Il gruppo Maze abbandona le scene. È finita? Non proprio…

Ott 29, 2020 Marco Schiaffino In evidenza, Malware, News, Scenario 0

I cyber criminali protagonisti di una delle operazioni più devastanti degli ultimi mesi vogliono ritirarsi. Ma molti di loro sono pronti a ricominciare.

Hanno letteralmente terrorizzato aziende e organizzazioni in tutto il mondo, utilizzando uno schema basato sulla logica del "malware as a service" e cercando affiliazioni tra i vari gruppi di pirati informatici. Ora i membri del gruppo **Maze** sembrano aver deciso di abbandonare il campo e hanno cominciato a smantellare le infrastrutture che hanno usato fino a oggi.

La gang di cyber criminali specializzata in ransomware è conosciuta per aver inaugurato nuove modalità nella gestione della loro attività (ne abbiamo parlato in questo articolo) ed è, senza dubbio, tra i gruppi più pericolosi in circolazione.

Secondo quanto riporta **Bleeping Computer** in un articolo pubblicato su Internet, però, la carriera del gruppo potrebbe essere arrivata al termine. Sui forum di hacking e nei bassifondi di Internet gira voce che il fenomeno Maze sia giunto al capolinea.

A confermare la veridicità di queste indiscrezioni, spiegano i colleghi di Bleeping Computer, contribuisce il fatto che **i pirati di Maze avrebbero cancellato i dati pubblicati in passato** per fare pressione sulle loro vittime e forzarle a pagare i "riscatti" chiesti per non diffondere le informazioni rubate.

Vivremo quindi in un mondo più sicuro? Non proprio. Secondo quanto riportano i colleghi, molti degli affiliati a Maze si starebbero aggregando a un nuovo gruppo, chiamato **Egregor**.

La nuova operazione sfrutterebbe sempre la strategia dei ransomware e sarebbe partita già lo scorso settembre, quando Maze ha avviato lo "shutdown" delle sue operazioni.

Secondo i ricercatori che hanno analizzato le prime operazioni di Egregor, il ransomware sfrutterebbe buona parte del codice di Maze e utilizzerebbe le stesse strategie.

Insomma: l'abbandono del gruppo originale non comporta, necessariamente, una diminuzione delle minacce online. Molto probabilmente, anzi, ci troveremo di fronte a un soggetto

ancora più organizzato e in grado di sfruttare l’esperienza maturata negli ultimi anni per agire con maggiore efficacia.

Condividi l’articolo

Truffe bancarie: ora i pirati usano lo spoofing sul telefono

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/29/il-gruppo-maze-abbandona-le-scene-e-finita-non-proprio/?utm_source=rss&utm_medium=rss&utm_campaign=il-gruppo-maze-abbandona-le-scene-e-finita-non-proprio

---

Truffe bancarie: ora i pirati usano lo spoofing sul telefono

Ott 28, 2020 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS, Scenario 0

La strategia prevede l’uso di strumenti per alterare il numero da cui proviene la chiamata e attacchi di

phishing per rendere la truffa credibile.

Che i pirati informatici abbiano una passione per i servizi di home banking è cosa nota. La nuova tecnica messa a punto dai cyber criminali, però, non prevede l'uso di malware o complicati attacchi di hacking, ma il semplice utilizzo del telefono per "convincere" le vittime a regalargli i loro soldi.

A spiegare nei dettagli il funzionamento di questa truffa sono i ricercatori di **Malwarebytes Labs**, che in un post sul blog ufficiale della società di sicurezza ne illustrano le caratteristiche.

La tecnica prevede, in pratica, una semplice telefonata in cui i pirati informatici si spacciano per impiegati della banca in cui la vittima ha il suo conto corrente.

Per dare credibilità alla loro messa in scena, utilizzano strumenti di **spoofing del numero telefonico**, cioè software utilizzabili su servizi di telefonia **VoIP** che permettono di far visualizzare un falso numero di telefono (in questo caso quello della banca) sul telefono del destinatario della chiamata.

L'argomento della conversazione è semplice: i truffatori spiegano alla vittima che l'istituto di credito ha rilevato dei movimenti sospetti sul suo conto corrente bancario e che temono possa trattarsi di un attacco hacker che consentirebbe ai pirati di rubargli tutto il denaro conservato al suo interno.

