Il Perimetro di sicurezza cibernetica: la lunga strada per la protezione di reti e sistemi nazionali

Ott 05, 2020 Alessia Valentini Approfondimenti, In evidenza, Scenario, Women for Security 0

Cosa significa la sua istituzione, come è stato individuato il Perimetro di sicurezza Cibernetica e quali conseguenze comporta.

Sebbene il Cyberspazio sia considerato “senza confini”, sono lontani gli anni in cui era percepito anche come luogo libero da bandiere e ostilità. Da quei primi anni della “internet libera”, agli attacchi informatici svolti per motivi di spavalderia e/o Cyber-attivismo si sono inizialmente aggiunti quelli perpetrati dalla criminalità organizzata per azioni di Cybercrime e infine quelli indirizzati alla cyberwarfare nello scontro fra attori Statali, senza dimenticare che gli attacchi informatici possono diventare in qualsiasi momento anche un mezzo di Cyber-terrorismo.

Proteggere quindi reti e sistemi connessi al World Wide Web (internet) è progressivamente diventato una priorità non più rimandabile; anzi, in relazione alle nuove tecnologie ed ai sistemi che le adottano, il tema della sicurezza informatica è da considerarsi un elemento intrinseco abilitante senza il quale saremmo di fronte ad un "gigante tecnologico con le ginocchia di argilla". In Italia la definizione ed attuazione del Perimetro di Sicurezza Cibernetica è solo l'ultimo tassello in ordine temporale di un lungo percorso di organizzazione della Protezione Cyber e della sicurezza informatica per tutti gli operatori pubblici e privati e tutte le istituzioni del Bel Paese. Dunque, da spazio senza confini, l'ambito Cyber diventa una dimensione in cui si rende necessario definire un perimetro di sicurezza di carattere

nazionale, per organizzarne protezione e difesa. Il concetto stesso di perimetro, come vedremo, ha una accezione diversa da singolo bordo geometrico di una sola entità Nazionale. Infatti, il Perimetro Nazionale consta della sommatoria dei perimetri infrastrutturali delle reti di tante singole organizzazioni chiamate ad essere parte attiva della protezione nel proprio ambito.

Un primo importante passo in ambito militare

Un primo e importante momento nella roadmap della legislazione dedicata alla protezione e sicurezza informatica è avvenuto in ambito militare. In parte anche per motivi di attribuzione ma soprattutto per poter attuare azioni di difesa militare nel Cyberspazio, il primo passaggio è stata la sua identificazione come quinto dominio della conflittualità nell'ambito degli accordi fra nazioni (Summit NATO Varsavia 2016) a cui sono seguiti progressivi investimenti fatti dell'agenzia NCIA per potenziare esperti e struttura organizzativa dedicata in modo da poter fronteggiare situazioni critiche. Ne sono un esempio il Cyber Security Collaboration Hub che a regime dovrebbe consentire lo scambio sicuro di informazioni fra tutti gli stati dell'alleanza e l'agenzia NCIA e il Cyber Operations Center concordato nel Summit di Bruxelles nel 2018. Esercitazioni periodiche annuali internazionali come il Locked Shields organizzato dal CcdCoe (Cooperative Cyber Defence Centre of Excellence) di Tallin sono invece eseguite per mantenere e accrescere la prontezza dei difensori nei singoli stati.

La regolamentazione Civile Europea

Di pari passo alla definizione del quinto dominio, sempre nel 2016, anche il comparto civile ed in particolare l'Unione Europea, si sono mossi per introdurre misure di protezione e prevenzione che potessero contribuire a fortificare anche le reti e i sistemi civili, interconnessi con Internet. Dopo una gestazione significativa è stata emanata la Direttiva NIS che

insieme al successivo Cybersecurity Act traccia gli approcci e le modalità di gestione degli incidenti e della sicurezza informatica nel territorio dell'Unione. In egual misura al rafforzamento della sicurezza però, l'Europa ha voluto intervenire sulla privacy con il GDPR perché Sicurezza e Privacy possano essere due elementi paritetici. Ogni nazione Europea dunque ha dovuto procedere al recepimento della NIS e per la sua piena attuazione, avviare anche l'organizzare di una struttura nazionale Cyber.

Il perimetro di sicurezza nazionale

Senza addentrarci del dettaglio nella lunga serie di passi legislativi che hanno portato alla definizione del Perimetro di sicurezza cibernetica nazionale ricordiamo solo gli step principali della normativa italiana in tema di sicurezza informatica:

- DPCM del 24 gennaio 2013 che ha definito gli indirizzi per la protezione cibernetica e la sicurezza informatica, l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche informatizzate.
- Quadro strategico nazionale per la sicurezza dello spazio cibernetico ed il relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica che hanno stabilito gli indirizzi strategici e quelli operativi per la messa in sicurezza delle attività condotte nel cyber spazio.
- DPCM 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali
- Decreto Legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Per una rapida consultazione si consiglia di consultare la NIS in

pillole.

