Gli strani effetti collaterali degli attacchi ransomware

Lug 26, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

Raffica di black out in Sud Africa, mentre la Louisiana dichiara lo stato di emergenza per evitare di pagare troppo le società di sicurezza.

Di ransomware, negli ultimi tre anni, ne abbiamo parlato tanto e il fatto che continuino a colpire con una certa regolarità, ormai, non fa nemmeno più notizia.

In questi giorni, però, si sono registrati due casi in cui le conseguenze legate agli attacchi informatici hanno caratteristiche davvero peculiari.

Il primo si è verificato in **Sud Africa** il 24 luglio. Protagonista la compagnia energetica **City Power**, che rifornisce di elettricità utenti e altre società nella zona di **Johannesburg** attraverso un sistema di pre-pagamento.

Come riporta **Business Insider South Africa** in un articolo, la società è finita vittima di un attacco che sta avendo pesanti conseguenze sul territorio. Il ransomware che ha colpito i sistemi di City Power ha infatti crittografato il contenuto del database dell'azienda, rendendo impossibile le operazioni di pagamento.

Un problema tecnico che, normalmente, non avrebbe grossi impatti sulla fornitura di energia elettrica, ma considerato il peculiare modello di business (gli utenti acquistano pacchetti prepagati mensilmente) sta facendo parecchi danni.

Anche perché l'attacco si è verificato a ridosso della fine del mese, quando in Sud Africa vengono pagati gli stipendi. Il periodo, cioè, che molti clienti di City Power aspettano per acquistare la fornitura di energia elettrica per il mese dopo. **Risultato: parecchie abitazioni sono rimaste senza elettricità**.

Non solo: a fare le spese dell'attacco in questo momento sono anche gli utenti che utilizzano pannelli solari e che normalmente rivendono l'energia prodotta per "scontare" la bolletta.

Il secondo caso riguarda lo stato della **Louisiana**, il cui governatore ha dichiarato **lo stato di emergenza** dopo una serie di attacchi che hanno preso di mira degli istituti scolastici sul territorio.

La dichiarazione dello stato di emergenza, oltre a consentire di impiegare risorse specifiche (come la Guardia Nazionale, la Polizia di Stato e l'Ufficio dei Servizi Tecnologici) in stretta collaborazione tra loro, prevede anche **una disposizione di legge che vincola le società di sicurezza private**.

Una volta dichiarato lo stato di emergenza, queste **non possono infatti aumentare il compenso richiesto** per intervenire nella risoluzione dei problemi provocati dagli attacchi informatici.

Insomma: si tratta di una norma "anti-sciacallaggio" per impedire che le aziende di cyber-security approfittino dello stato di necessità per gonfiare i prezzi e "spremere" l'amministrazione statale.

Condividi l'articolo

Una nuova immagine, una nuova identità, una nuova visione del futuro: Earth 2050!

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/26/gli-strani-effetti-collaterali-degli-attacchi-ransomware/

Il 49% dei data breach provocati da un errore umano

Lug 25, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, Malware, News, RSS, Scenario 0

La ricerca è stata condotta di IBM e Ponemon Institute. Aumentano i costi per rimediare alle violazioni e le piccole aziende spendono di più di quelle grandi.

Per inquadrare una situazione, spesso, è più utile qualche numero che migliaia di parole. Da questo punto di vista, il report intitolato **Cost of a Data Breach** pubblicato da **IBM** in collaborazione con il **Ponemon** Institute è un esempio cristallino (e preoccupante) in termini di chiarezza.

Lo studio, che si può scaricare attraverso una procedura di registrazione da questo sito, si basa su un campione di 507

aziende e interviste sottoposte a 3.211 persone. I dati che emergono riescono a quantificare un fenomeno sul quale la sensibilità sta crescendo, anche se troppo lentamente.

Anche perché, secondo la ricerca, il costo medio per il recupero da un data breach non è esattamente a buon mercato: ammonterebbe infatti a **3,92 milioni di dollari**, con un costo medio di 150 dollari per record.

