Microsoft sbaglia la patch: lo zero-day è ancora una minaccia

Dic 28, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità consente di elevare i privilegi di amministrazione per avviare l'esecuzione di codice a livello kernel o creare utenti con privilegi di amministratore.

Avrebbe dovuto essere corretta a giugno, ma la patch per la vulnerabilità che affligge Windows (CVE-2020-0986) non ha ottenuto i risultati sperati.

Il bug, che interessa l'**API Print Spooler**, ha un livello di impatto piuttosto elevato (8.3 su 10) e rappresenta il classico strumento di cui i pirati informatici possono avvantaggiarsi quando riescono a introdursi nei sistemi aziendali.

Per sfruttare la vulnerabilità, è bene chiarirlo, è necessario avere già accesso a un dispositivo. Sfruttando la falla di sicurezza, però, è possibile eseguire un salto di qualità **acquisendo privilegi elevati e ottenere così una libertà d'azione maggiore rispetto a quella originale**.

Come spiegano i ricercatori di Trend Micro in un report pubblicato sul blog della società di sicurezza, la vulnerabilità è stata segnalata alla fine dell'anno scorso e, almeno in teoria, avrebbe dovuto essere corretta con l'update per Windows rilasciato lo scorso giugno.

Le cose, però, non sembrano essere andate per il verso giusto. L’aggiornamento messo a puto dagli sviluppatori di Microsoft, infatti, non ha risolto il problema e la falla di sicurezza può ancora essere sfruttata dai pirati per i loro scopi.

I ricercatori hanno contattato l’azienda per segnalare il mancato fix lo scorso settembre, assegnando **un termine di 90 giorni per risolvere il problema**. A oggi, però, dalle parti di Microsoft si sono limitati ad assegnare al bug un nuovo codice (CVE-2020-17008) prospettando il rilascio di un aggiornamento per il prossimo gennaio. Motivo per cui, i ricercatori di Trend Micro hanno reso (di nuovo) pubblica la vulnerabilità.

A questo punto, le aziende hanno un’unica soluzione: adottare politiche di mitigazione che prevedono una restrizione dei livelli di interazione con il servizio.

Condividi l’articolo

Finlandia: hacker colpiscono il parlamento Europol e Dipartimento di Giustizia USA “abbattono” tre servizi VPN

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/12/28/microsoft-sbaglia-la-patch-lo-zero-day-e-ancora-una-minaccia/?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-sbaglia-la-patch-lo-zero-day-e-ancora-una-minaccia

Europol e Dipartimento di Giustizia USA “abbattono” tre servizi VPN

Dic 23, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

I servizi sarebbero stati utilizzati per coprire le tracce di vari gruppi di pirati informatici autori di cyber attacchi in tutto il mondo.

La notizia, per come è stata veicolata dagli uffici stampa di Europol e Dipartimento di Giustizia USA, sembrerebbe il classico riassunto di un’operazione contro il cyber crimine. In realtà, le caratteristiche di quella che è stata battezzata

“Operation Nova” la collocano in un’area grigia in cui le ombre sembrano essere predominanti rispetto alle luci.

La fredda cronaca parla di un’operazione che ha portato al sequestro (e blocco) di tre servizi VPN. Si tratta, nel dettaglio, di **insorg.org**, **safe-inet.com** e **safe-inet.net**. Soggetti che fornivano funzionalità di Virtual Private Network (i sistemi che consentono di utilizzare una connessione crittografata non tracciabile – ndr) a livello mondiale.

La vicenda, però apre un tema piuttosto spinoso per quanto riguarda l’erogazione di servizi per la navigazione anonima su Internet.

Stando a quanto si legge nei comunicati pubblicati da Europol (qui il testo completo) e dal Dipartimento di Giustizia USA (qui il testo completo), il sequestro dei tre servizi VPN sarebbe stato motivato dal fatto che questi sarebbero stati usati da **numerosi gruppi di cyber criminali per coprire le tracce delle loro attività**.

In particolare, le autorità statunitensi descrivono i fornitori di connessioni protette come servizi “bulletproof”,

servizi cioè che sarebbero stati ideati con il preciso obiettivo di fornire funzionalità di hosting o di VPN per attività criminali.

