Torna la botnet Emotet. Gli esperti: “i server sono di nuovo attivi”

Ago 23, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS 0

Il gruppo comparso nel 2014 aveva cessato la sua attività ma ora sembra prepararsi a colpire di nuovo. Esperti di sicurezza in stato di allarme rosso.

È considerato uno dei gruppi più longevi nel settore del cyber-crimine e non a torto: i pirati informatici che utilizzano la botnet **Emotet**, infatti, sono sulla piazza dal 2014 e da tempo alternano periodi di inattività a campagne di diffusione malware che hanno sistematicamente conseguenze piuttosto pesanti.

L’ultimo allarme era scattato lo scorso ottobre (ne abbiamo parlato in questo articolo) quando gli hacker avevano cominciato a scaricare email da computer infettati con il loro trojan.

Ora, però, i ricercatori segnalano qualcosa di diverso. **Stando ai dati raccolti su Internet, infatti, i server Command and Control utilizzati dal gruppo avrebbero cominciato a inviare e ricevere traffico**.

Per il momento gli esperti non hanno individuato l’invio di malware, ma il timore è che si tratti di una fase preparatoria che prelude a un periodo di attività piuttosto intensa.

Ultimamente, infatti, l’infrastruttura di Emotet è stata utilizzata per distribuire un altro trojan chiamato **TrickBot** e, in una seconda fase degli attacchi, il ransomware **Ryuk**. Uno schema che era stato già utilizzato l’anno scorso e che ha effetti decisamente distruttivi.

La distribuzione dei server, dal punto di vista geografico, è

estremamente variegata. I ricercatori di **Malware Tech** (come si vede nell'immagine qui sopra) hanno individuato server attivi in Brasile, Messico, Germania, Giappone e Stati Uniti.

Insomma: è probabile che i pirati stiano preparando qualcosa di grosso. Non ci resta che aspettare per scoprire cosa succederà.

Condividi l'articolo

Texas bloccato dai ransomware. I pirati vogliono 2,5 milioni

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/23/torna-la-botnet-emotet-gli-esperti-i-server-sono-di-nuovo-attivi/

Texas bloccato dai ransomware. I pirati vogliono 2,5 milioni

Ago 22, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS 0

I cyber-criminali hanno violato i sistemi dell'azienda che gestisce il settore IT del governo statale e hanno colpito 22 enti pubblici contemporaneamente.

Quello che si è verificato in **Texas** lo scorso 16 agosto è probabilmente del più clamoroso attacco mai portato a uno stato da parte di "normali" pirati informatici.

Come spiega un comunicato stampa pubblicato sul sito ufficiale del governo texano, l'attacco ha coinvolto **22 enti pubblici** (in un primo momento si era parlato di 23) i cui sistemi sono stati bloccati attraverso un ransomware.

Se in un primo momento l'amministrazione del Texas era stata piuttosto avara di informazioni, limitandosi a parlare di un "attacco coordinato", ora però emergono maggiori dettagli.

Da quanto è emerso, i pirati informatici avrebbero preparato accuratamente l'attacco prendendo di mira il Managed Servic Provider (MSP) cui è affidata la gestione dei sistemi IT della pubblica amministrazione.

Una strategia terribilmente efficace, che sfrutta gli MSP come "testa di ponte" per colpire i sistemi informatici. Le aziende che forniscono questo tipo di servizio, infatti, utilizzano dei software per il controllo remoto attraverso cui possono gestire ogni singolo computer dei clienti.

Se i pirati riescono a ottenere l’accesso a questa funzionalità, possono distribuire un malware su migliaia di computer con il minimo sforzo.

Come abbiamo raccontato in questo articolo, non è la prima volta che succede qualcosa del genere. In precedenza, però, i cyber-criminali che hanno colpito gli MSP si sono limitati a sfruttare questa opportunità per portare attacchi “a pioggia”.

In questo caso, invece, il piano è decisamente più articolato. **Gli hacker hanno infatti coordinato l’attacco per mettere in ginocchio un intero stato**. Anche se non si conoscono tutte le vittime, alcune municipalità hanno ammesso di essere state colpite.

Tra queste la cittadina di **Borger** (13.000 abitanti) e quella di **Keene** (6.000 abitanti), che al momento hanno alcuni servizi bloccati, come l’amministrazione e l’anagrafe.

