Antivirus? Firewall? No: Israele usa i missili

Mag 06, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS, Scenario 0

L'esercito israeliano avrebbe "fermato" un attacco informatico bombardando l'edificio in cui si sarebbero trovati gli hacker.

Che la cyber warfare sia ormai una faccia dei conflitti militari lo sappiamo da tempo. Quello che è accaduto nella **striscia di Gaza** in queste ore, però, è qualcosa di assolutamente inedito.

Stando a quanto si legge in un tweet pubblicato dall'account ufficiale dell'**Israel Defense Forces**, infatti, l'esercito israeliano avrebbe reagito a un attacco informatico **bombardando l'edificio nel quale si sarebbero trovati gli hacker**.

Nel tweet, l'IDF spiega che l'attacco informatico è stato individuato e fermato dagli esperti di sicurezza israeliani, che hanno anche individuato l'edificio da cui sarebbe partito. **A questo punto l'aviazione israeliana avrebbe inviato dei jet che hanno bombardato l'edificio**.

[embedded content]

Il comunicato non specifica quante persone si trovassero al suo interno al momento del bombardamento e se nell'esplosione siano stati coinvolti dei civili oltre ai presunti hacker di **Hamas**.

Quello che è certo è che l'episodio segna il primo precedente

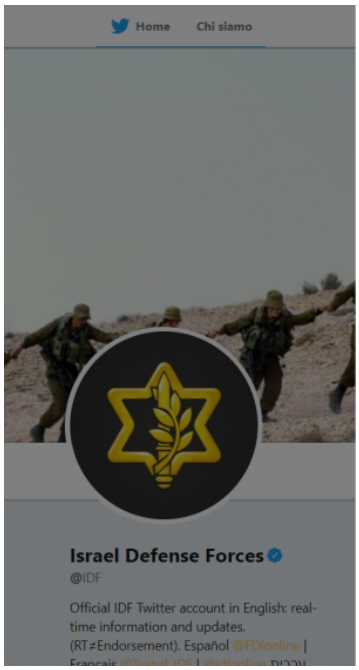
(conosciuto) di un attacco "fisico" come reazione alla cyber-guerriglia.

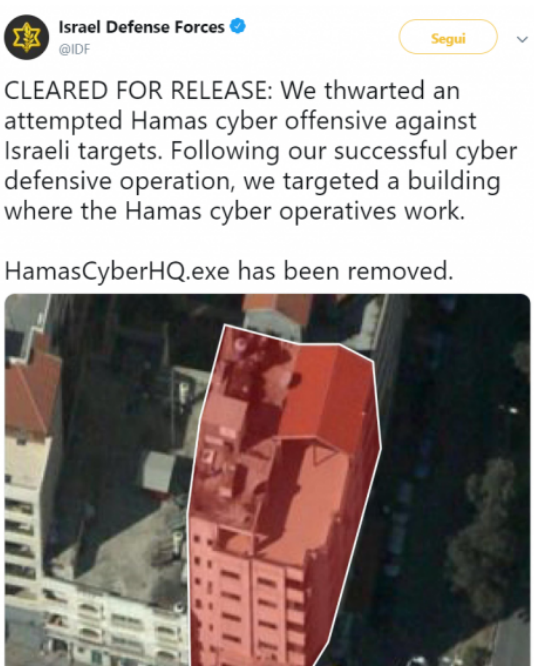
Difficile capire anche come si collochi l'azione dell'esercito israeliano nel quadro giuridico internazionale. Quasi un anno fa, infatti, l'ipotesi che un attacco hacker potesse essere considerato un "atto di guerra" era stata sollevata dal **Procuratore Generale della Gran Bretagna Jeremy Wright**.

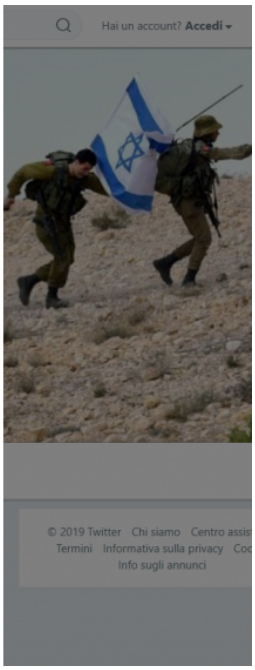
Secondo Wright, il fondamento di una reazione militare a un attacco informatico si baserebbe sul disposto dell'articolo 51 della **Carta delle Nazioni Unite**. Un'interpretazione che, secondo molti commentatori, è decisamente discutibile.

Nel caso dell'attacco di Israele, l'episodio ha però contorni decisamente diversi, visto che si inserisce in un conflitto dichiarato (Wright si riferiva ai cyber-attacchi come un possibile casus belli) che negli ultimi giorni ha già provocato decine di vittime.

Lasciando le valutazioni di carattere giuridico a chi ha la competenza per farle, ciò che rimane comunque indigesto è che il tweet si chiuda con una spiritosaggine (HamasCyberHQ.exe has been removed) **decisamente fuori luogo quando si parla di vite umane spazzate via dalle bombe**.







Please follow and like us:



Attacco DDoS al sistema energetico USA

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/06/antivirus-firewall-no-israele-usa-i-missili/

Attacco a Citrix: i pirati hanno avuto accesso ai sistemi per 6 mesi

Mag 03, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS 0

La vicenda è stata resa pubblica lo scorso marzo, ora emergono i dettagli. Rubate informazioni sensibili di dipendenti e collaboratori.

L'attacco portato ai sistemi di **Citrix**, denunciato dalla stessa azienda lo scorso 8 marzo, ha dimensioni decisamente ampie. Secondo quanto si legge in una lettera inviata dall'azienda alle persone potenzialmente coinvolte nel breach,

infatti, **i pirati avrebbero avuto accesso ai sistemi per la bellezza di 6 mesi**.

