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

Lug 12, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Malware, News, RSS 0

I cyber-criminali iniettano il loro codice di skimming nei server che non hanno protezione. Già infettati più di 17.000 siti Internet.

Il furto dei dati delle carte di credito rimane un grande classico della pirateria informatica e i protagonisti assoluti in questo settore sono i gruppi che gli esperti di sicurezza hanno battezzato con il nome di **MageCart**.

Si tratta di diversi gruppi di cyber-criminali, spesso in competizione tra loro, che prendono di mira i siti Internet che offrono servizi a pagamento (dall’e-commerce ai servizi) per inserire all’interno delle loro pagine un JavaScript che agisce come **skimmer**, rubando i dati delle carte di credito inseriti dai clienti.

In passato, i MageCart hanno messo a segno colpi clamorosi come quello a British Airways o a Forbes e di solito il loro modus operandi prevede attacchi mirati attentamente pianificati.

Come spiegano in un report i ricercatori di **RiskIQ**, adesso è comparso un nuovo gruppo che usa una strategia diversa. I pirati, secondo quanto riporta **Yonathan Klijnsma**, prende di mira i bucket S3 di Amazon che gli amministratori non proteggono adeguatamente per spargere a piene mani il loro script malevolo, modificando tutti i JavaScript che trovano.



Insomma: la nuova tecnica prevede di “sparare nel mucchio” utilizzando dei sistemi automatizzati. Chiaramente il livello di successo di questa tecnica, almeno da un punto di vista statistico, è piuttosto basso. Lo skimmer usato dai MageCart, infatti, funziona solo se i JavaScript infettati contengono un sistema di pagamento.

Dal punto di vista dei risultati complessivi, però, i pirati non si possono lamentare. **Secondo i ricercatori di RiskIQ, con questa tecnica sono riusciti a infettare più di 17.000 siti Web**.

Questo “successo” si spiega con il tipo di vittime che gli hacker sono riusciti a colpire. Tra queste, infatti, ci sono società come **Picreel**, **Alpaca Forms**, **AppLixir**, **RYVIU**, **OmniKick**, **eGain** e **AdMaxim**, che forniscono servizi a numerosi siti Internet.

Infettando i file presenti sui loro bucket, i MageCart hanno di conseguenza innescato un “effetto domino” che ha travolto rapidamente migliaia di siti collegati alle vittime principali, attraverso un meccanismo simile a quello della supply chain.

Condividi l’articolo

Agent Smith: il nuovo malware per Android fa strage di smartphone

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/12/un-nuovo-gruppo-magecart-attacca-a-tappeto-i-bucket-s3/

Agent Smith: il nuovo malware per Android fa strage di smartphone

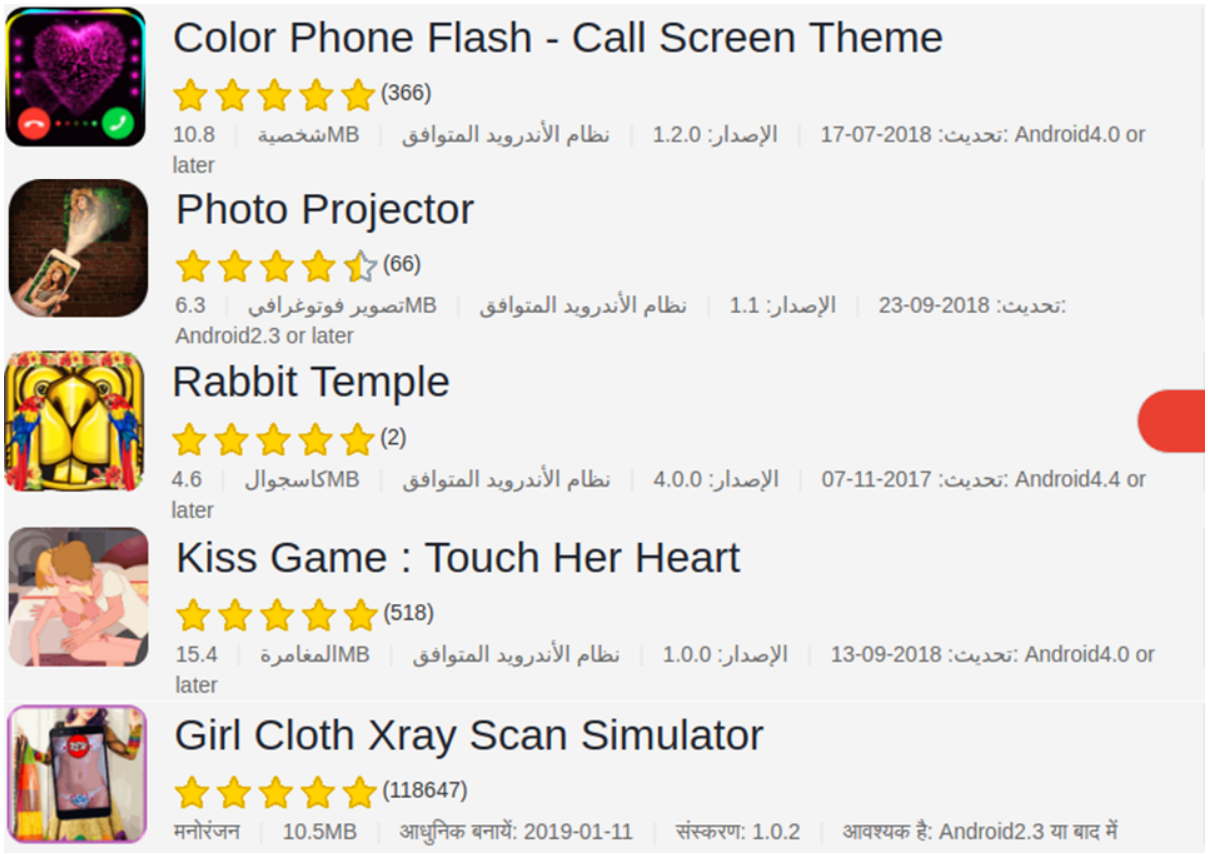
Lug 11, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Si nasconde sullo smartphone e modifica le applicazioni installate per bombardare la vittima di pubblicità. Già colpiti 25 milioni di dispositivi.

Si chiama **Agent Smith** il nuovo spauracchio che si aggira per la rete e che colpisce i dispositivi Android per intasarli di pubblicità indesiderate.

Il malware sarebbe comparso su alcuni store di terze parti, infettando la bellezza di **25 milioni di dispositivi Android**. Secondo **Check Point**, che descrive le caratteristiche del malware in un report sul suo sito Internet, il primo "focolaio" sarebbe stato **9Apps**, uno store Android molto usato in India.

Il malware, contenuto all'interno di applicazioni gratuite e giochi per smartphone, agisce in maniera particolarmente insidiosa. Il codice del modulo principale è crittografato all'interno di un'immagine JPEG.