- Decreto-Legge 21 settembre 2019, n. 105: disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica convertito, con modificazioni, nella legge 18 novembre 2019, n. 133.

L'ultimo decreto-legge/legge è quello che sancisce la creazione del Perimetro di Sicurezza Nazionale come insieme di reti e sistemi afferenti a tutti quegli operatori pubblici, privati e istituzionali che erogano servizi essenziali, il cui pregiudizio per incidente informatico possa comportare un problema di sicurezza nazionale (gli ambiti sono gli stessi della direttiva NIS). Su questa impostazione di sicurezza, fatta da un insieme di singoli che collettivamente contribuiscono alla protezione nazionale, il Ministro Lamorgese al recente Meeting Ambrosetti (6 settembre) ha dichiarato: "*In questa nuova arena digitale, non ci possiamo permettere nessun anello debole: è sufficiente una singola vulnerabilità perché tutto il sistema diventi permeabile alla minaccia, mentre la condivisione di competenze, risorse, informazioni e best practices rafforza, in progressione esponenziale, la capacità di tutelare le nostre collettività*".

Con tale decreto viene richiesto di nominare i soggetti che rientrano nel Perimetro di Sicurezza Nazionale. Attenzione a non confondere tale lista con quella dei soggetti identificati come Operatori di servizi Essenziali (OSE) dalle Autorità competenti NIS. Tale elenco è secretato per ovvi motivi di sicurezza perché potrebbero essere considerati dei TARGET. La differenza è che questi soggetti non sono ancora formalmente nominati nel Perimetro di Sicurezza Nazionale.

Nel decreto sono trattati anche ruolo e organizzazione del Centro di Valutazione e Certificazione Nazionale (CVCN) a cui è richiesto di elaborare e adottare schemi di certificazione cibernetica, valutare il rischio e verificare le condizioni di sicurezza nonché l'assenza di vulnerabilità e di contribuire all'elaborazione delle misure di sicurezza. Per completare

l’organico necessario al CVCN il DL prevede anche lo stanziamento di fondi per assunzione di nuovo personale specifico, il cui bando di selezione dei 70 esperti è stato pubblicato in Gazzetta Ufficiale ai primi di Agosto. I sistemi e apparati soggetti alle valutazioni del CVCN sono specificati con criteri tecnici e categorie di appartenenza. Ultimo ma non meno importante il ruolo del 5G trattato mediante adozione di poteri speciali (Golden Power) esercitabili dal Governo in settori ad alta intensità tecnologica (energia, trasporti e comunicazioni).

L’approccio introdotto dal DL 105 richiede ad ogni componente del Perimetro di Sicurezza Nazionale di attenersi alle indicazioni di protezione mediante analisi di rischio e di impatto sulla sicurezza dei propri sistemi e reti. Quindi ogni organizzazione è tenuta a identificare e mantenere una corretta postura di sicurezza e l’adozione di standard Ue e internazionali. Per ogni soggetto del Perimetro sono anche previsti obblighi di notifica degli incidenti e sanzioni in caso di inadempienze per tutte le prescrizioni previste. Sono inoltre individuati i soggetti preposti al controllo.

Le misure di sicurezza sono individuate nel Comma 3 lettera b e sono attinenti a:

- *“Politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio;*
- *mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;*
- *protezione fisica e logica e dei dati;*
- *integrità delle reti e dei sistemi informativi;*
- *gestione operativa, ivi compresa la continuità del servizio;*
- *monitoraggio, test e controllo;*
- *formazione e consapevolezza;*
- *affidamento di forniture di beni, sistemi e servizi di*

information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.”

L’attuazione della disciplina del Perimetro di Sicurezza Cibernetica è stata articolata in due fasi: un primo passo per definire i criteri per l’identificazione dei servizi e l’elenco degli operatori, individuando anche i criteri per stabilire, predisporre e aggiornare l’elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. Un secondo passo sarà invece dedicato alle specifiche per l’interazione con lo CSIRT Italia in occasione della notifica degli incidenti.

Lo Schema di D.P.C.M. in materia di Perimetro di Sicurezza Nazionale Cibernetica, che riguarda la fase uno è contenuta nell’Atto del Governo n.177 ed è tuttora soggetto all’esame della Commissione preposta e quindi passibile di eventuali variazioni. E’ stato anche predisposto un nuovo decreto che ha la forma di DPR centrato sulle procedura di valutazione del CVCN e dei CV, sulle categorie di tipologie di beni, sistemi e servizi ICT e sulle Ispezioni e verifiche dei controlli (Fonte StartMag).