Suggeriscono, di conseguenza, di spostare il denaro in un "conto sicuro" pensato proprio per proteggere i clienti da rischi come questi, avvisando anche che le somme trasferite "potrebbero non essere disponibili per qualche giorno".

Si tratta ovviamente di una montatura e il cosiddetto "conto sicuro" non è altro che un conto corrente intestato agli

stessi truffatori.

Oltre all’utilizzo di un falso numero di telefono, i cyber criminali usano altri stratagemmi per convincere le vittime di star parlando effettivamente con un impiegato della loro banca.

Secondo le informazioni raccolte dagli esperti di Malwarebytes, sarebbero infatti in grado di fornire informazioni come gli esatti importi presenti sui conti, o gli ultimi movimenti disposti attraverso i servizi di home banking.

Nel report viene spiegato che queste informazioni possono essere state raccolte in vari modi: sia grazie alla complicità di una “talpa” nella banca stessa, sia attraverso attacchi di phishing che hanno permesso ai pirati di accedere al conto della vittima.

L’ipotesi del phishing, spiegano gli autori del rapporto, è particolarmente credibile. La maggior parte dei servizi di home banking, infatti, consente l’accesso a informazioni generiche (come il saldo o i movimenti) con il semplice utilizzo di username e password, mentre richiede ulteriori fattori di autenticazione solo per disporre i movimenti.

Inutile dire che, nel caso la truffa vada a segno, il denaro trasferito sparirà in un lampo dal conto su cui è stato versato e la vittima, nel caso la sua banca non preveda un'assicurazione contro le truffe di questo tipo, resterà al verde.

Condividi l'articolo

Il gruppo Maze abbandona le scene. È finita? Non proprio… Hacker "buca" un servizio di psicoterapia. Pazienti sotto ricatto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/28/truffe-bancarie-ora-i-pirati-usano-lo-spoofing-sul-telefono/?utm_source=rss&utm_medium=rss&utm_campaign=truffe-bancarie-ora-i-pirati-usano-lo-spoofing-sul-telefono

---

Hacker "buca" un servizio di psicoterapia. Pazienti sotto ricatto

Ott 27, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, News, Privacy, RSS 0

Succede in Finlandia, dove gli utenti di una clinica privata stano subendo le minacce dei pirati informatici. Le vittime potrebbero essere 40.000.

Se gli allarmi riguardanti la necessità di proteggere i dati sanitari negli ultimi anni si stanno moltiplicando, quello che era mancato fino a oggi era un caso di cronaca che ponesse con prepotenza il problema.

L'episodio che promette di portare il tema in cima alla lista delle priorità arriva dalla **Finlandia** e, in particolare dal **Centro di Psicoterapia Vastaamo**, vittima di un attacco hacker le cui conseguenze sono ancora tutte da verificare.

Come riportano organi di stampa finlandesi, i sistemi informatici della clinica privata sarebbero stati infatti violati da un gruppo di pirati informatici che sono riusciti ad appropriarsi di un numero imprecisato di cartelle cliniche e che adesso starebbero utilizzando il materiale rubato per ricattare i pazienti della clinica stessa.

Secondo quanto è stato riportato dai siti di news locali (qui il collegamento a una pagina in finlandese) l'attacco risalirebbe addirittura a novembre 2018, periodo dal quale i pirati avrebbero avuto libero accesso al database della clinica.

La violazione è emersa soltanto lo scorso settembre, quando i pirati hanno evidentemente deciso di passare all'azione contattando il Centro di Psicoterapia chiedendo 450.00 dollari per non divulgare le informazioni sottratte.

In seguito, però, i cyber criminali avrebbero cominciato a contattare singolarmente i pazienti, minacciandoli di rendere pubbliche le informazioni riguardo la loro storia clinica nel caso in cui non avessero pagato un "riscatto" che oscillerebbe tra i 200 e i 500 euro.

Secondo quanto dichiarato dagli stessi amministratori della clinica, il numero di potenziali vittime supererebbe le 40.000.

La clinica ha avviato un'indagine interna (piuttosto tardiva, verrebbe da dire) per verificare il livello di sicurezza dei suoi sistemi, ma nel frattempo le informazioni di alcuni pazienti sarebbero già state pubblicate sul Dark Web.