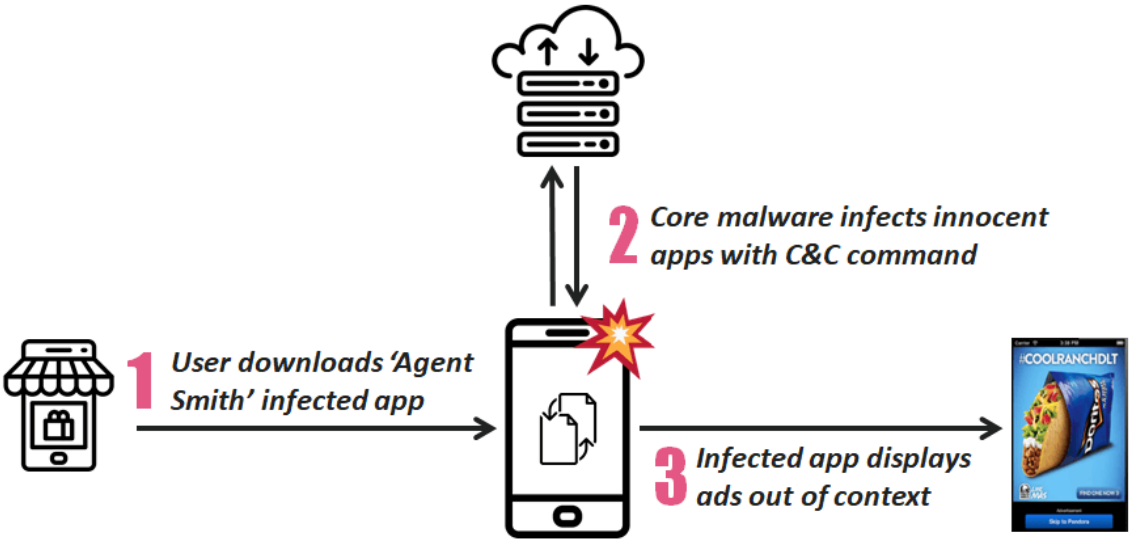
Una volta installata l'applicazione, il codice del malware viene estratto e avviato sullo smartphone sfruttando una serie di vulnerabilità conosciute che consentono la sua installazione senza che sia necessaria alcuna interazione da parte dell'utente.

Agent Smith si "mimetizza" per sembrare **un'applicazione di Google** e nasconde la sua icona in modo che la vittima non riesca a individuarne la presenza. I nomi utilizzati possono

cambiare, ma sono sempre del tipo “Google Updater” o “Google Update for U”.

In una seconda fase, il malware si collega al server Command and Control e, subito dopo, controlla l’elenco delle applicazioni installate sullo smartphone alla ricerca di alcune app di uso comune, come **Whatsapp.**

Utilizza poi una vulnerabilità conosciuta come Janus, che permette di sostituire le applicazioni legittime con una versione malevola, al cui interno è presente il modulo che gestisce la visualizzazione di pubblicità indesiderate sul telefono.



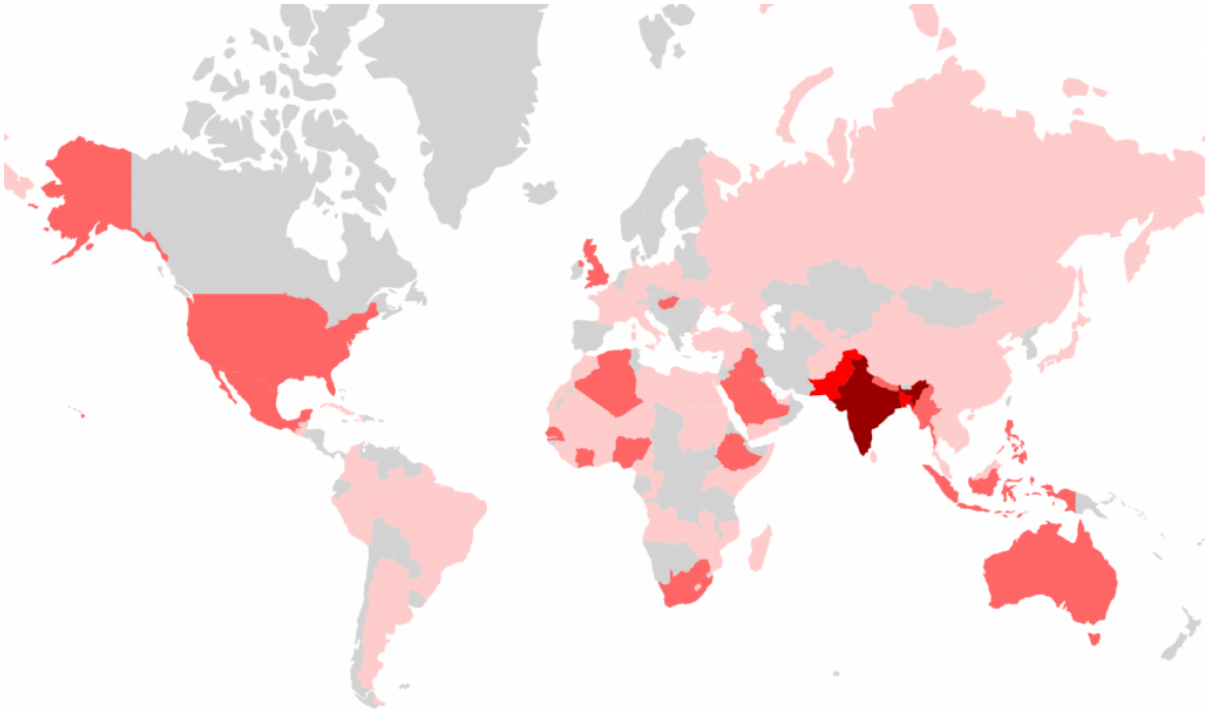
Una volta completata la sua opera, il malware deve solo preoccuparsi di garantire la persistenza delle applicazioni “modificate”. Per farlo, evita che possano eseguire gli aggiornamenti da parte del legittimo sistema di update.

I trucchi utilizzati sono due. Il primo è un sistema di monitoraggio che controlla costantemente la directory dedicata agli aggiornamenti e cancella immediatamente qualsiasi file di installazione compaia al suo interno.

Il secondo, invece, impatta sul sistema che gestisce il controllo degli aggiornamenti per fare in modo che l’applicazione non abbia scadenze per il controllo.

Oltre alle caratteristiche tecniche, i ricercatori di Check Point sottolineano nel loro report il fatto che la campagna di attacchi avviata da questo gruppo di pirati informatici è estremamente aggressiva. Analizzando lo store 9Apps, gli esperti hanno infatti individuato **più di 360 varianti del dropper**.

Non solo: l'elenco delle applicazioni che Agent Smith prende di mira è estremamente ampio. Secondo le analisi della società di sicurezza, i 25 milioni di dispositivi infetti conterrebbero in totale **2,8 miliardi di app "modificate"**. Una media di 112 per dispositivo.



