Attacchi a 360 gradi con il rootkit Scranos

Apr 17, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS, Trojan 0

Il malware è in grado di caricare payload in memoria e cancellarli per evitarne il rilevamento. Obiettivo: incassare denaro in qualsiasi modo possibile.

Ha colpito prima in Cina, ma adesso si sta diffondendo in tutto il mondo attraverso una campagna di attacchi che, secondo i ricercatori di **Bitdefender**, rischia di allargarsi a macchia d'olio. **Scranos**, d'altra parte, ha tutte le caratteristiche per avere un certo successo nel settore.

Si tratta di un **rootkit** che utilizza per l'installazione un certificato digitale valido, probabilmente rubato, e che integra una serie di funzionalità in continua evoluzione. Gli stessi ricercatori lo definiscono un "work in progress", che sembra evolversi mano a mano che i suoi autori aggiungono nuovi moduli e payload.

Come spiegano dalle parti di Bitdefender in un report pubblicato dalla società di sicurezza, Scranos ha caratteristiche uniche. Si tratta infatti di un rootkit multi-piattaforma che i pirati informatici diffondono inserendone il codice all'interno di software legittimi (come i reader per e-book) o nei classici crack per videogiochi o software.

Una tecnica piuttosto efficace, visto che i cyber-criminali non devono nemmeno preoccuparsi di utilizzare exploit o vulnerabilità per installare il malware, ma possono "introdurlo" in un processo di installazione avviato direttamente dall'utente.

L'uso del certificato digitale registrato a nome di **Yun Yu Health Management Consulting**, una società con sede a Shangai, gli permette di aggirare i controlli e mantenere un basso profilo.

Nel dettaglio, l'attacco sfrutta un processo distinto in varie fasi, che i ricercatori di Bitdefender hanno analizzato e descritto nel dettaglio.

Il primo componente installato è il dropper, che si preoccupa per prima cosa di rubare alcune informazioni come cookie, credenziali di login e pagamento attraverso delle DLL specializzate che prendono di mira in particolare **Facebook**, **Amazon** e **Airbnb**.

Lo stesso dropper si occupa poi di installare il rootkit sul sistema, che viene avviato a ogni accensione del dispositivo grazie a una modifica del registro.

A questo punto Scranos utilizza il collegamento con il server Command & Control per scaricare e avviare differenti payload, che il rootkit può gestire sotto ogni aspetto. In particolare Scranos adotta una tecnica piuttosto raffinata per far passare inosservata l'attività dei vari moduli che carica, iniettandoli all'interno del processo **svchost.exe**.

I payload individuati dai ricercatori sono estremamente variegati e comprendono la possibilità di promuovere canali **YouTube** attraverso Chrome, rubare le credenziali del servizio di gaming **Steam**, utilizzare l'account di **Facebook** per inviare spam e collegamenti ad app mobile infette, sottrarre i dati riguardanti la cronologia di navigazione su Internet.

Scranos, poi, dedica una particolare attenzione a **Chrome**, installando una serie di estensioni che hanno l’obiettivo di modificare il motore di ricerca predefinito e attirare la vittima su siti pericolosi, presumibilmente controllati dagli stessi pirati informatici o da loro affiliati.

Insomma: per gli autori di Scranos, le vittime sono come il maiale: non si butta via niente. Considerato l’impianto di base del rootkit, però, è probabile che in un prossimo futuro potremo vedere ulteriori evoluzioni.

Please follow and like us:

Falla negli smartwatch TicTocTrack e i pirati possono tracciare i bambini

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/17/attacchi-a-360-gradi-con-il-rootkit-scranos/

Falla negli smartwatch TicTocTrack e i pirati possono tracciare i bambini

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

I dispositivi sono pensati per "sorvegliare" i minorenni, ma è possibile violare l'account e contattare i bambini. L'azienda sospende il servizio durante le indagini.

Sono pensati per offrire un maggior livello di sicurezza per i genitori ansiosi, ma adesso si scopre che rappresentano essi stessi un potenziale pericolo per i minori.

Stiamo parlando degli smartwatch **TicTocTrack**, venduti in Australia come strumento di sorveglianza che i genitori possono utilizzare per monitorare gli spostamenti dei loro figli e, se lo desiderano, contattarli con un messaggio o una chiamata. Come hanno scoperto i ricercatori di **Pen Test Partners**, però, i dispositivi in questione sono tutt'altro che sicuri.

