assistendo, secondo quanto racconta l'azienda, sarebbe un attacco pianificato che sfrutta botnet di dispositivi IoT per cercare di accedere ai dispositivi utilizzando password di uso comune e credenziali predefinite.

Una volta ottenuto l’accesso al NAS, i pirati informatici utilizzano un classico cripto-ransomware per codificare tutti i dati memorizzati sul dispositivo e lasciano in chiaro soltanto un file di testo nel quale viene chiesto il riscatto per ottenere la chiave che consente di recuperare i dati.

L’alert pubblicato su Internet raccomanda agli utenti di disabilitare l’account di amministrazione predefinito e modificare la password per l’accesso utilizzandone una complessa. Nel caso dei prodotti Sinology, il consiglio è anche quello di abilitare la funzione **Auto Block**.



Si tratta di uno strumento che blocca automaticamente il collegamento a un indirizzo IP quando vengono effettuati troppi tentativi di accesso.

Non è un periodo felice per i proprietari di NAS. Solo qualche giorno fa è infatti emersa una vulnerabilità dei vecchi dispositivi **Iomega** (ne abbiamo parlato in questo articolo) mentre i modelli più recenti dello storico marchio (oggi proprietà di **Lenovo**)sembrano essere stati presi di mira da un gruppo di cyber-criminali che, anche in questo caso, punta a ottenere un riscatto dalle vittime.

Il modus operandi, però, è lievemente diverso da quello riportato da Sinology. **In questo caso, infatti, i file non vengono crittografati ma semplicemente cancellati**. Al pagamento del riscatto, sostengono i pirati nel messaggio che lasciano sul disco, seguirebbe la restituzione dei file.

Come riporta Bleeping Computer, sul cui forum sono arrivate numerose segnalazioni di utenti colpiti in questo modo, i file possono però essere recuperati utilizzando un software di recovery.

Condividi l'articolo

SystemBC: il malware per nascondere il malware LibreOffice corregge una falla ma suggerisce di usare la vecchia versione

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/01/raffica-di-attacchi-ransomware-ai-nas/

LibreOffice corregge una falla ma suggerisce di usare la vecchia versione

Lug 31, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug permette di sfruttare una Macro per eseguire codice. La nuova versione della suite la blocca, ma sul sito se ne consiglia l'uso solo agli "smanettoni".

Gioie e dolori della filosofia open source. A mettere in luce i secondi questa volta è **LibreOffice**, il pacchetto di programmi per l'ufficio che negli ultimi anni si è guadagnato un discreto spazio a livello di utenti.

Qual è il problema? Che dopo aver corretto una clamorosa falla di sicurezza, gli sviluppatori hanno pubblicato la nuova versione 6.2.5 sul sito sconsigliandone però l'utilizzo generalizzato. **Per "l'uso in ambito professionale" viene consigliata la vecchia versione 6.1.6**.



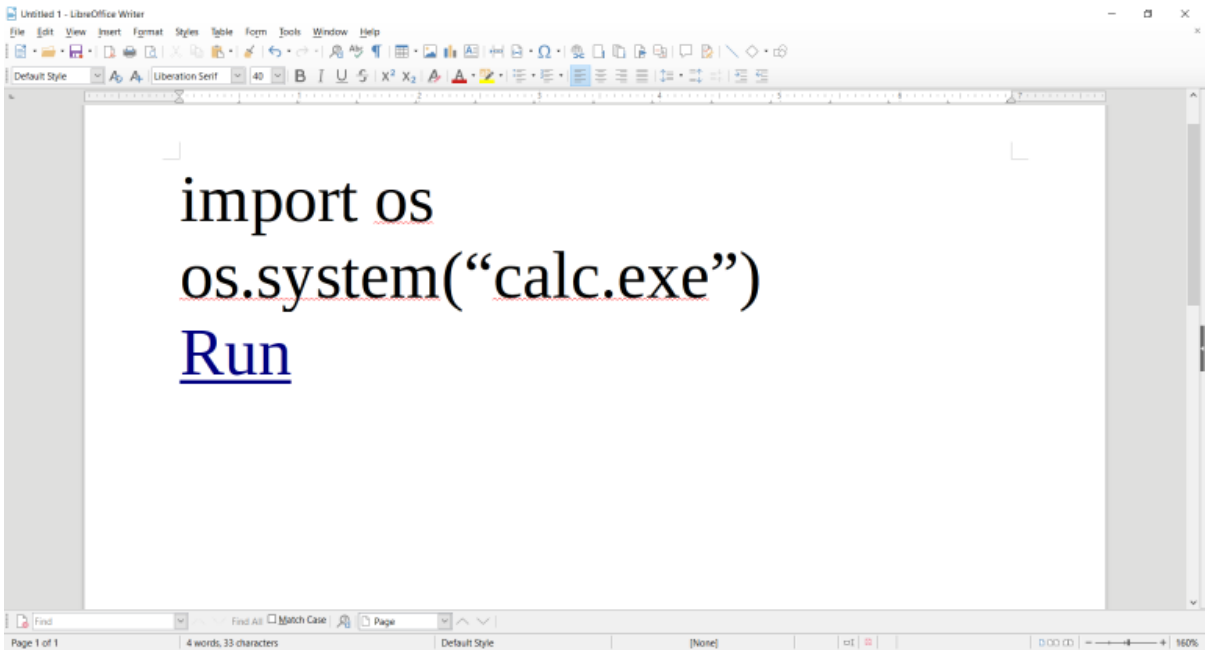
Si tratta di un'abitudine tipica dei progetti open source, ispirata da una certa prudenza nel distribuire le nuove release dei programmi che, effettivamente, potrebbero avere qualche bug o incompatibilità non ancora rilevata. In questo