Una valutazione che i ricercatori spiegano con il fatto che le conseguenze di un data breach si dispiegano in realtà per un lungo periodo di tempo. A incidere in maniera determinante sul danno è la perdita in termini di business, che lo studio quantifica nel 36% del costo totale.

Il concetto di “tempi lunghi” riguarda anche un altro aspetto, quello della scoperta e reazione al data breach. In media si parla di **279 giorni** (9 mesi!) necessari per individuare il

problema e risolverlo.

Cambiando la prospettiva, emerge come gli attacchi dei pirati informatici rimangano la causa più rilevante delle violazioni di dati. **Non solo: sono anche quelli che provocano maggiori danni (4,45 milioni di dollari) sotto il profilo dei danni e dei costi di ricovero**.

Il dato impressionante, però, riguarda il numero di breach provocati da semplici errori umani, come errate configurazioni ed esposizione involontaria dei dati. **Stiamo parlando del 49% dei casi studiati nel rapporto**. Per contro, questo tipo di incidenti hanno un costo inferiore per le aziende rispetto a quelli provocati dagli attacchi dei cyber-criminali. **Il costo medio varia tra i 3,24 e i 3,5 milioni di dollari**.

Un altro dato interessante riguarda l’impatto in termini di costi a seconda delle dimensioni della aziende. Quelle più grandi (più di 25.000 dipendenti) subiscono un danno medio di 5 milioni di dollari, cioè 200 dollari circa per impiegato.

Le imprese di dimensioni medie (tra 500 e 1.000 dipendenti) si collocano su una media di 2,65 milioni di dollari: **3.533 dollari per impiegato**. La differenza riguarderebbe un classico fenomeno di economia di scala, per cui le aziende più grandi riuscirebbero ad arginare con maggiore facilità il danno economico.

Per quanto riguarda invece il settore di attività, quello che subisce i maggiori danni è quello relativo alla sanità, seguito dai servizi finanziari, dal settore energetico e da quello industriale.

Insomma: se incontrate qualcuno che si ostina a dare scarsa importanza al tema della cyber-security, speditegli il link della ricerca IBM. Il risultato è assicurato.

Condividi l’articolo

Una nuova immagine, una nuova identità, una nuova visione del futuro: Earth 2050! C’è una falla in VLC? Sì, no, forse…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/25/il-49-dei-data-breach-provocati-da-un-errore-umano/

C’è una falla in VLC? Sì, no, forse…

Lug 24, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il NIST sostiene che il bug consenta l’esecuzione di codice attraverso un video infetto, ma gli sviluppatori dell’applicazione negano.

Secondo i programmatori di **VideoLAN** si tratterebbe di una vera e propria fake news. Sull’esistenza di un bug che consentirebbe di attaccare un computer utilizzando un video infetto, però, ci sarà ancora parecchio da discutere.

L’allarme è stato lanciato dal **National Institute of Standards and Technology (NIST)** statunitense e la vulnerabilità è stata classificata come CVE-2019-13615. Si tratterebbe, nel dettaglio, di una falla nel player **VLC** che potrebbe essere sfruttata per provocare un crash dell’applicazione e una possibile esecuzione di codice.

Per arrivare all’obiettivo, un pirata informatico dovrebbe solo fare in modo di indurre la vittima ad aprire un video opportunamente modificato. Insomma, qualcosa di molto simile (anche se in quel caso il rischio era rappresentato dai

sottotitoli) a quanto accaduto due anni fa.

Questa volta però l'efficacia dell'exploit, per lo meno a giudizio degli sviluppatori del player open source più popolare del mondo, è piuttosto dubbia.

Come spiegano in un articolo i colleghi di **The Register**, i dubbi dalle parti di VideoLAN riguardano la riproducibilità dell'exploit.

L'attacco, secondo il NIST, funzionerebbe con le ultime versioni di VLC per sistemi Linux e Windows. Gli sviluppatori di VLC, però, sostengono che il **Proof of Concept** (PoC) rilasciato dai ricercatori di sicurezza (un video MP4), alla prova dei fatti, non provoca alcun crash.