Nel frattempo l’ultimo decreto semplificazioni legge 11 settembre 2020, n. 120 si dedica a temi correlati al Perimetro di Sicurezza Nazionale ed in particolare, all’articolo 31 tratta gli obblighi di comunicazione in caso di affidamento di forniture ricadenti nel Perimetro di Sicurezza Nazionale Cibernetica e all’articolo 32 introduce il Codice di condotta tecnologica che “*disciplina le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali delle amministrazioni pubbliche, nel rispetto del principio di non discriminazione, dei diritti e delle libertà fondamentali delle persone e della disciplina in materia di Perimetro Nazionale di Sicurezza Cibernetica*.” (capo 2). Per approfondimenti si veda anche il

Dossier 275 della Camera.

Condividi l’articolo

MosaicRegressor: adesso il trojan si nasconde dentro UEFI
Gaming online: il vero “battle royale” è contro il cybercrime

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/05/il-perimetro-di-sicurezza-cibernetica-la-lunga-strada-per-la-protezione-di-reti-e-sistemi-nazionali/?utm_source=rss&utm_medium=rss&utm_campaign=il-perimetro-di-sicurezza-cibernetica-la-lunga-strada-per-la-protezione-di-reti-e-sistemi-nazionali

---

Hacker specializzati nella truffa BEC hanno già incassato 15 milioni

Ott 02, 2020 Marco Schiaffino Attacchi, In evidenza, News, Scenario 0

Lo schema usato dal gruppo è un classico Business Email

Compromise che avrebbe coinvolto più di 150 aziende nel giro di pochi mesi.

Niente da fare: nonostante i continui avvertimenti, le segnalazioni e gli allarmi (non ultimi quelli lanciati dall'FBI) le truffe BEC continuano a mietere decine di vittime tra le aziende di tutto il mondo.

Nel panorama delle truffe online, però, il gruppo di pirati informatici individuati dai ricercatori di **Mitiga**, meritano una segnalazione a parte. Sarebbero infatti riusciti a rubare la bellezza di **15 milioni di dollari** utilizzando sempre lo stesso schema.

Come spiegano gli autori del report pubblicato sul blog della società di sicurezza, i cyber criminali hanno un modus operandi ben preciso, che prevede una serie di accorgimenti grazie ai quali riescono a mettere a segno le loro truffe con una percentuale di successo elevatissima.

La tecnica, naturalmente, prevede la compromissione della casella di posta elettronica di un dirigente dell'azienda. I ricercatori di Mitiga non specificano quale vettore di attacco utilizzino i pirati, ma si concentrano sulla fase successiva.

Questa prevede l'impostazione di semplici regole per l'inoltro dei messaggi, che consentono ai truffatori di poter leggere tutti i messaggi ricevuti dalla vittima senza correre il rischio che gli accessi non autorizzati siano rilevati.

A questo punto, i truffatori iniziano una fase di studio e pianificazione, che secondo gli esperti può durare anche mesi. L'obiettivo è quello di individuare la transazione giusta per mettere a segno il colpo.

Quando individuano uno scambio di email “interessante” con un fornitore o un cliente, preparano il terreno registrando un dominio simile a quello dell’azienda che procederà all’acquisto. Di solito si tratta di nomi in cui viene semplicemente aggiunta una lettera (per esempio *www.securtyiinfo.it*), in modo che la differenza passi inosservata.

L’attacco, come in tutte le truffe di questo tipo, parte al momento dell’invio degli estremi per il pagamento: **l’email originale viene bloccata e, al suo posto, ne viene inviata una che riporta le coordinate bancarie di un conto controllato dai truffatori**.

Per mitigare il rischio che qualcosa vada storto, i pirati impostano a questo punto una serie di filtri nella casella di posta della vittima, che spostano automaticamente gli eventuali messaggi di risposta in una cartella nascosta. **Un trucco estremamente semplice, ma efficace**.

Eventuali messaggi che chiedono conferma delle coordinate bancarie per il pagamento o esprimono perplessità sulla

transazione finiscono infatti in una sorta di “buco nero” e le vittime della truffa non hanno modo di accorgersi di nulla.

I pirati, per le loro operazioni, avrebbero usato un singolo account di **Office 365** (la stessa piattaforma che prendono di mira nei loro attacchi) che i ricercatori hanno collegato a più di 150 attacchi. Un numero incredibile, che conferma il ritardo delle aziende nell’introduzione di sistemi di protezione degli account di posta elettronica e policy adeguate.

