Un “calzino sporco” minaccia gli utenti Ubuntu

Feb 14, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Dirty Sock permette di ottenere privilegi di root sui sistemi Canonical. Niente panico: l’aggiornamento è già disponibile.

La vulnerabilità è stata catalogata come CVE-2019-7304 e come spiega nel suo report **Chris Moberly**, il ricercatore che l’ha scoperta, consentirebbe di ottenere privilegi di root su tutti i sistemi (desktop e server) su cui gira **Ubuntu** nelle versioni precedenti alla 19.04.

La falla di sicurezza riguarda le **API Snapd** e in particolare il modo in cui gestiscono le richieste di dati HTTP. **Snap** è il sistema di gestione delle applicazioni, che mette a disposizione un ecosistema con il classico stile dello “store”.

L’attacco consente di sfruttare il bug nelle API di Snapd (il servizio systemd dedicato a Snap) per “ingannare” il sistema e fargli credere che l’utente corrente abbia un **UID** (User Identifier) pari a 0, cioè quello che indica l’utente di root.

Il risultato è che attraverso l'uso di **Dirty Sock** (questo il nome che Moberly ha coniato per l'exploit che ha pubblicato su Internet) è possibile prendere il completo controllo del sistema.

La buona notizia è che non si tratta di un exploit "completo". Dirty Sock, cioè, **non può essere usato in remoto** ed è quindi necessario che un eventuale pirata informatico abbia già ottenuto accesso al sistema.

Inutile dire che il suo utilizzo in abbinata ad altri exploit rimane però un rischio concreto. **Canonical** ha rilasciato un aggiornamento disponibile attraverso il sistema di update di Ubuntu ed è anche disponibile un aggiornamento (2.37.1) per Snapd.

Please follow and like us:

La Russia punta ad avere un'Internet "autosufficiente"

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/02/14/un-calzino-sporco-minaccia-gli-utenti-ubuntu/

La Russia punta ad avere un'Internet "autosufficiente"

Feb 13, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia 0

La proposta di legge è stata approvata dalla Duma e gli operatori si preparano a fare un test entro la primavera. Prove tecniche di cyber-war?

È possibile rendere completamente autosufficienti le infrastrutture Internet di una nazione? Secondo il parlamento russo sì.

La **Duma** ha infatti approvato in prima lettura una bozza di legge intitolata "Programma nazionale di economia digitale" che mette, tra i suoi obiettivi, quello di creare **RuNet**, una sorta di "Internet sovrana" che dovrebbe garantire il collegamento ai siti russi anche in caso di isolamento dal resto della Rete.

Lo scenario dal quale il governo russo vorrebbe tutelarsi è

quello di **un cyber-attacco che blocchi completamente Internet sul territorio della Federazione Russa** e per farlo si starebbe progettando una struttura che consenta alle autorità di filtrare il traffico sulla base della sua origine.

Il progetto di legge non fornisce i dettagli, ma secondo le informazioni riportate da agenzie di stampa russe (qui l'articolo che suggeriamo di leggere con la traduzione automatica in inglese) la logica dovrebbe essere quella di "scartare" tutto il traffico proveniente dall'esterno e consentire solo il traffico interno, trasformando Internet, in caso di necessità, in una sorta di **intranet**.

Le conseguenze di questo progetto, però, sono tutt'altro che banali e stanno suscitando polemiche anche in Russia. **Per arrivare a questo risultato, infatti, il governo dovrebbe avere il controllo totale degli exchange point**.

Una situazione, questa, che solleva la questione della possibilità di censurare i contenuti con (ancora) maggiore efficacia rispetto a quanto accade adesso.

Uno dei nodi focali, però, è quello che riguarda i **server DNS**. Per il momento, infatti, nessuno dei DNS primari si trova su territorio russo e la creazione di una RuNet funzionante richiederebbe la creazione di un circuito di DNS alternativo a quello attualmente in uso sul pianeta.

