Si moltiplicano le truffe su Aribnb. L'azienda: "nuove regole"

Nov 11, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

I truffatori approfittano di alcune lacune nel regolamento per frodare gli utenti dirottandoli su appartamenti diversi da quelli prenotati. Ecco come funziona.

Da anni rappresenta uno strumento formidabile per affittare un appartamento online spendendo relativamente poco. **Airbnb**, però, è diventata recentemente terreno di caccia per abili truffatori che sfruttano alcune lacune del sistema di affitto online.

Le truffe, come viene spiegato in un lungo articolo pubblicato su **Vice**, seguono uno schema piuttosto ingegnoso. Tutto comincia con la pubblicazione su Airbnb di un annuncio per un appartamento apparentemente splendido, collocato in una posizione ideale per visitare la città e disponibile a un prezzo decisamente attraente.

C'è un solo difetto: l'appartamento non esiste. Anzi: lo stesso appartamento (o per lo meno la sua descrizione e le fotografie, magari con qualche variante apportata con Photoshop) spesso appare essere disponibile in più città. Insomma: si tratta chiaramente di truffe.

Difficile, però, che i visitatori del sito possano accorgersene. Di solito, infatti, le ricerche vengono fatte usando come parola chiave la città che si vuole usare e, se

l’appartamento risulta essere messo a disposizione da host diversi, anche altri tipi di ricerche sono inutili per individuare la presenza del “clone”.

Tanto più che l’uso di immagini diverse impedisce anche ai sistemi di intelligenza artificiale di rilevare qualcosa di strano negli annunci.

Teoricamente, mettere in affitto su Aribnb un appartamento che non esiste è un trucco che non può funzionare. In casi del genere, infatti, la piattaforma prevede il rimborso totale di quanto pagato dall’utente e la cacciata dell’host. Le cose cambiano, però, se ospite e host si accordano per l’affitto di un appartamento diverso. **Qui le cose si fanno più sfumate e i truffatori hanno trovato il modo di approfittarsene**.

La tecnica è quella di contattare l’ospite quando è già arrivato in città, **pochi minuti prima dell’orario previsto per il check in**, per comunicare che l’appartamento prenotato non è disponibile. Di solito i truffatori accampano scuse come guasti o allagamenti, scusandosi e proponendo di fornire un altro alloggio.

La vittima si trova in una situazione decisamente scomoda:

meglio rinunciare all’appartamento per avere un rimborso pieno e andare in contro all’esborso per soggiornare in un hotel (**spendendo magari il doppio o il triplo di quanto preventivato**) o fidarsi dell’host e accettare la nuova sistemazione?

Molti scelgono la seconda opzione, finendo così in trappola. **Il nuovo appartamento, manco a dirlo, di solito una stamberga collocata in una zona della città che non ha niente a che fare con quella promessa**.

Teoricamente un cambiamento del genere potrebbe essere gestito attraverso la funzione di modifica della prenotazione, che permette anche di prevedere un rimborso. **Contrattare la modifica in una situazione del genere, però, non è facile ed è ovvio che in questo caso l’host ha il coltello dalla parte del manico**.

Ma c’è di peggio: in qualche caso la nuova sistemazione è solo temporanea e l’ospite è costretto a lasciare il nuovo appartamento il giorno dopo. È quello che è successo all’autore dell’articolo che abbiamo citato, che spiega anche la ragione per cui i truffatori agiscono in questo modo.

Se l’ospite passa almeno una notte in un alloggio dell’host, il rimborso previsto da Airbnb è solo parziale. Nel caso citato da **Allie Conti**, autrice dell’articolo di Vice, il rimborso ha coperto solo 399 dollari degli oltre 1.200 che aveva pagato per la prenotazione.

Ora Airbnb sembra aver deciso di prendere provvedimenti attraverso un sistema di “garanzia” che permetterebbe di accedere a un alloggio dello stesso livello tra quelli proposti dalla piattaforma nella stessa città e, se questo non fosse possibile, **rimborsare al 100% la spesa anche soltanto se l’annuncio in questione non “incontra gli standard di accuratezza” di Airbnb**.