Condividi l’articolo

La botnet IPStorm ora colpisce anche Linux, Android e Mac

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/02/hacker-specializzati-nella-truffa-bec-hanno-gia-incassato-15-milioni/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-specializzati-nella-truffa-bec-hanno-gia-incassato-15-milioni

---

La botnet IPStorm ora colpisce anche Linux, Android

e Mac

Ott 01, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L'evoluzione del malware prende di mira qualsiasi tipo di dispositivo. Gli esperti di sicurezza: "Non è ancora chiaro quale sia l'obiettivo".

In continua crescita e pronta a diversificare la sua attività: la botnet **IPStorm** in questo momento è in cima ai pensieri degli esperti di sicurezza, che ne stanno monitorando l'evoluzione con una certa preoccupazione.

Come spiegano in un report i ricercatori di **Barracuda**, il malware che diffonde IPStorm (abbreviazione di **InterPlanetary Storm**, ossia "Tempesta InterPlanetaria") si è presentato in una nuova variante che allarga il campo d'azione del gruppo di pirati informatici che lo distribuisce.

Se la prima versione di IPStorm colpiva solo i sistemi **Windows**, la nuova variante prende infatti di mira anche **Linux**, i sistemi **macOS** e **Android**.

L'evoluzione di IPStorm toglie qualsiasi dubbio sulla reale natura del malware. Molti ricercatori, infatti, lo consideravano un'anomalia, sia per le tecniche che usa (lo stesso nome Inter Planetary è derivato da un protocollo peer to peer utilizzato dal malware per comunicare) sia per il linguaggio di programmazione usato per crearlo, quel **Go** che fino a qualche tempo fa era raramente appannaggio di pirati informatici.

Insomma, il dubbio di molti esperti era che IPStorm fosse una sorta di esperimento e che non avese di fronte a sé un gran futuro. Invece, la nuova versione conferma le intenzioni di

sfruttare il malware per creare una botnet di tutto rispetto, che sta crescendo inesorabilmente.

Le tecniche di diffusione prevedono l'uso di attacchi a dizionario (una versione "evoluta" del brute forcing – ndr) verso i servizi SSH dei computer Linux e Mac, mentre per Android utilizza tecniche che prendono di mira i dispositivi in cui è attivo il sistema **ADB (Android Debug Bridge)** sfruttato da molti malware per dispositivi mobili.

Se nel maggio 2019 i dispositivi infetti erano poco più di 3.000, a oggi la rete ne conta più di 12.000 ed è probabile che la crescita continui.

Tanto più che l'allargamento ad altri sistemi operativi, e soprattutto al mondo degli smartphone, è un elemento di preoccupazione che lascia pensare a possibili futuri sviluppi.

In tutto ciò, rimane un mistero quale possa essere l'obiettivo dei pirati informatici che hanno creato IPStorm. Oltre a diffondersi, infatti, il malware non ha per il momento mostrato alcun comportamento riconducibile a uno dei soliti

obiettivi (attacchi **DDoS**, diffusione di altri payload) che solitamente caratterizzano le campagne malware.

Probabilmente, spiegano i più pessimisti, è solo quesitone di tempo prima di capire quale sia il reale obiettivo dei suoi autori.

Condividi l’articolo

Hacker specializzati nella truffa BEC hanno già incassato 15 milioni Come ti installo il malware sfruttando una falla del mouse

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/01/la-botnet-ipstorm-ora-colpisce-anche-linux-android-e-mac/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-ipstorm-ora-colpisce-anche-linux-android-e-mac

---

Come ti installo il malware sfruttando una falla del mouse

Set 30, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Nuova vulnerabilità nel software di gestione dei dispositivi Kensington. Basta attirare la vittima su un sito Web per installare un malware sul PC.

Dobbiamo preoccuparci di eventuali vulnerabilità del nostro mouse? La risposta è sì. A dimostrarlo, una nuova vulnerabilità nelle periferiche prodotte da **Kensington** che permetterebbe a un pirata informatico di avviare l'esecuzione di codice in remoto sul computer sfruttando una falla del software di gestione di un mouse.

Il programma si chiama **KensigntonWorks** e ha il compito di gestire il complicato sistema di controllo dei mouse a marchio Kensington.

A rendere pubblica la vulnerabilità è stato **Robert Heaton**, che in passato aveva già individuato altre falle di sicurezza nel software di Kensington.

Secondo il ricercatore, la vulnerabilità richiederebbe, per essere sfruttata, soltanto di indurre la vittima a visitare un sito Web sotto il controllo di un pirata informatico e fare in modo che vi rimanga collegato per qualche minuto. Nulla di troppo difficile, quindi.

Ma come funziona il bug? Tutto è collegato all'architettura utilizzata per la gestione delle impostazioni del mouse, che in realtà sfruttano una funzionalità **Web Server** sulla macchina dell'utente.