Un progetto, questo, che per la verità non è nuovo e per il momento era stato ventilato a livello di **BRICS**, il gruppo di "paesi emergenti" (**Brasile, Russia, India, Cina e Sud Africa**) che già in passato hanno mostrato una certa insofferenza nei confronti dell'egemonia statunitense nella gestione delle infrastrutture Internet.

Il prossimo passo, in ogni caso, si colloca in un orizzonte temporale piuttosto vicino. **Il primo "test di autosufficienza" dovrebbe infatti tenersi entro il 1 aprile 2019**.

L'esperimento prevederà la collaborazione di numerosi **Internet Service Provider** e comporterà un blocco della navigazione dall'interno verso l'esterno della federazione. Nulla si sa della durata che avrà il blocco o di come sarà gestito.

Tutta a vicenda, però, apre scenari completamente nuovi e che potrebbero impattare pesantemente sulla struttura stessa di Internet per come la conosciamo. **Se altri paesi dovessero seguire questa strada, nel giro di poco tempo potremmo trovarci a utilizzare una Rete molto diversa da quella che conosciamo oggi**. Con quali conseguenze, è tutto da vedere.

Please follow and like us:

Falla in Docker permette di portare attacchi negli ambienti cloud

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/02/13/la-russia-punta-ad-avere-uninternet-autosufficiente/

Usate Android? Attenti alle foto coi gattini!

Feb 08, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Vulnerabilità 0

Il sistema operativo mobile di Google ha una falla di sicurezza che permette di distribuire malware attraverso immagini in formato PNG.

Basta una semplice immagine in **formato PNG (Portable Network Graphic)** per avviare esecuzione di codice in remoto su un sistema Android. In altre parole, è sufficiente aprire una qualsiasi immagine per ritrovarsi un malware installato sullo smartphone.

L'allarme arriva dopo la pubblicazione del report di sicurezza Google che elenca le vulnerabilità corrette nella tornata di aggiornamenti di febbraio. Quelle relative il **media framework** (CVE-2019-1986, CVE-2019-1987 e CVE-2019-1988) riguardano appunto la possibilità che un'immagine sia usata come vettore

di attacco.

I ricercatori specificano che non sono ancora stati individuati attacchi che sfruttino questa tecnica, ma ora che la vulnerabilità è pubblica c'è da aspettarsi che nei bassifondi del Web qualcuno si stia già dando da fare per mettere a punto un exploit in grado di sfruttarla.

Le conseguenze di un eventuale attacco con questa tecnica, infatti, potrebbero essere devastanti. Per capirlo basta pensare alla quantità di immagini che circolano ogni giorno nelle varie chat e sui social.

Se un pirata informatico trovasse il modo di prevedere un sistema di diffusione che sfrutti i dispositivi compromessi per distribuire l'immagine infetta a tutti i contatti della vittima, si innescherebbe infatti un vero "effetto valanga".

Il suggerimento è ovviamente di aggiornare il prima possibile Android. Considerato però il meccanismo di distribuzione "a scaglioni" tipico dell'ecosistema Android, è difficile capire quali dispositivi possano essere ancora vulnerabili

all’attacco. **Per evitare problemi, Google non ha diffuso i dettagli tecnici della vulnerabilità**.

In questo caso, per lo meno, non si corre il rischio che ci siano milioni di dispositivi considerati “antiquati” che non possono eseguire l’update. **Il bug, infatti, interessa solo le versioni di Android 7, 8 e 9**.

Insomma: in un mondo perfetto in cui tutti gli utenti eseguono puntualmente gli aggiornamenti dei loro smartphone, il rischio dovrebbe essere superato in una manciata di settimane. Siete più tranquilli?

Please follow and like us:

Trova una falla zero-day in macOS, ma non fornisce i dettagli ad Apple

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/08/usate-android-attenti-alle-foto-coi-gattini/

Trova una falla zero-day in

macOS, ma non fornisce i dettagli ad Apple

Feb 07, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Il ricercatore ha diffuso un video in cui ne mostra l'efficacia. Per il sistema operativo desktop, però, non c'è un programma Bug Bounty.

