Smantellata la botnet Emotet

Gen 28, 2021 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

L'operazione congiunta tra Europol e FBI ha messo fuori combattimento centinaia di server usati dai pirati per gestire la rete di computer infetti.

Viene definito come uno dei maggiori successi mai ottenuti dalle forze di polizia nel contrasto al cyber crimine e l'entusiasmo che trasuda dal comunicato stampa pubblicato da **Europol** è più che giustificato: l'abbattimento della botnet **Emotet** rappresenta infatti un colpo storico nella lotta alla pirateria informatica.

L'operazione, che ha visto il coinvolgimento di diverse agenzie tra cui l'**FBI** e la britannica **National Crime Agency**, ha preso di mira centinaia di server che i pirati informatici utilizzavano per controllare a distanza i computer compromessi con il trojan, consentendo alle autorità di prenderne, di fatto, il controllo.

Emotet è una delle botnet più longeve e pericolose in circolazione, la cui diffusione è stata portata avanti sistematicamente attraverso tecniche di attacco che sfruttavano principalmente l'invio di documenti infetti di Word tramite messaggi email.

Il "peso" di Emotet, però, dipende anche dal fatto che i cyber criminali che gestivano le sue operazioni sono stati in grado, nel tempo, di tessere relazioni di affiliazione con altri gruppi di pirati informatici.

Emotet, in pratica, ha rappresentato per anni una sorta di vettore di attacco che consentiva ai cyber criminali di

installare ulteriore malware sui computer compromessi, favorendo così la diffusione di ransomware e trojan bancari come il famigerato **TrickBot**.

Uno schema, quello delle affiliazioni, che assume spesso la forma del "**malware as a service**" e che consente ai pirati informatici di espandere il loro raggio d'azione con estrema facilità.

L'operazione messa a segno si somma ad altre azioni simili portate negli ultimi mesi, tra cui la (parziale) distruzione della già citata botnet TrickBot, di cui abbiamo parlato in questo articolo.

La vicenda, in ogni caso, conferma come le agenzie delegate alla cyber sicurezza stiano adottando sempre più spesso un approccio "proattivo", che mira a disarticolare le organizzazioni criminali piuttosto che giocare la partita "in difesa".

Condividi l'articolo

La vulnerabilità Sudo “Baron Samedit” mette a rischio le distro Linux

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2021/01/28/smantellata-la-botnet-emotet/?utm_source=rss&utm_medium=rss&utm_campaign=smantellata-la-botnet-emotet

La vulnerabilità Sudo “Baron Samedit” mette a rischio le distro Linux

Gen 27, 2021 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug consente a qualsiasi utente di ottenere i privilegi di root. Gli esperti: “la falla di sicurezza è presente nel sistema da quasi 10 anni”.

Elevazione di privilegi ai massimi livelli disponibile per qualsiasi utente su un sistema **Linux**. È questa, in sintesi la

descrizione della nuova vulnerabilità (CVE-2021-3156) individuata dai ricercatori e prontamente corretta dal **Sudo Team** che si occupa dello sviluppo del sistema open source.

La falla di sicurezza, battezzata con il nome di **Baron Samedit**, è stata individuata dalla società di sicurezza **Qualys**, all'interno di un'indagine che ha fatto emergere altre due falle di sicurezza con caratteristiche simili. Gli altri bug, però, assumono una certa rilevanza in condizioni particolari (installazioni non-standard delle distro) e hanno quindi un impatto minore.

Baron Samedit, invece, affligge numerose distro Linux e consentirebbe a un qualsiasi utente di ottenere i privilegi di root esattamente come se fosse compreso nella lista dei "sudoer", cioè gli account cui è concesso di eseguire comandi **su** e **sudo**.

Stando al report redatto dai ricercatori, il bug sarebbe presente nei sistemi Linux **da luglio 2011**, cioè da quasi 10 anni.

[embedded content]

Gli scenari in cui la vulnerabilità potrebbe essere sfruttata sono numerosi, ma i principali sono due. Il primo riguarda l'ipotesi di un operatore che ha accesso a un account con privilegi limitati e che potrebbe sfruttare il bug per aumentarli.

Il secondo, invece, riguarda le **classiche botnet di dispositivi con sistemi Linux**, che grazie a Baron Samedit potrebbero fare un salto di qualità ottenendo uno strumento che gli permette di avere facilmente i privilegi di root.