Una soluzione che Heaton definisce "una pessima idea" e che affonderebbe le sue radici nella volontà degli sviluppatori di utilizzare **Electron**, una piattaforma che consente di creare applicazioni desktop utilizzando **HTML** e **JavaScript**.

Nel suo report, Heaton spiega che questa scelta consentirebbe a un pirata informatico di avviare un collegamento con il computer della vittima e aprire un reverse shell che consentirebbe di eseguire qualsiasi comando sul PC.

Insomma: il risultato sarebbe un margine di azione tale da consentire di eseguire codice malevolo sul computer del malcapitato e, di fatto, installarvi un malware.

L'elemento più preoccupante è che il produttore non avrebbe risposto in alcun modo alle segnalazioni di Heaton e, di conseguenza, tutti gli utenti che usano KensingtonWorks sarebbero vulnerabili a questa forma di attacco, che ora è

pubblica.

Condividi l’articolo

I pirati di REvil cercano soci e mettono sul piatto 1 milione di dollari

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/30/come-ti-installo-il-malware-sfruttando-una-falla-del-mouse/?utm_source=rss&utm_medium=rss&utm_campaign=come-ti-installo-il-malware-sfruttando-una-falla-del-mouse

---

I pirati di REvil cercano soci e mettono sul piatto 1 milione di dollari

Set 29, 2020 Marco Schiaffino Hacking, In evidenza, Malware, News, Scenario 0

Lo strano annuncio su un forum hacker, sul quale i cyber criminali hanno depositato 99 Bitcoin per dimostrare che si tratta di un ottimo affare.

Il marketing nel settore del cyber crimine non va tanto per il

sottile e a dimostrarlo, in questi giorni, sono i pirati informatici del gruppo **REvil**, tra i più attivi negli ultimi mesi.

I cyber criminali di REvil si sono fatti un nome attraverso la formula del **malware as a service**, una strategia sempre più utilizzata nei bassifondi del Web e che prevede una sorta di "affiliazione" tra criminali per spartirsi i profitti dei loro attacchi.

I REvil, nel dettaglio, forniscono ai loro partner il malware **Sodinokibi** in uno schema piuttosto semplice: i "collaboratori" che riescono a colpire un bersaglio incassano il 70-80% del riscatto eventualmente versato dalla vittima, mentre agli sviluppatori rimane in tasca il 20-30%.

L'ultima trovata per promuovere la loro attività, segnalata dai ricercatori di **Sophos** nel blog ufficiale della società di sicurezza è un annuncio su un forum hacker in cui il gruppo spiega di essere alla ricerca di "esperti in penetration testing".

Quali siano le loro intenzioni è evidente, soprattutto quando parlano di avere intenzione di "espandere la composizione dei team dedicati alla pubblicizzazione con risorse di talento" per "aumentare i profitti".

Dopo aver specificato che i "candidati" saranno sottoposti a una selezione, i pirati calano l'asso sul tavolo: **un deposito di 99 Bitcoin (circa un milione di dollari) sullo stesso forum per dimostrare quale sia la loro disponibilità economica**.

La logica è chiara: dal momento che chiunque può verificare il saldo dei conti in Bitcoin, il deposito rappresenta la migliore assicurazione che l'attività che propongono è decisamente lucrosa.

D'altra parte, il gruppo REvil non è nuovo a trovate piuttosto "estrose". In una campagna ransomware individuata dai ricercatori lo scorso dicembre, cercavano di convincere le loro vittime a pagare il riscatto sventolando lo spauracchio delle sanzioni legate al GDPR in caso di mancato pagamento.

Al di là delle note di colore, la vicenda conferma ancora una volta in quale direzione si stia muovendo il mondo della pirateria informatica, sempre più orientato a schemi "commerciali" ispirati alla collaborazione e affiliazione.

Condividi l'articolo

Dispositivi FortiGate VPN esposti ad attacchi Man in the Middle

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/09/29/i-pirati-di-revil-cercano-collaboratori-e-mettono-sul-piatto-1-milione-di-dollari/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-di-revil-cercano-collaboratori-e-mettono-sul-piatto-1-milione-di-dollari

---

Dispositivi FortiGate VPN esposti ad attacchi Man in the Middle

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

Le impostazioni predefinite permettono di dirottare il traffico e decrittarlo. Per Fortinet, però, non si tratta di una vulnerabilità.

Una brutta falla di sicurezza nei dispositivi **FortiGate VPN** di **Fortinet** mette a rischio la sicurezza di migliaia di reti aziendali, esposte alla possibilità di subire attacchi **Man in The Middle**.