Le preoccupazioni, però, riguardano anche altri aspetti. Secondo quanto si legge nel report, infatti, gli autori del malware starebbero pianificando un attacco che prenderebbe di mira direttamente **Google Play**. Gli esperti di Check Point, infatti, hanno individuato **11 app nello store ufficiale di Google** che contengono una versione "dormiente" del malware.

Il vero rischio, però, è che Agent Smith possa evolvere in maniera ancora più preoccupante. La struttura modulare del malware, infatti, permette di introdurre qualsiasi tipo di

funzionalità. **In futuro potremmo assistere alla comparsa di varianti con obiettivi decisamente più nocivi rispetto alla semplice visualizzazione di messaggi pubblicitari**.

Ma chi c'è dietro questo attacco? Dalle indagini dei ricercatori emerge un collegamento con una società cinese con sede a **Guangzhou**, che opera alla luce del sole, proponendo servizi di assistenza per gli sviluppatori Android che vogliono pubblicare le loro app sulle piattaforme estere. In pratica, una copertura perfetta.

Condividi l'articolo

Ecco come ti rubo i file con un bug di Firefox

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/11/agent-smith-il-nuovo-malware-per-android-fa-strage/

Ecco come ti rubo i file con un bug di Firefox

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

Una vulnerabilità vecchia di 17 anni può essere sfruttata ancora oggi per copiare tutti i file da una cartella e caricarli su un server esterno.

Da un punto di vista tecnico si definisce come un'implementazione errata della **Same Origin Policy (SOP)** ed è una vulnerabilità emersa in **Firefox** la bellezza di 17 anni fa.

Tutto gira intorno al fatto che il browser, oltre che pagine le pagine Web online, può essere utilizzato per aprire file HTML presenti nella memoria del dispositivo. Una funzionalità utile (anche se sempre meno) in qualche caso, ma che espone al rischio che un file malevolo possa avviare azioni nella directory in cui è memorizzato.

Il bug originale, segnalato nel 2002, riguardava la possibilità che un file potesse leggere gli altri dati nella sua stessa cartella e fosse così possibile accedervi. Per dirla tutta, non era un problema solo di Firefox: a esserne interessati erano tutti i browser disponibili in quel periodo, compreso (per chi se lo ricorda) **Netscape**.

Le soluzioni implementate dagli sviluppatori per correggere il bug sono state diverse e dalle parti di Mozilla hanno scelto di impedire ai file HTML di accedere all'elenco (indexing) dei file all'interno della cartella. In questo modo**, un pirata informatico che avesse voluto rubare un file avrebbe dovuto conoscerne posizione e nome**.



Perché non utilizzare soluzioni più drastiche? Perché la lettura via Browser di file HTML ha ancora qualche utilità, per esempio la visualizzazione delle guide software (molti produttori usano ancora HTML) e “troncare” la possibilità di visualizzarli avrebbe creato qualche problema.

La scelta di introdurre una protezione “light”, però, ha lasciato aperta la possibilità di sfruttare la vulnerabilità. Anche se in maniera decisamente elaborata. A segnalarlo agli sviluppatori di Mozilla è stato **Vladimir Bostanov** nel luglio del 2018.

Il ricercatore si è infatti reso conto che con qualche accorgimento (e un generoso uso di ingegneria sociale) è possibile sfruttare il bug anche oggi. La tecnica di attacco prevederebbe l’invio del file malevolo alla vittima che, una volta aperto, mostri un elenco dei file in cartella e un messaggio che chiede di “fare clic per sbloccare il contenuto”. **Il clic sul link potrebbe avviare il JavaScript che trasferirebbe i file della cartella sul server del pirata informatico**.

Complicato? Forse. Plausibile? Sicuramente. Nel passato, tutto sommato, abbiamo visto attacchi avere un discreto successo adottando strategie molto più improbabili.

La vulnerabilità è stata resa pubblica il **16 gennaio 2019**, ma nonostante ciò non è arrivata alcuna patch per correggere la falla.

Qualche giorno fa, però, a riaccendere i riflettori sul problema legato alla gestione della SOP in Firefox ci ha pensato un altro ricercatore, **Barak Tawily**.

Nel suo report, corredato anche da un video, Tawily spiega come sfruttare il bug per sottrarre informazioni dal computer dell'ignara vittima sfruttando la vulnerabilità.

[embedded content]

Ora sembra che dale parti di Mozilla abbiano deciso di prendere delle contromisure più serie e che il problema verrà risolto una volta per tutte. Nel frattempo, il suggerimento è quello di diffidare dei file HTML in download.

Condividi l'articolo

Zero-day nella versione Mac di Zoom. La webcam attivata in remoto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/10/ecco-come-ti-rubo-i-file-con-un-bug-di-firefox/

Zero-day nella versione Mac di Zoom. La webcam attivata in remoto

Lug 09, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug consente di attivare una chiamata quando la vittima visita un sito Internet infetto. Non solo: è possibile avviare la reinstallazione di Zoom se è stato rimosso.

Non c'è niente di peggio di una responsible disclosure che va male. Nel caso di **Zoom**, il popolare programma di videoconferenza pensato per le aziende, l'ultima segnalazione di vulnerabilità ha avuto esiti decisamente negativi.

La falla di sicurezza (ma sarebbe più corretto parlarne al plurale)è stata individuata da **Jonathan Leitschuh**, un ricercatore che ha pensato bene di approfondire una particolare funzione di Zoom: **quella che consente di usare un semplice link per avviare una conversazione su browser**.

Come spiega nel suo report, Leitschuh si è reso conto che questa funzionalità potrebbe essere utilizzata per **avviare la webcam di un computer Apple senza l'autorizzazione dell'utente o per bloccare il sistema portando, di fatto, un attacco DoS**.

Ficcando il naso nel programma, poi, il ricercatore si è anche reso conto in un'ulteriore falla che permette di "forzare" la reinstallazione del programma anche se l'utente lo ha rimosso.

Questo perché Zoom installa un Web Server sulla porta 19421 che rimane attivo anche dopo la disinstallazione. Per avviare la procedura di installazione basta un invito a unirsi a una conferenza.



```
/* @class ZMClientHelper */
+(void *)getDownLoadURL:(void *)arg2 {
    r15 = [arg2 retain];
    if ((r15 == 0x0) || ([r15 length] == 0x0)) {
            [@"www.zoom.us" retain];
            [r15 release];
            r15 = @"www.zoom.us";
    }
    rbx = [[NSString stringWithFormat:@"https://%@/upgrade?os=mac", r15] retain];
    r14 = [[NSURL URLWithString:rbx] retain];
    [rbx release];
    [r15 release];
    rax = [r14 autorelease];
    return rax;
}
```

Nulla di particolarmente difficile da risolvere, ma come racconta l'analista, il percorso verso la patch non è stato esattamente un esempio di "collaborazione virtuosa".

Dalle parti di Zoom, infatti, in questa occasione gli sviluppatori non hanno certamente brillato per reattività. Secondo quanto riporta Leitschuh, la conferma della vulnerabilità in risposta alla prima segnalazione (inviata il 26 di marzo) sarebbe arrivata solo 10 giorni dopo.