Insomma: il sequestro dei servizi sarebbe dovuto al fatto che si tratterebbe di attività funzionali al cyber crimine. In assenza di maggiori dettagli (nei comunicati non vengono forniti) l'operazione solleva però rilevanti perplessità sia a livello giuridico, sia a livello logico.

I gestori dei servizi in questione, infatti, non sarebbero stati accusati di alcun reato. Il sequestro, di conseguenza, non sarebbe giustificato da un'attività illecita "diretta" ma dal fatto che garantissero un livello di riservatezza tale da poter essere sfruttato (anche) da gruppi di cyber criminali.

Un precedente inquietante, che si colloca in uno scenario in cui le autorità sembrano essere sempre meno tolleranti nei confronti di chi offre servizi di anonimizzazione della navigazione su Internet e delle stesse tecnologie che consentono comunicazioni riservate (i protocolli di crittografia ed to end) su piattaforme digitali.

Condividi l'articolo

Arrestato per truffa l'amministratore di BITGRAIL. "Rubati 120 milioni"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/23/europol-e-dipartimento-di-giustizia-usa-abbattono-tre-servizi-vpn/?utm_source=rss&utm_medium=rss&utm_campaign=europol-e-

dipartimento-di-giustizia-usa-abbattono-tre-servizi-vpn

Arrestato per truffa l'amministratore di BITGRAIL. "Rubati 120 milioni"

Dic 22, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, News, RSS 0

L'imprenditore fiorentino gestiva l'exchange con 230.000 utenti. I fondi sottratti ai portafogli XRB NANO erano stati dirottati su conti correnti esteri.

Una delle più grandi cyber-truffe mai scoperte ha come protagonista un esperto di informatica italiano, che secondo la **Polizia Postale di Firenze** avrebbe architettato un sistema per sottrarre sistematicamente fondi dall'exchange di criptovalute **BITGRAIL**, che lui stesso gestiva fino al fallimento nel gennaio del 2019.

Come si legge nel comunicato stampa pubblicato dal **Commissariato di PS Online**, la vicenda è partita a causa della denuncia dello stesso indagato (indicato semplicemente come "F.F.") in qualità di amministratore unico di BITGRAIL.

Il trentaquattrenne fiorentino lamentava un furto ai danni della piattaforma di una somma pari a 120 milioni di euro, che sarebbero stati sottratti sfruttando un bug della piattaforma NANO (ex XRB). Nel corso delle indagini, però, gli investigatori hanno scoperto che lo stesso amministratore della piattaforma era coinvolto nella truffa.

La Polizia Postale, infatti, avrebbe accertato che F.F. avrebbe volontariamente lasciato “scoperta” la piattaforma, evitando di installare gli aggiornamenti pubblicati dal **Team Nano Developers** per correggere la falla di sicurezza.

I risultati delle indagini, condotte in collaborazione con l’FBI e del Servizio Polizia Postale e delle Comunicazioni di Roma, configurano uno schema in cui lo stesso gestore avrebbe in pratica consentito agli hacker di sfruttare il bug per distrarre i fondi di 230.000 utenti. **In totale le somme rubate ammonterebbero a 11.500.000 XRB, equivalenti a circa 120.000.000 di euro**.

A confermare i sospetti su F.F., però, sarebbero state alcune operazioni da lui compiute solo tre giorni prima di presentare la denuncia. Il gestore di BITGRAIL, infatti, avrebbe trasferito su un suo conto personale 230 Bitcoin (per un valore di circa 1,7 milioni di euro) da alcuni conti della piattaforma, cercando poi di svuotare il conto convertendoli in moneta corrente.

Un tentativo bloccato dalla magistratura, che ha sequestrato il denaro e bloccato i conti della piattaforma di criptovalute prima di procedere al fermo del sospetto. **L’uomo è adesso**

accusato di frode informatica, auto-riciclaggio e bancarotta fraudolenta.

L’operazione della Polizia Postale ha consentito, infine, di sequestrare una quantità di beni dell’indagato che coprono l’esposizione debitoria (120 milioni di euro) nei confronti degli utenti truffati.

