Cina: il software per pagare le tasse ha una backdoor. Spionaggio?

Giu 26, 2020 Marco Schiaffino In evidenza, Malware, News 0

Il programma è stato "imposto" a due aziende inglesi dalla banca locale. Secondo i ricercatori GoldenSpy potrebbe essere un classico hacking di stato.

Lo hanno battezzato con il nome di **GoldenSpy** e, da un punto di vista tecnico, è una semplice backdoor come tante altre in circolazione. Ciò che rende unico il (sospetto) malware, però, è il vettore di attacco usato: un software la cui installazione è stata richiesta direttamente da una banca cinese per pagare le tasse locali.

La vicenda, resa pubblica da **Trustwave**, ha come protagoniste due aziende del Regno Unito, che hanno recentemente aperto delle attività in Cina. Secondo quanto si legge nel report pubblicato dalla società di sicurezza, il programma in questione si chiama **Intelligent Tax** ed è prodotto dalla società cinese **Aisino**.

Il software, spiegano i ricercatori, non contiene direttamente il codice malevolo, ma il componente che agisce come backdoor (svm.exe) viene scaricato da un sito cinese circa due ore dopo il completamento dell'installazione di Intelligent Tax.

Nel descrivere il suo comportamento, i ricercatori sono estremamente cauti. In una nota che introduce l'analisi tecnica, infatti, spiegano che potrebbe anche trattarsi di una funzione di aggiornamento implementata in maniera sbagliata. Il dubbio che si tratti di un vero e proprio malware, però, è

decisamente consistente.

Oltre alla curiosa modalità di installazione, le funzionalità di GoldenSpy comprendono infatti la comunicazione a un server di alcune informazioni di base, la possibilità di eseguire codice sul computer e di inviare comandi al sistema operativo. **Insomma: tutto ciò che di solito si trova in un trojan**.

Il componente, inoltre, viene installato in duplice copia come servizio che viene avviato automaticamente e prevede un sistema di riavvio nel caso in cui venisse terminato. Agisce inoltre con privilegi di sistema e adotta una tecnica di collegamento al server a intervalli casuali. **Un accorgimento, sottolineano i ricercatori, che di solito viene adottato per offuscare il traffico tra malware e server Command and Control**.

Al di là dell'aspetto tecnico, l'elemento più rilevante è il fatto che l'uso del software che scarica e installa GoldenSpy è stato proposto alle aziende come "obbligatorio" per poter operare a livello commerciale sul territorio cinese.

Insomma: il dubbio è che si possa trattare non solo di un attacco informatico ai danni di imprese commerciali, ma che si tratti di **una prassi comune** con cui il governo di Pechino si

garantisce la possibilità di hackerare nel modo più semplice possibile le aziende straniere che operano sul suo territorio.

Condividi l’articolo

WatchGuard acquisisce Panda Security: cosa significa?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/26/goldenspy-cina-il-software-per-pagare-le-tasse-ha-una-backdoor-spionaggio/?utm_source=rss&utm_medium=rss&utm_campaign=goldenspy-cina-il-software-per-pagare-le-tasse-ha-una-backdoor-spionaggio

---

WatchGuard acquisisce Panda Security: cosa significa?

Giu 26, 2020 Giancarlo Calzetta Approfondimenti, In evidenza, Mercato 0

Dopo aver manifestato l’intenzione di acquisire Panda Security, WatchGuard ha finalizzato l’operazione all’inizio del mese di giugno. Ma cosa significa questo

consolidamento per le due aziende e per il mercato? Tante opportunità per i rivenditori di entrambe le realtà.

Nel continuo **movimento di consolidamento** che caratterizza il settore della sicurezza informatica, con aziende molto grandi che acquistano start-up o colossi che passano di mano in operazioni multi miliardarie, ci si trova spesso a chiedersi se le cose andranno per il verso giusto o se le sovrapposizioni non rischino di avere conseguenze negative.

> Nel caso di WatchGuard che compra Panda Security, sembra che i rischi siano davvero ridotti al minimo, mentre **le opportunità siano** molte soprattutto per il canale di vendita. Fabrizio Croce, il responsabile Sud Europa di WatchGuard, infatti è **molto positivo su tutta l'operazione** e durante una intervista esclusiva ci ha spiegato passo passo perché.