In seguito alla segnalazione dell'FBI, che ha avvisato Citrix del possibile attacco, gli esperti di sicurezza hanno infatti rilevato accessi "intermittenti" a partire dal 13 ottobre 2018.

Le informazioni a cui avrebbero avuto accesso i cyber-criminali, che secondo l'FBI farebbero parte di un "gruppo internazionale" non meglio definito, comprenderebbero **dati sensibili come il social security number, i dati anagrafici e le informazioni finanziarie di dipendenti e collaboratori**.



L'intrusione, secondo gli esperti che stanno ancora cercando di ricostruire l'effettiva entità dell'attacco, sarebbe avvenuta attraverso una tecnica di **password spraying**, utilizzata recentemente anche in un attacco massiccio che ha preso di mira migliaia di account di **Office 365** e **G Suite**.

Il password spraying è una sorta di **brute forcing al contrario**: al posto di tentare numerose password su un singolo

account, i pirati provano a usare la stessa password su più account, aggirando così i normali controlli che rilevano i tentativi continui di accesso a un singolo account.

Insomma: la violazione dei sistemi sarebbe ancora una volta da attribuire all'utilizzo di credenziali "deboli" che avrebbero permesso ai cyber-criminali di infiltrarsi nei sistemi di una delle più note aziende IT a livello mondiale.

Gli autori dell'attacco, che farebbero parte di un gruppo chiamato **Iridium**, sono noti alle cronache per prendere di mira le aziende di alto livello, soprattutto nel settore energetico. Il loro modus operandi prevede di solito di utilizzare le informazioni come leva per estorcere denaro alle vittime.

Please follow and like us:



Attacco DDoS al sistema energetico USA Le nuove funzioni di sicurezza di Windows 10 rallentano il sistema

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/03/attacco-a-citrix-i-pirati-hanno-avuto-accesso-ai-sistemi-per-6-mesi/

Le nuove funzioni di sicurezza di Windows 10 rallentano il sistema

Mag 02, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Tecnologia 0

Il calo di performance riguarda l'esecuzione di applicazioni particolarmente "voluminose". I tempi, in alcuni casi, arrivano addirittura al triplo.

Ogni volta che si parla di sistemi di sicurezza e controllo in chiave anti-malware, una delle preoccupazioni riguarda la possibilità che la loro introduzione possa provocare un rallentamento del sistema.

Naturalmente, sviluppatori e produttori di software di sicurezza si affannano ad assicurare che l'impatto delle loro soluzioni è minimo o addirittura trascurabile. In molti casi questo è vero. In altri no.

Nel caso del **Control Flow Guard (CFG)** introdotto da Microsoft in **Windows 10**, sembra proprio che il calo di prestazioni ci sia e si tratti anche di un calo particolarmente significativo.

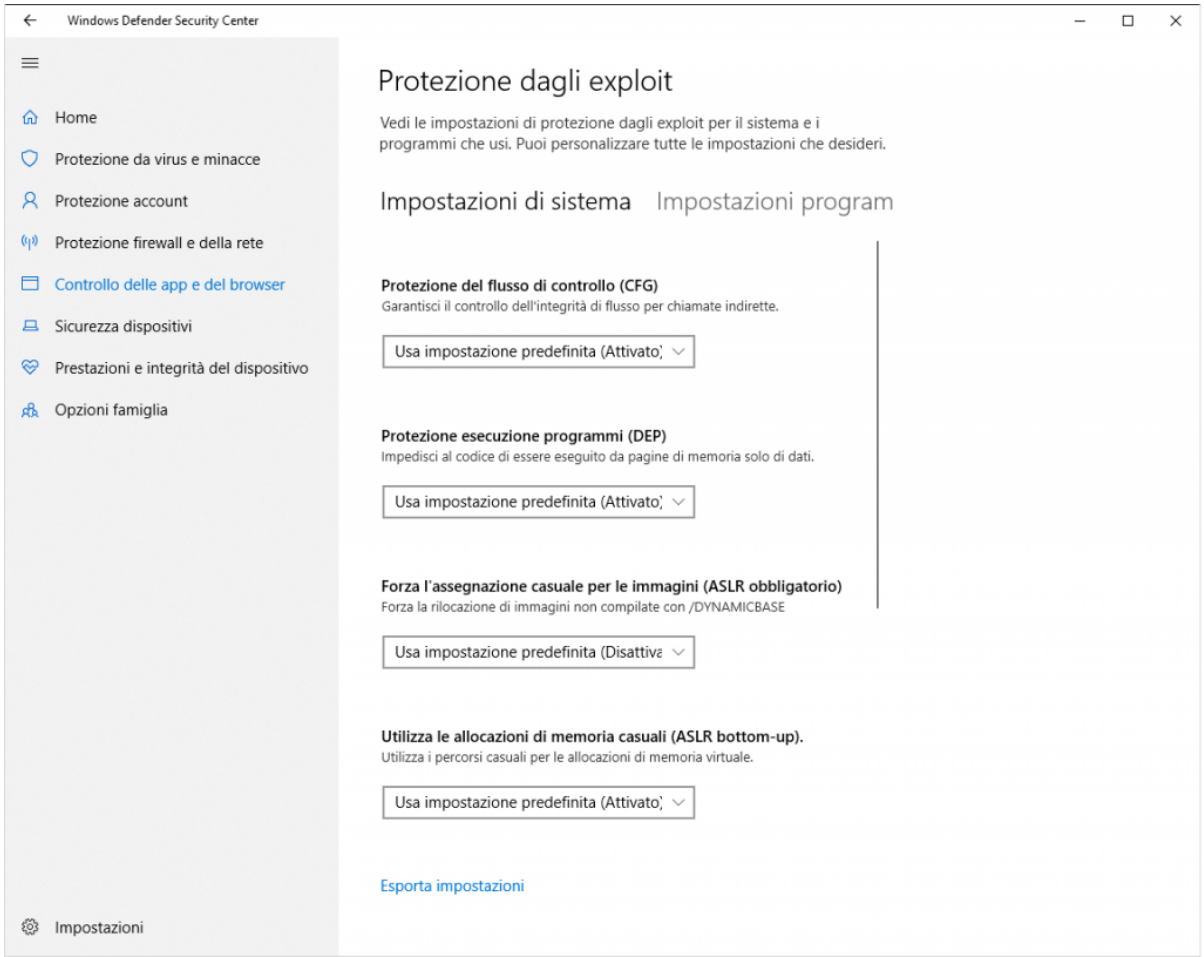
Ad accorgersene sono stati i ricercatori di **Vivaldi**, che hanno recentemente introdotto delle macchine virtuali con Windows 10 nei loro cluster per i test sui browser.