Ancor peggio, il primo incontro per discutere lo sviluppo della patch è avvenuto solo l'11 di giugno. Considerata la scadenza di 90 giorni data dal ricercatore, in quel momento rimanevano solo **18 giorni** per sistemare le cose. Non solo: il progetto di patch proposto dagli sviluppatori di Zoom in quell'occasione non convinceva Leitschuh, che riteneva il fix facilmente aggirabile.

Arrivati alla scadenza, spiega Jonathan Leitschuh, il risultato è stata la pubblicazione di una patch che conteneva il fix "parziale", che in seguito sarebbe stato ulteriormente degradato.

Insomma: le falle (con l'eccezione di quella relativa al DoS)

sarebbero ancora presenti. Peggio ancora: secondo Leitschuh buona parte dei più di **4 milioni di utenti Mac** di Zoom non utilizzerebbero una versione aggiornata del programma (che non prevede update automatici) e potrebbe, di conseguenza, essere vulnerabile anche alla falla che è stata corretta.

Il suggerimento, per gli utenti Mac di Zoom, è di eseguire manualmente gli aggiornamenti e di mettere in atto alcuni accorgimenti (indicati nel dettaglio nel suo report) per proteggersi da eventuali attacchi.

Condividi l'articolo

UK: laboratorio di forensica cede al ricatto di un ransomware

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/09/zero-day-nella-versione-mac-di-zoom-la-webcam-attivata-in-remoto/

UK: laboratorio di forensica cede al ricatto di un ransomware

Lug 08, 2019 Marco Schiaffino Attacchi, Gestione dati, In evidenza, News, Privacy, RSS 0

L’azienda è uno dei maggiori contractor del governo britannico e si occupa di analisi dei dati per conto della polizia e delle procure.

C’è un proverbio che dice che “il figlio del calzolaio va in giro con le scarpe rotte”. La notizia dell’attacco **ransomware** subito da **Eurofins Scientific**, società specializzata in analisi di ogni tipo (da quelli tossicologici all’ingegneria informatica forense) ci si adatta alla perfezione.

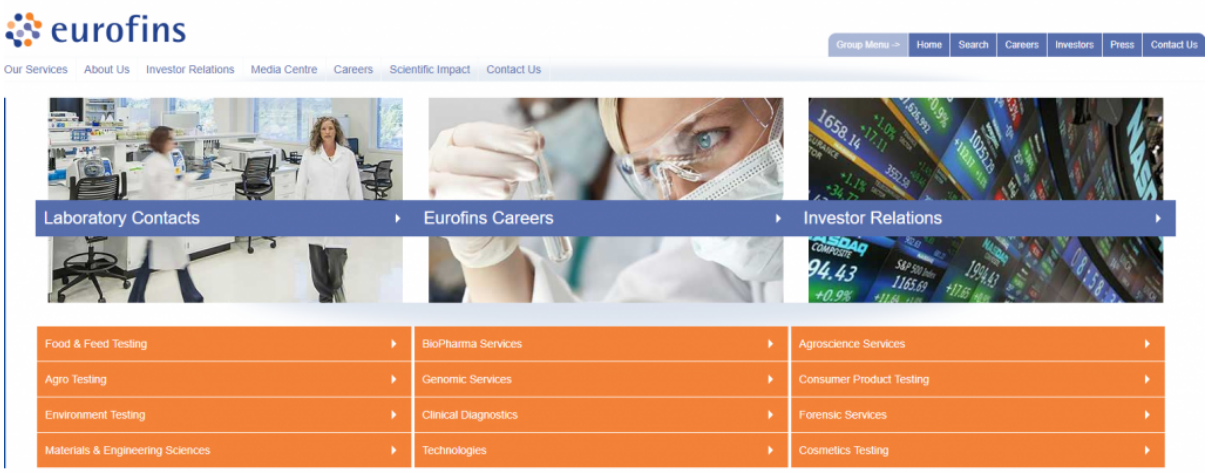
L’attacco, secondo quanto si può ricostruire dai vari comunicati dell’azienda, sarebbe avvenuto lo scorso 2 giugno. La dirigenza di Eurofins ha immediatamente denunciato l’accaduto con un comunicato stampa del giorno dopo.

Nel testo si parla di “un nuovo tipo di malware” ma, soprattutto, si fa esplicito riferimento a una procedura di ripristino dei dati a partire dal backup. Insomma: la notizia, fino a quel momento, rientrava nella normalità di un attacco ransomware che (non è la prima volta) aveva colpito un bersaglio di alto livello.

Certo, l’idea che tecnici abituati a lavorare nel settore forensico finiscano vittima di un malware ha fatto sollevare qualche sopracciglio, ma nulla di più.

Anche il successivo comunicato del 10 giugno, in cui l’azienda aggiornava sulla situazione delle sue infrastrutture IT, non conteneva alcuna notizia sconvolgente. **Le uniche notizie di rilievo riguardano il fatto che il malware in questione non sarebbe stato rilevato dagli antivirus e che il ripristino dei sistemi era in corso**.

Venerdì sera, però, Eurofins ha ammesso che il ripristino dei sistemi non è avvenuto attraverso l’uso dei backup, ma **pagando il riscatto richiesto dai pirati informatici**.



Un “dettaglio” che cambia decisamente le carte in tavola. In primo luogo perché una società che collabora regolarmente con le forze di polizia ha adottato una strategia (se la vogliamo chiamare così) che di solito viene sconsigliata dalle stesse forze dell’ordine.

In secondo luogo perché tutti i dati contenuti nei loro sistemi, alla luce di questa notizia, potrebbero essere considerati inaffidabili.

E non stiamo parlando di contratti e fatture, ma di esami del DNA e analisi tossicologiche che dovrebbero essere utilizzate in tribunale come prove.

Le autorità si sono affrettate a dichiarare di “non vedere alcuna ragione per credere che ci sia stato un impatto sulle prove elaborate dalla società”. L’affermazione, però, è decisamente ottimistica.

Considerato che tutti i dati nei sistemi di Eurofins hanno subito un processo di crittografia eseguito da un malware e una decodifica portata a termine con uno strumento fornito da cyber-criminali, sostenere che i dati possano essere considerati “integri” è un azzardo che qualsiasi avvocato in aula potrebbe sottolineare per mettere in dubbio l’affidabilità delle prove.

Insomma, sulla base dell’incidente avvenuto il 2 giugno,

centinaia (migliaia?) di processi potrebbero essere invalidati o ritardati a causa della possibile inaffidabilità dei dati forniti da Eurofins.

Condividi l’articolo

Tik Tok rischia (un’altra) multa per violata privacy dei minori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/08/uk-laboratorio-di-forensica-cede-al-ricatto-di-un-ransomware/

Tik Tok rischia (un’altra) multa per violata privacy dei minori

Lug 05, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Scenario 0

Il governo inglese ha avviato una procedura sul trattamento dei dati dei minori. L’azienda cinese

rischia una multa da 20 milioni di euro.