Gli sviluppatori hanno già rilasciato gli aggiornamenti che consentono di correggere il bug e invitano tutti gli utenti (con una certa urgenza) ad applicarli su tutte le installazioni.

Condividi l’articolo

Vulnerabilità in TikTok consentiva di violare la privacy degli utenti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/27/la-vulnerabilita-sudo-baron-samedit-mette-a-rischio-le-distro-linux/?utm_source=rss&utm_medium=rss&utm_campaign=la-vulnerabilita-sudo-baron-samedit-mette-a-rischio-le-distro-linux

---

Vulnerabilità in TikTok consentiva di violare la privacy degli utenti

Gen 26, 2021 Marco Schiaffino In evidenza, News, Privacy, RSS, Vulnerabilità 0

I bug avrebbero consentito di ottenere informazioni sugli account che i pirati informatici avrebbero potuto usare per portare attacchi di phishing.

I guai per **TikTok** non arrivano solo dal garante per la privacy

italiano, che ha recentemente intimato al social network cinese di interrompere il trattamento dei dati per gli utenti di cui non è in grado di verificare l'età. Qualche problema inerente la privacy emerge anche dai suoi sistemi di autenticazione.

A spiegarlo è **Check Point**, che nei mesi scorsi ha avviato un'analisi approfondita dei sistemi di autenticazione di TikTok, individuando una vulnerabilità che avrebbe permesso di accedere a informazioni sensibili riguardanti gli utenti del social network.

TikTok è uno dei social network che, negli ultimi anni, ha registrato il più elevato aumento di utenti, con una media di circa 100 milioni di nuovi utilizzatori al mese. **Secondo gli esperti, nel 2021 potrebbe superare il miliardo di utenti mensili**.

Come spiegano i ricercatori della società di sicurezza in un post pubblicato sul blog ufficiale di Check Point, il problema di privacy riguarda gli account che utilizzano come strumento di autenticazione **il numero di telefono dell'utente**.

Il sistema implementato da TikTok, infatti, sfrutta alcuni parametri (l'ID del dispositivo e un token di sessione) per verificare l'autenticità dell'account. Entrambi, però, hanno una durata di 60 giorni e la loro verifica avviene attraverso una query tramite messaggi su protocollo HTTP.

I ricercatori di Check Point, però, hanno trovato il modo di aggirare il sistema di verifica dei messaggi, consentendo così di avviare un'operazione in grande scala di profilazione degli utenti. **In altre parole, sfruttando il bug un pirata informatico potrebbe interrogare i server di TikTok per estrarre dai database le informazioni memorizzate al loro interno**.

Insomma: la vulnerabilità avrebbe permesso di associare il nome degli utenti ai rispettivi numeri di telefono, consentendo così ai pirati informatici di sfruttare queste informazioni per eventuali attacchi, basati ad esempio su tecniche di phishing.

La segnalazione di Check Point ha consentito agli sviluppatori del social network di correggere la falla e bloccare eventuali attacchi di questo genere.

Condividi l'articolo

SonicWall subisce un attacco che ha sfruttato una falla in un suo firewall

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/26/vulnerabilita-in-tiktok-consentiva-di-violare-la-privacy-degli-

utenti/?utm_source=rss&utm_medium=rss&utm_campaign=vulnerabilita-in-tiktok-consentiva-di-violare-la-privacy-degli-utenti

---

SonicWall subisce un attacco che ha sfruttato una falla in un suo firewall

Gen 25, 2021 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS, Vulnerabilità 0

I pirati avrebbero sfruttato un bug zero-day presente nel dispositivo. L'azienda indaga e prepara la patch per correggere la vulnerabilità.

Subire un attacco informatico è piuttosto frustrante. Scoprire che i pirati hanno colpito grazie a una vulnerabilità zero-day presente in un tuo prodotto lo è probabilmente di più.

È quanto successo a **SonicWall**, azienda che produce dispositivi di rete tra cui VPN e Firewall. L'annuncio della violazione, pubblicato lo scorso venerdì attraverso uno scarno comunicato pubblicato sul sito dell'azienda, parla di un "attacco sofisticato" che avrebbe (probabilmente) sfruttato una falla di sicurezza sconosciuta, presente nelle stesse appliance di sicurezza SonicWall.

I prodotti individuati in un primo momento dall'azienda come possibili bersagli dell'attacco sono due: i clienti **NetExtender VPN** e i gateway **Secure Mobile Access (SMA)**.