Innanzitutto, è bene specificare che **l'acquisizione è stata totale**: WatchGuard ha comprato marchio, asset, personale e tecnologie dell'azienda spagnola. Ma perché l'ha fatto?
"Il motivo" – ci dice Fabrizio Croce – "è semplice: con l'acquisizione di Panda Security, WatchGuard va a colmare un gap tecnologico, quello della mancanza di una soluzione end-point EDR completa. Ovviamente, ci portiamo in casa anche altre tecnologie e prodotti che troveremo il modo di mettere a frutto e che faranno bene al nostro portafoglio".

In effetti, l'operazione ha incluso anche la parte consumer di Panda Security, che appartiene a un mercato estraneo all'esperienza WatchGuard, ma che non verrà dismesso.

"La parte consumer" – conferma Croce – "verrà mantenuta

esattamente com’è e gestita dal team di Panda che se n’è occupata in passato. Qui in Italia non c’era neanche una struttura dedicata, quindi per noi cambia poco”.

I team delle due aziende verranno ovviamente consolidati in una struttura unica, ma Croce non vede grandi problemi in quanto la sovrapposizione era molto limitata. Dal momento che **i prodotti di riferimento sono molto diversi e complementari**, non dovrebbero esserci scossoni anche se, ovviamente, tutti faranno capo al country manager italiano di WatchGuard.

All’estero si dovrà lavorare un po’ di più perché Panda ha una presenza diretta su alcuni grandi clienti, ma **in Italia passava già tutto dal canale** e quindi le dinamiche resteranno molto simili a quelle attuali.

Dal punto di vista del mercato, c’è una certa identità di vedute. Entrambe le aziende nel nostro Paese fanno **il grosso del fatturato sulle PMI**, ma il fatto che il portafoglio prodotti sia così diverso **apre delle grandi opportunità al canale**.

“I nostri rivenditori” – spiega Croce – “hanno visto con grande ottimismo questa fusione. Il motivo è che solo il 10% dei rivenditori delle due aziende lavoravano già con i due marchi, mentre gli altri andranno a trovarsi nella posizione di poter proporre ai loro clienti una soluzione più completa e integrata. Questo, di solito, piace molto a chi deve usare i prodotti di sicurezza ed è un vantaggio enorme per noi, tanto che il canale ci sta facendo pressione per uniformare prima

possibile l’offerta e includerla nella nostra piattaforma nativamente”.

Da un punto di vista operativo, i rivenditori WatchGuard possono iniziare praticamente da subito a vendere i prodotti Panda tramite un programma di canale che si chiama Early Access Program. Croce prevede che entro 90 giorni i listini saranno unificati e che per l’inizio del 2021 i prodotti Panda saranno completamente integrati nella piattaforma WatchGuard.

Si vede qualche rischio all’orizzonte per questa operazione che sembra quasi troppo bella per essere vera?
“Di rischi” – dice Croce – “ne vedo davvero pochi perché le due aziende sono davvero complementari. Quello che ci preoccupa un po’ è il COVID che ha segnato profondamente il mercato. Noi siamo in posizione privilegiata e anche nei momenti più difficili arrivavano ordini e richieste mosse dalla trasformazione che le aziende stanno affrontando, ma cosa succederà poi? Sicuramente ci saranno delle conseguenze nel mercato, ma speriamo riesca a recuperare bene. Una preoccupazione secondaria è, invece, quella della fusione delle ‘mentalità’. Panda Security è un’azienda spagnola, molto snella, che sicuramente dovrà affrontare il nodo di integrarsi in un modo di lavorare ‘americano’, fatto di procedure pervasive e super strutturazione. Un bel cambiamento rispetto al modo di lavorare attuale, ma verrà assimilato che col tempo.”

Condividi l’articolo

Cina: il software per pagare le tasse ha una backdoor. Spionaggio? Attenzione a Lucifer: il malware che ne sa una più del diavolo

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/26/watchguard-acquisisce-panda-security-cosa-significa/?utm_source=rss&utm_medium=rss&utm_campaign=watchguard-acquisisce-panda-security-cosa-significa

---

Attenzione a Lucifer: il malware che ne sa una più del diavolo

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

Sfrutta un numero impressionante di vulnerabilità per colpire i sistemi Windows per installare miner di cripto-valuta e portare attacchi DDoS.