Il bug, individuato dal **SAM IoT Security Lab**, riguarda tutti i dispositivi che sono stati installati utilizzando le impostazioni predefinite e coinvolge il sistema di autenticazione a livello di VPN.

Come si legge nel report pubblicato dalla società di sicurezza, il problema si annida nel sistema di verifica dei certificati digitali utilizzato per la connessione. Il client

VPN, infatti, controlla la validità del certificato e altri parametri, ma non la corrispondenza tra il nome del server a cui si collega e quello inserito nel certificato.

Questo significa che il collegamento viene stabilito anche se il certificato proviene da un altro dispositivo Fortinet o da un ente certificatore considerato affidabile.

Insomma: secondo i ricercatori di SAM per i pirati informatici sarebbe possibile indurre un utente a collegarsi a un server da loro controllato e decrittare il contenuto del traffico. **Non solo: da questo è possibile estrarre le credenziali dell'utente e l'OPT, ottenendo di conseguenza l'accesso alla VPN**.

[embedded content]

Se l'assenza di verifiche complete per i ricercatori è una grave vulnerabilità, dalle parti di Fortinet però non la considerano tale. L'azienda ritiene infatti che il certificato predefinito può essere cambiato facilmente e, di conseguenza, non si tratti di una falla di sicurezza.

Tutto vero, ma come fanno notare gli analisti di SAM questo ragionamento si può applicare alle aziende di grandi dimensioni, che hanno competenze e risorse in grado di verificare l'efficacia delle impostazioni e correggerle.

Soggetti di dimensioni più piccole, come studi professionali e piccole-medie imprese, rischiano invece di rimanere esposti ad attacchi di questo genere. Quante sono? Non poche: da una ricerca su **Shodan** emergono circa 230.000 FortiGate VPN esposti su Internet. **Di questi, l'88% sarebbero vulnerabili all'attacco**.

A rischiare, presumibilmente, sono proprio tutte quelle aziende medio-piccole che si sono dotate di strumenti per il lavoro in remoto negli ultimi mesi e che difficilmente saranno in grado di individuare il problema e, tantomeno, risolverlo.

Condividi l'articolo

Hacker colpiscono agenzia federale USA. Ecco come hanno fatto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/28/dispositivi-fortigate-vpn-esposti-ad-attacchi-man-in-the-middle/?utm_source=rss&utm_medium=rss&utm_campaign=dispositivi-fortigate-vpn-esposti-ad-attacchi-man-in-the-middle

---

Hacker colpiscono agenzia federale USA. Ecco come hanno fatto

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

A confermarlo lo stesso governo statunitense. I pirati si sono infiltrati nella rete e hanno installato una backdoor per rubare i dati.

Ennesimo smacco per il governo USA, che si trova a dover ammettere ancora una volta di aver subito un'intrusione informatica a opera di ignoti pirati che sono riusciti a superare i sistemi di difesa federali.

La **Cybersecurity and Infrastructure Security Agency (CISA)** non specifica chi sia la vittima, indicata come una "agenzia federale degli Stati Uniti", ma nel suo comunicato fornisce tutti i dettagli di un attacco con caratteristiche estremamente sofisticate.

L'anatomia dell'attacco, ricostruita dagli esperti Made in USA, sarebbe estremamente complessa. Sul vettore primario di attacco, però, dalle parti del CISA non hanno certezze. L'ipotesi più accreditata è che gli hacker abbiano sfruttato una vulnerabilità (CVE-2019-11510) nella VPN **Pulse Secure** usata dall'agenzia vittima dell'attacco.

Attraverso la falla di sicurezza, avrebbero ottenuto alcune credenziali di **Office 365**, attraverso le quali avrebbero avuto accesso a **SharePoint** per scaricare un file.

Contemporaneamente, i pirati avrebbero avviato un'intensa attività di scansione della rete, partendo dall'analisi di tutte le email che contenevano nell'oggetto parole chiave come "Intranet access" e "VPN passwords".

Una volta individuate le chiavi per **Active Directory** e **Group Policy**, hanno provveduto a modificare una chiave di registro all'interno di Group Policy per ottenere maggiore libertà d'azione.

Gli hacker hanno utilizzato semplici comandi di Windows (conhost, ipconfig, net, query, netstat, ping, and whoami, plink.exe) per eseguire una mappatura completa del network e connettersi poi a un **Virtual Private Server** utilizzando il solito protocollo **Server Message Block**.

Solo a questo punto i pirati hanno avviato il loro malware **inetinfo.exe**, che utilizza un complicato sistema a scatole cinesi per aggirare i controlli antivirus e che ha permesso l'installazione di un secure Socket Shell (SSH) tunnel/reverse

SOCKS proxy, creando infine un account locale per raccogliere i dati sottratti dai dispositivi connessi.