Condividi l'articolo

Bug in Safari consente di falsificare l'URL a cui ci si collega

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/10/27/hacker-buca-i-sistemi-di-un-servizio-di-psicoterapia-pazienti-sotto-ricatto/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-buca-i-sistemi-di-un-servizio-di-psicoterapia-pazienti-sotto-ricatto

---

Bug in Safari consente di falsificare l'URL a cui ci si collega

Ott 26, 2020 Marco Schiaffino In evidenza, News, Phishing, RSS, Vulnerabilità 0

La falla interessa anche Opera Mini e Yandex. I pirati potrebbero sfruttarla per attacchi di phishing e come vettore per distribuire malware.

Ancora una volta vulnerabilità basata su **JavaScript** e, ancora una volta, una falla che consentirebbe di mettere a segno con estrema facilità attacchi di phishing.

La segnalazione arriva da **Rapid 7** e riguarda tre browser mobile che hanno un livello di utenza "medio" come **Safari**, **Opera Mini** e **Yandex**. Nel post pubblicato sul blog ufficiale della società di sicurezza, i ricercatori spiegano che la vulnerabilità consentirebbe, in pratica, di alterare l'indirizzo che compare sulla barra degli indirizzi.

Un pirata informatico in grado di sfruttare la falla potrebbe, di conseguenza, attirare le sue vittime su una pagina Web

facendo credere loro di essere su un sito affidabile, quando in realtà il sito cui si collegano è un altro.

Le potenziali applicazioni della vulnerabilità sono abbastanza intuitive e permetterebbero ai cyber criminali di mettere in atto attacchi di phishing estremamente efficaci. Sui dispositivi mobili, segnalano gli autori del report, l'URL visualizzata nella barra degli indirizzi è uno dei pochi elementi che consente agli utenti di verificare su quale sito si trovano e la scarsa attitudine a utilizzare software di protezione rende il settore ancora più permeabile ad attacchi di questo tipo.

Buona parte delle società coinvolte, per la verità, hanno corretto la falla di sicurezza con gli aggiornamenti di ottobre, ma l'incognita come al solito riguarda il numero di utenti che hanno applicato gli aggiornamenti di sicurezza.

Se il problema degli update viene normalmente sottolineato per quanto riguarda server e PC, la situazione sui dispositivi mobili è, se possibile, anche peggiore. Sono poche, infatti, le persone che avviano regolarmente gli aggiornamenti e le probabilità che molti utilizzatori usino versioni non aggiornate dei browser sono estremamente elevate.

Condividi l’articolo

Rischiamo davvero attacchi hacker ai dispositivi medicali?

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/10/26/bug-in-safari-consente-di-falsificare-lurl-a-cui-ci-si-collega/?utm_source=rss&utm_medium=rss&utm_campaign=bug-in-safari-consente-di-falsificare-lurl-a-cui-ci-si-collega

Rischiamo davvero attacchi hacker ai dispositivi medicali?

Ott 23, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Sempre più collegati e "intelligenti", ma i device di nuova generazione continuano a preoccupare per la possibilità che un pirata informatico li attacchi.

È possibile uccidere o ferire qualcuno con un attacco hacker? La domanda assilla molti esperti di cyber security e in particolare quelli che si occupano di controllare il livello di sicurezza dei dispositivi medicali personali: pacemaker, pompe per l'insulina e simili.

A fare il punto sui problemi legati alla protezione dagli hacker di questi particolarissimi dispositivi IoT è **ESET**, che

in un post sul blog ufficiale dell’azienda elenca le questioni più spinose.

Uno degli aspetti generali che sottolineano gli esperti riguarda per esempio gli aggiornamenti di sicurezza, che hanno un’importanza fondamentale per dispositivi che, si suppone, debbano funzionare per molti anni.

Esistono però questioni molto più specifiche, come il fatto che la maggior parte di questi IoT medicali utilizzino per comunicare un protocollo come **Bluetooth**, che in passato ha dimostrato di essere esposto frequentemente a vulnerabilità che possono aprire la strada ad attacchi informatici.

Ancora più preoccupante, nell’ottica legata al lungo periodo di utilizzo, è quello della compatibilità con i nuovi sistemi operativi. **Un tema, questo, che è già stato sottolineato in passato e che induce spesso gli ospedali e gli istituti sanitari in genere a utilizzare dei sistemi legacy anche oltre il periodo di supporto, degradando il livello complessivo dei sistemi**. Il caso di **Windows XP**, ampiamente utilizzato ancora in molti laboratori, è quello più indicativo.