La piattaforma ha anche annunciato di voler avviare un’operazione di verifica di tutti gli annunci e gli host entro dicembre 2020. **Un obiettivo decisamente ambizioso: sul sito ci sono circa 6 milioni di annunci e 650.000 host registrati**.

Condividi l’articolo

Errore negli SDK di Adobe. Le app non usano connessioni protette

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/11/si-moltiplicano-le-truffe-su-aribnb-lazienda-nuove-regole/

Errore negli SDK di Adobe. Le app non usano connessioni protette

Nov 08, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

I file di esempio usati nei kit di sviluppo usano una configurazione che lascia aperta la strada all'intercettazione dei dati trasmessi al cloud.

Per una volta i problemi di sicurezza di **Adobe** non riguardano **Flash** o **Acrobat Reader**. Malgrado le apparenze, però, la notizia non è affatto classificabile come "buona". **Questa volta, infatti, i problemi riguardano un numero potenzialmente elevatissimo di applicazioni**.

Ad avere qualche problema, infatti, non è un software specifico, ma il kit di sviluppo (**SDK**) messo a disposizione da Adobe per i programmatori che vogliono creare applicazioni mobile in grado di dialogare con i suoi servizi cloud.

Come si legge nel report pubblicato dalla società di sicurezza **Nightwatch Cybersecurity**, a creare apprensione è un file chiamato **ADBMobileConfig.json**, fornito nel pacchetto di

sviluppo. Il file, infatti, prevede una serie di configurazioni predefinite che vengono “riversate” nelle app.

Nel dettaglio, le impostazioni non prevedono l’utilizzo di una connessione protetta tramite SSL per alcuni tipi di informazioni, che di conseguenza potrebbero essere intercettate da chiunque potesse accedere al traccio Internet del dispositivo.

Si tratta principalmente dei dati di analisi del funzionamento, ma anche di informazioni che l’app invia eventualmente a terze parti. Insomma: informazioni potenzialmente sensibili, con maggiore o minore importanza a seconda del tipo di app di cui si parla.

Naturalmente gli sviluppatori potrebbero verificare le impostazioni in fase di programmazione e modificarle per fornire una connessione sicura, ma nella pratica questo avviene ben di rado. **Anche perché i manuali d’uso e i tutorial in circolazione suggeriscono di utilizzare il file fornito da Adobe**.

In seguito alla segnalazione, Adobe ha corretto le impostazioni del file, che è stato inserito nella nuova versione del **Adobe Experience Platform mobile SDK**.

Gli sviluppatori che volessero verificare l’appropriatezza delle impostazioni nelle loro app possono utilizzare uno strumento di analisi messo a punto da Nightwatch Cybersecurity

e disponibile per il download all’indirizzo https://github.com/nightwatchcybersecurity/truegaze.

Condividi l’articolo

DarkUniverse: il gruppo di cyber-spioni che conosceva solo l’NSA

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/08/errore-negli-sdk-di-adobe-le-app-non-usano-connessioni-protette/

DarkUniverse: il gruppo di cyber-spioni che conosceva solo l’NSA

Nov 07, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Leaks, Malware, News, RSS 0

Il gruppo ATP ha agito nell’ombra per anni e ha cessato la sua attività dopo che è stato scoperto grazie al leak degli… Shadow Brokers!

È stato battezzato **DarkUniverse** ed è un gruppo ATP (Advanced

Persistent Threat) che, probabilmente, opera da anni per conto di un qualche governo. La sua esistenza è stata svelata da **Kaspersky**, i cui ricercatori ritengono che Dark Universe sia attivo almeno dal 2009.

La parte più interessante di tutta la vicenda, però, riguarda il modo in cui gli esperti di sicurezza hanno individuato il gruppo di cyber-spioni.

Tutto comincia nel 2017, quando il misterioso gruppo hacker degli **Shadow Brokers** (che i nostri lettori più affezionati ricorderanno bene) rilascia su Internet un pacchetto di dati presumibilmente sottratto alla **National Security Agency**.