Come spiegano in un post pubblicato sul blog ufficiale dell'azienda, hanno immediatamente notato che qualcosa non andava. **In particolare, un test che di solito richiedeva circa 100 minuti per la sua esecuzione su Windows 7, con Windows 10**

ne richiedeva 300 e oltre.

Tutti i tentativi di mitigare il problema modificando le impostazioni del sistema sono stati inutili e gli sviluppatori hanno quindi deciso di contattare i colleghi di Google. Dalle loro analisi è emerso che la responsabilità sarebbe, appunto di CFG.

Il Control Flaw Guard è un sistema che ha la funzione di proteggere i processi dagli exploit che sfruttano la corruzione di memoria, come il buffer overflow. **È attivato come impostazione predefinita su Windows 10 e rappresenta uno degli strumenti che si sono dimostrati più efficaci per migliorare il livello di sicurezza del sistema Microsoft**.



Da quanto hanno capito i ricercatori, il rallentamento nel sistema è dovuto a un componente di CFG che si chiama **MiCopyToCfgBitMap** e risulta particolarmente “pesante” quando l’eseguibile avviato ha dimensioni piuttosto elevate (gli

eseguibili utilizzati nei test raggiungono i 122 MB).

In seguito alla segnalazione, Microsoft avrebbe messo a punto una patch che dovrebbe essere resa disponibile a breve e che consentirebbe di eliminare questo gap prestazionale.

Nel frattempo, chi fosse preoccupato di ritrovarsi un sistema "zoppo" dovrebbe in ogni caso resistere alla tentazione di disattivare Control Flaw Guard. Secondo gli esperti, infatti, il livello di sicurezza garantito dalla funzionalità è tale da essere irrinunciabile, anche al costo di pagare qualcosa (o anche tanto) in termini di prestazioni.

Please follow and like us:



Guardare a sbafo la Pay TV può costare caro

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/02/le-nuove-funzioni-di-sicurezza-di-windows-10-rallentano-il-sistema/

Guardare a sbafo la Pay TV può costare caro

Apr 30, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario 0

I dispositivi hardware per guardare in streaming contenuti protetti da copyright sono diventati l'obiettivo privilegiato dei pirati informatici.

Un tempo la pirateria era focalizzata su MP3 e film. Con l'esplosione del fenomeno dei pay-per-view, il nuovo orizzonte si è allargato all'accesso ai servizi di streaming.

Un fenomeno che, secondo un'indagine della **Digital Citizens Alliance**, coinvolgerebbe **12 milioni di persone solo negli Stati Uniti** e che sfrutta dei dispositivi hardware che consentono di utilizzare app pirata per visualizzare contenuti protetti, come quelli offerti da **Netflix, Amazon Prime Video e Hulu**. Come accade spesso, però, questa "zona grigia" offre ampi spazi di manovra anche per i pirati informatici.

Nel report pubblicato dalla Digital Citizens Alliance, vengono descritte alcune tecniche che i cyber-criminali sfruttano per compromettere i sistemi di chi utilizza i dispositivi e le app pirata.

Lo schema adottato è semplice ed efficace. Le vittime, per accedere illegalmente ai contenuti protetti, utilizzano di solito dei dispositivi hardware che funzionano come Smart TV, come il popolare **Kodi box**, sviluppato dalla **XBMC Foundation**.



Si tratta di un media player open source, che consente di installare sia applicazioni legittime, sia applicazioni pirata che consentono, appunto, di accedere gratuitamente a contenuti protetti da copyright.

Il rovescio della medaglia è che spesso queste applicazioni contengono malware in grado di rubare informazioni sensibili dai dispositivi delle vittime.

Nel corso dell'indagine, condotta in collaborazione con la società di sicurezza **Dark Wolfe Consulting**, i ricercatori hanno analizzato il comportamento delle applicazioni pirata, che in buona parte si comportano come veri e propri malware.

La casistica è quanto mai varia. Nel caso di **Mobdro**, un'app che consente di visualizzare "a scrocco" film e trasmissioni sportive, i ricercatori si sono accorti che l'applicazione aveva inviato nome e password della rete Wi-Fi a un server apparentemente posizionato in Indonesia.

In un altro caso, il malware ha sfruttato una serie di vulnerabilità per accedere a un altro dispositivo collegato alla rete locale e ha trasferito 1,5 terabyte di dati verso l'esterno.

A rendere particolarmente insidiosa la tecnica di attacco c'è

il fatto che il malware “gira” direttamente su un dispositivo che è collegato all’interno della rete locale ed è quindi in grado **di aggirare i normali sistemi di protezione, come il firewall integrato nel router**.