Gli esperti di The Register, si legge nell'articolo, hanno provato a loro volta il PoC in questione su un sistema Linux e confermano che il programma è andato in crash. Non è chiaro, quindi, se le perplessità degli sviluppatori (espresse in termini anche piuttosto coloriti) riguardino il semplice crash o la possibilità che questo porti all'esecuzione di codice.

La discussione, animata su una pagina dedicata al ticket relativo al bug in questione, non sembra essere arrivata a una conclusione ed è quindi difficile capire se VideoLAN rilascerà una patch per correggere la (presunta) falla di sicurezza.

Il consiglio, in ogni caso, è di tenere le antenne dritte e aggiornare immediatamente VLC nel caso in cui comparisse un update disponibile.

Condividi l’articolo

Falla in ProFTPd. Un milione di server vulnerabili

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/24/ce-una-falla-in-vlc-si-no-forse/

Falla in ProFTPd. Un milione di server vulnerabili

Lug 23, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug permette di avviare l'esecuzione di codice in remoto. Pubblicata la patch, ma per il momento i server che l'hanno installata sono… quattro!

Si chiama **ProFTPd** ed è uno di quei componenti che probabilmente non abbiamo mai sentito nominare. Si tratta di un server FTP cross-platform che supporta sia i sistemi basati su Unix, sia Windows. Il software, però, contiene una falla di sicurezza (CVE-2019-12815) che apre la strada ad attacchi in remoto.

Come spiega **Tobias Mädel**, il ricercatore che ha individuato la vulnerabilità, il problema riguarda il modulo **mod_copy**, che nelle installazioni di ProFTPd è attivato come impostazione predefinita.

Il bug, che rappresenta una variante di una vulnerabilità del 2015, consentirebbe di usare i comandi *SITE CPFR* e *SITE CPTO* per eseguire operazioni di lettura e scrittura sui server vulnerabili aggirando i sistemi di autenticazione. In pratica, spiega Mädel, è possibile copiare qualsiasi file in remoto sui server.

Eseguendo una ricerca su **Shodan** (il servizio online che permette di individuare qualsiasi dispositivo o processo su Internet) risultano più di un milione di server con ProFTPd attivo.

La maggior parte di questi sarebbe vulnerabile a un eventuale attacco. La vulnerabilità, infatti, non interessa la versione **1.3.6** del componente, pubblicata il 17 luglio scorso. **Peccato che, sempre su Shodan, i server con la versione aggiornata siano soltanto quattro**.

Non è detto però che tutti i server non aggiornati siano vulnerabili. **Come spiegano i ricercatori, per eliminare il rischio di un attacco è sufficiente disabilitare il modulo mod_copy**. Accettiamo scommesse su quanti amministratori lo abbiano fatto.

Condividi l’articolo

Come funziona la smart home e come è possibile hackerarla!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/23/falla-in-proftpd-un-milione-di-server-vulnerabili/

La Russia come gli USA: ecco i piani di spionaggio sul Web

Lug 22, 2019 Marco Schiaffino In evidenza, Leaks, News, Privacy, RSS 0

Un gruppo hacker ha violato i sistemi di un contractor dei servizi segreti russi. Tra i progetti un sistema per de-anonimizzare il circuito Tor.

Non è ancora comparso nessun "**Edward Snowden** russo", ma a svelare i progetti di Mosca per il controllo di Internet è bastata l'azione di un gruppo hacker.

Protagonista dell'azione un gruppo chiamato **0v1ru$**, che ha preso di mira i server della **SyTech**. Si tratta di un'azienda russa che lavora per conto del **FSB** (l'ex **KGB**) portando avanti numerosi progetti collegati alla cyber-warfare e al controllo dei cittadini russi sul Web.

Dopo aver violato la Active Directory dell'azienda, gli hacker hanno sostituito la homepage con una Yoba-face (immagine molto in voga in Russia, che sta per "trolling") prima di pubblicare il contenuto dei documenti (**7.5 terabytes di dati**) ottenuti

dai sistemi di SyTech.

Come racconta in un articolo la versione russa di BBC (il testo è in russo, consigliamo di usare la traduzione in inglese) il materiale è stato diffuso attraverso un account Twitter registrato il giorno stesso. Dai documenti emergono alcuni progetti segreti su cui SyTech starebbe lavorando per conto del FSB.