Il tema della "responsible disclosure" sta diventando sempre più attuale e nel settore della sicurezza informatica si stanno moltiplicando i casi in cui gli stessi ricercatori esprimono un certo disagio per un meccanismo che non dà molte certezze.

Anche se molti sviluppatori hanno avviato **programmi di Bug Bounty** molto strutturati (le procedure che prevedono un compenso per chi segnala un bug – ndr) nel panorama IT ci sono ancora dei "buchi neri" che rendono il percorso piuttosto difficoltoso.

Uno di questi riguarda **Apple**, che non ha ancora avviato un programma del genere per **macOS**, limitandosi a prevedere dei compensi (anche generosi) per chi segnala vulnerabilità di **iOS**.

A prendersela con questa mancanza dell'azienda di Cupertino è oggi **Linus Henze**, un ricercatore che ha individuato una grave falla in **Accesso Portachiavi**, l'app che permette di gestire le credenziali (username e password) su macOS.

L'exploit messo a punto da Henze permette di rubare tutte le credenziali in una manciata di secondi e, stando a quanto spiega il ricercatore in un'intervista con Bleeping Computer,

funziona fino a quando il portachiavi è “aperto”, cioè fino a quando l’utente ha eseguito un login.

[embedded content]

Inutile dire che uno strumento simile nelle mani di un pirata informatico potrebbe avere effetti devastanti, ma **per il momento è difficile che arrivi una patch**.

Henze sostiene di essere stato contattato da Apple dopo la pubblicazione del video, ma di essersi rifiutato di fornire dettagli sulla vulnerabilità. L’azienda di Tim Cook, come abbiamo accennato in precedenza, **non ha un programma di Bug Bounty per macOS** e il ricercatore sembra farne un punto di principio.

Ora vedremo come si svilupperà la vicenda, mail problema rimane. **Per poter contare su un sistema “oliato” nel report delle vulnerabilità, infatti, l’esistenza di regole chiare per tutti sarebbe qualcosa di estremamente positivo**. Per il momento siamo ancora al Far West.

Please follow and like us:

Con la fattura elettronica esplode il rischio di attacchi tramite PEC

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/07/trova-una-falla-zero-day-in-macos-ma-non-fornisce-i-dettagli-ad-apple/

Con la fattura elettronica esplode il rischio di attacchi tramite PEC

Feb 06, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario 0

La nuova normativa ha "rilanciato" la PEC e i pirati informatici non si sono fatti sfuggire l'occasione. La settimana scorsa un nuovo attacco.

Dovrebbe essere uno strumento per garantire la tracciabilità del mittente e l'ufficialità delle comunicazioni. Oggi, però, la **Posta elettronica certificata (PEC)** rischia di trasformarsi in un formidabile strumento di attacco per i pirati informatici e in questi giorni si sono già registrati i primi casi di attacchi.

A rendere attualissimo questo rischio nel nostro paese è **il nuovo sistema di fatturazione elettronica**, entrato in vigore lo scorso 1 gennaio e che sta già procurando qualche grattacapo a chi si trova a doverlo usare.

Fino a oggi, infatti, la PEC veniva utilizzata in ambiti piuttosto limitati. La richiedevano le Pubbliche Amministrazioni, gli ordini professionali e altri soggetti per comunicazioni particolarmente "formali".

Con la fattura elettronica, invece, la quantità di corrispondenza via PEC è destinata a crescere esponenzialmente e il rischio che qualcuno ne approfitti è decisamente elevato.

Il vantaggio di utilizzare una PEC per un cyber-attacco è piuttosto evidente: per fare un parallelo con la classica corrispondenza "analogica", infatti, **la PEC sta all'email come una raccomandata con ricevuta di ritorno sta a una semplice lettera**.