Senza contare che il sistema open source adottato, a differenza di altri prodotti commerciali simili, non integra sistemi di protezione in grado di mitigare il rischio di un attacco. Insomma: mai come in questo caso è vero il detto per cui “se un prodotto è gratis, il prodotto sei tu”.

Please follow and like us:

Follow

Falle nell’infrastruttura IT di Microsoft. Il punto debole sono i server

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/30/guardare-a-sbafo-la-pay-tv-puo-costare-caro/

Falle nell’infrastruttura IT di Microsoft. Il punto debole

sono i server

Apr 29, 2019 Marco Schiaffino In evidenza, News, RSS, Tecnologia, Vulnerabilità 0

Swascan ha individuato una serie di vulnerabilità nei sistemi Microsoft. Un eventuale attacco consentirebbe di sottrarre informazioni riservate.

È stata una società italiana a individuare cinque vulnerabilità nell'infrastruttura IT di **Microsoft**, bug nei sistemi dell'azienda di Redmond che rappresentavano una vera voragine di sicurezza che i pirati informatici avrebbero potuto sfruttare per rendere più efficaci i loro attacchi.

Le vulnerabilità, comunicate da **Swascan** a Microsoft, hanno diverse caratteristiche ma hanno un elemento in comune: avrebbero permesso di avviare **l'esecuzione di codice in remoto sui sistemi**.

Il report di **Swascan**, società specializzata nell'individuazione di vulnerabilità attraverso un'infrastruttura basata su cloud, descrive nel dettaglio i bug, partendo da quello identificato come **CWE – 119**.



Secondo i ricercatori *“Il software esegue operazioni su un buffer di memoria, ma può leggere o scrivere in una posizione di memoria che si trova al di fuori del confine previsto del buffer. Alcuni linguaggi consentono l’indirizzamento diretto delle allocazioni di memoria e non garantiscono automaticamente che queste posizioni siano valide per il buffer di memoria a cui si fa riferimento. Ciò può causare* ***operazioni di lettura o scrittura su allocazioni di memoria che possono essere associate ad altre variabili, strutture dati o dati di programma interni****. Di conseguenza, un aggressore può essere in grado di eseguire codice arbitrario, alterare il flusso di controllo previsto, leggere informazioni sensibili o causare il crash del sistema*”.

Il bug identificato come **CWE-94** è **invece basato sull’injection di codice**. Secondo Swascan *“Il software costruisce tutto o parte di un segmento di codice utilizzando input influenzati esternamente da un componente a monte, ma non neutralizza – o lo fa in modo errato – elementi speciali che potrebbero modificare la sintassi o il comportamento del segmento di codice previsto. Quando il software permette all’input di un utente di contenere la sintassi del codice, potrebbe essere possibile per un potenziale aggressore creare il codice in*

modo tale da alterare il flusso di controllo previsto del software. Una tale alterazione potrebbe portare ad un'esecuzione arbitraria del codice".

Per quanto riguarda le vulnerabilità identificate come **CWE-200** si parla invece di una **information exposure**, cioè la divulgazione intenzionale o non intenzionale di informazioni a un attore che non è esplicitamente autorizzato ad avere accesso a tali informazioni. Tutti i bug sono stati prontamente corretti in seguito alla segnalazione di Swascan.

Please follow and like us:



Come (e quanto) guadagnano i pirati con le credenziali rubate?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/29/falle-nellinfrastruttura-it-di-microsoft-il-punto-debole-sono-i-server/

Come (e quanto) guadagnano i pirati con le credenziali rubate?

Apr 26, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Scenario 0

L’aumento esponenziale del Credential Stuffing è dovuto al fatto che i cyber-criminali hanno guadagni garantiti con un investimento tutto sommato modesto.

Da un punto di vista della pianificazione economica, il mondo del cyber-crimine avrebbe qualcosa da insegnare alle aziende. Le attività dei pirati informatici sono infatti improntate a logiche di guadagno estremamente rigide e la loro attività si sposta sempre in direzione dei settori più profittevoli.

L’aumento dell’attività legata al **Credential Stuffing**, cioè all’uso di credenziali rubate e disponibili sul Dark Web per cercare di violare altri account in cui gli utenti hanno usato la stessa email e password, non fa eccezione. **Secondo gli esperti, riescono a guadagnare fino a 20 volte il denaro investito**.

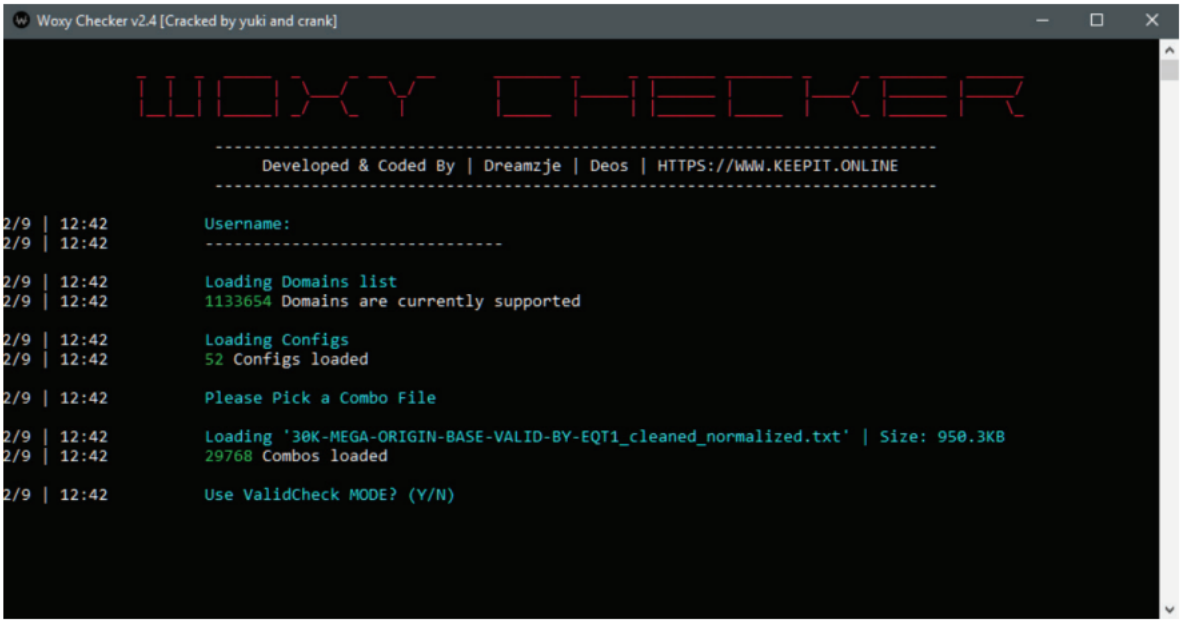
A fare luce sui meccanismo di questa attività criminale ci ha pensato **Recorded Future**, che in uno studio approfondito (si può scaricare il PDF a questo indirizzo) ricostruisce le strategie usate dai pirati informatici, i costi che affrontano e i loro guadagni.