Come spiegano nel loro report, i TicTocTrack sono uno spin-off per il mercato australiano degli smartwatch marchiati **Gator**,

che in passato avevano già dimostrato di avere qualche problema di sicurezza.

La versione australiana, però, è dotata di un back-end realizzato su misura e si pensava (il passato è d'obbligo) che non avesse gli stessi problemi. Ora, però, si scopre che nemmeno gli utenti australiani possono stare tranquilli.

Come si legge nel report pubblicato da Pen Test Partners, le API utilizzate per l'app di TicTocTrack (sviluppata da **Nibaya**, con sede in Sri Lanka) utilizzano un semplicissimo sistema di accesso tramite username e password che non prevede nessuna ulteriore autenticazione.

Chiunque abbia un account in pratica, può modificare i

parametri dell’app per collegarsi al dispositivo di un’altra persona, ottenendo immediatamente anche i dati anagrafici completi e le informazioni sulla posizione del bambino che indossa il dispositivo.

Peggio ancora: attraverso richieste mirate è possibile arrivare allo stesso risultato puntando direttamente ai sistemi che gestiscono le API.

In pratica, un pirata informatico potrebbe facilmente accedere ai dati di qualsiasi bambino indossi un TicTocTrack, ottenere informazioni personali e conoscerne la posizione.

Attraverso il sistema, poi, potrebbe anche **contattarlo con una chiamata audio o un SMS e addirittura modificare i dati sulla posizione in modo che i genitori non possano trovarlo**.

Insomma: quello che dovrebbe essere uno strumento per tenere sotto controllo i minori, si trasforma in una potenziale minaccia per la loro sicurezza.

La nota positiva, come sottolineano gli stessi ricercatori, riguarda la reazione dell’azienda. Una volta ricevuta la comunicazione riguardante la vulnerabilità del software, **il produttore ha immediatamente sospeso le funzionalità e avviato le operazioni necessarie per verificarle e correggerle, dandone immediato avviso a tutti i clienti**.

Please follow and like us:

Falla in Internet Explorer. Microsoft la ignora ma arriva l’exploit

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/16/falla-negli-smartwatch-tictoctrack-e-i-pirati-possono-tracciare-i-bambini/

Falla in Internet Explorer. Microsoft la ignora ma arriva l'exploit

Apr 15, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità permette di rubare qualsiasi file dal computer della vittima. Nessuna patch rilasciata e il ricercatore pubblica il codice per sfruttarla.

Questa volta, per lo meno, nessuno dalle parti di Microsoft ha provato a proporre la fatidica frase del tipo "non è un bug, è una feature", ma il risultato non è cambiato di molto.

La vulnerabilità individuata da **John Page**, secondo l'azienda di **Satya Nadella**, non rappresenta un problema "urgente" e di conseguenza non è stata pianificata alcun aggiornamento per correggerla.

E dire che non si tratta proprio di un problema da ridere. **Il bug, infatti, interessa Internet Explorer e la possibilità che il browser venga utilizzato per rubare file da un sistema**

Windows.

A renderlo possibile è il modo in cui IE gestisce alcuni comandi (duplicazione scheda, stampa e anteprima di stampa) che permetterebbero di sfruttare una tecnica di **injection XML** per sottrarre, appunto qualsiasi file presente sul sistema.

Il vettore di attacco, come spiega lo stesso Page sul suo sito, è un file in formato **.MHT**, usato un tempo dai browser per memorizzare in locale le pagine Web.

Nel dettaglio, tutto quello che dovrebbe fare un pirata informatico sarebbe inviare alla vittima il file MHT infetto e indurla ad aprirlo. Normalmente la presenza di codice attivo all'interno del file dovrebbe far scattare un avviso e una richiesta di conferma, ma **la procedura è aggirabile**.

[embedded content]

La scarsa attenzione di Microsoft per il problema, molto probabilmente, è dovuta al fatto che Internet Explorer è stato "abbandonato" da tempo e che il browser ha una diffusione piuttosto limitata. **Secondo gli ultimi dati disponibili, infatti, lo utilizzerebbero come browser di default poco più del 7% degli utenti**.