In quel database, gli esperti trovano decine di strumenti di hacking utilizzati dagli 007 americani, tra cui **EternalBlue**, l'exploit che in seguito è stato utilizzato per diffondere il ransomware **WannaCry**.

Nel pacchetto di strumenti pubblicato dagli Shadow Brokers, però, c'è anche un file chiamato **sigs.py**, uno script progettato per individuare l'eventuale presenza di altri malware APT su un computer. **L'ipotesi è che gli agenti segreti USA lo utilizzassero per individuare eventuali infiltrazioni di servizi "concorrenti" sulla macchina che stavano per compromettere**.

Analizzando lo script, dalle parti di Kaspersky si sono resi conto che l'NSA, sotto questo punto di vista, era molto più avanti di tutte le società di sicurezza private. **Lo strumento, infatti, consentiva di individuare una serie di tool di spionaggio ancora sconosciuti nel settore**.

Uno di questi APT, però, ha attirato in particolare l'attenzione dei ricercatori. Quando hanno approfondito lo studio, hanno individuato almeno 20 vittime colpite dal trojan. **Si tratta di enti pubblici (anche in campo militare) e organizzazioni private con sede in Siria, Iran, Afghanistan, Tanzania, Etiopia, Sudan, Russia, Bielorussia ed Emirati Arabi Uniti**.

DarkUniverse (il nome è stato scelto dagli analisti Kaspersky) è una vera piattaforma di spionaggio che consente di controllare a distanza il computer infetto attraverso un server Command and Control grazie al quale i pirati possono fare più o meno quello che vogliono.

Da un punto di vista tecnico, DarkUniverse integra un numero impressionante di funzioni e adotta "alcune finezze" come la

possibilità di spezzettare i file in blocchi da 400 KB per offuscare le operazioni di esflitrazione.

Ma chi ha realizzato e diffuso il malware? I ricercatori non si sbilanciano, ma nel loro report notano che alcune parti di codice sono identiche a quelle di **ItaDuke**, un trojan utilizzato dal governo cinese per spiare cittadini appartenenti alla minoranza mussulmana Uiguri e in Tibet.

Condividi l’articolo

Italia quarta al mondo per attacchi basati su Macro

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/07/darkuniverse-il-gruppo-di-cyber-spioni-che-conosceva-solo-lnsa/

Italia quarta al mondo per attacchi basati su Macro

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

I dati arrivano da Trend Micro. Nel nostro paese si verificano più del 7% degli attacchi che usano Macro Malware. E il numero cresce…

È una forzatura, ma possiamo dire che i **Macro Malware** sono i dinosauri del mondo della sicurezza informatica. Gli attacchi attraverso le istruzioni Macro (utilizzate dai documenti di testo e dai fogli di calcolo per automatizzare le operazioni) sono infatti tra i primi utilizzati dai cyber-criminali fin dagli anni ’90.

Dinosauri, però, che si stanno dimostrando estremamente resistenti. Ancora oggi, infatti, gli attacchi che sfruttano le Macro sono decisamente numerosi. In Italia, però, sembra che si tratti di una vera e propria emergenza.

A segnalarlo è **Trend Micro**, il cui sistema di rilevamento **Smart Protection Network** ha rilevato nel mese di settembre un numero di attacchi con Macro Malware tale da posizionare il nostro paese al quarto posto nel mondo dopo Giappone, Cina e Stati Uniti.

La società di sicurezza ha rilevato in Italia la bellezza di 1.812 attacchi, equivalenti al 7,7% di quelli individuati a livello globale nel corso del mese. Un dato, tra l’altro, che segna un netto aumento rispetto al mese precedente, quando l’Italia aveva “calamitato” solo il 3,8% di questo tipo di malware.

Quali sono le cause del successo (sigh!) dei Macro Malware? La prima è legata a una scarsa cultura della sicurezza. **Da anni, infatti, l'attivazione delle funzionalità Macro richiede una conferma da parte dell'utente**. Un accorgimento introdotto dagli sviluppatori software che, in teoria, dovrebbe mettere al riparo da attacchi di questo genere.