I suoi autori lo avevano battezzato **Satan DDoS**, ma i ricercatori di **Unit 42** di **Palo Alto Network** hanno deciso di chiamarlo **Lucifer**. IL motivo? Nei loro database esisteva già un ransomware con il nome di Satan.

Sul fatto che nel nuovo malware ci sia qualcosa di "diabolico", però, nessuno ha dubbi. Lucifer, infatti, ha caratteristiche decisamente uniche. Il primo rilevamento risale alla fine di maggio, quando i ricercatori stavano investigando su un exploit che prendeva di mira una

vulnerabilità specifica (CVE-2019-9081) nel framework **Lavarel**.

Quando hanno cominciato ad analizzare il malware, però, si sono resi conto di avere a che fare con qualcosa di estremamente versatile e pericoloso. Lucifer, infatti, per la sua attività sfrutta un arsenale di exploit (i ricercatori ne elencano un'altra decina) davvero impressionante, che varia da falle di sicurezza di **PHP** a exploit conosciuti del sistema Microsoft.

Tra questi, anche i famigerati **EternalBlue**, **EternalRomance** e **DoublePulsar**, che Lucifer utilizza per infettare altre macchine all'interno della rete locale, utilizzando anche tecniche di **brute forcing**.

L'obiettivo del malware, spiegano in un corposo report, è quello di installare **XMRig**, un miner in grado di sfruttare la potenza di calcolo della macchina infetta per generare **Monero**. Non solo: Lucifer contiene anche un modulo dedicato che consente di portare attacchi DDoS e un collegamento a un server **Command and Control** attraverso l quale può eseguire altre azioni.

Insomma: il quadro che ne emerge è estremamente complesso e, anche se per la sua diffusione fa leva su vulnerabilità per le

quali sono disponibili patch di correzione, è in grado di diffondersi con impressionante facilità.

Il motivo di questa efficacia è probabilmente legato al fatto che le falle di sicurezza che sfrutta riguardano un elevato numero di software, tra cui **Rejetto HTTP File Server**, **Jenkins**, **Oracle Weblogic**, **Drupal**, **Apache Struts**, **Laravel** e (ovviamente) **Microsoft Windows**.

Insomma: la scommessa degli autori di Lucifer e che, da qualche parte, qualcuno si sia dimenticato di applicare una patch. E di solito, a quanto pare, hanno ragione.

Condividi l’articolo

WatchGuard acquisisce Panda Security: cosa significa?
Microsoft cerca di frenare i malware nei documenti Office

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/25/attenzione-a-lucifer-il-malware-che-ne-sa-una-piu-del-diavolo/?utm_source=rss&utm_medium=rss&utm_campaign=attenzione-a-lucifer-il-malware-che-ne-sa-una-piu-del-diavolo

---

Microsoft cerca di frenare i

malware nei documenti Office

Giu 24, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Tecnologia 0

La nuova funzione si chiama Documenti Attendibili e dovrebbe consentire di ridurre il rischio di attacchi portati sfruttando i contenuti attivi.

Niente da fare: dopo più di 20 anni, i documenti **Office** rimangono uno dei vettori di attacco più utilizzati dai pirati informatici e, stando alle statistiche delle società di sicurezza, anche i più efficaci.

Microsoft, dopo aver introdotto nel corso del tempo modifiche di vario genere per mitigare il rischio di questa tipologia di attacchi, adesso prova un approccio diverso offrendo una nuova funzione nel suo pacchetto **Office 365**.

Si chiama **Documenti Attendibili** (**Safe Documents** nella versione inglese) e, in pratica, introduce un altro livello di controllo alla procedura di apertura dei file che hanno una provenienza potenzialmente sospetta.

Per la verità Office riserva già un trattamento particolare a tutti i documenti che provengono da Internet, come quelli allegati ai messaggi di posta elettronica. I file vengono aperti in **Visualizzazione Protetta**, cioè in una modalità "solo lettura". L'accesso completo per la modifica richiede una ulteriore conferma da parte dell'utente.