- **Nautilus** –Raccolta di informazioni sugli utenti dei social network come Facebook, MySpace e LinkedIn.
- **Nautilus-S** – De-anonimizzazione del traffico su **Tor** (il circuito per la navigazione anonima – ndr) utilizzando dei server "governativi" all'interno del circuito.
- **Reward** – Penetrazione dei circuiti Peer-to Peer, come Torrent.
- **Mentor** – Monitoraggio e ricercar di email sui server delle società russe.
- **Hope** – Creazione di un "mappa" delle rete Internet russa e delle modalità di connessione alle reti delle altre nazioni.

- **Tax-3** – Creazione di una intranet completamente separate degli altri network per memorizzare al suo interno informazioni sensibili riguardanti figure di primo piano dell'amministrazione, giudici e amministratori locali.

Alcuni dei progetti, come **Hope**, appaiono essere collegati a obiettivi più volte dichiarati dallo stesso governo russo, come la messa a punto di una "Internet autosufficiente" che sia in grado di rimanere attiva anche in caso di isolamento dalla rete globale.

Altri ricordano molto da vicino "esperimenti" simili portati avanti dagli USA. **A partire, per esempio, dal tentativo di inquinare la rete Tor, vista anche da Washington come un "problema"**.

Nautilus-S, tra le altre cose, sembra che sia uno dei progetti che è stato effettivamente messo in pratica. Stando ai documenti diffusi sarebbe stato avviato nel 2012 e a confermarne l'efficacia c'è un documento del 2014 che tratta esattamente della scoperta di server Tor su territorio russo che avevano la funzione di de-anonimizzare le comunicazioni sul circuito.

Condividi l'articolo

SonicWall Cloud App Security: sicurezza nell'età del cloud

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/22/la-russia-come-gli-usa-ecco-i-piani-di-spionaggio-sul-web/

Quali dati abbiamo diffuso in Rete? Ecco come scoprirlo

Lug 19, 2019 Marco Schiaffino In evidenza, News, Privacy, Prodotto, RSS, Scenario 0

Da F-Secure un sito che permette di collegarsi rapidamente ai servizi di aziende e social network per verificare quali sono i nostri dati che conservano.

Tutela della privacy, gestione responsabile dei dati, diritto all'oblio… teoricamente abbiamo in mano tutti gli strumenti per mantenere il controllo di ciò che condividiamo online e che viene registrato dai vari fornitori di servizio.

Nella pratica, però, il numero di persone che utilizzano davvero tutti questi strumenti è piuttosto esiguo. Il motivo? Oltre alla solita "scarsa sensibilità" sul tema, c'è anche il fatto che l'accesso alle funzionalità di questo tipo non sono sempre intuitive.

Se volessimo usare con un pizzico di malizia, potremmo dire che a concorrere a questa situazione c'è anche il fatto che i giganti del Web non hanno un grande interesse a incentivarne l'uso.

A cercare di sparigliare le carte ci ha pensato **F-Secure**. La società di sicurezza finlandese ha infatti inaugurato un nuovo servizio online chiamato **Data Discovery Portal** e accessibile a questo indirizzo.

Si tratta, in pratica, di un HUB che ci consente di raggiungere con un clic le sezioni dedicate alla gestione dei dati di diversi servizi: da **Google** ad **Apple**, da **Facebook** a **Snapchat**, fino a **Twitter** e **Alexa**.

Attenzione però: non ci troveremo di fronte a un sistema diverso da quello a cui potremmo comunque accedere normalmente. **Semplicemente possiamo farlo in maniera decisamente più rapida**.

La scelta di fare riferimento alle funzioni dei servizi stessi non è dettata da una forma di pigrizia, ma da una impostazione ben precisa. "*Ciò che accade con la raccolta dei dati è una questione che riguarda interamente te e il servizio*" spiega **Erka Koivunen**, Chief Information Security Officer di F-Secure. "*Non vediamo – né vogliamo vedere – le tue impostazioni o i tuoi dati. Il nostro unico scopo è aiutarti a scoprire quanto delle tue informazioni è là fuori*."