Per garantirsi un sistema più rapido (e meno visibile) per raccogliere i dati che gli interessavano, i pirati hanno poi creato in locale un disco per la condivisione in remoto, che ha permesso loro di lasciare meno tracce nel corso della loro attività.

Insomma: un'operazione estremamente complessa, che avrebbe portato alla raccolta di dati memorizzati in due file compressi in formato ZIP. Secondo gli esperti del CISA "è probabile che i due file siano stati esfiltrati, ma la loro trasmissione all'esterno non può essere confermata perché hanno coperto la loro attività".

Condividi l'articolo

Allarme di Microsoft per Zerologon: "I pirati stanno sfruttando la falla"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/25/hacker-colpiscono-agenzia-federale-usa-ecco-come-hanno-fatto/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-colpiscono-agenzia-federale-usa-ecco-come-hanno-fatto

---

Allarme di Microsoft per Zerologon: “I pirati stanno sfruttando la falla”

Set 24, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità consente di effettuare un’elevazione di privilegi in Windows Server e sul Web circolano diversi exploit per sfruttarla.

I primi avvisi erano arrivati dal **CISA** (Cybersecurity and Infrastructure Security Agency), che ha sollecitato tutte le agenzie federali negli USA a proteggere i sistemi da **Zerologon** entro la giornata di ieri, 23 settembre. Ora scende in campo **Microsoft**, specificando che la vulnerabilità è usata da numerosi gruppi di pirati informatici per portare attacchi a sistemi aziendali.

Zerologon (CVE-2020-1472) è una falla di sicurezza individuata da **Secura** e resa pubblica lo scorso 11 settembre con la

pubblicazione di un report sul blog della società di sicurezza.

Il bug affligge il sistema di autenticazione Microsoft **Netlogon** e consente, in pratica, di ottenere l'accesso con credenziali di amministratore all'interno di un dominio **Active Directory**, prendendone di fatto il controllo.

Come si legge nel report, il problema è dovuto alle modalità di implementazione del sistema crittografico **AES-128-CFB8**. L'algoritmo, infatti, è stato utilizzato in una versione semplificata, in cui il vettori di inizializzazione (**IV**) è pari a zero.

La conseguenza di questa scelta (per i dettagli è possibile leggere anche una corposa spiegazione pubblicata da **Sophos** a questo indirizzo) è che un pirata informatico può "ingannare" Netlogon semplicemente inviando una richiesta di collegamento in cui i dati per la creazione della chiave crittografica è composta da soli zero.

A causa delle impostazioni di AES-128-CFB8 in Netlogon, infatti, la **Netlogon Credential Computation** (che permette l'autenticazione) sarà composta di soli zero con una

probabilità di una volta su 256. **Abbastanza per avviare un attacco di brute forcing "sui generis" che permette di ottenere l'accesso come amministratore**.

L'aggiornamento che corregge la vulnerabilità è stato distribuito da Microsoft con la tornata di update dello scorso agosto, ma l'abituale inerzia nell'esecuzione delle operazioni di patch (soprattutto a livello aziendale) lascia pensare che molti sistemi siano ancora vulnerabili.

Le preoccupazioni, però, derivano dal fatto che su Internet sono comparsi nel giro di pochi giorni numerosi **PoC (Proof of Concept)** che permettono di sfruttare la falla di sicurezza in maniera piuttosto elementare.

L'allarme lanciato da Microsoft, quindi, rappresenta la ciliegina sulla torta e conferma che gruppi di cyber criminali stanno attivamente utilizzando gli exploit. **Inutile dirlo, il (caloroso) suggerimento è di aggiornare subito**.

Condividi l'articolo

Hacker colpiscono agenzia federale USA. Ecco come hanno fatto
Attacchi ransomware: una società di assicurazioni li ha ridotti del 65%

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/24/allarme-di-microsoft-per-zerologon-i-pirati-stanno-sfruttando-la-falla/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-di-microsoft-per-zerologon-i-pirati-stanno-sfruttando-la-falla

Attacchi ransomware: una società di assicurazioni li ha ridotti del 65%

Set 23, 2020 Marco Schiaffino Gestione dati, In evidenza, News, Prodotto, RSS, Scenario, Tecnologia, Vulnerabilità 0

Un miracolo? No. È bastato imporre ai suoi assicurati l'uso di software di sicurezza per eliminare le vulnerabilità dei sistemi IT.

A volte gli esperti di sicurezza vengono accusati di sembrare un disco rotto, soprattutto quando richiamano le aziende a implementare una pianificazione nelle strategie di cyber security. Come dimostra la vicenda di **Corvus**, però, gli esperti di sicurezza hanno ragione da vendere.