Secondo quanto riferito dalle autorità, che stanno lavorando per risolvere lasituazione, la richiesta di riscatto inviata dai pirati informatici è decisamente “importante”: avrebbero

infatti chiesto la bellezza di **2,5 milioni di dollari** per sbloccare i sistemi infetti.

Un’ipotesi che l’amministrazione del Texas sembra non considerare nemmeno. L’approccio delle autorità è infatti quello di recuperare le funzionalità dei sistemi informatici e, a quanto pare, i tecnici chiamati a fronteggiare l’attacco starebbero facendo progressi.

Condividi l’articolo

Raffica di bug in VLC: aggiornamento urgente!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/22/texas-bloccato-dai-ransomware-i-pirati-vogliono-25-milioni/

Raffica di bug in VLC: aggiornamento urgente!

Ago 21, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il nuovo update corregge 13 vulnerabilità del popolare player multimediale. Le più gravi consentono un attacco che installa un malware tramite un file video.

Dal punto di vista di un pirata informatico, poter portare un attacco attraverso un file video è una vera pacchia. Prima di tutto perché nessuno si aspetta che un file video possa essere pericoloso. **In secondo luogo perché l'uso di un video come vettore di attacco permette ai cyber-criminali di utilizzare canali alternativi come i circuiti peer to peer**.

Ogni volta che compare una falla di sicurezza in un player multimediale, di conseguenza, il livello di allerta schizza al massimo. Se poi la vulnerabilità interessa un software diffuso come **VLC**, possiamo parlare di un vero e proprio allarme rosso.

Il nuovo aggiornamento del player **VideoLan** alla versione 3.0.8, i cui dettagli sono accessibili attraverso questa pagina Web, corregge 13 vulnerabilità che permetterebbero a un pirata informatico di creare un file video che potrebbe portare al crash del programma o addirittura all'esecuzione di codice in remoto. I pirati informatici potrebbero sfruttare una gran varietà di formati: WMV, MP4, AVI, e OGG.

Le due vulnerabilità più gravi, si legge nel report, sono CVE-2019-13602 e CVE-2019-13962. **Le due falle di sicurezza sono state infatti classificate con un livello di rischio rispettivamente di 8.8 e 9.8**.

Sulla valutazione, però, dalla parti di VideoLan hanno qualche perplessità. Gli sviluppatori sono infatti convinti che le due falle di sicurezza non siano così gravi e che sarebbe più appropriata una valutazione di rischio di 4.3.

Al di là delle diatribe sulla pericolosità dei bug, sul sito di VideoLan viene specificato che la vulnerabilità identificata con il codice CVE-2019-13962 interessa soltanto alcune versioni (dalla 3.0.2 alla 3.0.7.1) di VLC.

Al netto di polemiche e precisazioni, il consiglio naturalmente è quello di aggiornare immediatamente il programma. Visto il rischio che si corre, vale la pena ritardare di un paio di minuti la riproduzione dell'ultimo episodio della nostra serie preferita per eseguire l'update.

Condividi l'articolo

I ransomware sono raddoppiati nel secondo trimestre del 2019

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/08/21/raffica-di-bug-in-vlc-aggiornamento-urgente/

Lo sponsor dei mHACKeroni: “non sono solo talenti da coltivare”

Ago 20, 2019 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario 0

Evolumia ha contribuito al crowd funding per mandare la squadra italiana al Def Con di Las Vegas, dove ha ottenuto un ottimo quinto posto.

Il successo dei **mHACKeroni** al **Def Con** di Las Vegas lo scorso 11 agosto ha entusiasmato l’ambiente della cyber-security italiana. Il gruppo di studenti si è piazzato quinto, ottenendo il miglior piazzamento tra i team europei.

Ma la vicenda dei mHACKeroni ha anche un aspetto “parallelo” alla competizione, che forse è stato ancora più impegnativo da

affrontare. Prima di potersi confrontare con gli altri gruppi di hacker etici in Nevada, i ragazzi hanno dovuto superare un problema molto più pratico: trovare i fondi per partecipare all'evento.

Lo hanno fatto attraverso un appello pubblico a cui hanno risposto numerose realtà, grandi e piccole, che operano nella cyber-security in Italia. Un intervento che ha consentito di ottenere questa bella soddisfazione.

"Quando abbiamo letto l'appello dei mHACKeroni abbiamo deciso subito di impegnare le nostre risorse per aiutarli" spiega a Security Info **Lino Fornaro**, Security Consultant di **Evolumia**, una delle società che ha deciso di aiutare il team italiano.

