Cyber attacco all'Australia, Morrison: "Dietro c'è un Paese straniero"

Pubblica Amministrazione, industria, principali imprese e organizzazioni politiche, istruzione, sanità ed energia, sono diversi e molteplici i settori strategici dell'**Australia sotto attacco informatico**. Il Governo di Canberra ha informato ieri i suoi cittadini e il mondo che dietro ci potrebbe essere un "*attore statale*" straniero.

"*Sappiamo che si tratta di un sofisticato attore statale a causa delle dimensioni e della natura degli obiettivi e della tecnica utilizzato. Purtroppo, questa attività non è nuova. La frequenza è in aumento*", ha dichiarato il Primo ministro australiano, **Scott Morrison**, secondo quanto riportato dall'Agi stamattina.

Australia sotto attacco

Ciò che preoccupa l'esecutivo australiano è che nel mirino degli attacchi ci sono le infrastrutture critiche e i fornitori di servizi essenziali.

Morrison ha poi denunciato pubblicamente che tra i possibili attori statali stranieri, sospettati di aver partecipato all'attacco, non possono che esserci **Cina, Russia o Iran**: "*Non ci sono troppi attori statali al mondo che hanno le capacità necessarie per compiere attacchi del genere*".

I sospetti su quale sia questo "*state-based cyber actor*" si stanno rapidamente indirizzando verso la Cina, più che gli

altri due Paesi menzionati.

Peter Jennings, direttore dell'Australian Strategic Policy Institute (ASPI), ha detto alla CNN che "*al 95% si tratta della Cina, c'è la Cina dietro questi attacchi informatici*".

Principalmente perché Pechino era già indiziato di altri cyber attacchi condotti contro il Parlamento australiano e importanti istituzioni pubbliche nel febbraio dell'anno passato, prima delle elezioni politiche.

La questione cinese

In un'indagine indipendente, condotta dal Governo e pubblicata dalla Reuters a settembre 2019, la cyber intelligence australiana (*Australian Signals Directorate*) ha individuato nel Ministero della Sicurezza di Stato il responsabile di quegli attacchi.

L'Australia non ha mai nascosto il suo timore reverenziale nei confronti del gitante asiatico, sia perché la Cina è ormai una potenza economico-finanziaria in tutto il Pacifico meridionale, sia per i crescenti investimenti in armamenti e tecnologie militari.

La risposta cinese non si è fatta attendere, con dazi commerciali e una comunicazione che mette continuamente in cattiva luce l'Australia, per esempio criticandone il razzismo, invitando anche i propri giovani a non scegliere le università australiane.

Situazione che di fatto vede l'Australia sempre più schiacciata sulla politica americana anti-cinese. A partire dalla richiesta di Canberra di un'inchiesta indipendente mondiale sull'origine della pandemia di COvid-19, con l'intenzione evidente di colpire Pechino.

> *Cyber attacco all'Australia, Morrison: "Dietro c'è un Paese straniero"*

Ursnif, il malware più diffuso in Italia che mette a rischio i conti online

Il trojan bancario **Ursnif**, scoperto nell'estate 2018 si è diffuso in questi anni attraverso diverse campagne malspam sfruttando temi di vario genere ed ispirati a situazioni e/o eventi contemporanei. Questo tipo di malware finalizzato alla sottrazione di credenziali relative a servizi di home banking, continua purtroppo a rappresentare una reale minaccia che riappare periodicamente sfruttando sempre strategie diverse.

Non a caso secondo il recente rapporto di Check Point Research (Global Threat Index 05/2020) questo malware è entrato per la prima volta nella top 10 delle minacce rilevate, posizionandosi al quinto posto a livello globale.

Nello specifico in Italia, nel mese di maggio Ursnif si è piazzato al primo posto registrando un impatto sulle organizzazioni di oltre il 14% (contro una media mondiale del 2%).

A confermare ulteriormente questo trend ci sono anche gli ultimi comunicati del CSIRT che allertano riguardo a diverse nuove campagne malspam ancora attive e che coinvolgono specificatamente utenze italiane.

Ursnif – Prima campagna malspam

Nella prima campagna segnalata, un massiccio invio di email invita gli utenti ad aprire una falsa fattura, un file Excel denominato “fattura_38.xls” che, contenendo una macro di tipo Excel4, in realtà si occupa, una volta aperto, di scaricare da un server di controllo remoto un eseguibile malevolo (“fattura.exe”).