Evidentemente, però, sono ancora troppo poche le persone che capiscono quale sia il rischio collegato all'attivazione di questa funzionalità.

La seconda causa, che riguarda invece i casi in cui i pirati informatici trovano il modo di aggirare il sistema di controllo sfruttando delle vulnerabilità, è da individuare probabilmente nella pessima abitudine di non aggiornare regolarmente i software.

Le falle di sicurezza relative alle funzionalità Macro vengono infatti segnalate con grande tempestività e, normalmente, corrette attraverso patch di sicurezza. Se gli utenti non aggiornano i loro programmi, però, i software rimangono vulnerabili agli attacchi (abbastanza sporadici, per la verità) che permettono di attivare le Macro automaticamente. Insomma: il problema non è tecnico. È squisitamente legato al fattore umano.

Condividi l’articolo

WP-VCD: ecco come i pirati fanno strage di siti WordPress

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/06/italia-quarta-al-mondo-per-attacchi-basati-su-macro/

WP-VCD: ecco come i pirati fanno strage di siti WordPress

Nov 05, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 1

Gli attacchi vanno avanti da almeno due anni e sfruttano plugin e temi “taroccati” al cui interno si nasconde il codice malevolo.

Una gang di pirati informatici sta infettando migliaia di siti Internet basati su WordPress per utilizzarli come trampolino di lancio per distribuire pubblicità indesiderate e pop-up che conducono a pagine contenenti malware.

Si chiamano **WP-VCD** e sono stati individuati dagli esperti di sicurezza di **WordFence**. Come riportano in un articolo i colleghi di **ZDNet**, che hanno ricevuto in esclusiva il report, il gruppo di cyber-criminali è attivo almeno dal febbraio 2017 e ha infettato un numero impressionante di siti Web.

Piuttosto che utilizzare vulnerabilità del popolare **Content Management System (CMS)**, WP-VCD usa come vettore di attacco temi e plugin piratati che distribuisce attraverso una serie di siti Internet specializzati.

www.download-freethemes.download
www.downloadfreethemes.co
www.downloadfreethemes.space
www.downloadnulled.pw
www.downloadnulled.top
www.freenulled.top
www.nulledzip.download
www.themesfreedownload.net
www.themesfreedownload.top
www.vestathemes.com

I siti in questione, spiegano i ricercatori, possono contare su un SEO strepitoso e di conseguenza compaiono in cima alla lista dei risultati sui motori di ricerca quando vengono usate parole chiave relative a temi piratati (nulled) per WordPress.

A dare una mano ai pirati informatici è anche il sistema usato da Google per classificare i risultati delle ricerche. Com'è noto, infatti, l'algoritmo di **Google** considera principalmente i collegamenti esterni e WP-VCD ha quindi gioco facile a "pompare" il SEO di questi siti, semplicemente inserendo i collegamenti nei siti Internet che compromettono.

Insomma: una sorta di circolo vizioso (o di loop) che gli consente di rendere sempre più efficaci i loro strumenti di attacco man mano che mietono nuove vittime.

Il malware che i pirati informatici utilizzano per prendere il controllo dei siti su cui vengono installati i temi infetti è decisamente "rognoso". Come prima cosa crea una backdoor creando un utente (100010010) con privilegi di amministratore.

In secondo luogo, inserisce una copia di sé stesso in tutti i temi caricati sul CMS. La logica è cristallina: nel caso in cui il legittimo amministratore del sito decida di cambiare tema (magari perché ha soltanto provato quello scaricato) il malware rimarrà attivo.

Condividi l'articolo

Italia quarta al mondo per attacchi basati su Macro Microsoft lavora per rendere più sicuro il suo ecosistema

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/11/05/wp-vcd-ecco-come-i-pirati-fanno-strage-di-siti-wordpress/

Microsoft lavora per rendere più sicuro il suo ecosistema

Nov 04, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario 0

Raffica di novità per gli utenti di Office 365. L'azienda di Redmond introduce una serie di strumenti e procedure per bloccare malware e attacchi sulla sua piattaforma.