Molte persone, infatti, tendono a sottovalutare la portata del

fenomeno. “*Spesso senti dire, ‘se non stai pagando, il prodotto sei tu.’ Ma i tuoi dati sono un asset per qualsiasi azienda, sia che tu stia pagando per un prodotto oppure no*,” precisa Koivunen. “*I dati permettono alle aziende tecnologiche di vendere miliardi in pubblicità e prodotti, alimentando quello che viene considerato come il più grande business nella storia del denaro*.”

L’azienda cita un’indagine che ha condotto, dalla quale emerge che il 54% degli utenti Internet sopra i 25 anni teme che qualcuno violi i propri account social media. Bene, ma non benissimo.

La logica dell’operazione, spiegano dalle parti di F-Secure, è quella di fare in modo che aumenti la consapevolezza riguardo l’importanza di proteggere in maniera adeguata gli account di questi servizi.

“*Sebbene gli utenti forniscano volontariamente queste informazioni, dovrebbero comprendere quali sono le implicazioni sulla privacy e la sicurezza che si generano col creare account che posseggono più dettagli sulla nostra identità di quanti potremmo condividere con la nostra famiglia*,”conclude Koivunen. “*Tutte queste informazioni potrebbero finire nelle mani di un hacker con una violazione o una compromissione di un account*.”

Condividi l’articolo

Protezione dei minori? Sì, ma tutelando la privacy

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/19/quali-dati-abbiamo-diffuso-in-rete-ecco-come-scoprirlo/

Protezione dei minori? Sì, ma tutelando la privacy

Lug 18, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

La nuova edizione dell'antivirus Bitdefender introduce nuove funzionalità di parental control. Nel mirino il fenomeno del cyber-bullismo.

Il concetto di sicurezza informatica si sta allargando progressivamente: dal semplice rilevamento (ed eliminazione) dei malware, si è progressivamente passati a strumenti di protezione che comprendono aspetti molto differenti della dimensione digitale della nostra vita.

La conferma arriva da **Bitdefender**, che oggi ha lanciato sul mercato le nuove versioni dei suoi software di sicurezza per il 2020. Tra le novità, una funzione di parental control "evoluta" e tanta attenzione per la privacy.

A partire, per esempio, da **una funzione dedicata al blocco del tracciamento della navigazione tramite browser**, che molti utenti cominciano a sentire come una priorità per tutelare la loro privacy.

La vera novità riguarda però l'introduzione di un nuovo sistema di parental control che, oltre a funzioni "standard"

come la limitazione dei tempi di navigazione e il blocco di applicazioni e contenuti inappropriati, introduce funzioni avanzate come gli strumenti per bloccare contatti “indesiderati” e nuovi mezzi di contrasto del cyber-bullismo.

Ma di cosa si tratta in pratica? **Parental Control Premium** introduce una serie di sistemi di controllo basati sull’Intelligenza Artificiale (AI) che consentono di rilevare richieste o scambi di foto inappropriate, inviti ad appuntamenti da parte di sconosciuti e divulgazione di informazioni personali come l’indirizzo di casa o i dati della carta di credito.

Il fiore all’occhiello del nuovo strumento è però il sistema di **contrasto al cyber-bullismo**. Il software analizza infatti le comunicazioni (le nuove funzionalità sono disponibili per il momento solo per gli utenti di lingua inglese) per individuare messaggi o indizi di vario genere che possono corrispondere a dinamiche legate al cyber-bullismo.

Anche in questo ambito, però, gli sviluppatori di Bitdefender si sono preoccupati di tutelare la privacy, anche nei confronti dei genitori. Il controllo delle immagini (che

individua nudità ma anche documenti o carte di credito) per esempio, viene eseguito in locale senza coinvolgere i server della società di sicurezza.

Anche i messaggi (**Facebook, Whatsapp e Instagram**), che vengono dati in pasto a un algoritmo dedicato che non opera per parole chiave ma analizza il contesto per capire cosa stia succedendo, **vengono cancellati immediatamente dopo l'analisi in modo che non si aprano spazi che possano ledere la riservatezza della sfera privata**.