Ursnif – Seconda campagna malspam

L’altra campagna osservata, sempre finalizzata alla diffusione di Ursnif tramite presunte fatture, invita i destinatari a scaricare, fornendo anche delle credenziali di accesso ad un sito web proposto (hxxp://attenzione.hazlotumismapr[.]com/), un file di archivio compresso in cui sarebbe contenuto un ordine di acquisto ma che si rivela essere anche in questo caso un file eseguibile (“pagament1.exe”) che installa il trojan bancario.

Ursnif – Terza campagna malspam

L’ultima campagna malspam osservata, secondo il solito rituale e facendo riferimento ad un ordine di pagamento con codice specifico identificativo, invita i destinatari ad aprire ancora un allegato Excel (“pagamento_722.xls”) ma questa volta contenente una macro malevola di tipo VBA (Visual Basic Application). Qualora si concedesse il permesso ad eseguire la macro, il payload Ursnif verrebbe scaricato attraverso

l’esecuzione di uno script Powershell.

Conclusioni

Come dimostrato anche da queste ultime campagne rilevate dal CSIRT, poiché il trojan bancario noto con il come di Ursnif o Gozi, si diffonde prevalentemente tramite messaggi di posta elettronica ed allegati sfruttando quelle abili tecniche di ingegneria sociale usualmente adoperate negli attacchi di phishing, per mitigare il rischio di subirne un’infezione occorre, oltre che dotarsi di un antivirus attendibile e sempre aggiornato, prestare la massima attenzione:

- alla lettura dei messaggi email e dei file che si ricevono;
- nel visitare siti web verosimili ed improbabili.

Imparare a saper interpretare in modo corretto la struttura della nomenclatura di un file, di un indirizzo WEB o di posta elettronica deve diventare un must che bisogna assolutamente perseguire, prendendo responsabilmente coscienza che dietro ad ognuno di questi elementi potrebbe celarsi una trappola informatica.

https://www.key4biz.it/ursnif-il-malware-piu-diffuso-in-italia-che-mette-a-rischio-i-conti-online/310763/

“Black lives matter”, allarme Csirt in Italia per il trojan Trickbot

Da qualche giorno in tutto il mondo si associa il popolare tema “***Black lives matter***” (Blm) alla diffusione di nuove campagne ***malicious spam*** o *malspam*, cioè email di spam tese ad infettare l’hardware del malcapitato attraverso *malware* veicolato in file o link allegati al messaggio.

Il *Computer security incident response team* (**Csirt**) per l’Italia ha lanciato l’allarme anche nel nostro Paese per la diffusione di attività *malspam* legata al tema attualissimo e dibattutissimo, tra media e social, del movimento “*black lives matter*” e dell’antirazzismo.

La minaccia in questione è rappresentata dal **trojan “*Trickbot*“**, che possiamo trovare in allegato alle email nell’inbox.

In realtà una minaccia non nuova, perché il team se n’era occupato già ai primi di giugno, evidenziando nuove funzionalità e un nuovo modello di propagazione del virus informatico.

Se quanto sta accadendo negli Stati Uniti e non solo, con il movimento Blm e le rivendicazioni antirazziali, è un ottimo “*tema esca*” per attirare nuove vittime, tecnicamente, una volta che si attiva il *trojan*, si da il via ad una catena di infezioni di hardware e software che potrebbe durare per lungo tempo.

Nello specifico, si legge sul sito del Csirt italia:

“*L’oggetto delle missive fa riferimento a richieste di fantomatiche recensioni confidenziali da rilasciare sul suddetto movimento*”.

Fondamentalmente, alle persone è chiesto di caricare un commento, la propria opinione, anche dei giudizi, in relazione a quanto sta accadendo nel mondo successivamente alla tragica morte di George Floyd per mano di un gruppo di agenti di Polizia di Minneapolis.

I messaggi di *malspam* presentano diverse variazioni nei nomi dei mittenti, fingendo di provenire da entità governative quali State Government, State Ministry, State Office, Country Authority o State Administration.

La pagina del *Response team* nazionale consiglia anche delle azioni utili a migliorare il livello di difesa dei propri device e a non cadere vittima di queste campagne di *spamming* particolarmente insidiose.