La logica di questo passaggio è legata al fatto che, in visualizzazione protetta, eventuali exploit contenuti nel documento non possono attivarsi.

Con Documenti Attendibili, la strategia si arricchisce di un

ulteriore passaggio: il file viene aperto in visualizzazione protetta e, contemporaneamente, viene inviato al software di protezione **Microsoft Defender Advanced Threat Protection** (ATP) per un controllo approfondito.

Solo una volta verificata l’assenza di codice malevolo, il software propone la possibilità di abilitare la modifica del file.

La funzionalità, che ha superato una fase di rodaggio avviata nel febbraio scorso, è adesso disponibile per (quasi) tutti. Documenti Attendibili, infatti, è integrata nel pacchetto **Office 365 E5**, la versione più “accessoriata” (e costosa) del prodotto Microsoft.

Per impostazione predefinita, però, la funzione è disabilitata. Sarà quindi compito degli amministratori di sistema impostarne il funzionamento in modo che si attivi.

Condividi l’articolo

BlueLeaks: Anonymous negli USA “buca” i sistemi di polizia e FBI

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/06/24/office-documenti-attendibili/?utm_source=rss&utm_medium=rss&utm_campaign=office-documenti-attendibili

BlueLeaks: Anonymous negli USA “buca” i sistemi di polizia e FBI

Giu 23, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, News, RSS 0

Dietro le quinte del clamoroso leak che ha reso pubblici i dati provenienti dai sistemi delle forze di polizia USA c’è un attacco a un’azienda privata.

Un vero terremoto che rischia di avere ripercussioni pesantissime sull’attività delle forze di polizia locali e

federali negli Stati Uniti. È stato battezzato con il nome di **BluLeaks** e, secondo le prime ricostruzioni, sarebbe il frutto di un attacco informatico condotto da membri di **Anonymous** ai danni di un'azienda texana.

Il materiale, composto da 269GB di documenti provenienti da oltre 200 enti tra commissariati di polizia e agenzie federali, è stato consegnato dagli hacker a **DDoSecret** (**Distributed Denial of Secret**), un sito che opera con la stessa logica di **WikiLeaks** e che ha pubblicato i dati in una pagina Web in cui è possibile consultarli attraverso un sistema di ricerca.

L'enorme mole di documenti coprirebbe **24 anni di attività di polizia e FBI**, comprese informazioni riservate (ci sarebbero circa 3.000 file classificati **Top Secret**) che comprenderebbero informazioni sensibili come indirizzi email, numeri di telefono e addirittura gli IBAN di alcuni soggetti coinvolti nelle indagini.

Se a livello di opinione pubblica l'attenzione si sta concentrando sui contenuti del leak, soprattutto per quanto riguarda le comunicazioni interne della polizia in merito alle recenti proteste antirazziste sul territorio statunitense, sono ancora pochi i dettagli riguardo le modalità con cui gli Anonymous sono entrati in possesso dei dati.

> *If you're trying to download #BlueLeaks, please make sure you're using the most recent version of the torrent at https://t.co/XMEguCpIPH https://t.co/die52NK2yA*
>
> *— Distributed Denial of Secrets (@DDoSecrets) June 23, 2020*

Tutto il materiale sembrerebbe provenire dai cosiddetti **fusion center**, una sorta di hub telematico creato dall'amministrazione statunitense in chiave anti-terroristica dopo gli eventi dell'11 settembre 2001.

Il network, che mette in comunicazione le forze di polizia locali con le agenzie federali, è pensato per consentire la condivisione di informazioni sulle potenziali minacce alla sicurezza nazionale e funziona come una sorta di strato di coordinamento tra i vari soggetti coinvolti.

L'ipotesi più credibile è che gli hacker di Anonymous siano riusciti a ottenere i dati colpendo l'anello debole della catena, cioè l'azienda privata che ha sviluppato il software sui cui "gira" il sistema dei fusion center. Si tratta di **Netsential**, azienda di sviluppo software con sede a Houston, in Texas.

Non proprio un player di prima grandezza, come si può intuire dal (modesto) sito Web di rappresentanza, nel quale tra l'altro non è presente nemmeno una sezione dedicata ai comunicati stampa. Il quadro che si prospetta, però, è quello di un classico attacco **supply chain**, che ha permesso agli hacktivist di mettere a segno un colpo davvero clamoroso.