L'attenzione per la privacy, però, è anche (e soprattutto) confermata nelle procedure previste in caso di pericolo. Nell'eventualità in cui vengano rilevati indizi che possono far pensare a una vessazione da parte di cyber-culli, i genitori ricevono una segnalazione che **non comprende i messaggi scambiati**.

Questo per evitare che il sistema di parental control si trasformi in una sorta di "grande fratello" che il minore vivrebbe come uno strumento di controllo invasivo.

La procedura, messa a punto con la collaborazione di psicologi e professionisti del settore pedagogico, prevede anche la visualizzazione di suggerimenti su come affrontare il tema con il bambino.

Insomma: la nuova interpretazione del parental control abbandona la logica del semplice "controllo" per approdare a una concezione in cui l'uso dell'intelligenza artificiale consente di segnalare potenziali pericoli mantenendo quegli "spazi privati" che anche un bambino o un ragazzo ha diritto di avere.

Condividi l'articolo

Quali dati abbiamo diffuso in Rete? Ecco come scoprirlo Bug

nei NAS Iomega. Milioni di file esposti su Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/18/protezione-dei-minori-si-ma-tutelando-la-privacy/

Bug nei NAS Iomega. Milioni di file esposti su Internet

Lug 17, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il problema riguarda una API che consente di accedere a qualsiasi file senza autenticazione. La patch? Lenovo ci sta ancora lavorando…

Anche se il marchio sembra arrivare da un passato remoto, la vulnerabilità che affligge i NAS **Iomega** (storico brand del settore storage che nel 2013 è stato "resuscitato" da **Lenovo**) è un problema terribilmente attuale e che probabilmente vedrà una soluzione solo nel futuro. Quanto prossimo, si vedrà.

A riportare la vicenda sono i colleghi di **The Register**, che in un articolo pubblicato ieri citano come fonti le due società di sicurezza (la statunitense **WhiteHat Security** e la nord-irlandese **Vertical Structure**) che hanno individuato il bug.

I ricercatori non diffondono dettagli tecnici, ma si tratterebbe di una falla di sicurezza in una API che, in pratica, espone tutti i file su Internet e che consentirebbe a chiunque di accedervi liberamente.

La scoperta sarebbe seguita a una ricerca su **Shodan** (il servizio online che permette di tracciare qualsiasi dispositivo su Internet) da cui è emersa la presenza di milioni di file accessibili a chiunque.

Insomma: qualcosa di molto simile a quello che succede sempre più spesso con i famigerati Bucket S3 "aperti" che vengono individuati con sconcertante frequenza su Internet.

Nel dettaglio, i ricercatori hanno individuato 13.000 fogli di calcolo contenenti l'indicizzazione di 3.030.106 file per un totale di 36 terabyte di dati.

Buona parte di questi (405.398) sono immagini, ma ci sono anche 20.055 documenti, 13.677 fogli di calcolo e 13.972 documenti di testo. **Tra i dati ci sono anche file che contengono informazioni finanziarie, numeri di carte di**

credito e le immancabili scansioni di passaporti e documenti.

Il bug interesserebbe un software installato su vecchi modelli Iomega, che sfrutta la API incrimanata per la condivisione dei file in rete. Lenovo, dopo la segnalazione (inviata lo scorso autunno) si è impegnata a correggere la falla di sicurezza. **Al momento, però, non c'è ancora nessuna traccia della patch**.

Il consiglio, per chi possiede un NAS Iomega e teme di essere vittima del bug, è quello di controllare periodicamente la pagina di segnalazione degli aggiornamenti di Lenovo Prima o poi salterà fuori qualcosa.

L'importante è che non vi colleghiate assolutamente al sito iomega.com che compare se si cerca "Iomega" su Google. Ci siamo finiti durante la redazione di questo articolo e abbiamo scoperto che **reindirizza a pagine Web letteralmente infestate di truffe, malware e altro codice pericoloso**.