Evolumia è una società di cyber security pugliese e la scelta di sponsorizzare i mHACKeroni non rappresenta solo un bel gesto o un'operazione di marketing. Rappresenta prima di tutto la volontà di supportare nuove risorse per un settore che ha un gran bisogno di crescere.

Non siamo di fronte, però, al classico meccanismo per cui le società informatiche guardano ai giovani talenti con il solo interesse dettato dall'idea di reclutarli nelle proprie fila. "*L'idea di avere con noi qualcuno dei mHACKeroni ci piace sicuramente*" ammette Fornaro. "*Le motivazioni che ci hanno spinti a rispondere al loro appello sono però più ampie*".

“*La nostra azienda è nata prima di tutto sulla scia della passione per la sicurezza informatica di chi ci lavora*” spiega. “*Uno dei nostri obiettivi è contribuire alla creazione di una reale cultura della cyber-security, che anche in Italia sembra finalmente prendere corpo*”.

A contribuire a questa sorta di “risveglio”, precisa Fornaro, ha contribuito certamente l’entrata in vigore del **GDPR** e gli obblighi connessi al nuovo regolamento, ma non solo. “*L’escalation di attacchi informatici a cui abbiamo assistito negli ultimi anni hanno aumentato la consapevolezza dei rischi che si corrono*” sottolinea l’esperto di Evolumia.

L’impegno nella community che gravita intorno alla cyber-sicurezza, secondo Fornaro, rappresenta un tassello fondamentale per fare in modo che questo processo acquisti più vigore. Anche con una connotazione più squisitamente territoriale.

“*Gli imprenditori del sud Italia faticano ancora a pensare di poter trovare le risorse che gli servono in ambito tecnologico sul loro stesso territorio*” spiega. “*Iniziative come queste o come il **Confsec**, l’appuntamento annuale che dal 2015 raduna ogni anno esperti di sicurezza informatica a Bari* (la prossima

edizione è prevista per il prossimo 3 ottobre – ndr), *permettono anche di superare questa percezione*”.

Per quanto riguarda il rapporto con il team dei mHACKeroni, Fornaro assicura che non finisce qui. In attesa di incontrare i ragazzi per festeggiare l’ottimo piazzamento al Def Con, dalle parti di Evolumia hanno deciso di prevedere da subito un ulteriore contributo economico per supportare la loro attività.

Condividi l’articolo

Attacco hacker alla BCE. I pirati nei sistemi per mesi

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/20/lo-sponsor-dei-mhackeroni-non-sono-solo-talenti-da-coltivare/

Attacco hacker alla BCE. I pirati nei sistemi per mesi

Ago 19, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS 0

La Banca Centrale Europea ha dovuto mettere offline il servizio BIRD. I pirati informatici hanno avuto accesso ai dati di tutti gli utenti iscritti.

Che le banche siano uno dei bersagli prediletti dei pirati informatici è arcinoto. Questa volta, però, la vittima è eccellente e la violazione dei dati potrebbe avere conseguenze imprevedibili a medio o lungo termine. A finire nel mirino di un gruppo di hacker è stato infatti il sito relativo al servizio **BIRD**, gestito dalla **Banca Centrale Europea**.

La violazione, confermata dalla stessa BCE con un comunicato stampa, ha interessato in realtà i sistemi di un soggetto esterno alla Banca Centrale Europea, che gestisce BIRD per conto dell'istituto. Il sito è stato messo offline e sono in corso indagini per appurare eventuali ulteriori attacchi collegati al primo.

Ma che cos'è BIRD e perché i pirati si sono interessati al sito? Il **Banks' Integrated Reporting Dictionary** è un servizio pensato per gli istituti di credito, che fornisce informazioni puntuali sui regolamenti e gli obblighi che le banche devono rispettare nella gestione delle comunicazioni. Insomma: una sorta di "Wiki" destinato al settore del credito internazionale.

È evidente, quindi, che i dati di chi è iscritto a BIRD

possano essere molto preziosi per i pirati informatici, che grazie all'accesso al sistema hanno avuto la possibilità di ottenere informazioni utili per portare, ad esempio, attacchi di phishing particolarmente efficaci. **Chi potrebbe infatti diffidare di un'email proveniente nientemeno che dalla BCE?**

Secondo quanto si legge nel comunicato, l'attacco avrebbe messo a rischio i dati di 481 soggetti iscritti al servizio, anche se si specifica che la violazione non ha interessato le password. Pochi i dettagli riguardo le modalità usate dai pirati per portare l'attacco. Si parla di una "iniezione di malware" nei server.