Da un punto di vista storico, le prime attività di Credential Stuffing di un certo rilievo sono state individuate nel 2014, quando i cyber-criminali hanno cominciato a utilizzare sistemi automatizzati per tentare di accedere agli account attraverso l’utilizzo di credenziali rubate da servizi online e acquistate sul mercato nero.

Un processo che richiede, oltre all’investimento per acquistare i database contenenti le credenziali rubate (**costo di circa 150 dollari**) anche quello per le infrastrutture necessarie per battere a tappeto siti e social network senza dare troppo nell’occhio.

I software più utilizzati per questa attività sono sei, anche

se i ricercatori segnalano che esistono decine di varianti utilizzate dai criminali. **Il loro costo varia tra i 50 e i 250 dollari, a seconda delle funzionalità che mettono a disposizione**.



Il costo maggiore che devono sopportare, in realtà, è legato ai **servizi Proxy** che permettono di eseguire più tentativi di accesso cambiando ogni volta indirizzo IP. **Un servizio del genere ha un costo di 250 dollari a settimana**.

Secondo i ricercatori di Recorded Future, quindi, nel complesso una campagna di Credential Stuffing costa in media **550 dollari**.

A fronte di questo modesto investimento, per ogni milione di credenziali utilizzate sono in grado di compromettere tra i 10.000 e i 30.000 account.

Ma quanto guadagnano per ogni account compromesso? Normalmente i pirati li rivendono e, anche se i prezzi sono calati negli ultimi tempi a causa di un aumento dell'offerta, i profitti sono notevoli. Ogni singolo account frutta infatti dai 50 centesimi ai 3,50 dollari.



Nel complesso, secondo lo studio, **i cyber-criminali possono arrivare a guadagnare fino a 19.700 dollari a fronte di 550 dollari spesi, con un "utile" di 19.150 dollari**. Anche pensando che non arrivino a tanto, ma solo alla metà, stiamo parlando appunto di un rapporto di 20 a 1.

Insomma: si tratta di un mercato estremamente profittevole e con margini di rischio (economico) davvero ridotti. L'ipotesi che qualcuno possa andare in perdita, infatti, è estremamente remota. L'impressione, letto lo studio, è che di Credential Stuffing sentiremo parlare ancora per un bel po' di tempo.

Please follow and like us:



Raffica di attacchi a WordPress sfruttano due bug in Social Warfare

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/26/come-e-quanto-guadagnano-i-pirati-con-le-credenziali-rubate/

Raffica di attacchi a WordPress sfruttano due bug in Social Warfare

Apr 24, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Le falle di sicurezza nel popolare plugin permettono di prendere il controllo del Content Management System. A rischio più di 40.000 siti Internet.

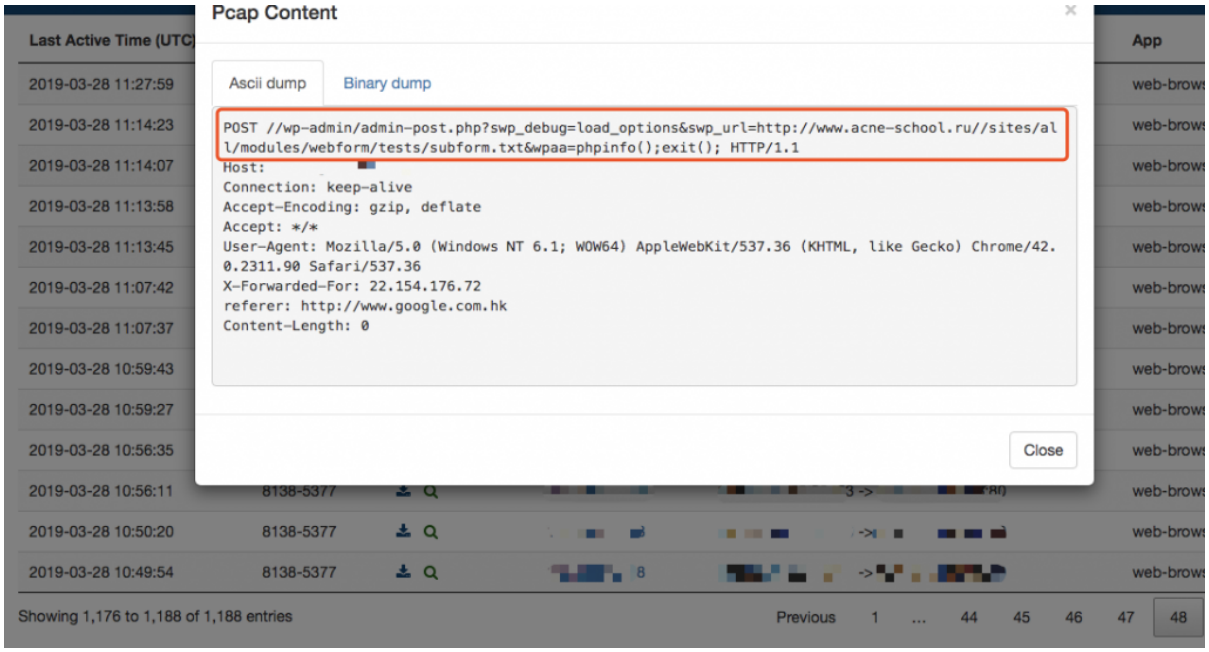
Si chiama **Social Warfare** ed è un plugin piuttosto popolare tra gli utenti **WordPress**. La sua funzione è quella di consentire la condivisione di contenuti sui social media.