> *“Black lives matter”, allarme Csirt in Italia per il trojan Trickbot*

Geox sotto attacco ransomware, azienda bloccata da due giorni

Il colosso italiano delle calzature “**Geox**” nel mirino dei criminal hacker. Secondo quanto riporta il Mattino di Padova la produzione e la logistica dell’azienda trevigiana è bloccata da due giorni a causa di un ransomware diffuso

all’interno dei propri sistemi informatici.

I criminal hacker, spiega il quotidiano, tramite un ransomware hanno paralizzato i sistemi dell’azienda: dalla logistica, all’eCommerce, passando pure per le email aziendali, tanto che molti dei lavoratori dell’headquater di Montebelluna (TV) sono stati lasciati a casa per due giorni.

Abbiamo provato a contattare l’ufficio stampa dell’azienda, ma al momento non abbiamo ricevuto nessuna risposta.

La truffa delle false email

Non è la prima volta che l’azienda italiana è vittima del cybercrime. A maggio la Polizia Postale aveva scoperto e segnalato un sito fake “**geoxoutlet.online**” riportanti logo e informazioni del tutto simili a quelli dei canali ufficiali dell’azienda della “*scarpa che respira*“, inducendo l’ignaro utente finale a fare acquisti online nella convinzione di trovarsi su uno “store outlet” ufficiale del marchio “GEOX”. Ma era una truffa.

Ransomware, imprese e cybersecurity

La nuova generazione di attacchi ransomware colpisce i sistemi informativi delle imprese con varie azioni malevole e adoperando diverse componenti.

Le azioni malevole possono di vari tipi:

- sequestro file, criptando dischi e contenuti digitali;
- compromissione dell’operatività stessa dei sistemi colpiti, rendendoli inutilizzabili;
- esfiltrazione dei dati sensibili, intimandone la divulgazione pubblica

Non è non è scontato che il danno e i relativi problemi possano effettivamente risolversi con il pagamento del riscatto (solitamente richiesto in criptovaluta bitcoin), che richiede ogni ransomware.

Ma proteggere la propria attività da minacce esterne diventa fondamentale nel 2020. Gli attacchi informatici stanno diventando sempre più frequenti e il rischio di un blocco prolungato della produzione, come sta accadendo all'azienda trevigiana di scarpe, può avere effetti pesantissimi in termini di fatturato.

In media, nel 2019, il costo sostenuto da ogni organizzazione colpita da cyber attacchi è stato di quasi 4 milioni di euro.

Cifre da capogiro, che rappresentano un trasferimento di ricchezza unico nel suo genere, nella storia recente. Un settore, quello della sicurezza informatica, che diventerà per forza di cose molto più redditizio rispetto allo stesso traffico di stupefacenti, motivo per cui le organizzazioni di cyber crime stanno proliferando un po' ovunque.

https://www.key4biz.it/geox-sotto-attacco-ransomware-azienda-bloccata-da-due-giorni/310321/

Contact tracing: altre app Android malevole a tema Covid-19

È ancora alto il potenziale rischio relativo alla sicurezza dei dispostivi e alla privacy dei relativi utilizzatori che possono incappare nell'**installazione di false app a tema**

COVID-19.

Continuano infatti truffe e campagne ingannevoli da parte di attori criminali che attraverso l'abuso e le imitazioni di marchi di app ufficiali riescono a trarre vantaggio e profitti illeciti dalla relativa fiducia impropriamente acquisita.

App malevole

I ricercatori di Anomali Threat Research hanno di recente identificato delle **campagne di distribuzione di false applicazioni Android per il tracciamento dei contatti COVID-19,** propinate su store di terze parti o su siti web malevoli (comunque al momento della pubblicazione della ricerca, nessuna delle app individuate risulterebbe presente in Google Play Store).

Queste attività non coordinate ma manifestatesi in episodi separati stanno interessando diversi paesi tra cui anche l'Italia.

Le app segnalate che contengono *malware*, principalmente appartenenti alle famiglie dei *Trojan Anubis*, *SpyNote* o generici, una volta installate sui dispositivi, presentano tutte un comune denominatore: iniettano codice arbitrario per monitorare e carpire credenziali bancarie e dati personali dai dispositivi infetti.

Anubis e Spynote

Mentre Anubis è un trojan bancario Android che mascherandosi da applicazioni legittime in realtà tramite un overlay controllato e posizionato sopra l'applicazione viene utilizzato per rubare dati sensibili e credenziali.

Ecco alcune funzionalità:

- accesso a messaggi SMS, posizione, elenco contatti,

informazioni di sistema;
- keylogging;
- Registrazioni di telefonate;
- uso dell’overlay per rubare credenziali.