Nell'aggiornamento pubblicato nella giornata di sabato, però,

SonicWall ha specificato che il campo è stato ristretto ai **dispositivi SMA della serie 100**, escludendo che il problema possa trovarsi nel client VPN.

Mentre gli esperti di SonicWall continuano a investigare per definire i contorni e le dinamiche dell'attacco subito dall'azienda, i suoi tecnici si sono preoccupati di comunicare alcuni accorgimenti che permetterebbero di mitigare il rischio di attacchi per gli utenti che usano i due prodotti in questione.

Nel dettaglio, il loro suggerimento è di **limitare le connessioni ai dispositivi SMA attraverso la predisposizione di una White List che consenta di bloccare eventuali comunicazioni malevole**. Questo, spiegano nel comunicato, può essere fatto attraverso un firewall o utilizzando gli stessi sistemi di configurazione di SMA.

L'attacco a SonicWall conferma una nuova tendenza, emersa in queste ultime settimane, che vede evidentemente i pirati informatici particolarmente interessati agli strumenti e alle tecnologie in uso alle società di sicurezza. Prima dell'azienda californiana, infatti, a subire le "attenzioni" dei cyber criminali sono stati **FireEye**, **Microsoft** e **Malwarebytes**.

Condividi l’articolo

Rubano le credenziali a migliaia di utenti ma i dati finiscono su… Google!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/25/sonicwall-subisce-un-attacco-che-ha-sfruttato-una-falla-in-un-suo-firewall/?utm_source=rss&utm_medium=rss&utm_campaign=sonicwall-subisce-un-attacco-che-ha-sfruttato-una-falla-in-un-suo-firewall

---

Rubano le credenziali a migliaia di utenti ma i dati finiscono su… Google!

Gen 22, 2021 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS, Scenario 0

I dati rubati dai cyber criminali attraverso una campagna di phishing sono stati indicizzati dal motore di ricerca e chiunque vi ha potuto accedere.

Anche i pirati informatici sbagliano. E per una sorta di legge

del contrappasso, capita che commettano gli stessi errori che in altre occasioni hanno sfruttato per mettere a segno le loro azioni.

Nel caso specifico, un gruppo di cyber criminali ha condiviso con il resto del mondo tutte le credenziali che avevano rubato attraverso una complessa campagna di phishing.

A raccontare la vicenda sono i ricercatori di Check Point, che in un post pubblicato sul blog ufficiale della società di sicurezza descrivono lo strano caso del gruppo di pirati che ha diffuso involontariamente i dati che avevano (faticosamente) raccolto da migliaia di ignari utenti.

Gli attacchi spiegano gli analisti, erano ben congegnati e sfruttavano una tecnica estremamente efficace, che prevedeva come vettore iniziale di attacco un'email con un allegato in formato HTML.

Quando la vittima apriva il file allegato, si trovava di fronte a un'immagine sfocata di un documento, con una finestra pop-up che richiedeva l'inserimento delle credenziali di **Microsoft 365** per proseguire. Per rendere più credibile l'inganno, i pirati **hanno previsto un sistema di compilazione**

automatica del campo email, in cui veniva visualizzato automaticamente l'indirizzo di posta della vittima.

Una volta inserita la password, il dato veniva registrato dai sistemi dei pirati e la vittima veniva a questo punto indirizzata su una pagina di accesso legittima ai servizi Microsoft.

Insomma: uno schema piuttosto semplice, ma decisamente efficace. Tanto più che i pirati, nella predisposizione della campagna di attacchi, hanno usato una serie di tecniche di offuscamento per aggirare i controlli antivirus e hanno sfruttato numerosi siti **WordPress** compromessi come "drop zone".

L'obiettivo, in teoria, era quello di utilizzare un ulteriore livello di offuscamento per nascondere le loro tracce. **Ciò che non hanno considerato, però, è che l'algoritmo di indicizzazione di Google ha "pescato" i dati sui server Web che hanno usato per memorizzare le credenziali rubate e li ha proposti a tutti gli utenti Internet**.

Insomma: tutte le informazioni che avevano rubato sono state condivise con circa 5 miliardi di persone sul pianeta. Un vero erroraccio, che per i pirati informatici si è trasformato (oltre che in una figuraccia) in un disastro economico. Chi potrebbe mai comprare informazioni cui tutti hanno accesso?