Condividi l'articolo

Microsoft cerca di frenare i malware nei documenti Office Debellato il ransomware? Non basta…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/23/blueleaks-anonymous-negli-usa-buca-i-sistemi-informatici-di-polizia-e-fbi/?utm_source=rss&utm_medium=rss&utm_campaign=blueleaks-anonymous-negli-usa-buca-i-sistemi-informatici-di-polizia-e-fbi

Debellato il ransomware? Non basta…

Giu 22, 2020 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

I pirati informatici, oltre al malware principale, installano invariabilmente backdoor e altri strumenti per garantirsi una presenza nella rete.

Ricorda un po' il detto riguardante il dito e la luna, ma secondo gli esperti di sicurezza i recenti attacchi portati dal gruppo **Maze** potrebbero rappresentare una scossa in grado di convincere le aziende a un approccio più "saggio" nel caso in cui si verifichino attacchi ransomware.

Il tema, come spiega **Lawrence Abrams** su **Bleeping Computer**, è quello del rischio che il malware rappresenti solo la punta dell'iceberg. In molti casi, però, le aziende che vengono colpite commettono l'errore di considerare l'incidente chiuso una volta rimosso il ransomware, senza approfondire in maniera adeguata l'incidente.

Le ultime notizie di cronaca riguardanti i pirati di **Maze** (ne abbiamo parlato in questo articolo) dimostrano però quanto sia pericoloso un atteggiamento del genere. **Il loro modus operandi, che prevede il furto di dati oltre all'installazione del ransomware, dimostra che l'estorsione legata alla codifica dei file è solo uno dei problemi**.

L’equivoco, probabilmente, è legato alla similitudine con gli attacchi ransomware che prendono di mira i privati cittadini, in cui il vettore di infezione è spesso rappresentato da un file allegato a un messaggio di posta elettronica. Insomma: qualcosa che potremmo definire come un “incidente isolato”.

I cyber criminali che colpiscono le aziende, invece, agiscono seguendo una strategia attentamente pianificata che prevede, come prima mossa, la violazione dei sistemi aziendali e un’attività di movimento laterale che gli permette di ottenere l’accesso a tutte le risorse critiche.

Nella logica di un cyber criminale, infatti, un attacco con un ransomware è lo stadio finale di un’attività che può essere stata portata avanti per giorni, settimane o addirittura mesi.

Anche una volta rimosso il ransomware e recuperati i file, il rischio che i pirati abbiano ancora accesso a singoli dispositivi o all’intera rete aziendale è quindi elevatissimo. Ciò che è necessario, quindi, è fare un controllo accurato e una sorta di operazione di “bonifica” che metta al riparo i sistemi da ulteriori attacchi.

Non solo: l’analisi dei sistemi può consentire di individuare eventuali furti di dati che erano precedentemente passati inosservati.

Condividi l’articolo

InvisiMole: ecco come agiscono i professionisti del cyber-spionaggio

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/22/debellato-il-ransomware-non-basta/?utm_source=rss&utm_medium=rss&utm_campaign=debellato-il-ransomware-non-basta

---

InvisiMole: ecco come agiscono i professionisti del cyber-spionaggio

Giu 19, 2020 Marco Schiaffino In evidenza, Malware, Minacce, News, RSS 0

Lo studio di ESET analizza in profondità il modus operandi del gruppo, mettendo in luce la collaborazione con un’altra gang di pirati.

Sono conosciuti dal 2013, ma solo nelle ultime settimane i ricercatori di ESET sono riusciti a comprendere fino in fondo

le tecniche che usano. Dei cyber-spioni di **InvisiMole** (che suona come “talpa invisibile”) si sapeva solo che utilizzassero backdoor piuttosto sofisticate e che fossero specializzati nello spionaggio diretto a bersagli che operano nel settore diplomatico e militare in Europa orientale.

Ora, con un dettagliato report, i ricercatori di ESET hanno descritto le tecniche utilizzate dagli hacker per nascondere la loro presenza, muoversi all’interno delle reti compromesse e installare i loro strumenti di spionaggio. Di più: dallo studio emerge anche il fatto che InvisiMole collabora con un altro gruppo chiamato **Gamaredon**.