Il difficile rapporto tra tutela della privacy dei minori e Internet vive un nuovo capitolo che conferma (ancora una volta) la presenza di un problema cui si stenta a trovare una soluzione.

Protagonista è **TikTok**, l'applicazione social che spopola tra i ragazzini e che consente di registrare e condividere filmati in cui i protagonisti si esibiscono in performance musicali e non solo.

L'azienda cinese sarebbe finita nel mirino delle agenzie governative britanniche, che stanno valutando la possibilità di sanzionare TikTok per violazione della normativa in tema di protezione dei dati (**GDPR**) relativa ai contenuti pubblicati dai minori di 13 anni.

La normativa europea, infatti, prevede che qualsiasi trattamento dei dati di utenti minorenni (l'età può essere definita da ogni singolo stato) **debba essere autorizzata dai genitori**.

Una previsione di difficile applicazione pratica e piuttosto facile da aggirare, per esempio mentendo sull'età o fornendo un indirizzo email del presunto genitore che lo stesso minore gestisce.

Nel caso di TikTok, l'azienda ha cercato di tutelarsi da eventuali problemi inserendo nelle condizioni di utilizzo il **divieto di iscrizione ai minori di 13 anni**. Lo stratagemma, però, non sembra aver funzionato.



TikTok, infatti, è stata recentemente sanzionata negli Stati Uniti (dove il **Children's Online Privacy Protecion Act** prevede un sistema simile al GDPR) con una multa di **5,7 milioni di dollari** per non aver vigilato sul rispetto delle condizioni. All'azienda, nel dettaglio, è stato contestato il fatto di non aver bloccato contenuti condivisi da utenti che avevano palesemente un'età inferiore ai 13 anni.

La procedura avviata nel Regno Unito, però, rischia di essere ancora più pesante. Il mancato rispetto del GDPR, infatti, può portare a una sanzione pari al 4% del fatturato mondiale dell'azienda multata. **Per TikTok si parlerebbe di 20 milioni di euro di multa**.

Le preoccupazioni delle autorità, soprattutto, si concentrano sulla possibilità che i minori iscritti al servizio possano essere contattati direttamente da adulti che potrebbero approfittare dell'ingenuità dei ragazzi per circuirli allo scopo di indurli a condividere con loro informazioni personali o contenuti sessualmente espliciti.

Un fenomeno tristemente noto, che negli ultimi tempi sta però

vivendo preoccupanti evoluzioni. Secondo l'**FBI**, per esempio, negli Stati Uniti si stanno moltiplicando i casi di estorsioni ai danni di minori che in un primo momento vengono convinti a condividere video o immagini compromettenti e poi **vengono ricattati con la minaccia di renderli pubblici**.

Insomma: oltre ai "normali" predatori sessuali, alla lista delle minacce si stanno aggiungendo criminali senza scrupoli, che approfittano della vulnerabilità dei minori per ottenere guadagni illeciti. Allo schifo non c'è mai fine.

Condividi l'articolo

Android: 182 app malevole su Google Play e altri store

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/05/tik-tok-rischia-unaltra-multa-per-violazione-della-privacy/

Android: 182 app malevole su Google Play e altri store

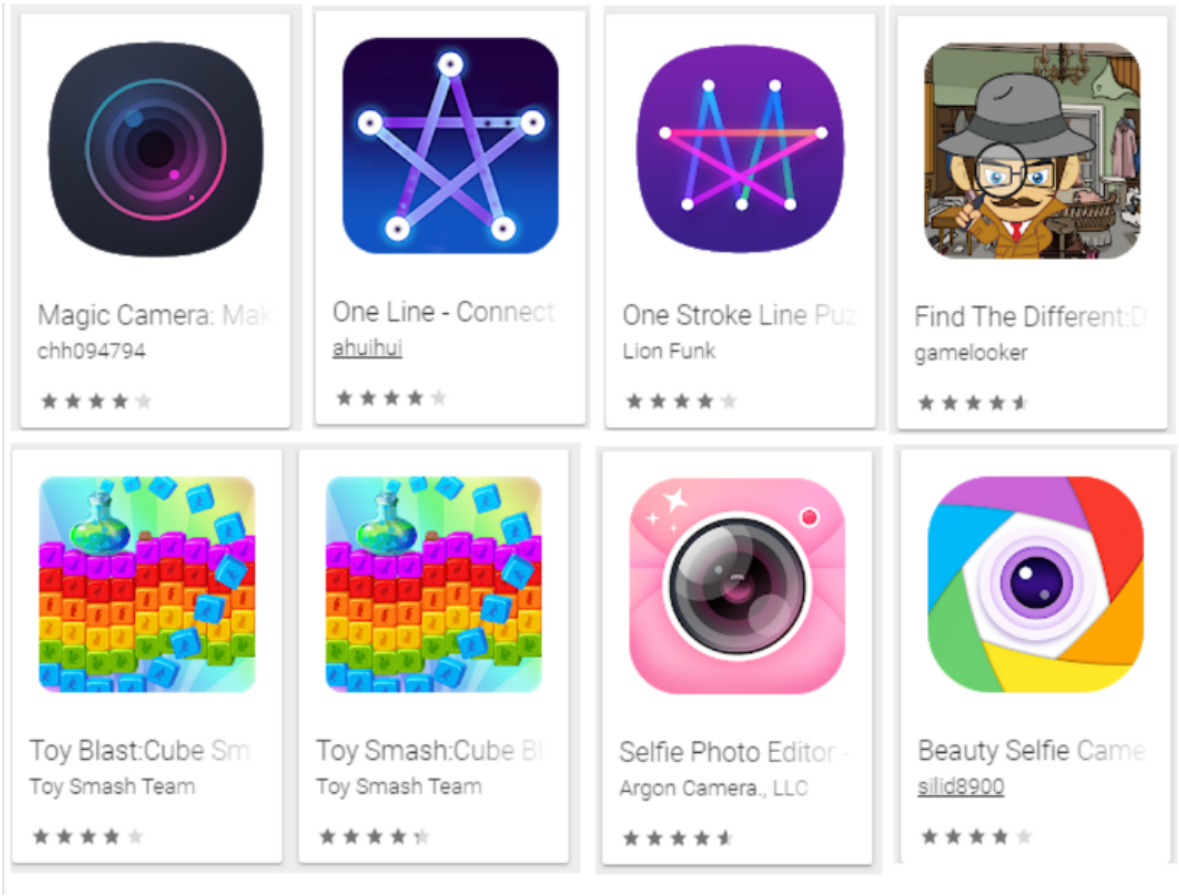
Lug 04, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La scoperta di Trend Micro, che ha identificato le applicazioni contenenti un adware. Gli uttenti coivolti sarebbero più di 9 miliioni.

Niente da fare: nonostante **Google** stia cercando di darsi da fare per migliorarne il livello di sicurezza, **Android** continua a rappresentare il bersaglio privilegiato di pirati informatici.

A confermarlo è **Trend Micro**, che oggi ha annunciato di aver individuato la bellezza di 182 applicazioni contenenti **adware** (malware pensati per visualizzare messaggi pubblicitari indesiderati – ndr) che sarebbero state scaricate da milioni di utenti.