Condividi l’articolo

Nuovi sviluppi e un (possibile) leak nel caso SolarWinds

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/22/rubano-le-credenziali-a-migliaia-di-utenti-ma-i-dati-finiscono-su-google/?utm_source=rss&utm_medium=rss&utm_campaign=rubano-le-credenziali-a-migliaia-di-utenti-ma-i-dati-finiscono-su-google

---

Nuovi sviluppi e un (possibile) leak nel caso SolarWinds

Gen 21, 2021 Marco Schiaffino Attacchi, In evidenza, Intrusione, Leaks, Malware, News, RSS, Scenario 0

I contorni dell'attacco che ha preso di mira la società texana continuano ad ampliarsi. Ecco il punto della situazione a più di un mese dalla scoperta.

Più di 250 reti informatiche compromesse, 18.000 organizzazioni tuttora considerate "a rischio" e una vicenda che, nel complesso, ha ancora molti lati oscuri.

A 40 giorni dal primo allarme, l'attacco che ha coinvolto **SolarWinds** e le aziende che utilizzano il suo software **Orion** è ancora oggetto di analisi da parte degli esperti di sicurezza.

La vicenda, di cui abbiamo riassunto i tratti salienti in questo articolo, si è infatti complicata a dismisura e nessuna delle ipotesi fin qui formulate sembra aver trovato un riscontro definitivo.

Le uniche certezze riguardano il fatto che i soggetti coinvolti, inizialmente stimati in un numero ridotto, sono molti più numerosi. Oltre ad alcuni dipartimenti dell'amministrazione statunitense, infatti, nella conta rientrerebbero anche aziende del settore tecnologico come **Intel**, **Microsoft** e **Cisco**.

Buio pesto, invece, per quanto riguarda la ricostruzione delle fasi dell'attacco. Oltre a **Sunburst**, il primo identificato dai ricercatori, sarebbero emersi **altri tre malware** utilizzati nell'attacco o comunque presenti sui server di SolarWinds.

Il primo, che i pirati avrebbero utilizzato nella fase iniziale dell'attacco ai sistemi dell'azienda, si chiama **Sunspot** e avrebbe avuto la funzione di consentire l'iniezione della backdoor Sunburst all'interno del codice di Orion.

Gli altri due malware (**Teardrop** e **Raindrop**) sarebbero invece stati utilizzati per compromettere le reti delle organizzazioni che hanno installato la versione malevola di Orion. I due trojan, identificati da **Symantec**, differiscono per alcune caratteristiche e sembrano essere lo "stadio

finale” dell’attacco.

Il caso, però, è reso ancora più complesso dalla presenza di un quinto malware, battezzato con il nome di **SuperNova**. Come spiegano i ricercatori di **Secureworks** in un post sul blog della società di sicurezza, si tratta di una **Web Shell** che sarebbe stata iniettata nei sistemi di SolarWinds sfruttando una vulnerabilità zero-day della piattaforma.

Secondo gli esperti che stanno analizzando l’attacco, la presenza di SuperNova non è necessariamente collegata all’attacco principale e potrebbe essere addirittura opera di un altro gruppo di pirati informatici.

Poche certezze anche per quanto riguarda l’attribuzione dell’attacco. Se il governo statunitense non ha esitato a puntare il dito contro i servizi segreti russi ipotizzando il coinvolgimento del famigerato gruppo APT **Cozy Bear**, gli ultimi sviluppi della vicenda hanno portato gli esperti di sicurezza a sollevare qualche dubbio.

Lo scorso 12 gennaio, infatti, è comparso su Internet il sito **Solarleaks.net**, il cui contenuto (impossibile da verificare) porterebbe alla conclusione che gli autori dell’attacco abbiano finalità ulteriori rispetto a quelle dello spionaggio.

Nel sito, infatti, viene promossa la vendita di informazioni riservate provenienti dai sistemi compromessi in cambio di denaro. **Qualcosa che stride decisamente con il modus operandi degli hacker di Cozy Bear**.

Nel dettaglio, i (presunti) autori dell’attacco offrirebbero il codice sorgente di prodotti di FireEye, Intel, Microsoft e Cisco in cambio di una contropartita che per il “pacchetto completo”, sarebbe di 1 milione di dollari.

Il sito, che si affida per l'hosting a **Njalla** (noto per offrire un elevato livello di segretezza – ndr) e i cui dati di registrazione riportano semplicemente la dicitura "**YOU CAN GET NO INFO**", riporta una firma digitale e un indirizzo che punta a un wallet **Monero** per il pagamento.