Il rapporto tra i due soggetti, secondo gli analisti, è una sorta di sinergia ispirata dall’opportunismo. I membri di Gamaredon utilizzano tecniche di attacco e malware piuttosto comuni, ma quando riescono a infiltrarsi in una rete che risulta essere particolarmente interessante, cedono il passo a InvisiMole, che sfrutta la breccia creata dai “colleghi” per installare i suoi strumenti di spionaggio.

In pratica i pirati di InvisiMole entrano in campo quando “il gioco si fa duro” per sfruttare al massimo l’opportunità creata dai loro gregari.

Nel report pubblicato da ESET sul suo sito Internet, emerge come l’arsenale di InvisMole utilizzi delle tecniche di offuscamento estremamente sofisticate. I pirati informatici utilizzano infatti un sistema che riduce le probabilità che i loro malware siano analizzati, attraverso un particolare sistema di crittografia che sfrutta la funzione **Data Protection API** di Windows, utilizzata per la memorizzazione di credenziali “sensibili” all’interno del sistema operativo.

In pratica, il codice del malware viene codificato utilizzando un sistema di crittografia simmetrica direttamente sul computer della vittima e può essere decrittato ed eseguito solo su quel computer.

Una tecnica, questa, che impedisce di decodificare e studiare il malware in altri ambienti e che permette quindi ai pirati di InvisiMole di eludere la maggior parte dei controlli, come quelli eseguiti nelle sandbox.

Il malware, inoltre, utilizza vari sistemi di comunicazione verso i server controllati dai pirati informatici, tra cui uno che sfrutta il sistema DNS e che permette loro di inviare e ricevere informazioni senza allertare i sistemi di controllo.

Non solo: i pirati utilizzano un formato eseguibile personalizzato, che i ricercatori hanno battezzato con il nome di “blob”, grazie al quale riescono a offuscare ulteriormente il codice dei loro strumenti di spionaggio.

La punta di diamante del loro arsenale informatico è però una backdoor chiamata **RC2CL**, le cui funzionalità sono descritte in un report precedente pubblicato da ESET e di cui abbiamo parlato in questo articolo.

Per colpire le altre macchine all’interno del network, i

pirati di InvisiMole utilizzano una serie di exploit derivati direttamente o indirettamente dal celebre leak degli **Shadow Brokers**, che conteneva una serie di vulnerabilità utilizzate dai servizi segreti statunitensi, come **EternalBlue** e **DoublePulsar**. On è escluso, però, che queste tecniche siano state utilizzate solo per un breve periodo di tempo e che ora vengano utilizzati nuovi strumenti che sfruttano exploit più aggiornati.

Insomma: il quadro complessivo è quello di un gruppo dedito al cyber spionaggio con caratteristiche di professionalità e la disponibilità di strumenti estremamente complessi.

Condividi l’articolo

Operation In(ter)ception: anatomia di un attacco mirato

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/19/invisimole-ecco-come-agiscono-i-professionisti-del-cyber-spionaggio/?utm_source=rss&utm_medium=rss&utm_campaign=invisimole-ecco-come-agiscono-i-professionisti-del-cyber-spionaggio

---

Operation In(ter)ception:

anatomia di un attacco mirato

Giu 18, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La campagna ha preso di mira bersagli in Europa e in Medioriente. Ecco come agiscono i cyber-spioni che collaborano con i governi stranieri.

Il modus operandi dei gruppi **APT (Advanced Persistent Threat)** è qualcosa che, per gli appassionati di cyber security, rappresenta un elemento di sicuro interesse. A differenza dei loro colleghi attivi nel settore della "semplice" criminalità informatica, infatti, adottano tecniche estremamente elaborate.

Il caso legato alla **Operation In(ter)ception** conferma la tendenza e rappresenta un cristallino esempio di attacco informatico che segue un'attenta pianificazione strutturata in più fasi.

Come raccontano i ricercatori di **ESET** in un rapporto che descrive le modalità utilizzate dai pirati informatici, l'attacco utilizza come vettore iniziale un messaggio apparentemente collegato a LinkedIn.