Insomma: il formato "ufficiale" rende più credibile il messaggio e spesso è sufficiente per far abbassare le difese alla potenziale vittima, che tende ad **aprire qualsiasi allegato o fare clic su qualsiasi link** senza preoccuparsi troppo delle possibili conseguenze.

Un tentativo di sfruttare la PEC in questo modo è già stato fatto nel **marzo del 2017**, quando un gruppo di pirati informatici ha utilizzato un indirizzo di posta certificata per distribuire in maniera massiccia una variante del ransomware **Crypt0L0cker**.

Da quest'anno, però, **il meccanismo rischia di essere ancora più efficace**. Quando la fattura elettronica sarà diventata un'abitudine è probabile che negli uffici il traffico di PEC aumenti notevolmente e la registrazione delle fatture recapitate tramite PEC diventino routine.

Qualcuno, per la verità, non ha nemmeno aspettato troppo tempo. Come spiegano i ricercatori di **Yoroy** sul blog ufficiale della società di sicurezza, l'attacco arriva tramite un messaggio proveniente da una casella PEC e ha un oggetto che fa pensare a una comunicazione collegata alla fatturazione elettronica.

- "I: Fattura corretta"
- "I: Obbligo fatturazione dal 1° Gennaio 2019"
- "R: SCADUTO"
- "Avv. scad."
- "fattura in scadenza"
- "I: AVVISO DI PAGAMENTO"
- "I: bonifico ricevuto in data odierna"
- "NS.ORDINE NR.0030961 DEL 30/01/19 "

L'allegato, in formato XLS, contiene una variante del malware **Ursnif** (ne abbiamo parlato anche in questo articolo) che viene attivato quando la vittima autorizza le funzionalità Macro del documento. I ricercatori fanno notare anche che il codice Macro si attiva solo se Office è configurato per la lingua italiana.

Il codice, in pratica, avvia un comando **PowerShell** che è

nascosto all’interno di un’immagine caricata su un sito Internet con la tecnica della **steganografia** e che avvia il download e l’installazione del malware.

Il consiglio, naturalmente, è quello di mantenere alta l’attenzione e verificare sempre chi sia il mittente del messaggio, senza lasciarsi ingannare dalla falsa sicurezza che può derivare dalla dicitura “PEC”.

Please follow and like us:

SpeakUp: il trojan per Linux ha cominciato a diffondersi in Cina

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/06/con-la-fattura-elettronica-esplode-il-rischio-di-attacchi-tramite-pec/

SpeakUp: il trojan per Linux ha cominciato a diffondersi in Cina

Feb 05, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Il malware è comparso lo scorso 14 gennaio. Gli esperti: "Per ora si diffonde in Asia e Sudamerica, ma potrebbero essere solo l'inizio".

Una leggenda metropolitana piuttosto diffusa sostiene che a preoccuparsi dei malware dovrebbero essere solo gli utenti Windows, storicamente bersagliati con maggiore frequenza dai pirati informatici.

A sconfessare questa credenza ci sta pensando (tra gli altri) un nuovo trojan che prende di mira eslcusivamente i sistemi **Linux e macOS**. Si chiama **SpeakUp** ed è stato individuato per la prima volta da **Check Point** a metà di gennaio.

Il trojan, che sfrutta una vulnerabilità (CVE-2018-20062) nel framework **ThinkPHP**, carica una shell PHP per installare una backdoor sul sistema. Come si legge nel report di Check Point, la piattaforma è di origine cinese ed è utilizzata principalmente in Asia. **Stando ai dati della società di sicurezza, però, il trojan si sta diffondendo anche il America Latina**.

I pirati informatici, però, non si sono limitati a sfruttare la falla di sicurezza di ThinkPHP, ma hanno dotato il loro malware di **un arsenale di exploit "secondari"** che SpeakUp usa per diffondersi sulle macchine collegate nella rete locale.