caso, però, questa forma di “prudenza” è decisamente fuori luogo. **La versione 6.2.5, infatti, contiene una patch che corregge una falla di sicurezza particolarmente grave**.

La vulnerabilità (CVE-2019-9848) è stata individuata da **Nils Emmerich**, che nel suo report spiega come sia possibile sfruttarla per trasformare un documento di LibreOffice in un perfetto vettore di attacco.

Il primo problema, spiega il ricercatore, è che LibreOffice esegue i comandi Macro senza chiedere alcuna conferma all’utente. Questo anche se si imposta il massimo livello di sicurezza.

Il secondo riguarda la presenza in LibreOffice di un componente chiamato **LibreLogo**, che permette di programmare in Python attraverso un sistema di controllo basato su grafica vettoriale. Ciò di cui si è accorto Emmerich, è che utilizzando un comando Macro è possibile sfruttare LireLogo per eseguire un comando.



Il documento qui sopra, per esempio, avvia la calcolatrice di Windows quando il cursore viene posizionato o semplicemente passa (non è necessario alcun clic) sulla scritta “Run”. Modificandolo, sarebbe possibile eseguire un malware.

Insomma: sul sito di LibreOffice viene suggerito di installare una versione "stabile" che contiene una vera voragine di sicurezza. Speriamo che le segnalazioni circolate in queste ore arrivino alle orecchie dei responsabili in modo che possano prendere provvedimenti.

Condividi l'articolo

URGENT11: raffica di vulnerabilità in dispositivi SCADA e IoT

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/31/libreoffice-corregge-una-falla-ma-suggerisce-di-usare-la-vecchia-versione/

URGENT11: raffica di vulnerabilità in dispositivi SCADA e IoT

Lug 30, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le 11 falle di sicurezza interessano il software

VxWorks. A rischio dispositivi medici, industriali e device IoT di ogni genere e tipo.

Si chiama **VxWorks** e , da un punto di vista tecnico, viene definito un "sistema operativo real-time" (RTOSes), cioè un software di controllo con funzionalità piuttosto limitate, installati normalmente sui chip che equipaggiano i dispositivi IoT o macchinari automatizzati.

Il fatto che sia pressoché sconosciuto al grande pubblico, non deve ingannare. Secondo quanto riporta i sito di **Wind River**, produttore del RTOSes, ci sarebbero infatti in circolazione la bellezza di 2 miliardi di dispositivi equipaggiati con VxWorks.

La notizia che un gruppo di ricercatori di **Armis** abbia individuato **11 falle di sicurezza** nel software (qui il documento che le riassume) di conseguenza, è più che sufficiente per mettere in fibrillazione l'intero settore della sicurezza.