Anche l’uso delle piattaforme cloud, che hanno dimostrato in più occasioni di essere tutt’altro che sicure a causa (principalmente) di frequenti errori di configurazione, rappresenta un rischio che gli autori del report considerano rilevante.

A preoccupare, poi, è la possibilità che i pirati utilizzino tecniche più sofisticate per intercettare dati sensibili come le password di accesso ai software di gestione, per esempio attraverso cavi ethernet modificati o dispositivi in grado di intercettare e decodificare i segnali inviati dalle tastiere wireless.

Insomma: il panorama rimane complesso e, anche se alcuni degli allarmi lanciati in passato si sono rivelati essere esagerati o addirittura gonfiati ad arte (come nel caso che abbiamo raccontato in questo articolo), si tratta di un tema che impegnerà gli esperti di sicurezza ancora per molto tempo.

Condividi l’articolo

Check Point: dopo il Covid il rischio è una pandemia cyber

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/23/rischiamo-davvero-attacchi-hacker-ai-dispositivi-medicali/?utm_source=rss&utm_medium=rss&utm_campaign=rischiamo-davvero-attacchi-hacker-ai-dispositivi-medicali

---

Check Point: dopo il Covid il rischio è una pandemia cyber

Il nuovo scenario del panorama IT delinea priorità e alcuni aspetti che aziend ed esperti di cyber security devono considerare. L'ondata di infezioni determinate dal Covid 19 è destinata a lasciare il segno anche nel settore IT. A confermarlo è Check Point, che in un incontro con la stampa ha cercato di fissare i fattori […]

L'articolo Check Point: dopo il Covid il rischio è una pandemia cyber proviene da Securityinfo.it.

https://www.securityinfo.it/2020/10/22/check-point-dopo-il-covid-il-rischio-e-una-pandemia-cyber/?utm_source=rss&utm_medium=rss&utm_campaign=check-point-dopo-il-covid-il-rischio-e-una-pandemia-cyber

---

Ecco le 25 vulnerabilità più usate dagli hacker cinesi secondo l'NSA

Ott 21, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Scenario, Vulnerabilità 0

Un report spiega quali sono i bug sfruttati dai cyber-spioni al soldo del governo di Pechino. La sorpresa? Li

conosciamo tutti e ci sono le patch.

Come agiscono gli hacker che operano per conto dei governi e i servizi segreti? Se istintivamente siamo portati a pensare che usino tecniche di attacco estremamente evolute e sconosciute agli esperti di sicurezza, la realtà descrive un altro scenario molto più prosaico.

A confermarlo è la **National Security Agency**, che in un report pubblicato su Internet elenca le vulnerabilità più sfruttate dai gruppi APT cinesi, tra i più pericolosi in circolazione.

Ebbene: nella maggior parte dei casi si tratta di falel di sicurezza ben conosciute e per le quali sono disponibili gli aggiornamenti che le correggono. Ecco l'elenco completo:

1) CVE-2019-11510 – Riguarda i server **Pulse Secure VPN**, in cui un pirata informatico può inviare un URL che avvia una falla per avviare la lettura di file e rubare così la password di accesso.

2) CVE-2020-5902 – La falla interessa I proxies e load balancer **F5 BIG-IP** a livello del **Traffic Management User Interface (TMUI)** cui è affidata la configurazione. La vulnerabilità consente l'esecuzione di codice in remote e, di conseguenza, la possibilità di assumere il controllo del dispositivo.

3) CVE-2019-19781 – Citrix Application Delivery Controller (ADC) sono vulnerabili a un bug "trasversale" che permette l'esecuzione di codice in remote che aggira il Sistema di autenticazione.

4+5+6) CVE-2020-8193, CVE-2020-8195, CVE-2020-8196 – Le vulnerabilità riguardano sempre Citrix e interessano anche I sistemi SDWAN WAN-OP. Sfruttandoli, è possibile ottenere informazioni sensibili anche attraverso un accesso con un basso livello di privilegi.

7) CVE-2019-0708 – Si tratta del famigerato **BlueKeep** (ne

abbiamo parlato in questo articolo) che affligge i sistemi Windows attraverso i servizi Remote Desktop.

8) CVE-2020-15505 – La falla riguarda il software di mobile device management (MDM) **MobileIron**. Sfruttandolo è possible prendere il controllo dei server aziendali.

9) CVE-2020-1350 – Conosciuto come **SigRed** (una descrizione in questo articolo) il bug è rimasto "nascosti" per ben 17 anni.