SpyNote è un trojan Android specializzato per raccogliere e monitorare dati di vario genere:

- accede a posizione GPS e contatti. Legge, scrive messaggi e contatti. Registra chiamate;
- scatta foto dalla fotocamera;
- controlla la cronologia browser;
- controlla le app installate e le informazioni sul dispositivo;
- esfiltra file.

L’app malevola italiana distribuita attraverso false promozioni INPS In Italia, come confermato tra l’altro anche dal CSIRT, l’app malevola, denominata “*COVID 19*”, si presenta come una legittima applicazione APK distribuita attraverso falsi siti INPS.

hXXps://inps-informa.website/download/INSPCovid.apk
hXXps://inps-forma.online/download/COVID-19.apk
e presenta l’icona di figura

Contact tracing: altre app Android malevole a tema Covid-19

Difendere la rete elettrica mondiale dai cyber attacchi, le linee guida del CNR

Sviluppare uno strumento pratico ed efficace per **proteggere la rete elettrica globale dai cyber attacchi**, ormai sempre più numerosi e sofisticati.

Su questo ha lavorato il Consiglio nazionale delle ricerche (**Cnr**) per sviluppare le linee guida sulla cybersecurity delle infrastrutture energetiche.

Curato da **Elena Ragazzi**, ricercatrice Cnr-Ircres, il documento dal titolo "*Evaluating the prudency of cybersecurity investments: Guidelines for Energy Regulators*" è stato realizzato dall'Istituto di ricerca sulla crescita economica sostenibile (**Ircres**) del Cnr su incarico della National Association of Regulatory Utility Commissioners degli Stati Uniti (**Naruc**).

Linee guida per difendere la rete elettrica

Le **linee guida** contenute nel testo sono state ideate per fornire alle autorità di regolamentazione dei Paesi di economie in transizione dell'area del Mar Nero (Armenia, Georgia, Moldavia e Ucraina) strumenti metodologici per il miglioramento della sicurezza del settore energetico contro l'emergente minaccia di attacchi informatici.

"*I cyberattacchi alla rete elettrica possono avere effetti devastanti sulla sicurezza, l'economia e il benessere pubblico*

di una nazione e rappresentano una potente minaccia per tutte le nazioni del mondo", ha spiegato Ragazzi in una nota tecnica allo studio.

"*Le minacce ai sistemi di controllo non vengono solo dai cyberterroristi; la guerra fredda cibernetica è uno strumento usato per marcare il controllo delle aree influenza geo-politica*".

"*La cybersicurezza, lungi dall'essere un mero problema tecnico-economico, è un tema che arriva a chiamare in causa anche la difesa della democrazia e dell'indipendenza delle nazioni*" , ha aggiunto la ricercatrice.

Valide per tutti i Paesi del mondo, tali linee guida sono il frutto di un'esperienza decennale del Cnr-Ircres nello studio dell'economia del sistema energetico.

I benefici della cyber protezione

In particolare, si legge sul sito del Consiglio, il progetto "***Essence***" (*Emerging Security Standards to the EU power Network controls and other Critical Equipment, 2011-2014*) ha consentito di stimare per la prima volta costi e benefici dell'attuazione di standard di sicurezza per la protezione delle infrastrutture critiche dagli attacchi informatici.

Un lavoro teso ad offrire alternative strategiche per affrontare il problema del cybercrime, a partire dalle diverse contromisure di *IT security* adottate con successo in diversi Paesi del mondo.

Altre valide azioni sono la valutazione dell'efficacia degli investimenti, un aiuto concreto alle autorità di regolamentazione nell'identificare e confrontare i costi della sicurezza informatica dagli altri costi operativi sostenuti dagli operatori.

Per ulteriori informazioni e approfondimenti si rimanda alla

Nota integrale Cnr-Ircres.

> *Difendere la rete elettrica mondiale dai cyber attacchi, le linee guida del CNR*

Cybersecurity sarà megatrend post Covid, attacchi informatici causeranno danni per 6 trilioni di dollari nel 2021

Nel gran caos globale generato dalla pandemia di Coronavirus e dal conseguente *lockdown*, che ha dato vita a sua vola ad una delle più gravi crisi economiche e sociali dell'ultimo secolo, **il digitale continua a rappresentare una valida *exit strategy*** e un trend positivo a cui aggrapparsi.