I ricercatori ne hanno individuate sei.

1. a) CVE-2012-0874: JBoss Enterprise Application Platform Multiple Security Bypass Vulnerabilities
2. b) CVE-2010-1871: JBoss Seam Framework remote code execution
3. c) JBoss AS 3/4/5/6: Remote Command Execution (exploit)
4. d) CVE-2017-10271: Oracle WebLogic wls-wsat Component Deserialization RCE
5. e) CVE-2018-2894: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware.
6. f) Hadoop YARN ResourceManager – Command Execution (exploit)
7. g) CVE-2016-3088: Apache ActiveMQ Fileserver File Upload Remote Code Execution Vulnerability.

SpeakUp ha tutte le funzionalità che ci si può aspettare da un trojan modulare, tra cui la possibilità di scaricare e installare ulteriori componenti.

Oltre a questi exploit, SpeakUp utilizza **un modulo di brute forcing** che utilizza un elenco di credenziali standard per cercare di violare le macchine raggiungibili in rete.

A renderlo particolarmente insidioso è il fatto che la maggior parte dei motori antivirus (ma la verifica su **Virus Total** fatta dai ricercatori risale allo scorso 9 gennaio) non lo identifica come un file pericoloso.

Per il momento il gruppo di cyber-criminali che sta utilizzando il trojan sembra essere interessato principalmente a sfruttare le macchine infette per **generare cripto-valuta attraverso dei miner installati sui server**.

Un modus operandi abbastanza comune tra i pirati informatici che prendono di mira i sistemi Linux, di solito installati su server con una discreta potenza di calcolo e che sono particolarmente appetibili per il mining.

Secondo i ricercatori, i miner installati per il momento avrebbero generato circa **107 Monero**, per un valore di 4.500 dollari.

Il timore, però, è che gli autori di SpeakUp possano modificare l'exploit principale allargando così la platea delle potenziali vittime.

Please follow and like us:

Ricattati da Siri? Con i Comandi Rapidi può succedere

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/05/speakup-il-trojan-per-linux-ha-cominciato-a-diffondersi-in-cina/

Ricattati da Siri? Con i Comandi Rapidi può succedere

Feb 04, 2019 Marco Schiaffino Hacking, In evidenza, News, Phishing, RSS, Scenario, Vulnerabilità 0

Un ricercatore di IBM lancia l'allarme sui rischi dei nuovi Comandi Rapidi: "potrebbero essere usate per ingannare gli utenti ed estorcergli denaro".

Con iOS 12, **Apple** ha introdotto una nuova funzione che permette di utilizzare **Siri** per eseguire operazioni complesse. Si chiama **Comandi Rapidi** e permette, in pratica di creare una sequenza di operazioni che vengono attivate da una frase personalizzata.

Si tratta in pratica di script che possono essere anche piuttosto complessi e che permettono, per esempio, di avvisare l'organizzatore di un evento del fatto che siamo in ritardo, usando la funzione mappe per comunicargli anche il tempo che ci manca per arrivare alla riunione.

Per crearli si utilizza un'app dedicata (disponibile gratis sullo store) che offre un sistema di controllo piuttosto intuitivo per creare gli script personalizzati.

Secondo il ricercatore **John Kuhn**, però, i Comandi Rapidi potrebbero essere usati da un cyber-criminale per i suoi scopi, ad esempio per tentare di estorcere denaro.

Il problema, come spiega nel suo report, è che gli script in questione (ce ne sono numerosi già pronto, ma ogni utente ne può creare di personalizzati) possono essere condivisi tramite iCloud.

Se un pirata informatico riuscisse a indurre la sua vittima a installarne uno, potrebbe utilizzarlo per ingannarlo, ad esempio facendogli credere di aver preso possesso del suo account.

[embedded content]

Nell'esempio mostrato dal ricercatore, il pirata informatico chiede un riscatto alla vittima mostrando alcuni dati recuperati dallo script che vengono usati per "dimostrare" che il criminale ha accesso a tutti i suoi dati.