Una vera mitragliata di annunci in tema sicurezza da parte di Microsoft, che sembra abbia deciso di prendere di petto il problema degli attacchi malware che sfruttano i formati Office puntando, inoltre, a introdurre strumenti per il rilevamento e la remediation sui suoi sistemi cloud.

Il primo riguarda **Application Guard**, una nuova funzionalità che utilizza una sandbox per limitare l'impatto di eventuale codice malevolo in modo che non possa interagire con Windows. Lo strumento, introdotto in **Edge** per Windows 10, starebbe ora per arrivare anche su **Office 365 ProPlus**.

Microsoft Office Application Guard permetterà di aprire i documenti in un container virtualizzato che mantiene il file completamente separato dall'ambiente Windows, offrendo così un livello di protezione estremamente elevato da malware ed

eventuali script nocivi contenuti nei documenti stessi.

Nel caso in cui l'utente decida di considerare il documento attendibile, questo verrà in ogni caso analizzato attraverso una scansione su cloud con **Microsoft Defender Advanced Threat Protection**.

Novità anche per **Office 365 Advanced Threat Protection**. Il servizio di Microsoft dedicato alle aziende si arricchisce di un sistema che consente di inviare segnalazioni automatiche ai responsabili di sicurezza sulla base dell'analisi dei processi rilevati all'interno dell'ecosistema Office (come l'invio di mail) con lo scopo di individuare con la massima tempestività eventuali violazioni dei sistemi di sicurezza.

Si tratta di una funzionalità attualmente in Public Preview e che Microsoft definisce come un sistema di **detection and response** automatizzato, che consentirebbe di avere immediatamente a disposizioni le informazioni sull'account compromesso, sulle azioni compiute in seguito alla violazione e quelle attuate in fase di response dal team di sicurezza.

Contemporaneamente, l'azienda di **Satya Nadella** sta introducendo una funzionalità dedicata alla "educazione" degli utenti all'interno di **Microsoft 365**. In questo caso la logica

è quella di inviare delle “raccomandazioni” agli utenti per sensibilizzarli a un uso sicuro dei sistemi.

Non solo: l’azienda di Redmond ha introdotto questo mese in Microsoft 365 la bellezza di 16 nuovi “ruoli” **Azure Active Directory** con bassi privilegi. Una modifica che punta a ridurre il numero di utenti con poteri di amministrazione e mitigare così il rischio in caso di compromissione degli account.

Infine, per gli utenti Microsoft 365 sarà disponibile un nuovo strumento chiamato **Insider Risk Management** (per il momento in Private Preview) che punta a individuare gli elementi di rischio legati all’accesso non autorizzato a dati e documenti all’interno dell’azienda.

Il sistema, pensato per mitigare il rischio di condivisioni “sbagliate” nei sistemi cloud, si basa su un sistema di “etichettatura” delle risorse che consente per esempio di **prevenire la condivisione di materiali riservati**.

Insomma: un vero giro di vite in ambito produttività e cloud che si spera, dovrebbe aumentare il livello di sicurezza nelle aziende che usano l’ecosistema Microsoft.

Condividi l’articolo

All’asta sul Dark Web 21 milioni di credenziali di aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/04/microsoft-lavora-per-rendere-piu-sicuro-il-suo-ecosistema/

All’asta sul Dark Web 21 milioni di credenziali di aziende

Ott 31, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, Phishing, Privacy, RSS, Scenario 0

Username e password fanno riferimento a società comprese nel Fortune 500. Coinvolti istituti di credito, aziende Tech e del settore sanitario.

Sono sparse su vari siti e forum nel **Dark Web** e tutte insieme raggiungono l’impressionante numero di **21.040.296 credenziali** (username e password) disponibili per qualsiasi cyber-criminale che sia disposto a spendere qualche dollaro.

Come si legge nel report pubblicato da **ImmuniWeb**, la statistica è stata stilata considerando solo (sigh!) le aziende comprese nella lista **Fortune 500**, che raccoglie le maggiori società statunitensi per fatturato.