Corvus è una società di assicurazione contro i rischi cyber, un settore che ha vissuto un'ampia crescita negli ultimi anni e che vede nei ransomware il maggior numero di eventi dannosi per i loro assicurati.

Per limitare il numero di incidenti ed evitare di trovarsi a dover pagare continuamente risarcimenti ai suoi assistiti, dalle parti di Corvus hanno pensato bene di agire in un'ottica di prevenzione, cercando di individuare il modus operandi più comune dei pirati e mettendo in campo delle contromisure per mitigare il rischio di attacchi ransomware.

Sorpresa: non è stato per niente difficile. Analizzando le statistiche delle società di sicurezza e i documenti pubblicati da varie agenzie, emerge infatti come la maggior parte degli attacchi segua uno schema piuttosto definito e che il vettore di attacco più comune sia l'utilizzo di collegamenti **RDP (Remote Desktop)** che vengono compromessi per ottenere l'accesso alla rete.

Corvus ha quindi modificato le sue policy per gli assicurati prevedendo una scansione di sicurezza con un software fornito dalla società stessa, chiamato **Corvus Scan 2.0**. Il programma consente di individuare i server RDP esposti, così come impostazioni errate o vulnerabilità a livello di rete.

Risultato: dall'introduzione delle nuove policy (lo scorso aprile) a oggi i clienti di Corvus hanno subito un numero di attacchi ransomware inferiore del 65% rispetto al periodo precedente.

Nel comunicato stampa, viene spiegato anche che i clienti che hanno adottato le nuove policy non hanno subito alcun attacco

ransomware attraverso la violazione di sistemi RDP.

L’elemento sconcertante è che le aziende abbiano applicato una verifica della cyber security solo quando sono stati obbligati a farlo dal loro assicuratore. Evidentemente c’è ancora da lavorare parecchio su quella “cultura della sicurezza” di cui gli esperti continuano a parlare.

Condividi l’articolo

Un bug consente di superare il sistema di autenticazione Microsoft

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/23/attacchi-ransomware-una-societa-di-assicurazioni-li-ha-ridotti-del-65/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-ransomware-una-societa-di-assicurazioni-li-ha-ridotti-del-65

Un bug consente di superare il sistema di autenticazione Microsoft

Set 22, 2020 Marco Schiaffino In evidenza, News, Vulnerabilità 0

Le falle di sicurezza consentirebbero di prendere il controllo degli account di numerosi servizi cloud, tra cui Microsoft 365 e Azure.

Si chiama **WS-Trust** ed è uno standard di autenticazione delineato da **OASIS** (Organization for the Advancement of Structured Information Standards) che dovrebbe garantire la sicurezza nello scambio di messaggi.

Come hanno scoperto i ricercatori di **Proofpoint**, però, la sua implementazione nei sistemi cloud Microsoft è viziata da una serie di bug che permetterebbero a un pirata informatico di aggirare i sistemi di autenticazione e prendere il controllo di un account da remoto.

Nel report pubblicato sul blog della società di sicurezza, per la verità, non vengono forniti molti dettagli. DI sicuro si tratta di numerosi bug, che avrebbero consentito di eseguire l'accesso attraverso tecniche piuttosto semplici, come la falsificazione dell'indirizzo IP.

Il problema sarebbe generato da un mix di concause, tra cui

una debolezza intrinseca dello standard e una serie di errori nella sua implementazione.

Tra questi, la possibilità che il sistema non riconosca le modalità di autenticazione, aprendo la strada all'utilizzo di sistemi antiquati. **Secondo quanto riportano i ricercatori di Proofpoint, inoltre, uno dei bug consentirebbe di aggirare i controlli semplicemente modificando l'header della richiesta**.

Insomma: il rischio è che un cyber criminale possa mettere le mani su tutti i documenti e le informazioni legate all'account **Microsoft 365**, **Azure** o **Visual Studio**.

Un rischio che è ancora più elevato nel particolare omento che stiamo attraversando, con un uso sempre più intensivo di servizi cloud e collegamenti da remoto dovuti alla pandemia da Covid-19.

Un panorama che, segnalano gli esperti, ha già indotto molti pirati informatici a concentrare l'attenzione sulle tecniche di attacco che prendono di mira i sistemi di autenticazione multifattore.

Condividi l'articolo

Attacchi ransomware: una società di assicurazioni li ha ridotti del 65% Iran: malware per Android che aggira l'autenticazione a due fattori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/22/un-bug-consente-di-superare-il-sistema-di-autenticazione-

microsoft/?utm_source=rss&utm_medium=rss&utm_campaign=un-bug-consente-di-superare-il-sistema-di-autenticazione-microsoft