A quanto pare, il dominio è stato abbandonato e adesso è registrato da una società con sede alle isole Cayman. Abbiamo comunicato il problema a Lenovo e pubblicheremo eventuali aggiornamenti sulla vicenda.

Condividi l'articolo

Bug in Instagram permetteva di rubare gli account

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/17/bug-nei-nas-iomega-milioni-di-file-esposti-su-internet/

Bug in Instagram permetteva di rubare gli account

Lug 16, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una falla di sicurezza nel sistema di recupero password consentiva di eseguire un attacco di brute forcing per violare il codice di conferma.

L'utilizzo dei codici inviati via SMS non è uno strumento particolarmente sicuro quando viene usato come sistema di autenticazione a due fattori. Se viene usato come unico strumento per l'autenticazione, però, rischia di trasformarsi in una vera voragine di sicurezza.

Per spiegarlo agli sviluppatori di **Instagram**, però, c'è voluto l'intervento di **Laxman Muthiyah**, un ricercatore di sicurezza che ha scovato una clamorosa falla nel sistema di autenticazione del social network.

Come spiega in un articolo pubblicato su Internet, nella sua attività di "cacciatore di bug" Muthiyah si è concentrato per qualche tempo sul sistema di recupero della password di Instagram. Il social network, infatti, prevede diverse modalità per chiedere il reste della password.

Quello per la versione Web utilizza un classico link che ha tutte le carte in regola per resistere a qualsiasi attacco. Quello per mobile, invece, sfrutta un codice a sei cifre che viene inviato tramite SMS al telefono del legittimo proprietario dell'account.

Ciò è che si è chiesto Muthiyah è: cosa succede se qualcuno prova a violare il codice provando tutte le possibili combinazioni?

Teoricamente, operazioni come queste (con un codice a sei cifre stiamo parlando di **un milione di possibili combinazioni**) dovrebbero essere bloccate automaticamente. Prima di escludere a priori l'ipotesi, però, il ricercatore ha deciso di provarci.

Il primo tentativo, spiega nel suo articolo, gli ha permesso di capire che il sistema di protezione scelto da Instagram contro gli attacchi di brute forcing è quello di limitare il numero di tentativi di accesso. Non solo: la validità del codice è di 10 minuti.

Nello specifico, Muthiyah ha scoperto di essere in grado di inviare fino a un massimo di 200 codici in 10 minuti da un singolo computer.

Quello che ha scoperto, però, è che il sistema di protezione considera soltanto il singolo dispositivo, individuandolo attraverso l'indirizzo IP. Un attacco contemporaneo da parte di più computer (o da differenti indirizzi IP) però, può far saltare la protezione.

[embedded content]

Nel video qui sopra, Muthiyah mostra come sia riuscito a eseguire 200.000 tentativi di accesso utilizzando 1.000

indirizzi IP.

Per garantire un successo al 100%, di conseguenza, basterebbe utilizzare **5.000 IP differenti** e una potenza di calcolo sufficiente per inviare un milione di richieste in 10 minuti. Impossibile? Non proprio. **Secondo il ricercatore, le risorse su cloud per un'operazione del genere richiedono un investimento di soli 150 dollari**.

Molti se si pensa di hackerare account a caso, ma decisamente pochi se si vuole colpire uno specifico bersaglio di "alto profilo", come un politico o una celebrità.

Prima di correre ad affittare server su Amazon, sappiate che dopo la segnalazione di Muthiyah Instagram ha tempestivamente corretto la falla di sicurezza, ricompensando il ricercatore con 30.000 dollari.

La cifra (piuttosto modesta) riconosciuta come "taglia" per il bug è giustificata, tutto sommato, dalla relativa pericolosità del bug. **Per poter portare l'attacco, infatti, è necessario conoscere il numero di telefono della vittima**. Un dettaglio che, nel caso di bersagli di alto profilo, non dovrebbe essere facile da ottenere.

Condividi l'articolo

Nuovi attacchi ai router. La minaccia arriva dal Brasile

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/16/bug-in-instagram-permetteva-di-rubare-gli-account/

Nuovi attacchi ai router. La minaccia arriva dal Brasile

Lug 15, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, News, Phishing, RSS, Vulnerabilità 0

La tecnica punta a modificare le impostazioni DNS per dirottare le vittime su siti di phishing per rubare credenziali bancarie o di servizi online come Netflix.