Nel dettaglio, la campagna dei cyber-criminali avrebbe utilizzato due diversi malware: **AndroidOS HiddenAd.HRXAA** e **AndroidOS HiddenAd.GCLA** caricati all'interno delle app su **Google Play** e su store di terze parti.



Gli adware, spiegano dalle parti di Trend Micro, sfruttano

tecniche di offuscamento per nascondere la loro presenza ed evadere le rilevazioni sandbox, per poi **generare pubblicità a tutto schermo che non possono essere chiuse immediatamente**, creare pop-up che infestano il dispositivo dell'utente compromettendo la memoria (oltre che l'autonomia del dispositivo) e dirottare gli utenti su siti maligni.

A impressionare, inoltre, è il fatto che lo store ufficiale di Google rimanga così permeabile agli attacchi**. Gli esperti di Trend Micro hanno individuato su Google Play la bellezza di 111 app infette**. I download complessivi, spiega la società di sicurezza, sono stati 9.349.000.

Condividi l'articolo

Cina: turisti obbligati a installare uno spyware sullo smartphone

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/04/android-182-app-malevole-su-google-play-e-altri-store/

Cina: turisti obbligati a installare uno spyware sullo

smartphone

Lug 04, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

Chi attraversa il confine Xinjiang viene messo sotto sorveglianza attraverso un'applicazione che controlla messaggi, telefonate e file.

Una vera **campagna di sorveglianza di massa** che prende di mira i turisti. È questa l'ultima trovata del governo cinese, che secondo numerosi organi di stampa starebbe obbligando tutti i cittadini stranieri che visitano la regione dello **Xinjiang** a installare un'applicazione che controlla la loro attività sullo smartphone.

La polizia di frontiera cinese, a quanto si legge nell'articolo del Guardian, obbligherebbe i visitatori a consegnare il loro telefono al momento dell'ingresso dal vicino **Kyrgyzstan** e installerebbero sullo smartphone un'applicazione chiamata **Fengcai**.

Secondo l'inchiesta condotta da **Guardian**, **New York Times**, **Motherboard**, **Süddeutsche Zeitung** e **NDR**, il malware verrebbe installato sia sui telefoni **Android**, sia sugli **iPhone**. Per questi ultimi la polizia cinese utilizzerebbe **un dispositivo hardware** che, presumibilmente, effettua un jailbreak del sistema.

Lo spyware sarebbe in grado di controllare tutti i messaggi ricevuti e inviati, i log delle telefonate effettuate ed eseguirebbe anche una scansione nella memoria del telefono per individuare l'eventuale presenza di documenti "proibiti" (l'elenco ne comprende 73.000) collegati alla propaganda dell'ISIS o con contenuti relativi al terrorismo, come manuali per la costruzione di ordigni.

Lo Xinjiang è una regione in cui la tensione con la minoranza **Uiguri** (di religione musulmana) è da sempre elevata e in cui si sono registrati frequenti scontri tra la popolazione e le forze governative.



Lo scorso febbraio erano già emerse prove (ne abbiamo parlato in questo articolo) che il governo cinese tenesse sotto controllo i cittadini della regione attraverso potenti sistemi di sorveglianza che utilizzano **telecamere e sistemi di riconoscimento facciale** per registrare ogni movimento degli abitanti.

L'estensione di sistemi di spionaggio ai cittadini stranieri, però, è una novità che segna un ulteriore giro di vite e conferma la tendenza di Pechino ad adottare tecniche di sorveglianza sempre più invasive.

L'ultima mossa in questo senso era stata l'approvazione di una normativa che "legalizza" l'hacking di stato nei confronti delle aziende che operano sul territorio cinese.

Condividi l'articolo

Android: 182 app malevole su Google Play e altri store Dopo 10 anni i pirati usano ancora Heaven’s Gate

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/04/cina-turisti-obbligati-a-installare-uno-spyware-sullo-smartphone/

Dopo 10 anni i pirati usano ancora Heaven’s Gate

Lug 03, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Vulnerabilità 0

La tecnica permette di aggirare i controlli degli antivirus sfruttando un trucchetto che sui sistemi operativi precedenti a Windows 10 funziona ancora.

Normalmente la rincorsa tra pirati informatici ed esperti di sicurezza è terribilmente frenetica. Tutto si gioca sul fattore tempo: ogni volta che i cyber-criminali individuano una tecnica di attacco, cercano di sfruttarla al massimo in tempi ridotti, prima che le società antivirus riescano a mettere in campo le contromisure che la “sterilizzano”. Ci sono, però, delle eccezioni e una di queste si chiama **Heaven’s Gate**.

A (ri)accendere i riflettori sul “cancello del paradiso” sono i ricercatori del team **Talos** di **Cisco**, che in un post sottolineano come esistano ancora numerosi malware che sfruttano questa tecnica, comparsa per la prima volta nei primi anni 2000.

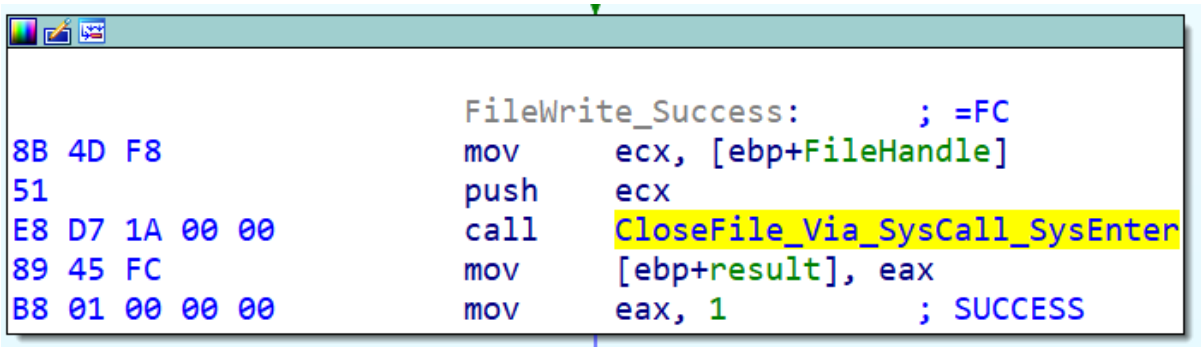
Heaven’s Gate, nel dettaglio, è considerata una tecnica di evasione, che consente cioè a un malware di eseguire codice sul sistema operativo sfuggendo al controllo degli antivirus.

Il trucchetto sfrutta la presenza dei due ambienti a 32 e 64 bit sui sistemi Microsoft. Le versioni di Windows a 64 bit, infatti, utilizzano una procedura particolare per eseguire le applicazioni a 32 bit.

Il compito è affidato a un sottosistema chiamato **Microsoft WOW64**, che ha la funzione di “adattare” l’ambiente di lavoro in modo che i programmi a 32 bit possano funzionare correttamente.