Il vero problema è che, secondo gli esperti, la violazione sarebbe avvenuta diversi mesi fa: addirittura nel dicembre del 2018. Non è escluso, quindi, che i pirati abbiano già sfruttato il sito di BIRD come "pivot" per portare degli attacchi agli istituti bancari che usano il servizio.

Condividi l'articolo

Hackerata Suprema. Gli esperti: "Società di (in)sicurezza biometrica"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/19/attacco-hacker-alla-bce-i-pirati-nei-sistemi-per-mesi/

Hackerata Suprema. Gli esperti: “Società di (in)sicurezza biometrica”

Ago 16, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, News, RSS, Scenario, Vulnerabilità 1

La vittima è Suprema, che gestisce la piattaforma di sicurezza Bio Star 2. Rubate impronte digitali e le credenziali di amministrazione.

Utilizzare un sistema di riconoscimento facciale e scansione delle impronte digitali per regolare l’accesso agli edifici e controllare gli spostamenti al loro interno può sembrare la soluzione per “blindare” la sede di un’azienda.

Se chi gestisce i sistemi ha però un’infrastruttura informatica che è un colabrodo, però, rischia di essere tutto inutile. Anzi: a ben guardare può trasformarsi in un boomerang.

È successo ai clienti di **Suprema**, una società sud coreana specializzata nella fornitura di sistemi di sicurezza basati sull’analisi biometrica e che ha recentemente avviato una partnership per integrare i suoi sistemi di controllo in **AEOS**, un sistema di controllo venduto da **Nedap**.

Come spiegano **Noam Rotem** e **Ran Locar**, ricercatori della società di sicurezza **vpnMentor**, Suprema è stata vittima di un attacco hacker che ha portato a un clamoroso leak di dati relativi alla sua piattaforma **Bio Star 2**.

I 23 gigabyte di dati individuati dai due analisti, che i

pirati informatici hanno “estratto” dai sistemi di Suprema, comprendono 27,8 milioni di record, tra cui un milione di impronte digitali di dipendenti delle aziende che usano i sistemi Bio Star 2, i dati di riconoscimento facciale e i log di accesso.

Non solo: i cyber-criminali sono riusciti anche a mettere le mani sulle credenziali di amministrazione del sistema. **Un compito non troppo difficile, per la verità, visto che secondo i ricercatori le credenziali erano conservate in chiaro, senza l’uso di hashing o crittografia**.

Gli hacker che hanno violato i sistemi di Suprema, in pratica, hanno a disposizione tutto quello che gli serve per modificare gli account esistenti o crearne di nuovi. **In altre parole: possono superare i sistemi di sicurezza di circa 5.700 organizzazioni in 83 paesi diversi**.

La parte più sconcertante, però, riguarda alcuni elementi che emergono dal report pubblicato sul sito ufficiale di vpnMentor, come il fatto che la maggior parte delle password avesse un livello di sicurezza ridicolo, con credenziali che

comprendevano le solite “Password” e “abcd1234”.

Anche il livello di reattività di Suprema, secondo i ricercatori, lascia parecchio a desiderare. **Dopo aver inviato numerose email, Rotem e Locar sarebbero stati addirittura “rimbalzati” al telefono da un impiegato di Suprema**.

La situazione si è risolta solo quando i due esperti di sicurezza sono riusciti a contattare la sede francese dell’azienda, dove hanno trovato una maggiore collaborazione.

Tutta la vicenda, però, accende i riflettori anche su un altro aspetto collegato all’uso di sistemi biometrici. A differenza di quanto accade con le normali credenziali, infatti, i sistemi di autenticazione come le impronte digitali o il riconoscimento facciale scontano un “piccolissimo” svantaggio: non possono essere modificate.

Una volta che sono state rubate, non c’è più nulla da fare se non cambiare sistema di autenticazione. Una considerazione che dovrebbe far riflettere chi sta considerando di battere questa via per sostituire l’utilizzo di password e PIN.

Condividi l’articolo

Quattro app per appuntamenti rivelano l’esatta posizione degli utenti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/16/hackerata-suprema-gli-esperti-societa-di-insicurezza-biometrica/

Quattro app per appuntamenti rivelano l’esatta posizione degli utenti

Ago 14, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Vulnerabilità 0

Le informazioni fornite dalle applicazioni permettono di ricavare l’esatta posizione di 10 milioni di utenti iscritti. Una manna per stalker, spioni e regimi omofobi.