Lo scorso 21 marzo, però, sono emerse due vulnerabilità (CVE-2019-9978) che affliggono le versioni di Social Warfare precedenti alla 3.5.3.

La **Unit 42** di **Palo Alto Networks**, che ha individuato le falle di sicurezza, spiega nel suo report che l'uso combinato dei due bug (uno è un classico Cross Site Scripting, l'altro un'esecuzione di codice in remoto) permette nella pratica di eseguire codice PHP sul sito e, di conseguenza, prenderne il completo controllo.

A distanza di un mese, sempre secondo i ricercatori della Unit 42, la situazione è tutt'altro che risolta. Nonostante la disponibilità di un aggiornamento che corregge i bug, infatti, sono ancora tantissimi i siti Internet gestiti con WordPress che utilizzano una versione vulnerabile del plugin.

Nel frattempo, i cyber-criminali stanno sfruttando la situazione in ogni modo e nei bassifondi del Web si moltiplicano gli exploit che sfruttano le falle di sicurezza.



Gli attacchi individuati dai ricercatori puntano a prendere il possesso dei siti per poi sfruttarli per i loro scopi. I payload utilizzati variano **dall'iniezione di JavaScript per la generazione di cripto-valute** (sullo stile di CoinHive) al **dirottamento del traffico verso pagine Web con inserzioni pubblicitarie o exploit che installano malware sui computer dei visitatori**.

E il fenomeno non accenna a decrescere: una ricerca su Internet, sempre riportata nello studio della Unit 42, indica che ci sono attualmente più di **42.000 siti che utilizzano il plugin** e molti di questi hanno ancora una versione non aggiornata.

Un problema, quello dei plugin WordPress vulnerabili ad attacchi, che nel mondo della sicurezza è ben conosciuto ma per il quale si stenta ancora a trovare soluzioni efficaci. Secondo una ricerca di **Imperva**, infatti, il 98% delle vulnerabilità di WordPress del 2018 sono collegate a un plugin.

Please follow and like us:

Follow

Database senza protezione: esposte le password di 2 milioni di reti Wi-Fi

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/24/raffica-di-attacchi-a-wordpress-sfruttano-due-bug-in-social-warfare/

Database senza protezione: esposte le password di 2 milioni di reti Wi-Fi

Apr 23, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Vulnerabilità 0

I dati raccolti dall'app WiFi Finder conservati senza alcuna protezione all'interno di un server aperto a tutti. Festa grande per i pirati informatici.

Perché perdere tempo a portare attacchi di Brute Forcing contro un router o un hot spot quando si può trovare la password su Internet?

L'opportunità per i cyber-criminali di accedere a questa pratica scorciatoia l'ha offerta **WiFi Finder**, un'applicazione

per **Android** sviluppata da una società cinese che è stata scaricata e utilizzata da decine di migliaia di utenti.

L’app, come si legge nella descrizione pubblicata su Google Play, dovrebbe permettere di trovare hotspot gratuiti attraverso un sistema di geolocalizzazione, che permetterebbe in buona sostanza di trovare una rete Wi-Fi disponibile nel luogo in cui ci si trova.

A quanto pare, però, l’app non si limita a registrare gli hot spot gratuiti, ma anche le credenziali di accesso alle reti Wi-Fi casalinghe.

A scoprirlo sono stati i ricercatori della **GDI Foundation**, che hanno individuato su Internet un server liberamente accessibile al cui interno sono memorizzate (in chiaro) circa 2 milioni di credenziali di reti Wi-Fi.

Insomma: si tratterebbe di un gigantesco “elenco del telefono” che contiene la posizione degli hot spot e le credenziali per accedervi.



Il problema, spiegano i ricercatori, non riguarda però soltanto le reti Wi-Fi private che sarebbero finite nel calderone. Anche nel caso di punti di accesso pubblici, il fatto che qualcuno abbia a disposizione direttamente delle credenziali, senza che debba richiederle, rappresenta un potenziale problema di sicurezza. Pensiamo al caso degli alberghi, che normalmente forniscono l'accesso solo ai clienti registrati.

Il rischio è che un pirata informatico si garantisca in questo modo la possibilità di accedere a sistemi a cui normalmente non avrebbe accesso, ottenendo una situazione di vantaggio che gli consentirebbe, per esempio, di portare un attacco **Man in the Middle**.

Non solo: nel caso in cui siano indicati hot spot che non utilizzano sistemi di autenticazione, una mappatura di questo genere può venire estremamente comoda per pianificare attacchi

che consentirebbero il furto di informazioni riservate da tutti i dispositivi che vi si collegano. **Insomma: da qualsiasi parte la si guardi, si tratta di un potenziale incubo per la sicurezza di milioni di persone**.

Dalle parti della GDI Foundation non hanno avuto nemmeno vita facile nel risolvere la situazione. **I loro tentativi di contattare lo sviluppatore, infatti, sono stati vani**.