Condividi l’articolo

Attacco ai giornalisti di Al Jazeera con uno zero-day per iOS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/22/arrestato-per-truffa-lamministratore-di-bitgrail-rubati-120-milioni/?utm_source=rss&utm_medium=rss&utm_campaign=arrestato-per-truffa-lamministratore-di-bitgrail-rubati-120-milioni

---

Attacco ai giornalisti di Al Jazeera con uno zero-day per iOS

Dic 21, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, Privacy, RSS, Vulnerabilità 0

I reporter sono stati infettati con Pegasus, il trojan sviluppato da NSO Group. La denuncia di Citizen Lab: "è spionaggio di stato".

Hanno usato un exploit zero-day in grado di colpire i sistemi iOS, prendendo di mira giornalisti, produttori e collaboratori della sede londinese di **Al Jazeera**. Secondo quanto si legge nel report pubblicato da **Citizen Lab**, gli attacchi sarebbero avvenuti lo scorso luglio 2020.

Stando a quanto si legge nel documento, i soggetti coinvolti sarebbero almeno 36. Buona parte di questi avrebbero chiesto di mantenere l'anonimato, mentre due di loro, entrambi giornalisti, hanno accettato di rendere pubblici i dettagli degli attacchi che hanno subito.

Il vettore di attacco utilizzato, spiegano gli esperti di sicurezza legati a Citizen Lab, avrebbe sfruttato **un exploit zero-day per iOS**, che prende di mira **iMessage**.

Non è la prima volta che il servizio di messaggistica Apple offre il fianco ad attacchi di questo tipo, a causa di una particolare (errata) implementazione della sandbox che isola l'applicazione dal resto del sistema.

Nel caso specifico, l'attacco avrebbe sfruttato una catena di exploit chiamata in gergo **Kismet**. Secondo i ricercatori dell'Università di Toronto, lo strumento di hacking farebbe parte dell'arsenale a disposizione di **NSO Group**, la società israeliana specializzata in cyber spionaggio e finita spesso al centro di polemiche per aver fornito i suoi tool a governi che li utilizzano per controllare attivisti per i diritti umani, oppositori politici e, appunto, giornalisti.

Nel caso specifico, l'attacco all'emittente con sede in **Qatar** coinvolgerebbe alcuni dei paesi dell'area mediorientale. In particolare, i ricercatori avrebbero individuato due "operatori" (**Monarchy** e **Sneaky Kestrel**) collegati, rispettivamente, al governo dell'**Arabia Saudita** e a quello degli **Emirati Arabi Uniti**.

Il payload distribuito attraverso l'attacco, che consente **l'esecuzione di codice senza che sia necessaria alcuna forma di interazione da parte dell'utente**, sarebbe il solito **Pegasus**, il trojan prodotto da NSO Group che permette di accedere a tutte le informazioni memorizzate sul dispositivo, tracciarne la posizione e utilizzare il microfono per spiare le vittime a loro insaputa.

Stando a quanto si legge nel report, la tecnica di attacco con Kismet avrebbe permesso di colpire anche i modelli di iPhone più recenti. **Le vulnerabilità che sfrutta, infatti, sono state corrette soltanto con l'aggiornamento iOS alla versione 14, rilasciata nel settembre 2020**.

Condividi l'articolo

Sophos: puntiamo sull'Intelligenza Artificiale "aperta"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/21/attacco-ai-giornalisti-

di-al-jazeera-con-uno-zero-day-per-ios/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-ai-giornalisti-di-al-jazeera-con-uno-zero-day-per-ios

---

Sophos: puntiamo sull'Intelligenza Artificiale "aperta"

Dic 18, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia 0

L'iniziativa della società di sicurezza mira a creare una maggiore "apertura" nel settore dell'AI per favorirne la diffusione nella cyber security.

Già adottata largamente in molti strumenti di rilevamento e analisi, l'Intelligenza Artificiale (AI) ha però ampi margini di miglioramento e possibilità di ulteriore sviluppo. Secondo **Sophos**, il percorso più efficace per facilitarne la crescita è quella di affidarsi alla logica "open".

Il progetto è stato battezzato **SophosAI** e prevede la "messa in comune" di una serie di strumenti e risorse sviluppati dalla società di sicurezza.

Il primo di questi si chiama **SOREL-20M** ed è il frutto di un progetto congiunto tra SophoAI e **ReversingLabs**. SI tratta di un dataset production-scale contenente metadati, etichette e caratteristiche per 20 milioni di file Windows Portable Executable (PE).