Il problema, però, è che su Windows rimane il programma predefinito per aprire i file .MHT. L'attacco, quindi, mantiene tutta la sua pericolosità anche nel caso in cui l'utente usi un altro browser per navigare.

Tanto più che dopo il diniego di Microsoft riguardo lo sviluppo di una patch, Page ha pubblicato sulla sua pagina il codice che permette di sfruttare l'exploit. Ora non resta che aspettare e vedere se qualcuno deciderà di sfruttarla. Il suggerimento, nel frattempo, è quello di diffidare di qualsiasi allegato nel formato incriminato.

Please follow and like us:

Il 67% degli alberghi fornisce informazioni riservate a terze parti

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/15/falla-in-internet-explorer-microsoft-la-ignora-ma-arriva-lexploit/

Il 67% degli alberghi fornisce informazioni riservate a terze parti

Apr 12, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Vulnerabilità 0

I dati inseriti nei siti Web delle strutture vengono acquisiti da società pubblicitarie e di marketing. Potrebbero usarli anche per modificare o cancellare le prenotazioni.

Difficile pensare che i ricercatori di **Symantec**, quando hanno iniziato a passare al setaccio i siti Internet delle strutture

alberghiere, si aspettassero di trovarsi di fronte a una simile voragine in termini di privacy e sicurezza.

A quanto si legge nel post pubblicato da **Candid Wueest**, però, quella che emerge è un vero scandalo: il 67% dei siti esaminati dal ricercatore di sicurezza contengono componenti gestite da soggetti terzi e permettono loro di accedere a informazioni che dovrebbero essere riservate.

Stiamo parlando, nella maggior parte dei casi di **dati anagrafici, indirizzo di posta elettronica, residenza, numero telefonico, del numero di passaporto e alcuni dati della carta di credito come le ultime quattro cifre del numero, il tipo di carta e la data di scadenza**.

Quanto basta, insomma, per fornire a chiunque abbastanza informazioni per portare attacchi di phishing o addirittura prendere il possesso dell'account di un qualsiasi servizio Internet che usa queste informazioni come strumento per il recupero della password.

Come mai avviene tutto questo? Secondo Wueest, il vettore principale del leak è dovuto all'abitudine di inviare un'email di conferma ai clienti attraverso un link che permette di accedere direttamente alla prenotazione effettuata.

Siccome, però, la pagina visualizzata contiene normalmente numerosi elementi esterni e ogni richiesta contiene l’url completa, tutti i soggetti coinvolti possono accedere a questi dati.

Secondo il ricercatore, mediamente ogni prenotazione online “condivide” i suoi dati con almeno 30 service provider, compresi social network, aziende pubblicitarie e società di

marketing.

Accedendo al link, però, tutti questi soggetti potrebbero non limitarsi a registrare le informazioni, ma anche accedere alla prenotazione per modificarla o cancellarla.

Il problema riguarda anche i siti che offrono servizi di aggregazione delle offerte alberghiere. Dei cinque analizzati dal ricercatore, due trasmettono le credenziali e uno invia i link senza alcuna protezione crittografica.

Una modalità, quest'ultima, che viene adottata dal 29% dei siti di prenotazione e che apre la strada alla possibilità che un pirata informatico possa "sniffare" il link quando la trasmissione avviene per esempio in una rete Wi-Fi compromessa.

Inutile dire che una situazione del genere è assolutamente incompatibile con il nuovo GDPR, che prevede l'implementazione di strumenti per la tutela della privacy e protezione dei dati piuttosto stringenti.

I gestori dei servizi, però, non sembrano preoccuparsene più di tanto. Il tasso di risposta dei responsabili della protezione dei dati alle segnalazioni inviate da Wueest nel corso di sei settimane è sconsolante: **il 25% le ha completamente ignorate**.

Please follow and like us:

Ecco Dragonblood, la prima vulnerabilità di WPA3

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/12/il-67-degli-alberghi-fornisce-informazioni-riservate-a-terze-parti/

Ecco Dragonblood, la prima vulnerabilità di WPA3

Apr 11, 2019 Marco Schiaffino In evidenza, News, RSS, Tecnologia, Vulnerabilità 0

Il nuovo standard non è ancora entrato a regime ma spunta già una falla di sicurezza che consente di violare il sistema di autenticazione.