Certo, un utente abbastanza smaliziato capirebbe immediatamente il trucchetto, ma i più ingenui (e sappiamo che non sono pochi) potrebbero facilmente cadere nel tranello.

Peggio ancora, scrive Kuhn**, lo script stesso può essere utilizzato per diffondersi da solo, inviando il link per il suo download a tutti i contatti presenti in rubrica**.

Insomma: secondo il ricercatore di IBM, Comandi Rapidi rischia di diventare una piattaforma per la creazione di truffe ai danni degli utenti iOS che potrebbe davvero sfuggire di mano.

Il suo consiglio a tutti gli utilizzatori di iPhone e dispositivi iOS è di non installare mai script di cui non si conosce l'origine o, ancor meglio, di non installare mai script condivisi da qualsiasi utente.

Fondamentale, inoltre, verificare tutti i permessi richiesti dallo script stesso. Per fortuna, infatti, **Comandi Rapidi chiede un permesso per ogni app con cui deve interagire**.

Please follow and like us:

Ora i pirati usano le botnet IoT per le frodi pubblicitarie su YouTube

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/04/ricattati-da-siri-con-i-comandi-rapidi-puo-succedere/

Ora i pirati usano le botnet IoT per le frodi pubblicitarie su YouTube

Feb 01, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

Router, videocamere e altri dispositivi "smart" vengono utilizzati per gonfiare i clic sui banner pubblicitari e generare profitti illeciti.

L'incubo della **Internet of Things** si arricchisce di un nuovo capitolo. Prima il pericolo erano solo gli attacchi **DDoS**. Ora la fantasia dei cyber-criminali ha trasformato le botnet composte da dispositivi IoT in macchine da soldi che sfruttano il classico schema della frode pubblicitaria online.

L'allarme è stato lanciato da **CenturyLink**, che ha individuato l'attività da parte di una botnet già operativa da qualche tempo su Internet.

Come spiegano i ricercatori in un report pubblicato su Internet, sembra che il gruppo di criminali che controlla **TheMoon** hanno cambiato il loro "modello di business", che fino a qualche tempo fa prevedeva una formula del tipo "DDoS as a service", cioè l'affitto della botnet per portare attacchi massicci a siti Internet.

TheMoon ora opera piuttosto come una rete proxy, che permette di eseguire migliaia di collegamenti a siti **YouTube** con lo scopo di gonfiare illecitamente il numero di visualizzazioni

e, di conseguenza, i proventi pubblicitari.

Non solo: il gruppo che la controlla sta lavorando per espandere la botnet, utilizzando le solite tecniche che sfruttano le vulnerabilità dei device IoT.

Nel dettaglio, TheMoon sfrutta una serie di exploit che fanno leva sui bug delle **web application presenti sui dispositivi**, normalmente raggiungibili in remoto attraverso la porta 8080.

Il download del codice malevolo avviene grazie a uno **ShellScript** che sfrutta un server per scaricare e installare il payload, che una volta operativo comunica con i server Command and Control utilizzando tre diverse porte che cambiano a seconda del tipo di architettura del dispositivo. Nel caso di quelli basati su **MIPS**, per esempio, le porte utilizzate sono la 5184, 5784 e 4584.

Il nuovo modulo introdotto dai pirati consente la funzionalità di proxy che viene avviata selezionando **una porta casuale e che viene modificata più volte nel corso di una giornata**.

Secondo la ricostruzione effettuata dai ricercatori, nell'aprile 2018 i pirati hanno aggiunto anche una funzionalità di autenticazione.

Dopo aver monitorato per qualche mese l'attività della botnet sulle loro reti (CenturyLink è un'azienda di telecomunicazioni statunitense – ndr) gli analisti hanno individuato tutti i dispositivi coinvolti e sono riusciti ad abbattere la botnet.