Impossibile, almeno in questa fase, capire se la rivendicazione sia credibile o meno. I dubbi, però, sono tanti. A moltiplicarli è stata anche un'ulteriore mossa fatta dai (presunti) pirati informatici.

Il giorno seguente alla pubblicazione, infatti, gli amministratori del sito hanno pubblicato una nuova porzione di testo in cui chiedono a chiunque voglia mettersi in contatto con loro di versare anticipatamente 100 Monero (XMR), l'equivalente al cambio attuale di **15.000 euro**.

Insomma: il sospetto che si tratti semplicemente di qualcuno che stia cercando di approfittare della situazione è più che concreto, ma il (presunto) leak per il momento ha l'unico effetto di rendere ancora più confuso tutto il quadro.

Condividi l'articolo

Rubano le credenziali a migliaia di utenti ma i dati finiscono su… Google! Trend Micro: ecco cosa ci aspetta nel 2021 nel mondo della cyber security

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/21/nuovi-sviluppi-e-un-possibile-leak-nel-caso-solarwinds/?utm_source=rss&utm_medium=rss&utm_campaign=nuovi-

sviluppi-e-un-possibile-leak-nel-caso-solarwinds

Trend Micro: ecco cosa ci aspetta nel 2021 nel mondo della cyber security

Gen 20, 2021 Marco Schiaffino In evidenza, News, RSS, Scenario 0

La società di sicurezza ha pubblicato le previsioni per il prossimo anno. Una vera "marea" di attacchi previsti per il prossimo futuro.

Dopo i bilanci di fine anno, è arrivato il momento per le previsioni per il prossimo futuro. A farle è anche **Trend Micro**, che ha pubblicato il report che illustra le tendenze in ambito cyber security per il nuovo anno. Intitolato "**Turning The Tide**", lo studio evidenzia alcuni degli elementi critici che caratterizzeranno questo 2021.

Il punto di partenza, naturalmente, investe i grandi cambiamenti introdotti da questo (terribile) 2020 appena terminato. Primo tra tutti il fenomeno dell'home working, che secondo gli esperti è destinato a mantenere un ruolo centrale anche nei prossimi 12 mesi.

Nella prospettiva di chi si occupa di sicurezza, questo porterà prevedibilmente a **un aumento degli attacchi rivolti ai dispositivi personali e alle reti domestiche**, che i pirati informatici potranno sfruttare come "testa di ponte" per arrivare alle reti aziendali.

Di più: come hanno spiegato gli esperti di Trend Micro nel corso della conferenza stampa in cui è stato presentato il report, la nuova geografia del lavoro potrà portare anche a una crescita di attacchi “indiretti”.

La logica è semplice quanto inquietante: **potendo far leva sul fatto che i dispositivi casalinghi sono spesso utilizzati da più membri della famiglia, i cyber criminali potranno prendere di mira i congiunti del loro reale bersaglio per rendere più efficaci le loro tattiche di attacco**.

Sotto un profilo più tecnico, l’attenzione degli autori del report si concentra sulla probabile crescita degli attacchi basati su exploit “n-day”, cioè gli attacchi che sfruttano vulnerabilità conosciute ma estremamente recenti.

Quello che ci si aspetta, in pratica, è che i i pirati informatici saranno in grado di sfruttare le falle di sicurezza con (ancora) maggiore rapidità. Secondo gli esperti di Trend Micro, di conseguenza, **sarà necessario ridurre i tempi per installare le patch che correggono i bug individuati dalla community dei ricercatori**.

Tra i vettori di attacco che ci si aspetta possano vivere una

fase di crescita ci sono poi le API, i componenti utilizzati per far interfacciare diverse applicazioni.

In questo caso le problematiche sono legate al fatto che l'uso sempre più diffuso delle **API**, utilizzate per esempio per accedere a servizi collegati a quelli cui fanno riferimento, aprono facilmente la strada ad abusi e violazioni da parte dei cyber criminali.

Un fenomeno cui i ricercatori stanno già assistendo, che nel prossimo futuro sarebbe destinato a crescere di intensità e frequenza.