Nel caso specifico, gli hacker hanno preso di mira professionisti operanti nel settore aerospaziale impiegati in varie aziende europee e mediorientali, inviando loro una (falsa) proposta di assunzione apparentemente proveniente da un dirigente di **Collins Aerospace**, un'azienda piuttosto conosciuta nel settore.

Il messaggio serve come esca iniziale, che consente ai pirati di stabilire una corrispondenza con la potenziale vittima. Nel prosieguo dell’attacco, i pirati intavolano una vera e propria trattativa in cui inducono la vittima a credere di essere oggetto del loro interesse per un’assunzione.

Il colpo di grazia arriva al momento dell’invio della proposta economica: il file che contiene lo stipendio prospettato per l’assunzione viene infatti inviato attraverso un archivio compresso in formato **RAR** che contiene un documento **LNK**.

Quando il contenuto viene aperto, sul computer della vittima viene visualizzato un documento PDF con un contenuto del tutto normale. Dietro le quinte, però, sta accadendo ben altro: l'apertura avvia infatti l'esecuzione di un **Command Prompt** che pianifica l'avvio in remoto di uno **script XML**.

L'obiettivo dei pirati, secondo i ricercatori, sarebbe quello di ottenere informazioni sulle credenziali di rete in prospettiva di portare attacchi di brute forcing per comprometterle. Insomma: si tratterebbe di un classico attacco di phishing che punta a garantire un punto di accesso e permetter un conseguente movimento laterale all'interno della rete.

L'analisi del malware, per quanto riguarda l'attribuzione, evidenzierebbe alcune similitudini con il gruppo Lazarus (connesso al governo della Nord Corea) ma, nel report, i ricercatori non si sbilanciano più di tanto. Quello che è certo è che In(ter)ception è un'operazione di alto livello che rientra a pieno titolo nella categoria dello spionaggio di stato.

Condividi l'articolo

Ripple20: ecco le vulnerabilità che fanno tremare il mondo IoT

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/18/operation-interception-anoatomia-di-un-attacco-mirato/?utm_source=rss&utm_medium=rss&utm_campaign=operation-interception-anoatomia-di-un-attacco-mirato

Ripple20: ecco le vulnerabilità che fanno tremare il mondo IoT

Giu 17, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le 19 falle di sicurezza derivano dall'uso di una libreria sviluppata negli anni '90 e mettono a rischio centinaia di milioni di dispositivi.

Non c'è pace per il mondo della **Internet of Things**. Se la sensibilità per una migliore gestione della sicurezza a livello di gestione (ma soprattutto di progettazione) sta crescendo, continuano a emergere problemi e vulnerabilità che impattano in maniera devastante sui dispositivi **IoT**.

L'allarme arriva ora da **JSOF**, che in una pagina Web dedicata illustra un "pacchetto" di 19 falle di sicurezza scoperte in una libreria software utilizzata da milioni di device. Lo hanno battezzato **Ripple20** e rischia di andare a ingrossare l'arsenale dei pirati informatici specializzati negli attacchi ai dispositivi IoT.

Il componente software in questione è stato sviluppato da **Treck** nel 1996 e consente l'utilizzo di comunicazioni su protocollo TCP/IP. La libreria è stata utilizzata per fornire una connessione Internet a un'ampia gamma di prodotti, che dalle parti di JSOF stimano in **centinaia di milioni**.

Ora, però, tutti questi dispositivi si trovano a fare i conti

con una raffica di vulnerabilità che, se sfruttate dai cyber-criminali, potrebbero trasformarsi in un vero disastro.

Tra le vulnerabilità scoperte (ma i ricercatori specificano che si tratta solo delle prime di una potenziale lunga serie) ce ne sono alcune decisamente gravi.

La prima (CVE-2020-11896) riguarda un problema nella gestione del componente IPv4/UDP e consentirebbe di avviare l'esecuzione di codice in remoto, con la possibilità di installare un malware. Stesso rischio per una falla in IPv6 (CVE-2020-11897) che consentirebbe la scrittura arbitraria di dati.

Tra le vulnerabilità che possono essere sfruttate da eventuali pirati ce n'è anche una che riguarda il componente IPv4/ICMPv4 della libreria (CVE-2020-11898) e che potrebbe portare al rilascio di informazioni sensibili. Stesse conseguenze per un problema di validazione di input del componente IPv6.