Il dataset comprende **10 milioni di campioni di malware**,

precedentemente resi innocui, disponibili per il download al fine di supportare l’analisi delle funzionalità e migliorare così la sicurezza in tutto il settore.

Gli altri tre progetti incorporati nell’iniziativa non comprendono semplici collezioni di dati, ma metodologie specifiche basate sull’AI, che la società di sicurezza ha reso pubbliche.

Particolarmente attuale, **Impersonation Protection** ha come obiettivo quello di individuare le cosiddette **BEC (Business Email Compromise)**, cioè le truffe rivolte alle aziende che puntano a dirottare pagamenti legittimi su conti correnti controllati dai pirati informatici.

Altrettanto incisiva l’iniziativa che mette a disposizione di tutti la **Signature Generation YaraML**, un sistema di elaborazione delle signature basato su AI che permette di ridurre notevolmente i tempi per elaborare le definizioni utilizzate nel rilevamento dei malware.

Il quartetto è completato da una nuova metodologia che sfrutta

le logiche dell'emidemiologia per l'analisi dei malware e che Sophos ha messo in comune con il mondo della cyber security per consentire di sfruttarne le caratteristiche a livello globale.

"Con la nuova iniziativa di SophosAI, possiamo contribuire a influenzare il modo in cui l'IA è posizionata e discussa nell'ambito della sicurezza informatica. Al giorno d'oggi il numero sempre crescente di affermazioni discordanti sulle capacità o sull'efficacia dell'IA rende difficile o addirittura impossibile per gli utenti comprenderle o convalidarle" spiega **Joe Levy, chief technology officer di Sophos**. "Questo porta allo scetticismo da parte dei clienti, creando una resistenza al progresso, proprio nel momento in cui stiamo iniziando a ottenere grandi risultati".

"Tentare di correggere questa situazione attraverso l'adozione di standard o di regolamentazioni esterne non sarebbe abbastanza rapido. **Ciò che serve è un cambiamento radicale all'interno della nostra comunità per produrre un insieme di pratiche e un linguaggio che faccia progredire il settore in modo efficace, aperto e trasparente**" conclude Levy.

Condividi l'articolo

Attacco online: emulatori usati per rubare milioni di euro alle banche

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/18/sophos-puntiamo-sullintelligenza-artificiale-aperta/?utm_source=rss&utm_medium=rss&utm_campaign=sophos-

puntiamo-sullintelligenza-artificiale-aperta

Attacco online: emulatori usati per rubare milioni di euro alle banche

Dic 17, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS 0

L'azione ha sfruttato software di emulazione per "impersonare" i dispositivi degli utenti a cui sono state rubate le credenziali dei servizi di home banking.

Sono bastati pochi giorni e i pirati informatici sono riusciti a incassare milioni di euro sottraendoli ai conti correnti delle ignare vittime. L'operazione ha sfruttato sistemi di emulazione online che hanno permesso ai cyber criminali di trasferire il denaro aggirando tutti i sistemi di controllo.

Secondo quanto riportato dai ricercatori di **IBM** in un report pubblicato su Internet, l'operazione avrebbe interessato migliaia di conti correnti i cui account sarebbero stati compromessi attraverso attacchi di phishing o con malware veicolati ai dispositivi delle vittime.

La tecnica utilizzata per incassare i proventi delle azioni criminali sarebbe estremamente complessa: secondo i ricercatori i pirati informatici sarebbero riusciti ad **aggirare i sistemi di controllo (compresi quelli di autenticazione a due fattori basati su codici) adottando una**

serie di accorgimenti, come l’uso di VPN per mascherare l’origine dei collegamenti.

Per farlo, i criminali avrebbero utilizzato fino a **20 emulatori in grado di “impersonare” 16.000 dispositivi** delle vittime. Tutto il sistema sarebbe stato automatizzato, usando strumenti normalmente utilizzati per i test che, in questo caso, hanno permesso di rendere “credibili” le operazioni.

Secondo i ricercatori, i pirati avrebbero utilizzato anche un sistema in grado di monitorare le reazioni delle applicazioni alle richieste, per verificare che l’intera operazione si svolgesse come previsto.