Ormai li conosciamo per essere tra i ricercatori più “tignosi” e scrupolosi nel loro lavoro. Gli analisti di **Pen Tester Partners**, che hanno recentemente reso pubbliche le vulnerabilità di alcuni router 4G, questa volta hanno messo nel mirino le applicazioni per incontri e appuntamenti.

Tutto è cominciato con il report su **3fun**, un’app per smartphone pensata per chi vuole trovare via Internet partner disposti a mettere insieme dei “triangoli amorosi”.

Nel segnalare le voragini di sicurezza di 3fun, che permette di recuperare facilmente informazioni personali degli iscritti al servizio, i ricercatori hanno sottolineato anche la possibilità di individuarne l’esatta posizione attraverso una tecnica chiamata “trilaterazione”.

Il concetto, simile a quello della triangolazione utilizzato per conoscere la propria posizione partendo dalla distanza da due punti conosciuti, sfrutta una funzione introdotta in molte

applicazioni di questo genere, cioè quella che **permette di conoscere la propria distanza dagli altri utenti**.

Come spiegano i ricercatori, utilizzare questa funzione per ottenere l’esatta posizione di un utente è piuttosto semplice. Basta inviare una serie di false coordinate per la propria posizione e utilizzare un programmino che analizza i dati ottenuti relativi a un determinato utente. La precisione, grazie ai sistemi GPS, è elevatissima.

Il tutto funziona in tempo reale e permette, partendo dallo username, di ricostruire gli spostamenti di una persona nell'arco della giornata arrivando a scoprire potenzialmente quale sia la sua abitazione, dove lavori e quali luoghi visiti nel corso della giornata.

A distanza di una settimana dall'analisi di 3fun, i ricercatori hanno scoperto che la stessa cosa si può fare anche con altre tre applicazioni simili: **Romeo**, **Recon** e il (decisamente) più celebre **Grindr**. La loro analisi è pubblicata in un report che rischia di trasformarsi in una vera "bomba".

Il risultato è infatti una mappa che permette di localizzare e tracciare i circa 10 milioni di utenti iscritti ai quattro servizi.

La mappa qui sopra mostra gli iscritti alle quattro app individuati nel centro di Londra.

Un bel problema, visto che un'informazione del genere potrebbe essere usata da uno stalker o da un semplice ficcanaso che abbia voglia di sgretolare la (fragile) privacy garantita dalla dimensione digitale.

Per spiegare meglio la questione, i ricercatori sottolineano

come nei loro test abbiano facilmente individuato utenti che risultavano posizionati stabilmente alla **Casa Bianca** così come al **10 di Downing Street**, la residenza e sede del Primo Ministro del Regno Unito. Roba per cui i paparazzi potrebbero andare matti.

Ma c'è di peggio. Visto che le app riportano l'orientamento sessuale degli iscritti (e nel caso di Grinder l'intera utenza appartiene alla sfera gay e bisessuale) la funzionalità potrebbe essere usata anche a scopo discriminatorio, soprattutto in quei paesi in cui vigono legislazioni che reprimono la libertà sessuale.

Secondo i ricercatori, il rischio per la privacy potrebbe essere limitato utilizzando coordinate meno precise e adottando una serie di accorgimenti tecnici che possono impedire il recupero automatico di questi dati attraverso le API delle applicazioni.

Speriamo che gli sviluppatori delle quattro app gli diano retta. Prima che qualcuno decida di approfittarne davvero…

Condividi l'articolo

Nuove falle nel controllo remoto di Windows: aggiornare!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/14/quattro-app-per-appuntamenti-rivelano-lesatta-posizione-degli-utenti/

Nuove falle nel controllo remoto di Windows: aggiornare!

Ago 14, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'ultimo update di Microsoft corregge quattro vulnerabilità nel Remote Desktop Service che consentono attacchi in remoto senza autenticazione.

Dopo aver corretto in fretta e furia **Bluekeep**, la vulnerabilità che consentiva di violare un sistema Windows attraverso un collegamento in remoto che non richiede alcuna interazione da parte dell'utente, Microsoft si trova a fronteggiare altre quattro (quattro!) falle di sicurezza con le stesse caratteristiche.