Ciò che sono riusciti a fare è stato contattare **DigitalOcean**, che forniva l'hosting per il database in questione. I dati, di conseguenza, sono stati rimossi. Non ci sono garanzie, però del fatto che lo sviluppatore abbia capito l'antifona.

Please follow and like us:



Attacco massiccio ai dispositivi iOS e macOS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/23/database-senza-protezione-esposte-le-password-di-2-milioni-di-reti-wi-fi/

Attacco massiccio ai

dispositivi iOS e macOS

Apr 19, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario, Vulnerabilità 0

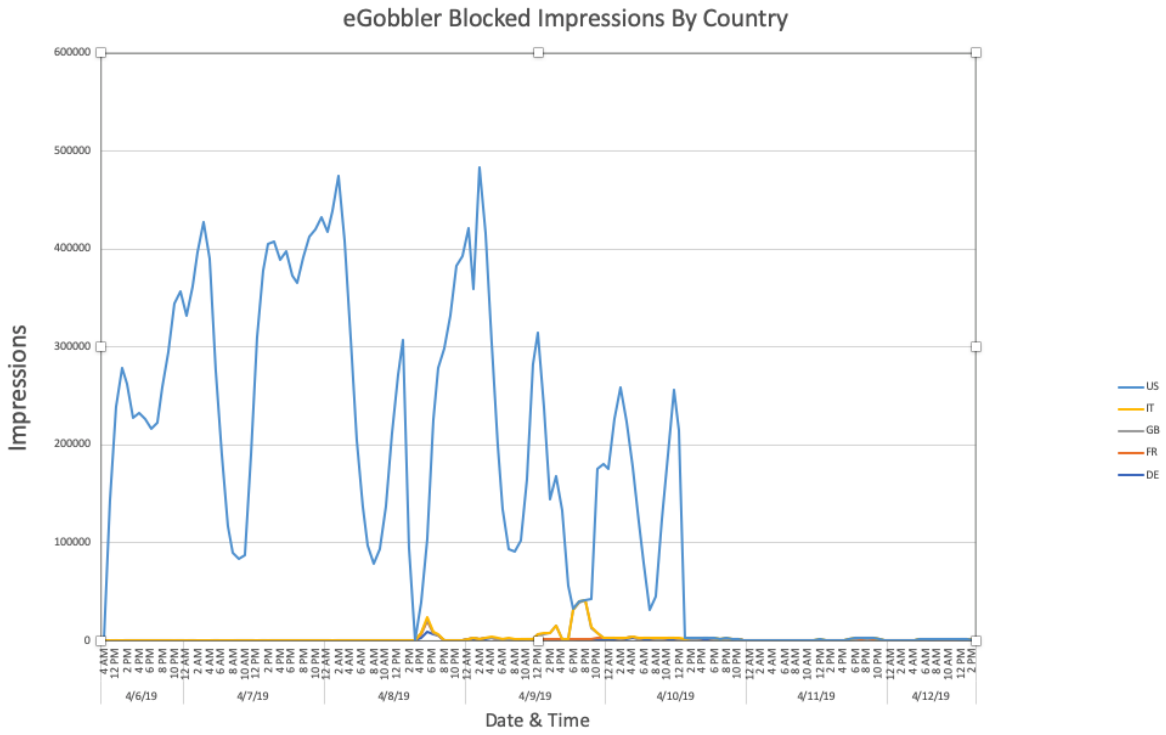
I pirati prendono di mira Mac e iPhone. La favola della "sicurezza intrinseca" di computer e dispositivi mobili di Apple traballa sempre di più.

La speranza è che le notizie di cronaca possano funzionare come un campanello di allarme che spezzi l'incantesimo di cui sono troppo spesso vittima gli utenti Apple, ancora convinti in gran parte che i loro dispositivi non abbiano bisogno di antivirus perché "immuni" a malware e attacchi informatici.

E proprio questa curiosa "allergia" a utilizzare software di protezione potrebbe essere alla base degli attacchi che hanno interessato gli utenti macOS e iOS in questi ultimi mesi.

Partiamo dalla campagna che ha preso di mira **iPhone e iPad**, attraverso una falla di sicurezza all'interno della **versione iOS di Chrome**. A sfruttarla è stato il gruppo **eGobbler**, dirottando la navigazione delle vittime su pagine o pop-up che contengono malware.

L'attacco, che secondo **Confiant** (qui il report completo) avrebbe colpito almeno 500 milioni di utenti, utilizza un JavaScript per sfuggire alla sandbox del browser di Google.



I guai derivanti dal gruppo eGobbler, però, è solo l'ultimo i una lunga serie per gli utenti Apple. In questi giorni il rapporto tra l'azienda di Cupertino e la cyber-security è finito anche sotto la lente d'ingrandimento di **Check Point**, che ha pubblicato su Internet una sorta di enciclopedia dei malware per macOS.

L'azienda israeliana, in un comunicato stampa, focalizza l'attenzione soprattutto su due episodi. Il primo riguarda CreativeUpdate, un cryptominer individuato nel febbraio 2018 e che è stato diffuso attraverso il sito MacUpdate.

Il vero "pezzo forte", però, è **Flashback**, un trojan comparso per la prima volta nel 2011 e che **ha colpito più di 500.000 Mac**.

Flashback utilizza una serie di tecniche estremamente sofisticate per nascondere la sua presenza e rendere più difficile la rilevazione. Tra queste, un complicatissimo sistema che subordina l'esecuzione del malware stesso all'identificativo della macchina su cui è stato installato.

In questo modo il codice non verrà eseguito correttamente su un'altra macchina eccetto quella su cui è stato iniettato in precedenza. Per ottenere questo risultato, **Flashback crittografa la struttura dei suo i dati usando l'UUID della macchina attraverso un sistema di cifratura RC4**.