Una volta effettuati i (cospicui) trasferimenti di denaro, hanno cancellato ogni traccia delle oerazioni per far perdere le loro tracce.

L’intera vicenda, sottolineano dalle parti di IBM, conferma come il cyber crimine abbia raggiunto livelli di sofisticazione estremamente elevati, sfruttando risorse specializzate nello sviluppo di applicazioni mobili e nel riciclaggio di denaro.

Condividi l’articolo

La password per i server di SolarWinds era in chiaro su GitHub

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/12/17/attacco-online-emulatori-usati-per-rubare-milioni-di-euro-alle-banche/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-online-emulatori-usati-per-rubare-milioni-di-euro-alle-banche

La password per i server di SolarWinds era in chiaro su GitHub

Dic 16, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, Malware, News, RSS, Vulnerabilità 0

Nessuna certezza sul fatto che sia stata usata per l'attacco che ha colpito l'azienda informatica, ma il livello della sicurezza era ridicolo.

Mentre gli esperti di cyber security si danno da fare per capire quali siano i reali contorni dell'attacco hacker che ha preso di mira decine (migliaia?) tra aziende ed enti pubblici, emergono nuovi dettagli sulle modalità con cui i pirati

informatici potrebbero aver avuto accesso ai sistemi di **SolarWinds**.

L’azienda texana, come abbiamo spiegato in questo articolo, è all’origine dell’attacco supply chain che ha permesso ai cyber criminali di inserire il trojan **SUNBURST** all’interno degli aggiornamenti di **Orion**, il suo software per la gestione delle infrastrutture IT che sarebbe stato scaricato da 33.000 tra aziende e istituzioni in tutto il mondo.

Ora emergono dettagli su alcuni “piccoli difetti” nei sistemi di sicurezza di SolarWinds, che potrebbero spiegare come sia stato possibile per i pirati introdursi nei suoi sistemi.

A riportarlo è **Vinoth Kumar**, un ricercatore che nel novembre 2019 ha segnalato agli amministratori dell’azienda che in un repository su **GitHub** erano accessibili **username e password** per il server FTP in cui sono memorizzati gli installer di Orion.

Come se non bastasse, il ricercatore fa notare che la password per l’accesso al servizio di upload degli eseguibili non era

proprio aderente alle best practice in tema di credenziali: era infatti “**solarwinds123**”. Qualcosa che avrebbe potuto indovinare un bambino di 7 anni.

Possibile che i pirati abbiano utilizzato questa password per portare l’attacco? Beh, da un punto di vista cronologico i conti tornano. **Secondo Kumar, le credenziali erano accessibili su GitHub già nel giugno 2018**.

La prima versione di Orion contenente il malware (2019.4) è stata distribuita da SolarWinds il 5 novembre 2019, **due settimane dopo la segnalazione di Kumar**.

Insomma: non c’è nessuna certezza, ma è possibile che il più grande attacco hacker degli ultimi 5 anni abbia avuto origine da un errore di configurazione e un banale leak a livello di documentazione.

Condividi l’articolo

Terzo data breach per Spotify. Cambio di password per gli utenti coinvolti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/16/la-password-per-i-server-di-solarwinds-era-in-chiaro-su-github/?utm_source=rss&utm_medium=rss&utm_campaign=la-password-per-i-server-di-solarwinds-era-in-chiaro-su-github

---

Terzo data breach per Spotify. Cambio di password per gli utenti coinvolti

Dic 15, 2020 Marco Schiaffino Attacchi, In evidenza, News, Privacy, RSS 0

L'azienda avrebbe condiviso involontariamente i dati degli utenti con alcuni partner. L'incidente arriva dopo altri due violazioni nell'ultimo mese.

Non è un bel periodo per **Spotify**, che sembra avere qualche problema nella gestione dei dati personali dei suoi utenti. L'ultima grana sembra derivare da un semplice errore, a causa del quale alcune informazioni degli utenti registrati sulla piattaforma di streaming musicale sarebbero stati esposti all'accesso da parte di alcuni soggetti terzi.

Nel dettaglio, il comunicato pubblicato da Spotify specifica che i partner commerciali della piattaforma avrebbero avuto accesso alle informazioni di registrazione, compresi username; password; genere e data di nascita.