Per gli investitori, infatti, la crisi scatenata dall'epidemia non avrà una fine rapida e allo stesso tempo sarà di difficile lettura nei prossimi mesi. Eppure, i mercati hanno bisogno di trovare nuove strade e soprattutto di ritrovare fiducia e ottimismo. Il digitale garantisce la soddisfazione di entrambi i bisogni.

I megatrend post virus

Sanità, trasformazione digitale e cybersecurity sono i cosiddetti *"megatrend"* del momento, secondo la definizione utilizzata su *financialounge.com* da Paolo Paschetta, Country Head per l'Italia di Pictet Asset Management, verso cui si sta orientando la spesa globale.

I primi due li ritroviamo quasi indistinti, tra *ehealth*, medicina digitale, robotica, *software tech*, *big data*, intelligenza artificiale applicata alla salute, dispositivi tecnologici sanitari, *biotech* e *med tech*. Poi c'è il terzo, cioè quello della sicurezza informatica e digitale.

Anch'esso fortemente integrato agli altri due, anche se in maniera meno evidente al grande pubblico, il segmento della cyber sicurezza sta prendendo progressivamente quota sui mercati azionari e non solo.

Lo *smart working*, la didattica a distanza, le operazioni finanziarie e bancarie online, le transazioni bancarie, i servizi della Pubblica Amministrazione, sono tutte aree fortemente esposte agli attacchi informatici e per questo necessitano di interventi e di nuove misure di protezione.

Cyber attacchi, quanto ci costano

Solo nel 2018, sono stati oltre 800 milioni i cyber attacchi censiti, secondo una ricerca di *LearnBonds.com*. Per questo, oggi, il 70% delle aziende sta incrementando gli investimenti in sicurezza informatica e, secondo il pensiero di Paschetta, le uniche **tre voci di spesa che cresceranno nelle aziende saranno cloud, software per i meeting online e IT security**.

Secondo uno studio pubblicato da Herjavec Group, **si passerà dai circa 3 mila miliardi di dollari di danni da attacchi informatici del 2015 ai 6 mila miliardi di dollari attesi per il 2021**.

In media, nel 2019, il costo sostenuto da ogni organizzazione colpita da cyber attacchi è stato di quasi 4 milioni di euro.

Cifre da capogiro, che rappresentano un trasferimento di ricchezza unico nel suo genere, nella storia recente. Un **settore** che diventerà per forza di cose molto più redditizio rispetto allo stesso traffico di stupefacenti, motivo per cui le organizzazioni di cyber crime stanno proliferando un po' ovunque.

Solo il flusso di dati crescerà in maniera esponenziale nei prossimi mesi (non anni, mesi) e questo perché il numero di macchine, oggetti intelligenti, dispositivi, edifici e infrastrutture raggiungerà le decine di miliardi di unità.

Quello che viene definito "*The Big data Bang*", per dare nuova applicazione alla celebre teoria cosmologica, rappresenta un mondo in cui oltre **200 miliardi di oggetti dell'Internet delle cose** sarà interconnesso e connesso alla rete secondo dati Intel, senza limiti di spazio e tempo.

> *Cybersecurity sarà megatrend post Covid, attacchi informatici causeranno danni per 6 trilioni di dollari nel 2021*

Cresce l'uso dell'IA nei sistemi di cybersecurity, spesa globale a 30 miliardi

di dollari entro il 2025

L’attuale pandemia di Covid-19 ha dimostrato quanto insidiosi e pericolosi sono gli **attacchi informatici** per qualsiasi tipo di organizzazione, dalle imprese alle amministrazioni pubbliche, passando per i sistemi sanitari.

Nel corso dell’ultimo anno, secondo stime NTT, **il comparto dell’*Information technology* è risultato il più colpito dai cyber attacchi, con il 25% del totale** (era al 17% nel 2018). Segue il settore della Pubblica Amministrazione (16%), quindi il finanziario e i servizi professionali (12%) e l’istruzione (9%).

IA nella cyber sicurezza

Per raggiungere un elevato grado di cyber-resilienza e mantenersi su livelli di rischio accettabili per le organizzazioni, fondamentale è risultato l’utilizzo di **sistemi di cybersecurity ad alta integrazione di soluzioni per intelligenza artificiale** (IA).

Una tendenza riscontrabile a livello mondiale e che secondo stime VynZ Research porterà gli investimenti in soluzioni IA per la cyber sicurezza a circa 12 miliardi di dollari entro la fine dell’anno in corso.