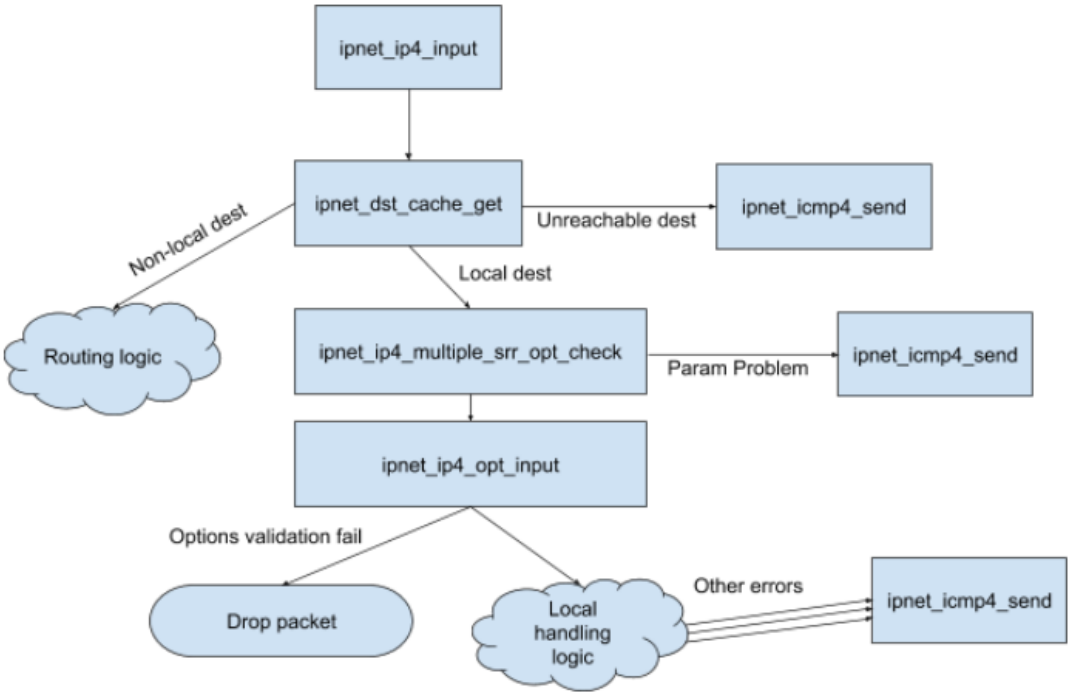
Il fatto che i ricercatori abbiano battezzato il "pacchetto" di vulnerabilità con il nome di **URGENT11** la dice lunga sul possibile impatto che possono avere.

Tanto più che sei di queste (in questo caso abbiamo deciso di lasciare la descrizione in inglese) sono state classificate "ad alto rischio", dal momento che possono portare all'esecuzione di codice in remoto.

1. Stack overflow in the parsing of IPv4 packets IP options (CVE-2019-12256)
2. TCP Urgent Pointer = 0 leads to integer underflow (CVE-2019-12255)
3. TCP Urgent Pointer state confusion caused by malformed TCP AO option (CVE-2019-12260)
4. TCP Urgent Pointer state confusion during connect to a remote host (CVE-2019-12261)
5. TCP Urgent Pointer state confusion due to race condition

(CVE-2019-12263)

6. Heap overflow in DHCP Offer/ACK parsing in ipdhcpc (CVE-2019-12257)



Le altre cinque, considerate meno gravi, possono comunque essere sfruttate per provocare errori, malfunzionamenti e blocco dei sistemi.

1. TCP connection DoS via malformed TCP options (CVE-2019-12258)
2. Handling of unsolicited Reverse ARP replies (Logical Flaw) (CVE-2019-12262)
3. Logical flaw in IPv4 assignment by the ipdhcpc DHCP client (CVE-2019-12264)
4. DoS via NULL dereference in IGMP parsing (CVE-2019-12259)
5. IGMP Information leak via IGMPv3 specific membership report (CVE-2019-12265)

Considerato il tipo di dispositivi coinvolti, però, sottovalutare l’impatto di eventuali attacchi che sfruttino anche queste vulnerabilità “minori” sarebbe pericolosissimo. **Pensiamo ai danni che può provocare un blocco su una catena di**

montaggio o il malfunzionamento di un dispositivo medico.

La nuova versione di VxWorks, con gli aggiornamenti che correggono le falle di sicurezza, è stata pubblicata dal produttore ed è disponibile dal mese scorso. Il problema, adesso, è capire come procederanno gli aggiornamenti.

Purtroppo l'esperienza porta a un certo pessimismo e non ci sono dubbi che sentiremo parlare di nuovo del sistema operativo real-time nel prossimo futuro.

Condividi l'articolo

Kaspersky supera l'audit indipendente SOC 2

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/30/urgent11-raffica-di-vulnerabilita-in-dispositivi-scada-e-iot/

Arrestati gli hacker che hanno violato l'account Telegram di Bolsonaro

Lug 29, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, News, RSS 0

Il presidente del Brasile e numerosi esponenti del governo vittime di un attacco piuttosto artigianale. La tecnica si conosce dal 2016.