L'anello debole, ancora una volta, è quel **Remote Desktop Service** che le aziende trovano terribilmente utile per gestire a distanza i loro computer ma che si sta dimostrando anche incredibilmente fragile sotto li profilo della sicurezza.

Questa volta le vulnerabilità sono state scoperte dal team di sicurezza interno di Microsoft. I bug (CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 e CVE-2019-1226) interessano tutte le versioni del sistema operativo: **Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012 e Windows 10**.

La descrizione delle vulnerabilità, piuttosto stringata, è uguale per tutte: sfruttandole un pirata informatico potrebbe

ottenere il controllo completo di un computer semplicemente inviando dei pacchetti attraverso il **Remote Desktop Protocol**.

Niente autenticazione e nessuna necessità di ingannare l'utente per fargli fare clic su un collegamento o aprire un file. **Insomma: saremmo di fronte a un classico exploit che permetterebbe ai cyber-criminali di creare un worm in grado di diffondersi autonomamente**.

Le falle di sicurezza sono state corrette nell'ultimo aggiornamento per i sistemi Windows e si spera, di conseguenza, che il pericolo sia scampato.

Per tutti quelli che non potessero applicare le patch (non si capisce bene per quale motivo, ma ce ne sono ancora) l'alternativa è quella di disabilitare il servizio di controllo remoto o inserire un blocco da firewall sulla porta TCP 3389.

La buona notizia è che, fino a ora, non è comparso alcun exploit in grado di sfruttare le vulnerabilità. Dal punto di vista dei pirati, quindi, si è all'anno zero.

Condividi l'articolo

Quattro app per appuntamenti rivelano l’esatta posizione degli utenti Router 4G a rischio attacco. Avete aggiornato il firmware?

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/08/14/nuove-falle-nel-controllo-remoto-di-windows-aggiornare/

Router 4G a rischio attacco. Avete aggiornato il firmware?

Ago 13, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Una raffica di bug individuata nei modelli più diffusi consentirebbe a un pirata informatico di rubare informazioni e portare attacchi al dispositivo.

A ben vedere, l’allarme lanciato riguardo le vulnerabilità dei **router 4G** rappresenta un clamoroso paradosso. I dispositivi che consentono il collegamento a Internet in mobilità, infatti, sono usati per lo più da chi ha a cuore la sicurezza e preferisce portarsi con sé una rete Wi-Fi di “proprietà” piuttosto che usare i vari hotspot gratuiti.

Stando a quanto spiegano in un report i ricercatori di **Pen Test Partners**, però, questo tipo di dispositivi soffre di numerose falle di sicurezza che rischiano di esporre gli utenti al rischio di attacchi e furti di informazioni. Peggio ancora: i produttori sembrano preoccuparsi ben poco dei rischi individuati dai ricercatori.

I router 4G sono, essenzialmente, molto simili ai router domestici, con una semplice differenza: al posto di collegarsi a una linea fissa, utilizzano una SIM dati per garantire la connessione.

Il problema è che con l'introduzione di funzionalità hotspot per le SIM in dotazione ai normali smartphone (la disponibilità della funzione dipende dall'operatore) i router 4G hanno perso un po' di appeal sul mercato. **Come se non bastasse, il prossimo passaggio al 5G viene visto dai produttori come un passaggio che renderà obsoleti gli attuali modelli**.

Risultato: secondo Pen Test Partners stiamo assistendo a una pericolosa inerzia nell'aggiornamento dei software di controllo dei dispositivi. Un'ipotesi confermata dal racconto che i ricercatori fanno delle procedure di disclosure avviate con vari produttori.

Partiamo da **ZTE**, i cui router **MF910** sono finiti sotto la lente di ingrandimento dei ricercatori. Le vulnerabilità individuate in questo caso sono due: la prima (CVE-2019-3411) riguarda un leak di informazioni (la password di amministrazione) mentre la seconda (CVE-2019-3412) consentirebbe di iniettare comandi e, di conseguenza, **avviare l'esecuzione di codice in remoto**.

Quando i dettagli dei bug sono stati comunicati, il produttore ha però deciso di non correggerli. Motivo? Il prodotto sarebbe arrivato "a fine vita". Peccato che, come fanno notare dalle parti di Pen Test Partners, i router M910 sono ancora in vendita su numerosi siti come **Amazon**.