Questo non esclude, specificano nel report, che ve ne sia **una parte che sfrutta dispositivi collegati su altre reti** o che in questo preciso momento non siano attive altre botnet con funzionalità simili.

Please follow and like us:

Attacchi mirati col trojan Remexi alle sedi diplomatiche in Iran

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/01/ora-i-pirati-usano-le-botnet-iot-per-le-frodi-pubblicitarie-su-youtube/

Attacchi mirati col trojan Remexi alle sedi diplomatiche in Iran

Gen 31, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware è stato utilizzato per compromettere i computer in ambasciate e consolati stranieri sul territorio iraniano. Gli esperti: è il gruppo Chafer.

Gli esperti lo avevano previsto e la cronaca lo conferma: per il 2019 non dobbiamo aspettarci nessun rallentamento dell'attività dei gruppi **APT (Advanced Persistent Threat)**, quelli cioè dedicati al cyber-spionaggio.

Una conferma arriva (anche) oggi da **Kaspersky**, che sul suo blog pubblica un report riguardante una serie di attacchi che hanno preso di mira numerose sedi diplomatiche sul territorio dell'Iran.

Lo strumento utilizzato è una variante di un trojan con caratteristiche decisamente evolute. Si chiama **Remexi** e la sua prima comparsa risale a tre anni fa. La nuova variante, spiegano i ricercatori, sarebbe stata realizzata nel marzo del 2018 e ha una struttura modulare.

Le sue funzioni principali prevedono la **registrazione di tutto ciò che viene digitato sulla tastiera**, la cattura di screenshot, il furto di credenziali e la possibilità di avviare l'esecuzione di comandi sul computer infetto. Una caratteristica, quest'ultima, che consente ai pirati informatici di ampliare ulteriormente il loro campo d'azione installando ulteriori malware o moduli di Remexi.

A confermare la natura del malware, c’è il fatto che i comandi a disposizione dei pirati sembrano fatti apposta per individuare documenti e dati conservati sul computer.

Le informazioni rubate vengono crittografate con XOR utilizzando una chiave di 25 caratteri (del tipo “waEHleblxiQjoxFJQaIMLdHKz”) e le comunicazioni verso l’esterno sono gestite su protocollo HTTP sfruttando il **Microsoft Background Intelligent Transfer Service (BITS)**.

L’autore degli attacchi, secondo quanto ricostruito dai ricercatori, sarebbe il gruppo **Chafer**. Un soggetto già individuato in passato e che avrebbe legami con il governo iraniano.

A giustificare l’attribuzione ci sono numerosi indizi, tra cui la presenza della parola “salamati” all’interno di una delle chiavi crittografiche, che secondo i ricercatori potrebbe essere la trascrizione in caratteri occidentali della parola che in lingua farsi significa “salute”.

Tra gli indizi individuati dagli analisti, inoltre, c’è una porzione di dati che fa riferimento a un utente Windows chiamato **Mohamadreza New**.

Un nome, quello di **Mohammad Reza**, che compare nell’elenco dell’**FBI** e corrisponderebbe a un cybercriminale iraniano ricercato dal bureau. I ricercatori, però, specificano che si tratta di un nome piuttosto comune e che, in ogni caso potrebbe trattarsi di una “flase flag”, cioè un tentativo di

depistare le indagini per individuare l’autore.

A prescindere dalla (doverosa) cautela nell’attirbuzione, tutta la vicenda conferma ancora una volta che il livello di attenzione per lo “spionaggio di stato” deve rimanere alto.

Please follow and like us:

Furti di cripto-valuta: nel 2018 rubati 1,7 miliardi di dollari

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/01/31/attacchi-mirati-col-trojan-remexi-alle-sedi-diplomatiche-in-iran/

Furti di cripto-valuta: nel 2018 rubati 1,7 miliardi di dollari

Gen 30, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

La stima in una ricerca che analizza le tecniche usate dai cyber-criminali per rubare Bitcoin e altre cripto-valute attraverso attacchi hacker e truffe online.