Si tratta di informazioni raccolte in vari breach e attacchi informatici, alcune direttamente in chiaro, altre già cracckate. **E non si tratta di dati "vecchi": il report specifica infatti che più di 16 milioni di credenziali sui 21 milioni complessivi sono state sottratte negli ultimi 12 mesi**.

L'analisi dei settori interessati evidenzia come quelli più colpiti siano il settore tecnologico, quello finanziario, energetico, industriale e sanitario.

Le note dolenti, oltre che dall'ovvia considerazione che tutte le credenziali in questione erano evidentemente protette in maniera inadeguata, arrivano dall'analisi delle password utilizzate.

Dopo anni in cui tutti gli esperti di sicurezza hanno

predicato per diffondere quel minimo di consapevolezza che dovrebbe portare all'uso di password "robuste", ci troviamo ancora ad avere a che fare con password ridicolmente facili da violare.

Le più utilizzate sono la classica "password" (con astute varianti come "passw0rd") accompagnata da "123456"; "000000"; "opensesame" ("apriti sesamo" – ndr) e altre schifezze del genere. **Sotto il profilo statistico, i ricercatori sottolineano come il database complessivo contenga solo 4,9 milioni di password uniche**.

Non solo: il 42% delle password hanno un qualche collegamento con il nome dell'azienda, rendendo così gli attacchi di brute forcing estremamente semplici.

La principale fonte di approvvigionamento dei pirati informatici sembra essere il phishing. Secondo quanto viene riportato nello studio, infatti, il numero di credenziali sottratte è direttamente proporzionale al numero di pagine di

phishing individuate sul Web.

Condividi l’articolo

Facebook denuncia NSO Group per gli attacchi agli utenti Whatsapp

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/31/allasta-sul-dark-web-21-milioni-di-credenziali-di-aziende/

Facebook denuncia NSO Group per gli attacchi agli utenti Whatsapp

Ott 30, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, Privacy, RSS, Scenario 0

L’azienda di Zuckerberg porta NSO Group in tribunale. Avrebbero usato lo zero-day di Whatsapp per colpire 1.400 utenti con il loro spyware Pegasus.

Quando lo scorso maggio è comparsa una grave vulnerabilità zero-day di **Whatsapp**, il nome di **NSO Group** ha cominciato

immediatamente a rimbalzare sui siti specializzati. Il sospetto, infatti, era che gli attacchi registrati da Whatsapp fossero opera di uno dei tanti “clienti” della società israeliana.

Ora il sospetto è diventato qualcosa di più concreto e **Facebook**, proprietaria di Whatsapp, ha deciso di **presentare una denuncia nei confronti di NSO Group** per la violazione di leggi degli Stati Uniti e della California.

NSO Group, di cui abbiamo parlato spesso su queste pagine, è un’azienda specializzata in sistemi informatici di sorveglianza (software di spionaggio) che vende a forze di polizia e servizi segreti di tutto il mondo.

L’azienda con sede a **Herzliya** è da tempo al centro di polemiche. Come riportato in più occasioni da associazioni per la difesa dei diritti umani come la canadese **Citizen Lab**, NSO Group è sospettata di fornire i suoi software spia anche a regimi dittatoriali e a governi che utilizzerebbero i suoi software per spiare giornalisti, avvocati dei diritti civili, dissidenti politici e attivisti.

Il suo best-seller è **Pegasus**, un trojan per Android e iOS in grado di tracciare i dispositivi tramite GPS, intercettare il traffico telefonico come quello Internet o utilizzare il microfono per spiare a distanza il possessore del telefono.

Stando a quanto riportano in un report gli attivisti di Citizen Lab, gli attacchi dello scorso maggio agli utenti di Whatsapp avrebbe avuto proprio lo scopo di installare il trojan di NSO Group sugli smartphone di **centinaia di esponenti della società civile** finiti nel mirino di uno dei tanti clienti "impresentabili" dell'azienda.

Come si legge nella denuncia inoltrata da Facebook, le vittime degli attacchi (in tutto 1.400) sono cittadini del Bahrein, dell'Arabia Saudita e del Messico.