10) CVE-2020-1472 – La vulnerabilità, battezzata con il nome di **ZeroLogon**, è una delle più recenti emerse in ambiente Windows. I dettagli in questo articolo su **Security Info**.

11) CVE-2019-1040 – Sempre relative ai sistemi Microsoft, il bug consente di portare un attacco Man in The Middle ai danni di NTLM MIC (Message Integrity Check).

12) CVE-2018-6789 – La falla consente di provocare un buffer overflow (e conseguente esecuzione di codice) inviando una mail **Exim**.

13) CVE-2020-0688 – La falla riguarda **Microsoft Exchange** e, in particolare, un problema nella gestione di oggetti a livello di memoria.

14) CVE-2018-4939 – Una vulnerabilità che consente di avviare l'esecuzione di codice in remoto su alcune versioni di **Adobe ColdFusion**.

15) CVE-2015-4852 – I server **Oracle WebLogic 15** soffrono di un bug a livello di un componente (WLS Security che permette di inviare comandi in remoto attraverso oggetti Java.

16) CVE-2020-2555 – Un bug all'interno di **Oracle Coherence** (presente all'interno della suite **Oracle Fusion Middleware**) che permette di compromettere i sistemi.

17) CVE-2019-3396 – La macro **Widget Connector** dei server **Atlassian Confluence 17** permette di iniettare cei modelli che portano all'esecuzione di codice in remoto.

18) CVE-2019-11580 – Il bug interessa **Atlassian Crowd** e I **Crowd Data Center**. Sfruttandolo, è possible installare plugin che permettono di eseguire codice in remote.

19) CVE-2020-10189 – **Zoho ManageEngine Desktop Central** è vulnerabile a un attacco che porta a esecuzione di codice in remoto.

20) CVE-2019-18935 – Un rischio di esecuzione di codice in remoto a causa di una errata procedura di deserializzazione in

Progress Telerik UI per **ASP.NET AJAX**.

21) CVE-2020-0601 – **CurveBall** è una falla di sicurezza di Windows che riguarda le **CryptoAPI (Crypt32.dll)** e il modo in cui gestiscono i certificati **Elliptic Curve Cryptography (ECC)**. Sfruttandola, un pirata informatico può creare un falso certificato digitale per un malware.

22) CVE-2019-0803 – La vulnerabilità consente di elevare i privilegi dell'utente nei sistemi Windows.

23) CVE-2017-6327 – Il bug consente di eseguire codice in remote all'interno del **Symantec Messaging Gateway**.

24) CVE-2020-3118 – Il bug interessa l'implementazione del **Cisco Discovery Protocol** implementation in **IOS XR Software**. Le conseguenze consistono in un possible attacco che porta il riavvio del dispositivo o l'esecuzione di codice al suo interno.

25) CVE-2020-8515 – I dispositive **DrayTek Vigor** permettono l'esecuzione di codice in remote con privilege di root attraverso "metacaratteri" vi a shell.

Condividi l'articolo

Hai controllato quali app 0Auth accedono al tuo account Microsoft 365?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/21/ecco-le-25-vulnerabilita-piu-usate-dagli-hacker-cinesi-secondo-lnsa/?utm_source=rss&utm_medium=rss&utm_campaign=ecco-le-25-

vulnerabilita-piu-usate-dagli-hacker-cinesi-secondo-lnsa

Hai controllato quali app 0Auth accedono al tuo account Microsoft 365?

Ott 20, 2020 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS, Scenario 0

Una nuova tecnica di phishing permette ai pirati di ottenere l'accesso a email e informazioni riservate sfruttando la funzionalità del servizio.

Sempre più connessi e versatili: i servizi cloud sono i veri protagonisti di questi ultimi anni. A sfruttarne le caratteristiche, però, sono anche i pirati informatici che hanno studiato nuove tecniche di attacco basate sulle caratteristiche del "software as a service".

Il caso, segnalato in un articolo da **Bleeping Computer**, riguarda una campagna di phishing avviata da un gruppo di pirati informatici che sfrutta la funzionalità **0Auth** di **Microsoft 365**.

Il sistema sviluppato da Microsoft è pensato per consentire agli utenti di implementare rapidamente funzionalità aggiuntive nel loro account, consentendo alle applicazioni 0Auth di accedere ai dati di Microsoft 365 per vari scopi.