Ad un tasso di crescita media annua (Cagr 2020-2025) valutato attorno al +20%, **entro cinque anni la spesa in tecnologie IA per la sicurezza raggiungerà i 30,5 miliardi di dollari**.

Mercato e segmenti in crescita

A guidare il mercato saranno diversi segmenti chiave, tra cui:

protezione dei dati personali, più alti livelli di sicurezza di infrastrutture e organizzazioni, l'accelerazione del processo di trasformazione digitale, ricorso crescente alle soluzioni cloud, ma anche le smart cities, la giga society e l'industria 4.0.

Tra le soluzioni sui cui al momento si concentrano maggiormente investitori e ricercatori, ci sono l'elaborazione del linguaggio naturale da parte delle macchine (natural language processing), il loro apprendimento automatico o machine learning, il riconoscimento vocale (speech recognition) e l'elaborazione digitale delle immagini (image processing).

In particolare, i ricercatori si attendono un aumento delle risorse finanziarie soprattutto per il settore del linguaggio naturale. Un processo complesso, quello dell'elaborazione del linguaggio umano da parte delle macchine, ma fondamentale per facilitare l'interazione uomo-computer e favorire la nascita di un ambiente sicuro.

https://www.key4biz.it/cresce-luso-dellia-nei-sistemi-di-cyber security-spesa-globale-a-30-miliardi-di-dollari-entro-il-2025/309684/

Defensor ID: come funziona l'app che evade la sicurezza dell'App Store

I ricercatori di ESET, hanno di recente pubblicato un articolo riguardo un'applicazione Android, ora non più disponibile su **Google Play Store**, che al momento dell'analisi si è rivelata

essere in realtà un temibile trojan bancario.

Il punto debole di Android sfruttato dagli hacker

Il malware camuffato da app **DEFENSOR ID** è risultato abbastanza insidioso e dotato di diverse funzionalità per il furto di informazioni, ed è riuscito a evadere tutti i meccanismi di protezione dello store Android ufficiale, inclusi i motori di rilevamento (App Defense Alliance) e addirittura a superare i test di analisi di "VirusTotal".

Tutto questo è stato reso possibile, ha commentato **Lukáš Štefanko** di ESET Research, perché gli sviluppatori criminali hanno ridotto al minimo la sua visibilità, rimuovendo tutte quei fattori caratterizzanti un trojan che potenzialmente potevano essere rilevati dai controlli come dannosi, utilizzando invece come "Cavallo di Troia" l'abuso dei permessi di accessibilità. Purtroppo questo servizio, molto utile perché permette anche agli utenti **ipovedenti o non vedenti** di utilizzare smartphone e tablet, rappresenta un punto debole del sistema operativo Android. Infatti le soluzioni di sicurezza lo riconoscono e lo segnalano come potenzialmente pericoloso solo se trovato in combinazioni con altre funzioni sospette o malevole.

Defensor ID: come funziona il

trojan bancario

La falsa app DEFENSOR ID richiedeva all'avvio tre autorizzazioni in particolare per poter funzionare:

1. Il consenso per la modifica delle impostazioni di sistema;
2. Il consenso per il drawing su altre app;
3. l'attivazione dei servizi di accessibilità.

Attraverso la concessione di queste autorizzazioni l'utente incautamente dava al trojan la possibilità non solo di leggere qualsiasi testo visualizzato sullo schermo e app avviata ma anche di instaurare una comunicazione con gli attaccanti, rubando credenziali, SMS, e-mail, chiavi di criptovaluta e codici multi fattore (2FA), consentendo di fatto il controllo completo di un eventuale conto bancario online della vittima. Sono stati rilevati ben 17 comandi che la versione malevola di DEFENSOR ID poteva ottenere dalla centrale di comando presidiata dagli aggressori.

Conclusioni

In considerazione del fatto che l'app in oggetto è stata disponibile sul Play Store dal mese di febbraio di quest'anno e che l'analisi è stata condotta solo sull'ultima versione ovvero la v1.4 rilasciata il 6 maggio 2020, non è stato possibile determinare, da parte dei ricercatori, l'affidabilità delle versioni precedenti.

In ogni caso, la segnalazione responsabile inviata a Google

nello scorso mese di maggio, ha prontamente consentito il ritiro dell'app dallo store. Solo successivamente sono stati pubblicati i risultati dell'indagine con tutti i dettagli e gli indici di compromissione.