La vulnerabilità utilizzata per colpire i dispositivi era terribilmente efficace: consentiva infatti di installare in remoto il trojan semplicemente avviando una videochiamata Whatsapp. **Per avviare l'esecuzione di codice non era nemmeno necessario che la vittima rispondesse alla chiamata**.

Il cuore della denuncia riguarda la violazione di una serie di normative (prima tra tutte il **Computer Fraud and Abuse Act**) e delle condizioni di utilizzo di Whatsapp.

La battaglia legale, come già accaduto in passato, si combatterà sul livello di responsabilità di NSO Group, che invariabilmente sostiene di non essere responsabile per eventuali utilizzi "inappropriati" dei suoi strumenti di spionaggio. **Questa volta, però, l'azienda israeliana non si trova di fronte la solita associazione per i diritti civili, ma uno dei giganti del Web.**

Non solo: a collegare l'azienda israeliana agli attacchi sarebbero alcuni elementi che smentiscono la "neutralità" che NSO Group sbandiera invariabilmente. Prima di tutto i tecnici di Whatsapp avrebbero individuato alcuni server utilizzati per portare gli attacchi, che risulterebbero essere stati usati in passato da NSO Group. **In secondo luogo, gli stessi account Whatsapp utilizzati per colpire le vittime sarebbero collegati direttamente all'azienda israeliana**.

Insomma: le solite tesi difensive di NSO Group in questo caso rischiano di essere ben poco efficaci e l'intera vicenda promette di riservare non poche sorprese.

Condividi l'articolo

Si spacciano per Fancy Bear per ricattare le aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/30/facebook-denuncia-nso-group-per-gli-attacchi-agli-utenti-whatsapp/

Si spacciano per Fancy Bear per ricattare le aziende

Ott 29, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, Scenario 0

I pirati informatici hanno cercato di impersonare il celebre gruppo APT per intimorire le vittime. Ma i casi di "false flag" si moltiplicano.

Anche nel mondo del cyber-crimine ci sono delle gerarchie dettate dalla celebrità e qualcuno ha pensato bene di approfittarne prendendo "in prestito" il nome di uno dei più famigerati gruppi di hacker russi per intimidire le loro vittime.

Come riporta Threatpost, il caso riguarda una gang di pirati informatici che ha cominciato sistematicamente a spacciarsi per **Fancy Bear**, il gruppo APT (Advanced Persistent Threat) collegato ai servizi segreti russi e autore, tra le altre cose, di attacchi al Partito Democratico USA e al governo tedesco.

Il gruppo, nel dettaglio, avrebbe cercato di estorcere denaro a numerose istituzioni finanziarie lanciando degli **attacchi DDoS** accompagnati da richieste di riscatto (2 Bitcoin) dirette alle vittime. Per rendere l'estorsione più efficace, si firmavano con il nome del celebre gruppo APT.

La tecnica di attacco adottata, spiegano gli esperti, era molto specifica e decisamente efficace. Al posto di colpire i siti Internet, che normalmente hanno sistemi di protezione

contro gli attacchi di **Distributed Denial of Service**, puntavano direttamente ai server del back-end, più vulnerabili a questo tipo di attacchi.

L’idea di utilizzare il nome di un gruppo conosciuto (e temuto) come Fancy Bear era probabilmente quella di gettare nel panico le vittime per fargli credere di avere a che fare con un avversario formidabile e indurli a cedere al ricatto senza troppe storie.

Negli ultimi tempi i casi in cui gruppi di pirati informatici hanno messo in campo stratagemmi simili si stanno moltiplicando, anche se normalmente lo scopo è diverso e sfrutta delle “false flag” per depistare le indagini degli esperti di sicurezza.

L’ultimo caso, emerso grazie a un report del **National Cyber Security Centre** britannico, riguarda il gruppo **Turla**. La gang di cyber-criminali russi (che al pari di Fancy Bear vengono considerati “vicini” ai servizi segreti russi) avrebbe infatti utilizzato degli strumenti di attacco normalmente usati da un gruppo iraniano per colpire una serie di bersagli in

Medioriente.