Niente panico: per una volta, la vulnerabilità è spuntata esattamente quando doveva farlo, cioè quando i dispositivi che implementano lo standard sono pochi e vengono costantemente monitorati per verificare se spuntano eventuali problemi.

A specificarlo è la stessa **Wi-Fi Alliance**, nel comunicato stampa che ha pubblicato per segnalare la scoperta di **Dragonblood**, una falla di sicurezza che affligge il nuovo protocollo **WPA3-Personal**.

I problemi nascono dal fatto che il nuovo sistema di handshacking, noto come **Simultaneous Authentication of Equals (SAE)** o **Dragonfly**, permetterebbe di raccogliere informazioni attraverso un attacco side-channel, oltre a “non implementare

in maniera appropriata alcune operazioni crittografiche o usare componenti di crittografia indesiderati”.

Insomma: come spiegano **Mathy Vanhoef** ed **Eyal Ronen**, i due ricercatori che hanno scoperto la falla di sicurezza, si apre la possibilità che un pirata informatico possa violare la password di autenticazione attraverso una serie di azioni combinate.

Un attacco che permetterebbe di intercettare informazioni riservate come numeri di carte di credito, password, messaggi di chat, email e simili.

I due ricercatori hanno anche pubblicato su Internet una serie di tools che dimostrano l’efficacia delle tecniche di attacco, che si muovono su due binari.

Alcune sfruttano un sistema di **downgrade**, forzando in pratica il dispositivo ad “abbandonare” WPA3 per utilizzare WPA2, che utilizza il vecchio sistema di scambio di informazioni.

Queste ultime possono essere utilizzate per effettuare un attacco a dizionario offline che permetterebbe di violare il sistema di autenticazione del dispositivo.

Una variante di questo attacco, che i ricercatori definiscono “downgrade di gruppo”, prevede un attacco di jamming in grado di “ingannare” i dispositivi collegati alla rete Wi-Fi e **forzarli a utilizzare i protocolli di crittografia più deboli di quelli normalmente utilizzati**.

Il secondo binario è rappresentato dagli attacchi side-channel, sia di tipo cache che di tipo timing, che consentirebbero di recuperare la password attraverso una tecnica simile all'attacco a dizionario (**password partitioning**).

Vanhoef e Ronen, spiegano nel loro report, non hanno pubblicato tutti i dettagli delle vulnerabilità che hanno individuato e stanno collaborando con la Wi-Fi Alliance e i produttori per risolvere quelli ancora "aperti". Per tutti gli altri sarebbero già state realizzate le patch che correggono lo standard.

Please follow and like us:

Password predefinita nell'app: migliaia di auto a rischio furto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/11/ecco-dragonblood-la-prima-vulnerabilita-di-wpa3/

Password predefinita nell’app: migliaia di auto a rischio furto

Apr 10, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Gli sviluppatori di MyCar avevano “dimenticato” delle credenziali di amministratore inserite nel codice. Un ladro avrebbe potuto usarle per rubare le auto.

Così “smart” da essere facilissime da rubare. Le cosiddette “auto connesse” incappano nell’ennesimo incidente di sicurezza legato a un problema software.

Questa volta a finire sul banco degli imputati è **MyCar**, un set che consente di controllare a distanza alcune funzionalità dell’auto attraverso la connessione 3G e che può essere installato su numerosi modelli di veicoli per renderli “smart”.

Il sistema, come si legge sul sito, consente di aprire l’auto, accendere il motore, localizzare il veicolo, controllare la temperatura e molto altro ancora. Tutto attraverso un’app disponibile per **iOS** e **Android**.

Peccato che nel codice dell’app ci fosse **il classico account nascosto con privilegi di amministratore** che ogni tanto gli sviluppatori hanno la pessima abitudine di “dimenticare” nelle applicazioni. Risultato: chiunque lo avesse individuato avrebbe potuto accedere all’account di qualsiasi utente.

Foto di Will Dormann via Twitter

Insomma: un ladro avrebbe potuto collegarsi al server abbinando l'app a qualsiasi account, localizzare l'auto, aprirla e addirittura accenderla.

Ad accorgersene (qui il report originale) sono stati i ricercatori della **Carnagie Mellon University**, che hanno tempestivamente notificato il problema a MyCar e consentito allo sviluppatore di correggere il problema.