> *Defensor ID: come funziona l'app che evade la sicurezza dell'App Store*

Cybercrime e phishing, quanto conta il fattore umano?

È oramai assodato come il fattore umano rappresenti una condizione di rischio rilevante per la cybersecurity. Una delle principali cause di violazioni, phishing e incidenti è infatti la vulnerabilità dell'utente finale correlata alla sua debolezza nel riconoscere e fronteggiare una possibile trappola informatica, diventando spesso esso stesso vittima e complice inconsapevole dei criminal hacker.

Distribuzione degli attaccanti (fonte Rapporto Clusit 2020)

È un dato di fatto come il cybercrime, cresciuto tra l'altro rispetto al 2018 del +12,3% e del +162% rispetto al 2014, continui a sfruttare attraverso il phishing e anche l'impiego di servizi già pronti, sempre più efficaci, semplici da utilizzare e facilmente reperibili a basso costo sul dark web, la scarsa consapevolezza delle persone per indurle a eseguire azioni potenzialmente pericolose, carpendo dati, informazioni sensibili e altro ancora. Non è un caso, infatti, che il

phishing/social engineering insieme al malware costituiscano, con la loro frequenza, le principali tecniche d’attacco registrando rispettivamente un aumento percentuale dell’81,9% e del 24.8% rispetto al 2018.

Distribuzione delle tecniche di attacco (fonte Rapporto Clusit 2020)

Sono ben noti i danni arrecati dallo sfruttamento di exploit umani. È sufficiente aprire un allegato o un link malevolo, per compromettere una intera rete di sicurezza aziendale e generare una fuga di informazioni riservate che possono essere rivendute e riutilizzate in ulteriori truffe o attacchi pianificati.

Molto indicativi risultano i dati statistici emersi da una serie di simulazioni secondo i più tradizionali schemi di phishing, condotte dal Cefriel nel 2018 e che, purtroppo, continuano a confermare il trend attuale. Tali risultati oltre a dimostrare come le tattiche di ingegneria sociale riescano molto spesso a indurre l’interlocutore a cliccare su link, aprire allegati e fornire dati riservati di valore (un dipendente su tre visita il sito esca e uno su quattro inserisce le proprie credenziali aziendali), rilevano quanto l’efficacia degli attacchi risulti estremamente elevata nei primissimi minuti ovvero in quella finestra temporale nella quale con maggior successo si riescono a sollecitare negli utenti azioni precipitose. Ed i pericoli alla sicurezza, correlati al fattore umano, si aggravano ulteriormente se si considera anche:

- che spesso il personale non denuncia le violazioni subite sia per paura di ritorsioni che per vergogna;
- che spesso il personale non ha nessuna esitazione nell’utilizzare strumenti privati, quali pendrive USB e dispositivi esterni, che possono contenere malware e

infettare i computer.

Social Driven Vulnerability Assessment: analisi temporale (fonte: Cefriel 2018)

Tutti questi aspetti portano a riflettere su quanto sia fondamentale includere tra i fattori di rischio l'errore umano, al fine di attuare contromisure e metodi adeguati di prevenzione e mitigazione. Ma per farlo occorre prima di tutto che la stessa governance aziendale impari a comprendere e soprattutto a misurare tale rischio non solo da un punto di vista strettamente tecnologico. Una politica di sicurezza deve essere elaborata coinvolgendo tutta l'organizzazione, rendendo i team di sicurezza IT non solo un riferimento tecnico ma anche degli intermediari nella comunicazione riguardo ai problemi e alle raccomandazioni di sicurezza, anche attraverso delle azioni di sensibilizzazione e spesso di alfabetizzazione.

Può di sicuro venire in aiuto un adeguato programma di security awareness fornendo a tutti delle linee guida di prevenzione e di comportamento e promovendo campagne informative a tema che possano diffondere una cultura della sicurezza attraverso lezioni, newsletter e messaggi spot sulle intranet aziendali, riuscendo a raggiungere più capillarmente il personale.

Tutti gli accorgimenti e le soluzioni di protezione hw/sw da soli non possono essere sufficienti. Occorre di sicuro una collaborazione più sinergica che porti a considerare l'utente, una volta per tutte, il fulcro della sicurezza informatica e non più il suo anello debole.

https://www.key4biz.it/cybercrime-e-phishing-quanto-conta-il-fattore-umano/308975/