In via precauzionale, Spotify sta quindi chiedendo agli utenti coinvolti di modificare la password per evitare eventuali conseguenze legate all'esposizione dei dati. **Per quanto riguarda le altre informazioni, purtroppo, c'è poco da fare**.

L'incidente arriva in un periodo in cui la piattaforma di streaming, che vanta **320 milioni di utenti** (di cui 144 milioni con un account premium) sta inanellando una serie di inciampi in ambito sicurezza.

All’inizio di questo mese, infatti, Spotify ha subito un attacco che ha interessato le pagine di alcuni artisti, tra cui **Lana Del Rey**, **Dua Lipa**, **Future** e **Pop Smoke**.

Alla fine di novembre, invece, aveva dovuto fare i conti con una vasta campagna di attacchi basati su tecniche di **credential stuffing** che aveva interessato circa 350.000 account e che ha portato l’azienda a chiedere un reset della password per un vasto numero di utenti.

Insomma: niente di clamoroso, ma la concentrazione e la frequenza degli incidenti cominciano a essere preoccupanti.

Tanto più che, nonostante numerose richieste da parte degli utenti, **Spotify non ha ancora introdotto un sistema di autenticazione a due fattori**, che permetterebbe di aumentare il livello di sicurezza degli accessi.

Considerato che i servizi di streaming online sono tra i più bersagliati dai pirati informatici, sarebbe una bella idea provvedere. Anche con una certa urgenza.

Condividi l’articolo

SUNBURST: attacco alle agenzie federali USA. È stata la Russia?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/15/terzo-data-breach-per-spotify-cambio-di-password-per-gli-utenti-coinvolti/?utm_source=rss&utm_medium=rss&utm_campaign=terzo-data-breach-per-spotify-cambio-di-password-per-gli-utenti-coinvolti

---

SUNBURST: attacco alle agenzie federali USA. È stata la Russia?

Dic 14, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS 0

Compromessi i sistemi dei dipartimenti del Tesoro e del Commercio. Ma l'attacco potrebbe coinvolgere decine o centinaia di vittime in tutto il mondo.

È stato già descritto come il peggior attacco degli ultimi cinque anni, ma le dimensioni della vicenda potrebbero essere davvero clamorose. Soprattutto se dovesse essere confermato il coinvolgimento del gruppo **Cozy Bear**, considerato da sempre collegato ai servizi segreti russi.

Le vittime più illustri, per il momento, sono il **Dipartimento**

del Tesoro statunitense e la **NTIA** (National Telecommunications and Information Administration) in seno al **Dipartimento del Commercio**.

Il numero dei soggetti coinvolti, però, sembra essere destinato a crescere in maniera esponenziale. Quella denunciato dalle maggiori testate statunitensi (tra cui il Wall Street Journal) è infatti un'azione di hacking in grande stile, che potrebbe avere dimensioni senza precedenti.

L'intrusione nei sistemi informatici delle agenzie statunitensi, infatti, sarebbe avvenuto attraverso un attacco supply chain ai danni di **SolarWinds**, azienda con sede in Texas che produce software per la gestione centralizzata dei sistemi IT.

Secondo le prime ricostruzioni rese pubbliche da **FireEye**, i pirati informatici avrebbero "bucato" i sistemi di SolarWInds per inoculare un malware all'interno del file di installazione di **Orion**, la piattaforma per la gestione integrata dei sistemi IT che rappresenta il prodotto di punta dell'azienda.

Il malware, che i ricercatori hanno battezzato con il nome di **SUNBURST**, sarebbe stato distribuito all'interno di alcuni aggiornamenti di Orion (dalla 2019.4 alla 2020.2.1) tra marzo e maggio scorsi.

Il fatto che il malware sia stato segnalato per primo da FireEye non è un caso: **proprio la società di sicurezza sarebbe stata la prima ad accorgersi di essere finita vittima dell'attacco** (ne abbiamo parlato in questo articolo) la settimana scorsa.

SUNBURTS, secondo quanto riportano i ricercatori, sarebbe una backdoor estremamente elusiva, che non sfrutta moduli automatici, ma richiede interventi manuali da parte di chi la controlla.