Si tratta di una funzione estremamente utile, che consente, per esempio, di applicare filtri antispam o automatizzare

operazioni con altri strumenti sviluppati da terze parti.

I cyber criminali, però, hanno trovato il odo di approfittarne attraverso una semplice strategia di phishing, che nel caso specifico sfrutta la possibilità di collegare **Coinbase** (uno dei più conosciuti exchange di monete virtuali – ndr) a Microsoft 365.

L'attacco usa come vettore principale una semplice email che si spaccia per un aggiornamento dei termini di servizio di Coinbase. Se la vittima apre il link contenuto al suo interno, viene dirottato a una pagina di login del sito di Microsoft e, successivamente, a una finestra in cui viene chiesto di concedere una serie di permessi a **coinbaseterms.app**.

Si tratta di una procedura assolutamente legittima, con l'unico difetto che l'applicazione in questione non è in nessun modo legata a Coinbase, ma consente ai pirati di ottenere un accesso illimitato ai messaggi di posta elettronica della vittima, alle informazioni personali.

Non solo: se l’utente conferma l’autorizzazione, l’applicazione stessa avrà la possibilità di creare e inviare mail dall’account Microsoft 365.

Naturalmente, affinché il trucchetto funzioni serve una buona dose di “collaborazione” da parte della vittima, ma **l’esperienza insegna che i click frettolosi non sono affatto una rarità e che stratagemmi come quello descritto rischiano di funzionare fin troppo spesso.**

Al di là del caso specifico, il tema della app 0Auth rimane estremamente delicato. Il consiglio per gli utenti Microsoft 365, di conseguenza, è quello di controllare periodicamente le impostazioni del servizio per verificare quali applicazioni vi hanno accesso.

Condividi l’articolo

Si finge Zoom e infetta il computer: ecco il malware Vizom

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/20/hai-controllato-quali-app-0auth-accedono-al-tuo-account-microsoft-365/?utm_source=rss&utm_medium=rss&utm_campaign=hai-controllato-quali-app-0auth-accedono-al-tuo-account-microsoft-365

Si finge Zoom e infetta il computer: ecco il malware Vizom

Ott 19, 2020 Marco Schiaffino In evidenza, Keylogger, Malware, Minacce, News, RSS, Trojan 0

I pirati sfruttano la popolarità del software di videoconferenza per distribuirlo online. Una volta installato, cerca di rubare le credenziali per i servizi bancari.

Un malware studiato per infiltrarsi nei sistemi Windows sostituendo un file utilizzato da Zoom e rubare così le credenziali di accesso per i servizi di home banking. **Vimoz**, individuato dai ricercatori **IBM Security Trusteer**, è una delle minacce più originali comparse nelle ultime settimane.

Da un punto di vista tecnico, Vimoz è un classico trojan, che consente ai suoi autori di controllare in remoto alcune funzionalità del computer infetto. Le caratteristiche più interessanti del malware, però, riguardano la tecnica di diffusione e installazione.

Come spiegano nel report pubblicato su Internet i ricercatori che lo hanno scovato, Vimoz viene infatti diffuso attraverso campagne di spam e phishing, proponendo il file di installazione come un aggiornamento o una nuova versione di Zoom.

Uno stratagemma piuttosto banale, ma che in un periodo caratterizzato dalla pandemia da **Covid** 19 e dal conseguente utilizzo intensivo di strumenti di videoconferenza può contare su buone probabilità di avere successo.

Una volta che la vittima ha avviato il file di installazione sul computer, Vimoz avvia una complicata catena di attività per installare il suo payload. Per prima cosa installa una serie di file legittimi correlati a Zoom, tra i quali però c'è una DLL malevola (**Cmmlib.dll**) che viene inserita nella cartella di installazione.

La tecnica adottata dai pirati fa leva su alcune caratteristiche di Windows e, in particolare, sulle procedure che il sistema operativo usa per eseguire le DLL relative a un software. **In questo caso, i pirati si assicurano l'esecuzione del codice contenuto al suo interno proprio grazie al fatto che la DLL malevola è memorizzata nella stessa cartella dell'eseguibile (legittimo) di Zoom**.

A questo punto, Vizom avvia il download di un secondo payload che viene prelevato da un repository su cloud e che contiene, ancora una volta, un file di installazione di un software assolutamente insospettabile come **Vivaldi**, un browser freeware multipiattaforma.