C’è anche il presidente **Jair Bolsonaro** nell’elenco di esponenti del governo brasiliano i cui account Telegram sono stati violati da un gruppo di hacker che le forze di polizia hanno arrestato la scorsa settimana. **Oltre a lui, nel mirino sono finiti il ministro della giustizia Sergio Moro e il ministro dell’economia Paulo Guedes**.

La vicenda è emersa dopo una serie di leak riguardanti messaggi scambiati tra i ministri pubblicati dal sito di news **The Intercept**, fondato dal giornalista **Glenn Greenwald**.

Il reporter statunitense, diventato celebre per aver “coperto” la vicenda di **Edward Snowden**, è considerato uno dei migliori nel settore del giornalismo investigativo e non stupisce che gli hacker abbiano scelto il suo giornale online per diffondere il materiale che hanno “acquisito”.

I messaggi, in particolare quelli del ministro della giustizia Moro, hanno creato un clamoroso terremoto politico in Brasile. Dalle chat sarebbe infatti emerso un vero e proprio piano per influenzare il processo nei confronti dell’ex-presidente **Luiz Inácio Lula da Silva**, deposto in seguito a un’inchiesta che a questo punto appare essere stata pilotata ad arte da Moro (che ai tempi era giudice) con lo scopo di screditarlo.



Gli arrestati sono il 33enne **Danilo Cristiano Marquez**, **Walter Delgatti Neto** (30), **Judy Gustavo Henrique Elias Santos** (28) e sua moglie **Suelen Priscilla de Oliveira** (25).

La parte davvero sorprendente di tutta la vicenda riguarda però il modo in cui avrebbero ottenuto l'accesso ai messaggi. **Per violare gli account dei politici brasiliani, gli hacker hanno usato un trucchetto che è emerso 3 anni fa e di cui abbiamo parlato ampiamente in questo articolo**.

Come funziona l'attacco? In pratica, fa leva sul sistema utilizzato da Telegram per attivare il servizio di messaggistica su desktop. La procedura prevede infatti l'inserimento del numero di telefono con cui è registrato l'account e una conferma attraverso **un codice di sicurezza** che viene inviato con un SMS al telefono stesso.



Telegram, però, prevede anche la possibilità di ottenere il codice attraverso **una chiamata vocale automatica**. Ed ecco qui la falla di sicurezza. Se il telefono non è raggiungibile (ad esempio perché è impegnato in un'altra chiamata) il messaggio con il codice viene registrato sulla segreteria telefonica.

Tutto quello che i pirati hanno dovuto fare, quindi, è stato chiamare il telefono in questione e, nel frattempo, tentare l'accesso via desktop chiedendo l'invio del codice tramite chiamata vocale.

A questo punto, non rimane che collegarsi alla segreteria telefonica della vittima per appropriarsi del codice di autenticazione. Farlo è più facile di quanto si possa credere.

Basta utilizzare un servizio VoIP (o un'app) che consenta di impostare il numero di telefono in uscita con lo stesso della vittima o "indovinare" il PIN di accesso al servizio che consente di ascoltare i messaggi da un altro telefono.

Visto che quasi nessuno modifica il PIN di accesso alla

segreteria telefonica, infatti, ci sono buone probabilità che sia quello predefinito, di solito “0000” o “1234”.

Insomma: nessuna tecnica sofisticata o strumenti fantascientifici, ma qualcosa che potrebbe utilizzare anche un ragazzino sufficientemente sveglio. Di più: per proteggersi da questo tipo di attacco basterebbe un piccolo accorgimento: **disattivare la segreteria telefonica**.

La ricostruzione fatta dagli investigatori, che per il momento non hanno ancora formalizzato le accuse, è però ancora tutta da verificare.

In seguito agli arresti e alle indagini che stanno seguendo, Greenwald ha infatti negato che i quattro arrestati fossero la fonte del leak riportato da The Intercept. Tanto più che, secondo Greenwald, i primi contatti con la sua fonte sarebbero avvenuti un mese prima del presunto hacking degli account come denunciati dal ministro Moro, che avrebbe indicato il 5 giugno come data in cui gli hacker avrebbero violato il sistema.

La vicenda, insomma, rimane ancora piuttosto intricata. L’unico dato certo è che Jair Bolsonaro e i suoi accoliti, già al centro delle polemiche per le loro politiche illiberali e per la malcelata nostalgia per i tempi della dittatura, non ne escono particolarmente bene. Per lo meno dal punto di vista dell’astuzia.

Condividi l’articolo

Kaspersky supera l’audit indipendente SOC 2 Gli strani effetti collaterali degli attacchi ransomware

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/29/arrestati-gli-hacker-che-hanno-violato-laccount-telegram-di-bolsonaro/