Condividi l'articolo

Kaspersky Automotive IT: focus sulla security nel settore automobilistico

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/20/trend-micro-ecco-cosa-ci-aspetta-nel-2021-nel-mondo-della-cyber-security/?utm_source=rss&utm_medium=rss&utm_campaign=trend-micro-ecco-cosa-ci-aspetta-nel-2021-nel-mondo-della-cyber-security

---

Kaspersky Automotive IT:

focus sulla security nel settore automobilistico

Gen 19, 2021 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario 0

La società di sicurezza espande i suoi servizi al settore dell'automotive. "Proteggere i veicoli di nuova generazione dagli attacchi cyber è una priorità".

Si chiama "Automotive IT" ed è un servizio che punta a fornire informazioni e risorse al settore automobilistico per garantire la sicurezza informatica dei sistemi digitali integrati nei veicoli di nuova generazione.

A proporlo è **Kaspersky**, società di sicurezza che ha recentemente deciso di ampliare il suo servizio di **threat intelligence reporting** alle organizzazioni che lavorano nel settore automobilistico. Il servizio, che in precedenza era disponibile solo per un numero selezionato di clienti, consente di ottenere un'analisi approfondita delle minacce alla sicurezza specifiche per il settore, identificando le informazioni che potrebbero essere utilizzate dai criminali informatici per lanciare attacchi ai veicoli, all'infrastruttura dei veicoli connessi e ad altri sistemi correlati.

Un tema, quello della sicurezza informatica nell'industria automobilistica, che suscita un crescente interesse e sta ottenendo grande attenzione a tutti i livelli. La cronaca recente, infatti, ha registrato un numero crescente di bug e falle di sicurezza che aprono la strada a possibili attacchi ai danni dei sistemi che gestiscono il funzionamento dei veicoli.

Quello messo in campo da Kaspersky è un vero ecosistema, che consente di avere una serie di report che comprendono **una panoramica e un’analisi dei trend tecnologici relativi agli attacchi informatici nell’industria automobilistica tra cui i cyber-incidenti**, gli studi più recenti sulla sicurezza, le conferenze, i dibattiti, i forum della community, nonché le informazioni sui potenziali vettori di attacco ai backend del veicolo e all’’infrastruttura dei servizi.

Insomma: qualcosa che permette agli operatori del settore di rimanere informati sulle criticità in tema di cyber security e che, in caso di minacce urgenti, consente di ricevere un alert in tempo reale.

“Il crescente numero di tecnologie utilizzate nei veicoli moderni impone non solo il rispetto dei requisiti normativi vigenti, ma anche di disporre di informazioni sulle potenziali minacce, dalle vulnerabilità delle unità di controllo elettronico agli attacchi ai componenti vehicle-to-everything” spiega **Sergey Zorin, Head of Kaspersky Transportation System Security di Kaspersky**. “Fornendo informazioni rilevanti sulle minacce, Kaspersky aiuta le case automobilistiche a fronteggiare queste criticità”.

Condividi l’articolo

Chiude Joker’s Stash. Lo shop di carte di credito rubate

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/19/kaspersky-automotive-it-focus-sulla-cyber-security-nel-settore-automobilistico/?utm_source=rss&utm_medium=rss&utm_campaign=kaspersky-automotive-it-focus-sulla-cyber-security-nel-settore-automobilistico

---

Chiude Joker’s Stash. Lo shop di carte di credito rubate

Gen 18, 2021 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario 0

L’addio è previsto per il prossimo 15 febbraio e il gestore del “negozio” lo ha comunicato su tutti i forum frequentati dai pirati informatici.

Fermarsi al culmine del successo ma prima di essere arrestati: è questa, probabilmente, la vera sfida per un cyber criminale. Non tutti ci riescono e l’elenco di chi ha finito la sua carriera dietro le sbarre è decisamente nutrito.

Tra questi, però, non ci sarà (forse) l'amministratore di **Joker's Stash**, il più famoso negozio online per la compravendita di dati di carte di credito rubate.

In un post pubblicato su numerosi forum frequentati da cyber criminali di ogni nazionalità, il "cervello" di Joker's Stash ha annunciato l'addio alle scene, avvisando anche il suo pubblico di riferimento che non ci sono margini per eventuali ritorni.

Un avvertimento, questo, che probabilmente mira a prevenire eventuali tentativi da parte di qualche concorrente di sfruttare il nome dello shop online per attirare clienti.

Joker’s Stash ha aperto i battenti nel 2014 e, nel corso dei seguenti sei anni, è stato il punto di riferimento per le transazioni illegali legate alla vendita di carte di credito rubate.