Per garantire l'esecuzione del browser, Vizom modifica tutti i collegamenti interni a Windows in modo che, qualunque sia il browser che la vittima intende aprire, venga avviato comunque Vivaldi.

L’utente, però, vedrà comunque aprirsi il browser che ha avviato. Questo, però, verrà eseguito come una dipendenza di Vivaldi. L’obiettivo, infatti, è esclusivamente quello di mantenere attiva la DLL associata a Vivaldi e consentire così ai pirati informatici di monitorare la navigazione della vittima.

Il loro obiettivo, spiegano i ricercatori, è quello di sapere quando si collegano a un servizi odi home banking e sfruttare un classico sistema basato su un **overlay** a tutto schermo (consentito proprio dalle caratteristiche di Vivaldi) che gli consente di catturare degli screenshot dal computer infetto, mentre un modulo a parte si occupa di registrare tutto ciò che viene digitato sulla tastiera (comprese ovviamente le password) attraverso un **keylogger**.

Gli attacchi, spiegano i ricercatori, sarebbero per il momento concentrati sul territorio brasiliano. Le particolarissime caratteristiche del malware, però, potrebbero portare i cyber

criminali ad allargare il loro campo d’azione o a estendere l’attività fornendone il codice ad altri pirati informatici, secondo la logica (ormai diffusissima) del “malware as a service”.

Condividi l’articolo

Bug nelle VPN SonicWall: 800.000 dispositivi a rischio

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/19/si-finge-zoom-e-infetta-il-computer-ecco-il-malware-vizom/?utm_source=rss&utm_medium=rss&utm_campaign=si-finge-zoom-e-infetta-il-computer-ecco-il-malware-vizom

---

Bug nelle VPN SonicWall: 800.000 dispositivi a rischio

Ott 16, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità consente di mandare in crash i firewall con estrema facilità. Basta conoscere

l’indirizzo IP a cui è assegnata l’appliance.

Da una ricerca su **Shodan**, le VPN potenzialmente vulnerabili risultano essere 800.000. Si tratta dei modelli **SonicWall Network Security Appliance**, utilizzati come firewall e filtri VPN a livello aziendale.

Il bug che preoccupa gli esperti (CVE-2020-5135) è stato individuato dalla società di sicurezza **Tripwire VERT**, che ha segnalato la falla di sicurezza in un post pubblicato sul blog ufficiale dell’azienda.

Come si legge nel report redatto da **Craig Young**, il problema si annida in **SonicOS**, il sistema operativo che gestisce i dispositivi SonicWall.

A rendere problematica la presenza della vulnerabilità contribuisce il fatto che, secondo i ricercatori, questa potrebbe essere sfruttata con estrema facilità, al punto che un “attaccante privo di particolari capacità” potrebbe **bloccarne il funzionamento**. Un bel guaio, visto che stiamo parlando di un componente cui è demandato il compito di proteggere il traffico di rete.

Non è escluso, però, che il bug possa essere sfruttato anche per attacchi più complessi (e pericolosi) che portino all'esecuzione di codice in remoto e, di conseguenza, a una completa compromissione del dispositivo.

La facilità nel portare l'attacco è dovuta al fatto che l'anello debole su cui fa leva è SSLVPN, un componente che è esposto su Internet. In altre parole, per raggiungerlo un pirata informatico non dovrebbe superare alcun ostacolo: basta conoscere l'indirizzo IP a cui è raggiungibile.

La vulnerabilità, cui è stato assegnato un punteggio di criticità di **9.4 punti su 10**, è stata corretta con le nuove versioni del sistema operativo SoincOS.

Si tratta, nel dettaglio, delle versioni:

- SonicOS 6.5.4.7-83n
- SonicOS 6.5.1.12-1n
- SonicOS 6.0.5.3-94o
- SonicOS 6.5.4.v-21s-987

- SonicOS 7 7.0.0.0-2

Il suggerimento, naturalmente, è quello di aggiornare immediatamente. Secondo i ricercatori, infatti, sarà presto disponibile un **Proof of Concept (PoC)** che potrebbe essere utilizzato per portare i primi attacchi.

Condividi l’articolo

Le azioni di contrasto a TrickBot falliscono, ma il successo è a livello legale

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/16/bug-nelle-vpn-sonicwall-800-000-dispositivi-a-rischio/?utm_source=rss&utm_medium=rss&utm_campaign=bug-nelle-vpn-sonicwall-800-000-dispositivi-a-rischio