Il mercato delle cripto-valute ha dimensioni ormai spaventose. Certo, siamo lontani dal picco del gennaio 2018, quando c'era in circolazione quasi l'equivalente di 800 miliardi di dollari, ma anche il valore attuale (**113 miliardi di dollari**) rappresenta una quota di tutto rispetto.

Senza contare che negli ultimi anni le cripto-valute sono spuntate con una frequenza impressionante, al punto che a oggi si contano la bellezza di **2.121 monete virtuali** che vengono scambiate su Internet.

Con numeri simili, non stupisce che il cyber-crimine riesca ad accaparrarsene una bella fetta. Secondo il report di **CypherTrace** (scaricabile da questo indirizzo) i frutto di truffe, furti e attacchi hacker ammonterebbe a **1,7 miliardi di dollari**. Per capirci, un valore che supera **il prodotto interno lordo del Messico**.

La ricerca, però, non si limita a quantificare i proventi della cybercriminalità, ma stila una sorta di classifica delle tecniche utilizzate da truffatori e pirati informatici per rubare le cripto-monete.

Quella più “efficace”, si legge nello studio, è la classica truffa del “prendi i soldi e scappa”, o exit scam. Il meccanismo prevede il lancio di una **ICO (Initial Coin Offering)** che raccoglie denaro dagli investitori promettendo un successivo guadagno. Il truffatore, poi, si eclissa con tutto il denaro. **Nel corso dell’anno passato, truffe come queste hanno fruttato ai criminali circa 750 milioni di dollari**.

Il record in Vietnam, dove i truffatori sono riusciti a mettere a segno il colpo grosso intascandosi **660 milioni di dollari** raccolti con la ICO di **Pincoin**. A farne le spese sono

stati **32.000 investitori**, ai quali era stato promesso un (davvero poco credibile) margine di guadagno del 48% mensile.

Accanto alle truffe, ci sono anche i furti perpetrati attraverso attacchi alle piattaforme che gestiscono le cripto-valute (gli exchange – ndr) e quelli legati alla "semplice" pirateria che utilizza malware per violare gli account degli utenti.

La nuova frontiera però è quella del **SIM swapping**, di cui abbiamo parlato anche in questo articolo riguardante un caso di cronaca recente.

La tecnica sfrutta i sistemi di **autenticazione a due fattori tramite SMS** e funziona così: il criminale individua la sua vittima e contatta un negozio di telefonia, fingendo di aver perso il telefono o la SIM e chiedendone la sostituzione.

La procedura in teoria richiederebbe rigorosi controlli sull'identità del richiedente, ma i pirati informatici, spesso con la complicità di un dipendente infedele, sono abilissimi ad aggirarli.

A questo punto il truffatore agisce rapidamente chiedendo la modifica della password del wallet della vittima e confermando l'identità usando la SIM ottenuta attraverso lo scambio (swap) precedente. **Prima che la vittima possa fare qualsiasi cosa, tutta la cripto-valuta presente sul suo conto viene trasferita su un conto controllato dai criminali**.

L’ultimo aspetto che gli esperti di CypherTrace mettono in luce è quello legato al **riciclaggio delle cripto-valute**. Contrariamente a quanto si pensa, infatti, mettersi in tasca quanto si è rubato non è così facile e i criminali sono costretti a utilizzare varie tecniche che gli consentono di rendere difficile tracciare la provenienza del denaro che incassano.

Un “anello debole” che potrebbe anche rappresentare la chiave per mitigare il fenomeno del furto di moneta virtuale ma che richiede **una regolamentazione omogenea a livello mondiale** che siamo ben lontani dal poter anche solo immaginare.

Please follow and like us:

Backdoor del governo russo in migliaia di siti Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/01/30/furti-di-cripto-valuta-nel-2018-rubati-17-miliardi-di-dollari/