Una strategia che permette ai pirati informatici di offuscare la loro attività, sfruttando anche il fatto di operare in un ambito (la piattaforma Orion) ideale per nascondere le loro azioni. D'altra parte, **quale miglior paravento di un software di gestione per nascondere l'attività di movimento laterale?**

Gli autori dell'attacco, secondo quanto indicato dal governo statunitense, sarebbero da individuare nel gruppo **Cozy Bear** (APT29), ben conosciuto per aver messo a segno una serie di attacchi clamorosi in passato, tra cui la violazione dei server del Partito Democratico USA alla vigilia delle elezioni presidenziali del 2016.

Se l'attribuzione si dimostrasse corretta, sarebbe un attacco dai contorni davvero clamorosi. **Oltre a numerose aziende private ed enti pubblici, SolarWind vanta tra i suoi clienti anche le forze armate statunitensi (dall'esercito alla marina); il Parlamento Europeo; il sistema sanitario britannico (NHS) e alcune agenzie della NATO**.

Insomma: i pirati legati al Cremlino avrebbero avuto potenzialmente accesso a tutti i servizi email di alcune delle maggiori organizzazioni politiche e militari sul pianeta.

Condividi l’articolo

Facebook smaschera APT32: è una società di “sicurezza” vietnamita

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/14/sunburst-attacco-alle-agenzie-federali-usa-e-stata-la-russia/?utm_source=rss&utm_medium=rss&utm_campaign=sunburst-attacco-alle-agenzie-federali-usa-e-stata-la-russia

---

Facebook smaschera APT32: è una società di “sicurezza” vietnamita

Dic 11, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS, Scenario 0

I tecnici del social network puntano il dito su CyberOne Group, che sarebbe un paravento per le attività dei servizi segreti di Hanoi.

È uno dei gruppi hacker più attivi e pericolosi, ma da oggi ha un volto. **APT32**, conosciuta anche come **OceanLotus**, è finita

nel mirino degli esperti di cyber sicurezza di Facebook, che ha attivato una serie di indagini in seguito ad alcuni attacchi che hanno sfruttato la piattaforma del social network.

Nel dettaglio, Facebook ha rilevato una serie di attività malevole attraverso le quali i cyber criminali legati ad APT32 avrebbero cercato di colpire **attivisti dei diritti umani, giornalisti, governi stranieri (Laos e Cambogia), organizzazioni non governative e numerose aziende operanti in vari settori**.

Come si legge nel comunicato stampa pubblicato da Facebook, gli attacchi sfruttavano falsi profili e utilizzavano messaggi composti ad arte per attirare le potenziali vittime su pagine Web contenenti codice malevolo.

Dietro le operazioni ci sarebbe **CyberOne Group**, un'azienda di sicurezza informatica che avrebbe agito in realtà per condurre gli attacchi sul territorio vietnamita e all'estero.

L'azienda, il cui sito Internet è stato oscurato (così come le pagine Facebook) avrebbe agito come paravento per le attività di spionaggio, **presumibilmente utilizzando l'attività commerciale anche per reclutare "risorse" da impiegare nelle**

sue attività meno confessabili.

Secondo gli autori del report, l'azienda nel corso del tempo avrebbe usato diversi nomi (**CyberOne Security**, **CyberOne Technologies**, **Hành Tinh Company Limited**, **Planet**, **Diacauso**) e adesso sarebbe stata "tagliata fuori" definitivamente dal social network.

Oltre a tutto ciò, i responsabili della sicurezza di Facebook hanno contattato le potenziali vittime degli attacchi per metterli in guardia.

Tutta la vicenda, fanno notare molti commentatori, rappresenta qualcosa di inedito nel panorama della cyber security. **È la prima volta, infatti, che un soggetto privato come Facebook accusa pubblicamente qualcuno di "hacking di stato", tirando in ballo direttamente un governo straniero**.

Di solito, questo tipo di accuse vengono veicolate attraverso canali più "istituzionali", se non addirittura a livello governativo.

Condividi l'articolo

Attacco Kerberos Bronze Bit: ecco perché aggiornare subito i sistemi

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/12/11/facebook-smaschera-apt32-e-una-societa-di-sicurezza-vietnamita/?utm_source=rss&utm_medium=rss&utm_campaign=facebook-smaschera-apt32-e-una-societa-di-sicurezza-vietnamita