Per farlo, hanno “dirottato” i sistemi usati da **APT34** (conosciuto anche come **Oilrig**) prendendo il controllo del server Command and Control.

Nel 2018 era emerso invece un caso di “false flag” estremamente raffinato. Il caso era quello dell’attacco che ha preso di mira la cerimonia di inaugurazione delle olimpiadi invernali in Corea del Sud. Gli autori di **Olympic Destroyer**, infatti avevano inserito nel codice del malware alcune porzioni di codice utilizzate normalmente dal gruppo **Lazarus**, collegato alla Corea del Nord.

Le indagini successive, però, hanno portato gli esperti di sicurezza a rivedere l’attribuzione, puntando il dito verso un non meglio identificato gruppo di pirati informatici russi.

Condividi l’articolo

Violazione dei sistemi di UniCredit: rubati i dati di 3 milioni di clienti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/29/si-spacciano-per-fancy-bear-per-ricattare-le-aziende/

Violazione dei sistemi di UniCredit: rubati i dati di 3 milioni di clienti

Ott 28, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, News, RSS 0

L'annuncio dello stesso istituto bancario. Il database risalirebbe al 2015 e conterrebbe informazioni personali di clienti italiani di UniCredit.

Un "leak" di proporzioni notevoli, che avrebbe coinvolto 3 milioni di titolari di conto corrente (tutti italiani) di **UniCredit**. La notizia è stata diffusa con una nota dalla stessa banca, che ha contestualmente informato le autorità e le forze di polizia.

Il comunicato, piuttosto stringato e privo di dettagli, parla di un "incidente" che avrebbe coinvolto "un file generato nel 2015" contenente informazioni sensibili (**nome, città di residenza, numero di telefono e indirizzo di posta elettronica**) dei clienti dell'istituto di credito.

La buona notizia è che nel leak non sarebbero coinvolte le password dei servizi di home banking e, di conseguenza, UniCredit esclude che ci possano essere state ripercussioni dirette sui conti delle persone coinvolte.

Resta da capire come si siano svolti esattamente i fatti, a partire dalla data esatta in cui i pirati informatici sarebbero riusciti a mettere le mani sui dati. L'ipotesi più probabile, visto che il comunicato stampa si intitola "UniCredit 2015 data incident" è che la violazione sia avvenuta proprio 4 anni fa.

Una versione che coinciderebbe con alcune informazioni riportate da organi di stampa (ma la fonte è indicata come “fonti investigative qualificate”) secondo le quali la scoperta sarebbe avvenuta con l’individuazione del database sul Dark Web. **Questo significherebbe che i dati sono circolati nei bassifondi di Internet per 4 anni**.

Se è vero che le informazioni trafugate non sono sufficienti per colpire direttamente ai conti bancari degli utenti (UniCredit da tempo utilizza sistemi di autenticazione a due fattori per il suo sistema di Home Banking) rimane la possibilità che i dati siano stati usati o possano essere usati per portare **attacchi di phishing o truffe più elaborate attraverso chiamate telefoniche o invio di SMS** alle vittime del leak.

Qualcosa di simile era avvenuto già nel 2017, quando l’istituto di credito aveva subito il furto dei dati relativi a 400.000 clienti. In quell’occasione, però, UniCredit aveva subito chiarito che il leak era avvenuto a causa della compromissione dei sistemi di un soggetto terzo.

Unicredit ha annunciato che sta contattando, tramite posta tradizionale e notifiche tramite il suo servizio di Online Banking, tutte le persone potenzialmente interessate. I correntisti possono in ogni caso avere maggiori informazioni attraverso il servizio clienti di UniCredit o chiamando il numero verde **800 323285**.

Condividi l’articolo

Si spacciano per Fancy Bear per ricattare le aziende Trojan per iOS nascosto in 17 app disponibili sull’App Store

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/28/violazione-dei-sistemi-di-unicredit-rubati-i-dati-di-3-milioni-di-clienti/