L'account è stato rimosso nelle nuove versioni dell'app (3.4.24 per iOS, 4.1.2 per Android) e, soprattutto, dai server del sistema. In questo modo anche gli utenti che non hanno ancora eseguito l'aggiornamento non rischiano più il furto "smart" della loro auto.

Tutta la vicenda si inserisce in una nuova fase delle vulnerabilità per le smart card. Se i primi casi hanno riguardato infatti i sistemi sviluppati dai produttori automobilistici, adesso le maggiori preoccupazioni riguardano i produttori di accessori, come è successo nel caso di alcuni antifurti "intelligenti" qualche settimana fa.

E visto che la sbornia di automazione attraverso i controlli via smartphone non sembra destinata a ridursi in tempi brevi,

è probabile (purtroppo) che ci troveremo a parlare ancora di casi simili.

Please follow and like us:

Ecco Dragonblood, la prima vulnerabilità di WPA3 Crittografia a prova di violazione? La soluzione è EverCrypt

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/10/password-predefinita-nellapp-migliaia-di-auto-a-rischio-furto/

Crypto-Jacking via browser in calo: ora si mina con il malware

Apr 08, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario, Tecnologia 0

L'ondata di attacchi ai siti Web sta scemando e

crescono i malware dedicati. Gli esperti: “i cyber-criminali riescono a guadagnare più denaro”.

Bitcoin e altre cripto-valute rimangono il metodo preferito dai pirati informatici per riempirsi le tasche tecniche ai danni delle loro vittime.

Secondo i ricercatori del team **X-Force di IBM**, però, la strategia dei cyber-criminali si sta lentamente evolvendo. Come spiega **Charles DeBeck** in un report pubblicato su Internet, la sbornia legata all’uso di JavaScript inseriti all’interno di siti Internet (**Crypto-Jacking**) sta passando e i pirati puntano sempre più spesso sui malware.

Il motivo? Una questione di efficacia. Il Crypto-Jacking, infatti, fa comunque leva sul browser delle vittime e consente di sfruttare solo una parte della potenza di calcolo del computer per generare cripto-valuta. L’uso di veri e propri malware permette invece di agire con maggiore libertà.

Nel corso del 2018 il Crypto-Jacking l’ha fatta da padrone, come confermano i casi registrati dalle società di sicurezza.

Il progressivo abbandono del Crypto-Jacking è dovuto a numerosi fattori. IL primo riguarda il fatto he hanno cominciato a comparire strumenti specializzati per rilevare la presenza di JavaScript sui siti che visualizzano un avviso agli utenti quando uno di questi è presente.

Contemporaneamente, molti software antivirus hanno cominciato a rilevare i JavaScript di questo tipo e segnalarne la presenza.

Non ultimo, c'è da considerare l'abbandono di **CoinHive**, uno degli script più usati per questo scopo e di cui abbiamo parlato ampiamente in questo articolo.

In particolare, la questione si focalizza sulle diverse caratteristiche delle varie cripto-valute. I JavaScript sui siti Internet (come CoinHive) possono avere buone prestazioni solo quando generano **Monero**, una valuta digitale i cui algoritmi di elaborazione sono ottimizzati per i calcoli della CPU.

La maggior parte delle cripto-valute, però, **forniscono prestazioni migliori quando si sfrutta il processore grafico** e, per farlo, è necessario avere un livello di accesso al sistema più "profondo".

Ecco perché i cyber-criminali sembrano aver deciso di puntare con decisione sulla diffusione di malware, investendo anche nell'evoluzione del codice usato per impedire che gli antivirus siano in grado di individuarli.

Un esempio di questo tipo di evoluzione è la comparsa di **GhostMiner**, un malware "fileless", residente cioè solo in memoria e che è di conseguenza molto più difficile da individuare rispetto a quelli tradizionali.

Please follow and like us:

Crittografia a prova di violazione? La soluzione è EverCrypt Autogol di Xiaomi: il software di sicurezza ha una falla… di sicurezza

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/08/crypto-jacking-in-calo-ora-i-pirati-puntano-piu-sui-malware/

Autogol di Xiaomi: il software di sicurezza ha una falla… di sicurezza

Apr 05, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug si nascondeva in Guard Provider, un'app preinstallata sui dispositivi Xiaomi. La vulnerabilità permette un attacco Man-in-the-Middle.