Lo scorso ottobre lo store ha avuto un momento di crisi quando il suo amministratore, stando a quanto emerge dalle sue comunicazioni online, è stato ricoverato per una settimana a causa di un’infezione di Covid-19.

Non è chiaro se la disavventura sanitaria abbia giocato un ruolo nella decisione di abbandonare la sua (lucrosa) attività criminale**. Quello che è certo è che l’admin di Joker’s Stash non dovrà certo preoccuparsi della pensione: secondo le stime degli esperti, nel corso della sua attività lo store clandestino avrebbe raggranellato più di un miliardo di dollari**.

Ora i clienti di Joker’s Stash hanno 30 giorni per incassare quanto hanno accumulato sui conti del marketplace. Stando al numero di market attivi nel settore, in ogni caso, non avranno molte difficoltà a trovare delle alternative.

Condividi l’articolo

Bug in Windows 10 manda in crash il disco con… un’icona!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/18/chiude-jokers-stash-lo-shop-di-carte-di-credito-rubate-ha-fruttato-1-miliardo-di-dollari/?utm_source=rss&utm_medium=rss&utm_campaign=chiude-jokers-stash-lo-shop-di-carte-di-credito-rubate-ha-fruttato-1-

miliardo-di-dollari

Bug in Windows 10 manda in crash il disco con… un’icona!

Gen 15, 2021 Marco Schiaffino In evidenza, News, Vulnerabilità 0

La falla di sicurezza provoca un errore che corrompe il file system. Non serve nessun click: basta visualizzare il file in qualsiasi cartella.

Scarichiamo un archivio ZIP, lo apriamo e all’improvviso… Windows visualizza un errore nel file system, avvia una procedura di correzione e ci tiene inchiodati per ore con il PC bloccato. Un malware russo? Un attacco alieno? No: è l’effetto di un misterioso bug del sistema operativo **Microsoft**.

A lanciare l’allarme riguardo la possibilità che la falla di sicurezza possa trasformarsi in un vero cataclisma è **Bleeping Computer**, che in un articolo pubblicato nella giornata di ieri ha analizzato le caratteristiche del bug e le sue possibili applicazioni in un attacco informatico.

Il bug, che nessun sviluppatore riesce a spiegare, è terribilmente semplice: basta inviare uno specifico comando a Windows 10 affinché il sistema registri un’impostazione che provoca la corruzione del **file system NTFS** e renda illeggibile l’unità a cui fa riferimento. Se si tratta di C:, la partizione su cui è normalmente installato il sistema, il PC diventa inutilizzabile.

ATTENZIONE, NON UTILIZZARE IL COMANDO IN QUESTIONE SUL COMPUTER. IL RISULTATO SAREBBE UN CRASH CHE POTREBBE PORTARE AL BLOCCO DEL SISTEMA ALLA PERDITA DEI DATI MEMORIZZATI ALL'INTERNO DEL DISCO

Il comando è estremamente semplice: **cd C:\:$i30:$bitmap**. La sua esecuzione avvia la corruzione del file system e un loop di procedure di correzione che hanno, in pratica, l'effetto di mettere K.O. il sistema.

Ma come potrebbero sfruttarlo dei pirati informatici? Qui viene il bello. Perché i colleghi di Bleeping Computer hanno provato a immaginare metodi che permettono la sua attivazione con il minimo livello di interazione da parte dell'utente.

Quello più efficace è indicare il percorso questione come oggetto dell'icona di un file. Con questa strategia, un cyber criminale dovrebbe solo "convincere" la vittima a scaricare un file o un archivio compresso che contiene il file cui è associata l'icona. **A questo punto, basterebbe che l'utente visualizzi il contenuto della cartella per avviare il caricamento del file e, di conseguenza l'attacco**.

L’ipotesi descritta qui sopra è solo una di innumerevoli possibili tattiche che possono portare all’utilizzo dell’exploit. Insomma: Microsoft si trova ad avere a che fare con un bug potenzialmente devastante, che potrebbe essere utilizzato da chiunque nel prossimo futuro. Incrociamo le dita…

Condividi l’articolo

Attacchi a Windows e Android sfruttavano falle zero-day

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/15/un-bug-in-windows-10-permette-di-mandare-in-crash-il-disco-con-unicona/?utm_source=rss&utm_medium=rss&utm_campaign=un-bug-in-windows-10-permette-di-mandare-in-crash-il-disco-con-unicona