La tecnica Heaven’s Gate, in buona sostanza, sfrutta questo “doppio binario” per eseguire parte del codice in una maniera che gli antivirus non si aspettano. Il malware avvia la sua esecuzione come programma a 32 bit in modo da essere “assegnato” a WOW64.

A metà della procedura, però, esegue delle operazioni dirette all’ambiente nativo a 64 bit. Un comportamento, questo, che molti antivirus faticano a individuare. Risultato: le operazioni nell’ambiente nativo sfuggono al controllo.



Il problema è stato risolto da Microsoft introducendo una funzionalità chiamata **Control Flow Guard**, presente però **solo in Windows 10**. I sistemi operativi più vecchi, quindi, rimangono vulnerabili alla tecnica di evasione. E visto che le installazioni di **Windows 7** o addirittura (sigh!) di **Windows XP** sono ancora tutt'altro che irrilevanti a livello statistico, è ovvio che i pirati informatici ci puntino ancora.

Secondo i ricercatori di Talos, tra i malware che hanno rispolverato questa tecnica c'è per esempio **HawkEye Reborn**, un keylogger distribuito recentemente su Internet, ma anche numerosi miner.

Insomma: se qualcuno dovesse avere ancora bisogno di un buon motivo per passare a un sistema operativo aggiornato, Heaven's Gate può essere quello giusto.

Condividi l'articolo

Benvenuti nel mondo del voto elettronico…. e benvenuta Ecsite!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/03/dopo-10-anni-i-pirati-usano-ancora-heavens-gate/

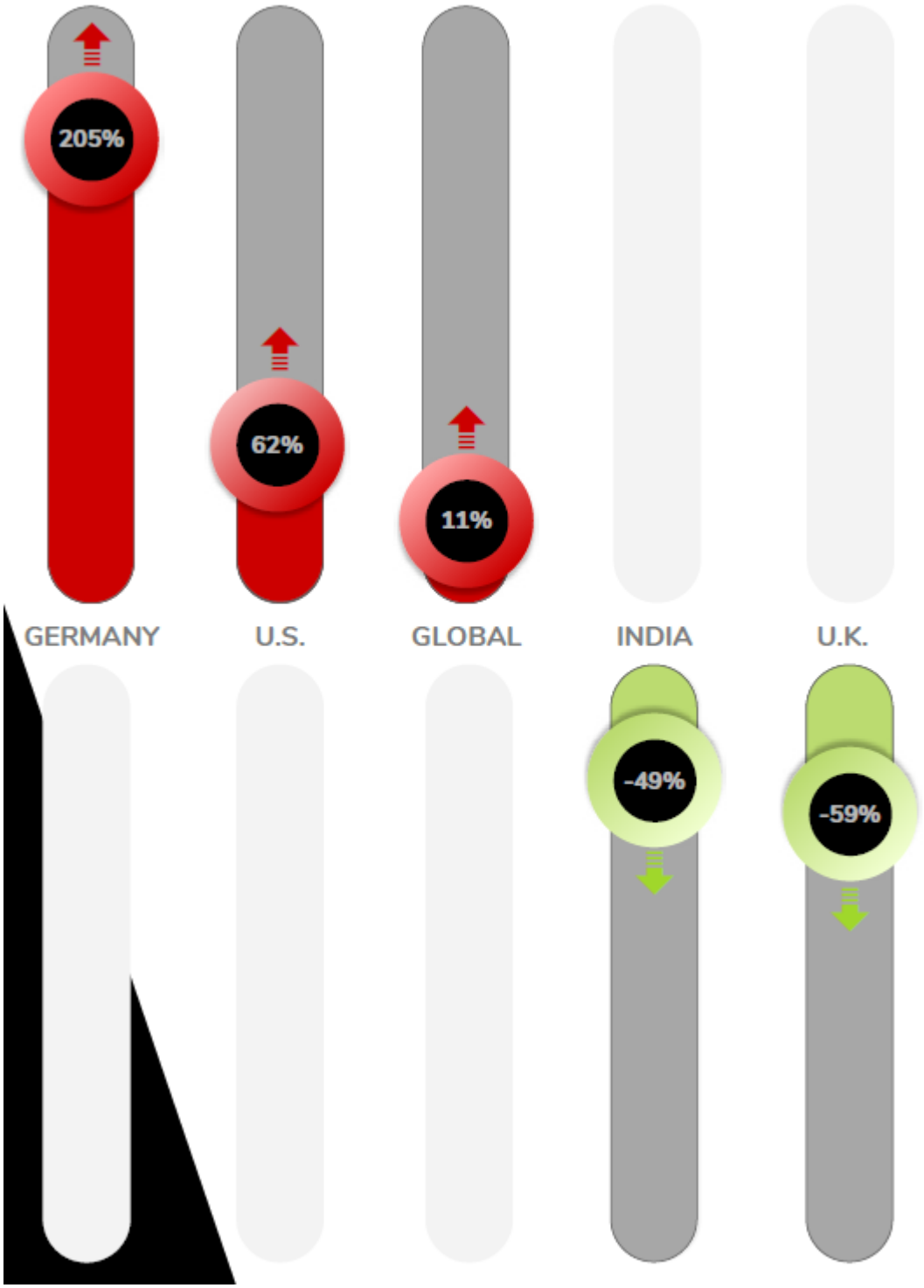
Affidarsi all’Intelligenza Artificiale? Si può (e si deve) fare

Lug 02, 2019 Marco Schiaffino Approfondimenti, Attacchi, In evidenza, Malware, RSS, Scenario, Tecnologia 0

Dalla ricerca SonicWall emerge uno scenario in cui gli attacchi alle aziende raggiungono volumi impressionanti come frequenza e intensità. Serve l’AI.

Un panorama in costante evoluzione in cui gli attacchi sono sempre più sofisticati e la pressione sulle infrastrutture informatiche di aziende e governi aumenta esponenzialmente. È questo ciò che emerge dal **Cyber Threat Report 2019** pubblicato da **SonicWall**.

Partiamo dalle buone notizie e in particolare dalla perdita di efficacia dei **ransomware**. Sfortunatamente l’arretramento di questa tipologia di malware non interessa tutto il mondo, ma alcune nazioni chiave come **Regno Unito e India**. A livello globale, invece, gli attacchi con ransomware segnano un +11% rispetto all’anno precedente.