Insomma: quello a cui potremmo assistere è un vero tsunami di attacchi basati su Ripple20. Con un elemento ancora più inquietante. Dal momento che la libreria si colloca all'interno di una filiera piuttosto "lunga", gli stessi sviluppatori di Treck non hanno idea di quante e quali implementazioni abbia avuto la libreria.

I ricercatori consigliano a tutti i produttori di contattare Treck per ottenere gli aggiornamenti della libreria in questione. Nel loro report, però, segnalano che l'update potrebbe non essere possibile.

Per gli utenti, invece, l'unica soluzione è quella di attendere gli aggiornamenti dei singoli prodotti (sperando che arrivino) e, se possibile, mitigare il rischio impostando dei filtri alla rete. Guardando al panorama degli utilizzatori non professionali, insomma, non resta che incrociare le dita.

Condividi l'articolo

I problemi di sicurezza del 5G arrivano dal passato

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/17/ripple20-ecco-le-vulnerabilita-che-fanno-tremare-il-mondo-iot/?utm_source=rss&utm_medium=rss&utm_campaign=ripple20-ecco-le-vulnerabilita-che-fanno-tremare-il-mondo-iot

---

I problemi di sicurezza del 5G arrivano dal passato

Giu 16, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia, Vulnerabilità 0

La nuova rete “eredita” bug e difetti del protocollo GTP, ideato per il GPRS. Possibili problemi a livello di continuità di servizio e abusi.

Alla fine, il problema più grosso per il **5G** sotto il profilo della sicurezza potrebbe non riguardare le possibili (e presunte) violazioni dei dati da parte di **Huawei**. Secondo molti ricercatori, sarebbe meglio concentrare l’attenzione sulle vulnerabilità a livello di protocollo che derivano da vecchi sistemi di trasmissione.

L’indiziato numero uno è **GTP** (**GPRS Tunnelling Protocol**), un sistema ideato per creare collegamenti tra dispositivi e le diversi reti sfruttando un sistema basato su IP.

Come spiegano in un corposo report i ricercatori di **Positive Technologies**, il protocollo ha una serie di problemi che potrebbero portare ad attacchi Denial of Service, al furto di informazioni sensibili (come la posizione geografica) e alla falsificazione dei dati relativi al mittente di messaggi SMS o MMS.

Ciò che manca in GTP oltre alla protezione crittografica, infatti, è un sistema efficace per l’autenticazione dei dispositivi che si collegano. D’altra parte, il protocollo è stato sviluppato in un’era in cui il GPRS (2.5G) rappresentava una novità e l’utilizzo di Internet da dispositivi mobili era ancora un fenomeno di nicchia.

La conseguenza, però, è che chiunque può sfruttare questa mancanza per inviare pacchetti con dati falsificati, ad esempio per impersonare un altro dispositivo.

Il supporto per GTP all’interno del nuovo 5G, però, viene spesso mantenuto. La nuova rete, infatti, deve garantire la retrocompatibilità e di dispositivi che usano ancora GTP ce ne sono in circolazione parecchi.

Lo studio di Positive Technologies, effettuato nel 2018 e 2019 analizzando le infrastrutture di diversi operatori che gestiscono reti 4G e 5G, lo conferma.

Quali sono le possibili soluzioni? I ricercatori ne elencano alcune, ma nessuna sembra essere risolutiva. L’uso di white list che limitino la possibilità di connettersi a chi è cliente del provider, per esempio, lascia una falla legata alla possibilità che un pirata informatico utilizzi un dispositivo che ha violato attraverso un attacco informatico.

Il problema, in definitiva, richiede un’approfondita analisi del protocollo GTP e lo sviluppo di soluzioni di sicurezza su misura in grado di contrastare ogni specifica modalità di attacco. Insomma: in vista dell’era del 5G c’è ancora parecchio da fare.

Condividi l’articolo

Database ElasticSearch (ancora) nel mirino dei pirati

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/06/16/i-problemi-di-sicurezza-del-5g-arrivano-dal-passato/?utm_source=rss&utm_medium=rss&utm_campaign=i-problemi-di-sicurezza-del-5g-arrivano-dal-passato