Una nota curiosa: il malware utilizza **Twitter** come vettore per inviare i comandi tra server Command & Control e computer infettato.

Gli esempi citati, però, sono solo alcuni dei più clamorosi in un casistica molto più ampia che dimostra, ancora una volta, come la piattaforma non possa essere considerata un fattore di riduzione del rischio di attacchi informatici.

Quando riusciremo a spiegarlo ai "talebani del Mac", forse, avremo fatto un passo avanti nel garantire un maggior livello di protezione per tutti.

Please follow and like us:

Follow

I bot pirata rappresentano il 20% del traffico su Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/19/attacco-massiccio-ai-dispositivi-ios-e-macos/

I bot pirata rappresentano il 20% del traffico su Internet

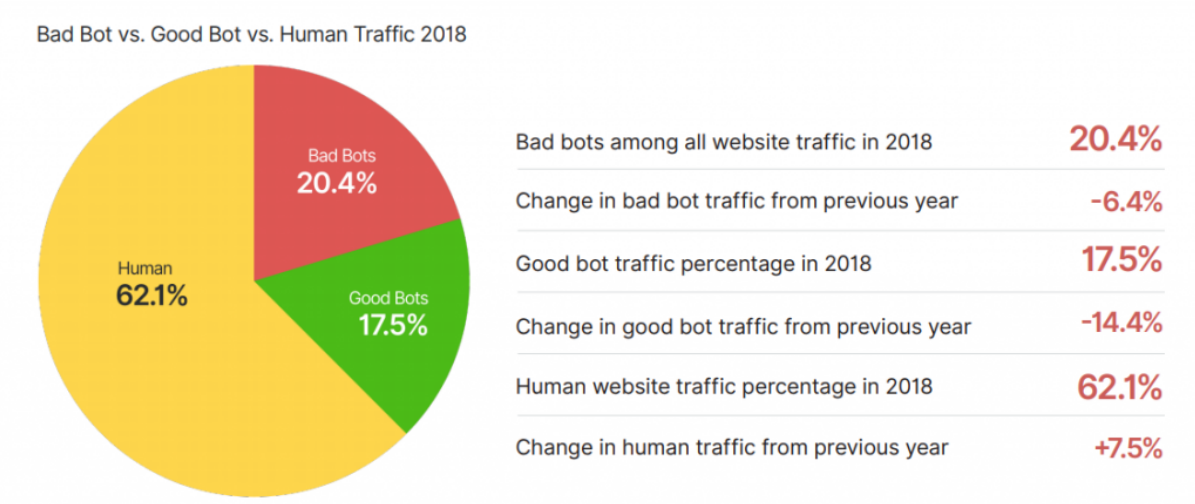
Apr 18, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Una ricerca analizza l'attività dei bot malevoli. Sono in crescita costante e rappresentano un pericolo per il funzionamento della rete e la sicurezza degli utenti.

Non tutto il traffico su Internet è generato da persone in carne e ossa, questo lo sappiamo. La Rete pullula di **bot**, sistemi automatizzati che "viaggiano" sul Web per i motivi più disparati. Un esempio è quello dei crawler usati dai motori di ricerca come **Google**.

Si stima che oltre il 37% del traffico Internet sia generato da questi software automatici, che in molti casi hanno funzioni perfettamente legittime. La vera sorpresa è che oltre la metà di questi bot è invece controllato da cyber-criminali o soggetti che ne fanno un uso scorretto.

Un report pubblicato su Internet da **Distill Network** ne analizza l'attività, arrivando alla conclusione che questo tipo di attività malevole **rappresentano il 20% di tutto il traffico Internet**.



Ma di cosa stiamo parlando esattamente? Nella maggior parte dei casi si tratta di attività di raccolta e aggregazione dei dati che hanno scopi commerciali.

I ricercatori ne hanno individuate tre che vanno per la maggiore. La prima è quella del **settore aereo**, in cui un "ecosistema" di operatori, agenzie e aggregatori utilizzano i bot per registrare le offerte e i dati sui voli.

Qualcosa di simile accade anche nel settore dell'e-commerce e addirittura nella **vendita online dei biglietti per eventi e concerti**, nel quale è piuttosto comune utilizzare i bot per verificare la disponibilità di biglietti o acquistarli per poi metterli in vendita sul mercato secondario.

Un capitolo a parte è rappresentato dai classici pirati informatici, che utilizzano i bot per tentare di violare gli account degli utenti. A "spingere" questo fenomeno c'è il fatto che negli ultimi anni il mercato delle credenziali rubate è cresciuto esponenzialmente, come testimoniato dalla comparsa di giganteschi database come il celebre **Collection#1** di cui abbiamo parlato qualche settimana fa.

Le conseguenze dell'attività di questo esercito di bot sono molteplici. Oltre ai problemi di concorrenza sleale collegata all'aggregazione dei dati e al pericolo degli attacchi informatici agli account dei servizi Internet, c'è anche un

ulteriore elemento: i problemi collegati all'aumento anomalo di traffico, che spesso possono sfociare in veri e propri attacchi DoS.

Le infrastrutture dei servizi presi di mira dai bot, infatti, vengono "stressate" oltre ogni limite e il rischio che vadano in crash è estremamente concreto.

Tanto più che i cyber-criminali si stanno evolvendo e sfruttano sempre di più i sistemi cloud per gestire i loro bot, rendendo più difficile il blocco delle attività illecite. Per la cronaca, il record dal punto di vista geografico spetta agli **Stati Uniti**, da cui proviene il 53,4% del traffico.

Please follow and like us:



Attacchi a 360 gradi con il rootkit Scranos

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/18/i-bot-pirata-rappresentano-il-20-del-traffico-su-internet/