Nel mondo della pirateria informatica, la scuola brasiliana ha una storia tutta sua. I cyber-criminali che operano in **Brasile**, infatti, si distinguono spesso per utilizzare tecniche di attacco piuttosto particolari. L'ultima in ordine di tempo prende di mira i router casalinghi.

L'obiettivo è quello di modificare le impostazioni del server DNS allo scopo di dirottare a loro piacimento la navigazione delle vittime.

Come spiegano i ricercatori di **Avast** in un report pubblicato settimana scorsa, i pirati in questione utilizzano due diversi Exploit Kit chiamati **GhostDNS** e **Sonar DNS**. Si tratta di strumenti di hacking che i cyber-criminali utilizzerebbero inserendoli all'interno di **siti Internet per lo streaming di video pirata o con contenuti per adulti**.

Una mossa decisamente brillante: l'attacco, spiegano i ricercatori, richiede infatti un po' di tempo e utilizzare dei siti di streaming garantisce che le vittime rimangano collegate per un periodo di tempo piuttosto lungo.

Una delle tecniche utilizzate è quella di eseguire un brute forcing utilizzando credenziali predefinite. Per farlo, i pirati utilizzano uno strumento che identifica il modello di router usato dalla potenziale vittima e prova ad accedervi con le relative credenziali.

Analizzando il codice di GhostDNS, per esempio, i ricercatori hanno individuato una collezione di credenziali che comprende la combinazione **user name: admin – password: gvt12345**. Si tratta dei dati di accesso predefiniti che venivano usati qualche tempo fa da **GVT**, ora acquisita da **Teleônica Brasil**, uno dei maggiori provider del paese.

In altri casi, invece, i cyber-criminali utilizzano trucchi più tradizionali, come la visualizzazione di falsi messaggi che richiedono l'aggiornamento del browser ma che, in realtà, avviano una procedura di modifica delle impostazioni del server DNS in modo che il PC si colleghi a un server controllato dai pirati.

SonarDSN è uno strumento decisamente più sofisticato. Si tratterebbe, spiegano i ricercatori, di un software derivato da uno strumento di hacking chiamato sonar.js e che viene utilizzato normalmente dagli esperti di penetration testing, gli hacker "etici" che violano le reti aziendali per verificarne il livello di sicurezza.

SonarDNS è in grado di individuare i dispositivi collegati in rete e scegliere automaticamente gli exploit che consentono di violarne la configurazione da un "arsenale" opportunamente selezionato.

Ma qual è l'obiettivo dell'attacco? Secondo i ricercatori di Avst, si tratterebbe di una classica campagna di phishing. Una volta modificata l'impostazione del DNS, infatti, la navigazione può essere dirottata a piacimento. **I pirati brasiliani utilizzano questa opportunità per rubare le credenziali di accesso a servizi bancari o ad altri siti Internet, come Netflix**.

Tutto quello che devono fare è aspettare che la vittima provi a collegarsi al sito originale, per esempio **lamiabanca.com**. Normalmente, questa richiesta verrebbe inviata al server DNS che ha il compito di risolvere l'indirizzo e fornire l'IP corrispondente, del tipo **104.55.555.555**.

Quando però la richiesta viene inviata al server DNS controllato dai pirati, questo indica un indirizzo IP diverso da quello del sito legittimo, ma che ospita una pagina Web del tutto simile a quella originale**. La vittima, in questo modo, è convinta di essere collegata al sito della sua banca, ma è in realtà su un sito controllato dai pirati informatici. E se inserisce le sue credenziali di accesso…**

Secondo il report di Avast, questo genere di attacchi starebbe aumentando vertiginosamente e nel solo Brasile i cyber-criminali avrebbero compromesso più di **180.000 router**.

Condividi l’articolo

Un nuovo gruppo MageCart attacca “a tappeto” i bucket S3

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/15/nuovi-attacchi-ai-router-la-minaccia-arriva-dal-brasile/