In ambiente **Android** ormai i maggiori problemi sembrano derivare dalle applicazioni preinstallate sui dispositivi.

Succede nel caso degli attacchi che colpiscono la filiera di produzione (ne abbiamo parlato in questo articolo) ma anche per altri motivi.

Nel caso di **Xiaom**i, per esempio, la grana si è presentata sotto forma di una vulnerabilità in grado di consentire un attacco di tipo **Man-in-the-Middle (MiTM)** ai danni dei dispositivi del produttore cinese.

E non stiamo parlando di poca cosa: l'azienda con sede a Pechino, infatti, detiene **una quota di mercato dell'8% nel settore mobile, che ne fa il terzo produttore al mondo**. Stiamo parlando, quindi, di milioni di smartphone potenzialmente a rischio attacco.

Ma qual è esattamente il problema? Come spiegano i ricercatori di **Check Point**, che hanno individuato la falla e ne hanno descritto i dettagli in un report pubblicato su Internet, la vulnerabilità in questione si trova in un'applicazione di sicurezza preinstallata sui dispositivi Xiaomi.

Si chiama **Guard Provider** e avrebbe il compito di individuare eventuali malware, ma il bug nel suo codice avrebbe permesso a un eventuale pirata di portare l'attacco nel momento in cui si fosse trovato connesso alla stessa rete Wi-Fi.

All’origine del problema, secondo i ricercatori, c’è il fatto che l’applicazione è stata usata sfruttando troppi **SDK (Software Development Kit)** di terze parti che hanno portato, in buon sostanza, a un conflitto che ha messo a rischio gli utenti Xiaomi. In gergo questo fenomeno viene definito **SDK Fatigue**.

L’uso di questi kit di sviluppo, che per gli sviluppatori rappresentano una pratica scorciatoia per inserire funzionalità senza dover scrivere troppo codice, ha infatti un rovescio della medaglia: utilizzando porzioni di codice che non sono state scritte per lavorare insieme, si rischia il patatrac.

In questo caso è andata tutto sommato bene, visto che in seguito alla segnalazione di Check Point il produttore ha potuto sviluppare e distribuire tempestivamente la patch che corregge la falla di sicurezza e non sono stati registrati tentativi di attacco che sfruttassero il bug. La prossima volta, però, potrebbe finire peggio.

Please follow and like us:

Facebook: 540 milioni di profili “dimenticati” su un server aperto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/05/autogol-di-xiaomi-il-software-di-sicurezza-ha-una-falla-di-sicurezza/

Facebook: 540 milioni di profili “dimenticati” su un server aperto

Apr 04, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Scenario 1

Il fattaccio è responsabilità degli amministratori di app di terze parti, che hanno lasciato i dati su bucket Amazon S3 privi di sistemi di autenticazione.

Si allunga l’elenco di esposizioni di dati personali dovuti a dimenticanze (sarebbe meglio chiamarla sciatteria) di amministratori di sistema che **lasciano informazioni sensibili su server che possono essere visitati da chiunque**.

Questa volta la vittima (indiretta) è una delle più celebri: **Facebook**. Gli utenti coinvolti sono **540 milioni** e i loro dati (username, password, interessi, relazioni e molto altro) sono rimasti per chissà quanto tempo accessibili a chiunque sui server utilizzati da due app attive sul social network.

La prima si chiama At the Pool e contiene “solo” 22.000 record, tra cui gli account e **le password memorizzate in chiaro**. Secondo i ricercatori che hanno individuato il database non si tratterebbe presumibilmente delle password di Facebook, ma di quelle relative all’app.

Magra consolazione, visto che molti (troppi) utenti tendono a utilizzare la stessa password del loro account anche per le app a cui si iscrivono sul social network.

Il vero “pesce grosso” individuato dai ricercatori del **Cyber Risk team di UpGuard** è però **Cultura Colectiva**, una società con sede in Messico che raccoglie tramite la sua app Facebook informazioni sugli interessi di almeno **540 milioni di utenti Facebook**.

Le informazioni (146 GB) erano conservate su un Bucket S3 di Amazon configurato in modo da permettere il download dei dati senza che fosse necessario fornire alcuna credenziale di accesso. Come spiegano i ricercatori di sicurezza nel loro report, il database **cc-datalake** conteneva informazioni su like e commenti, ma anche gli account, l’identificativo utente e altre informazioni personali.