Tanto più che i ricercatori hanno trovato gli stessi problemi anche sul modello MF920, per il quale il supporto è ancora attivo. **Niente da fare: ZTE ha corretto il firmware solo per MF920 e il "vecchio" router rimane vulnerabile**.

L'altro produttore citato nel report è **Netgear**, il cui router **Nighthawk M1** sarebbe affetto da due falle di sicurezza che, ancora una volta, potrebbero portare a un attacco che consentirebbe l'esecuzione di codice in remoto.

Il primo problema riguarda una vulnerabilità (CVE-2019-14526) descritta come un "Cross-Site Request Forgery Protection Bypass" e che consentirebbe di **violare il sistema di protezione attraverso l'uso di un JavaScript inserito in una qualsiasi pagina Web**.

Il secondo, registrato come CVE-2019-14527, è relativo a un bug che consente a qualsiasi utente connesso di eseguire comandi attraverso l'interfaccia Web per la gestione del dispositivo.

In questo caso, spiegano gli analisti di Pen Test Partners, il produttore non ha risposto alla segnalazione inviata 5 mesi

fa.

Insomma: il panorama nel settore dei router 4G è decisamente preoccupante e lo diventa ancora di più in vista del passaggio al 5G, che potrebbe coincidere con un "rilancio" dei router mobili. Se le cose continuano così, ci aspettano tempi duri…

Condividi l'articolo

Attacco ransomware a una fotocamera? Si può fare!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/13/router-4g-a-rischio-attacco-avete-aggiornato-il-firmware/

Attacco ransomware a una fotocamera? Si può fare!

Ago 12, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una serie di falle nel Picture Transfer Protocol ha permesso a un ricercatore di installare un malware su

una Canon EOS 80D DSLR tramite Wi-Fi.

Provate a immaginare di tornare dalle ferie con la vostra fidata fotocamera sottobraccio. Sulla scheda di memoria, qualche centinaio di fotografie che non vedete l'ora di pubblicare sui social dopo la tradizionale post-produzione su PC.

Mentre state guardando gli scatti, però, il display si oscura e compare un messaggio di riscatto. **Nessun guasto: siete stati colpiti da un ransomware**.

Diciamolo subito: non c'è nessun malware di questo tipo in circolazione. Almeno per il momento. Lo scenario, però, è quello descritto dai ricercatori di **Check Point**, che hanno scoperto una serie di bug nel **Picture Transfer Protocol** utilizzato dalle fotocamere Canon per il trasferimento dei file.

CVE-2019-5994 – Buffer Overflow in SendObjectInfo (opcode 0x100C)

CVE-2019-5998 – Buffer Overflow in NotifyBtStatus (opcode

0x91F9)

CVE-2019-5999– Buffer Overflow in BLERequest (opcode 0x914C)

CVE-2019-6000– Buffer Overflow in SendHostInfo (opcode0x91E4)

CVE-2019-6001– Buffer Overflow in SetAdapterBatteryReport (opcode 0x91FD)

CVE-2019-5995 – Silent malicious firmware update

Le vulnerabilità riguardano una serie di comandi e non servono tutte per portare un attacco. La maggior parte di queste consentono di portare l'attacco alla fotocamera quando è connessa via USB a un computer già compromesso. Uno scenario che, sinceramente, non ha tratti sconvolgenti.

L'ultima falla di sicurezza nell'elenco, però, è decisamente più preoccupante. **I ricercatori, infatti, hanno scoperto che esiste la possibilità di avviare un aggiornamento del firmware tramite Wi-Fi senza che sia necessario alcun intervento da parte dell'utente**.

[embedded content]

Di più: nel corso dei loro test, i ricercatori sono riusciti a sfruttare il sistema di crittografia pensato per proteggere i dati del firmware per raggiungere uno scopo diverso: **crittografare le fotografie presenti in memoria e ottenere, di fatto, un ransomware**.

Insomma un pirata informatico potrebbe utilizzare una rete Wi-Fi per portare un attacco che non potrebbe essere individuato in nessun modo e che potrebbe mettere K.O. il dispositivo.

In seguito alla segnalazione di Check Point, Canon ha sviluppato e rilasciato un aggiornamento per le sue fotocamere che corregge le falle di sicurezza. L'aggiornamento, per gli utenti europei, è disponibile a questo indirizzo Internet.

Condividi l’articolo

Varenyky: è arrivato il “trojan a luci rosse”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/12/attacco-ransomware-a-una-fotocamera-si-puo-fare/