L’elemento più preoccupante di tutta la vicenda, però, è come si è svolta. UpGuard spiega di aver individuato e segnalato a Cultura Colectiva il database “aperto” lo scorso **10 gennaio**, senza ricevere risposta. Una seconda email sarebbe stata inviata il **14 gennaio**, con lo stesso esito.

A questo punto i ricercatori hanno deciso di contattare direttamente **Amazon Web Services**. All’email inviata il 28

gennaio arriva tempestiva risposta (1 febbraio) in cui l'azienda annuncia di aver iniziato a cercare di gestire la situazione in un altro modo.

La svolta arriva solo il 3 aprile, quando Bloomberg contatta Facebook per chiedere spiegazioni e Cultura Colectiva, probabilmente "pressata" dal gigante dei social, si decide a proteggere il database in maniera appropriata.

Insomma, senza voler mettere in dubbio la buona volontà di Zuckerberg e soci nel tutelare la privacy degli iscritti a Facebook, siamo di fronte all'ennesima dimostrazione del fatto che la protezione dei dati personali rimane estremamente problematica.

Soprattutto in un ecosistema in cui operano centinaia di attori diversi e introdurre strumenti di controllo diventa estremamente problematico. Insomma: l'appello di Zuckerberg lanciato in una lettera aperta pubblicata sul **Washington Post** rimane attualissimo e impone ai governi di affrontare la questione.

Please follow and like us:

Microsoft mette al bando le password "deboli"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/04/facebook-540-milioni-di-profili-dimenticati-su-un-server-aperto/

Microsoft mette al bando le password “deboli”

Apr 03, 2019 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Scenario, Tecnologia 0

Con Azure AD Password Protection gli amministratori possono impedire agli utenti di impostare le password di uso comune. L’elenco è aggiornato automaticamente.

La mossa decisiva per contrastare l’uso di password comuni e facilmente individuabili? Questa volta potrebbe averla azzeccata **Microsoft**.

L’azienda di **Satya Nadella** ha infatti annunciato la disponibilità di **Azure AD Password Protection**, un sistema che permette agli amministratori di rete di limitare la scelta delle password.

L’idea è quella di arginare il fenomeno del **password spraying**, cioè la tecnica che i pirati usano per eseguire attacchi di brute forcing contro gli account aziendali utilizzando database con le password più comuni.

Il password spraying funziona come un brute forcing al contrario: al posto di provare tutte le possibili password su un singolo account, i cyber-criminali tentano l’accesso con la stessa password su tutti gli account che individuano.

Questa modalità di attacco (ne abbiamo parlato in questo articolo) “distribuisce” i tentativi di accesso ed è molto difficile da individuare rispetto a un attacco portato con le

modalità classiche. **Gli accessi falliti, infatti, non hanno una frequenza tale da allertare i sistemi di controllo**.

I pirati, di solito, per portare questi attacchi usano i database disponibili sul Web che contengono gli elenchi di password sottratte ai servizi online, come il mastodontico **Collection#1**, individuato lo scorso gennaio su Internet.

Azure AD Password Protection utilizza in pratica la stessa fonte per creare una black list di password che gli utenti non possono utilizzare all'interno della rete. Quando un utente prova a impostare una password considerata debole, viene visualizzato un messaggio che gli chiede di utilizzarne un'altra.

Come viene spiegato nella documentazione relativa (purtroppo il sito traduce automaticamente i contenuti con risultati drammatici, consigliamo la versione in inglese) la black list viene generata partendo dalle 500 password di uso più comune e le possibili varianti. **Nel complesso, si arriva a un milione di password "bandite" dai sistemi**.

Il database, poi, viene aggiornato automaticamente da

Microsoft attraverso le risorse reperite attraverso i sistemi di intelligence che eseguono un costante monitoraggio delle password rubate in circolazione.

Rispetto alle solite policy, che controllano solo lunghezza della password e presenza di maiuscole/minuscole, caratteri speciali e numeri, con Azure AD Password Protection si passa certamente a un altro livello. Quanto sarà efficace, però, lo scopriremo solo nel prossimo futuro.

Please follow and like us:

Il backup si sposta verso il cloud

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/03/microsoft-mette-al-bando-le-password-deboli/