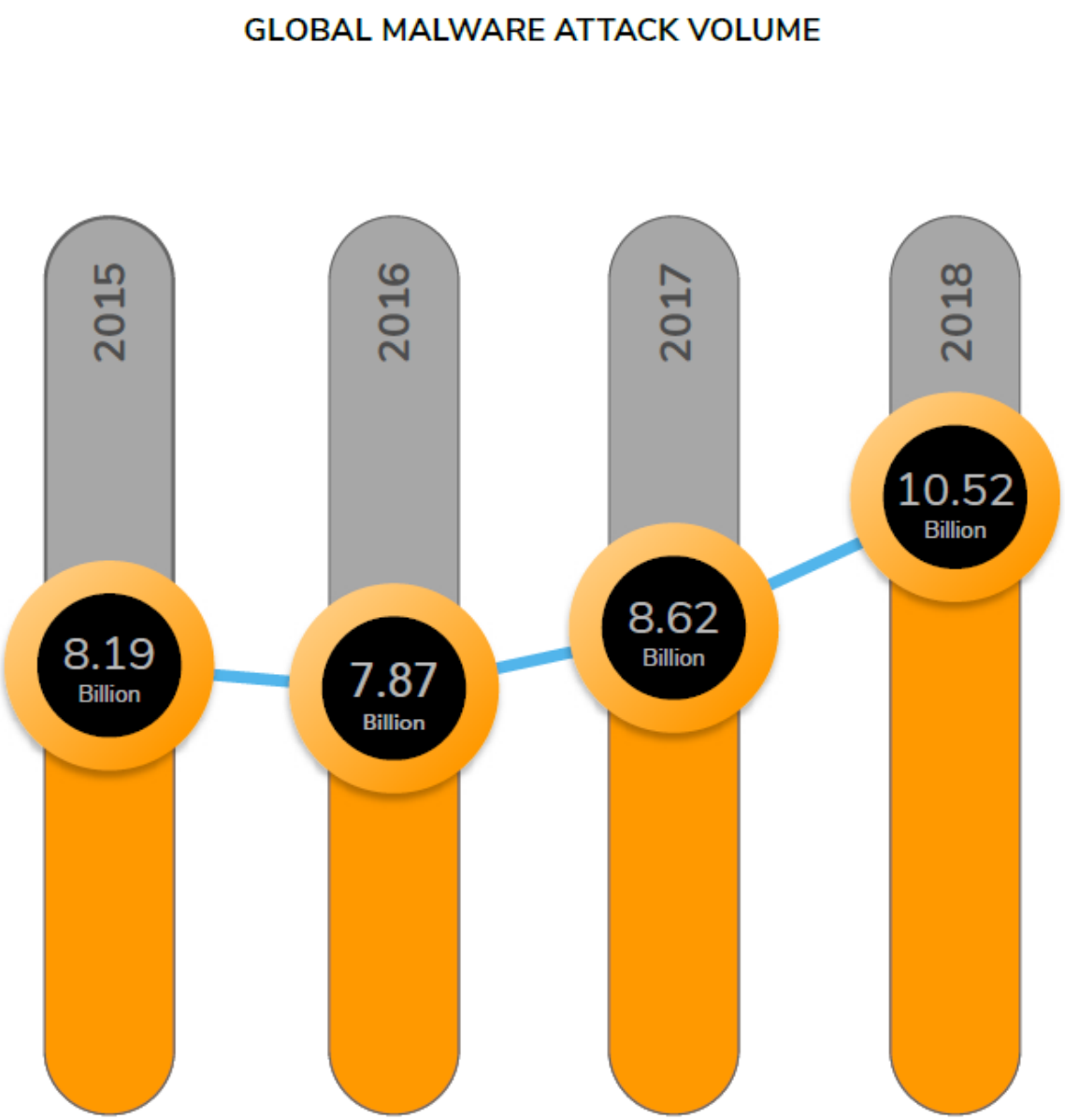


La seconda buona notizia riguarda il numero di vulnerabilità individuate dai ricercatori nel 2018. Sono 18.097, in netto aumento rispetto al 2017, con 12.920 CVE pubblicate.

Perché è una buona notizia? Principalmente perché sembra che la diffusione dei programmi di bug bounty stiano sortendo i risultati che ci si aspettava. Più ricercatori al lavoro, più falle di sicurezza individuate prima che qualcuno riuscisse ad

approfittarne.

Le buone notizie finiscono qui. Secondo i rilevamenti di SonicWall, basati sui dati raccolti in tempo reale da circa **1,3 milioni di endpoint** in tutto il mondo, il volume complessivo di attacchi attraverso malware nel 2018 è infatti cresciuto notevolmente, arrivando a **10,5 miliardi** (erano 8,6 miliardi nel 2017) confermando una tendenza che ha avuto una flessione solo nel 2016.



Accanto alla crescita di attacchi malware, SonicWall segnala i rischi legati alle nuove tecniche di attacco side-channel come Spectre e Meltdown. “È solo una questione di tempo” ci spiega

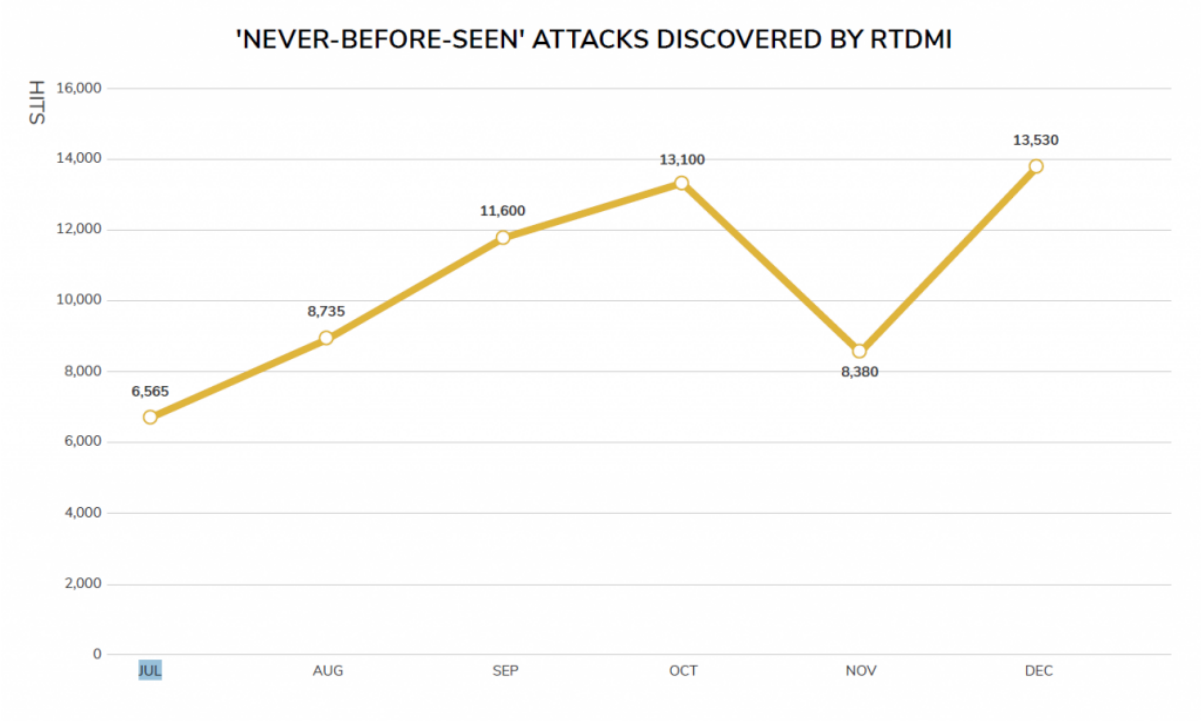
Bob Vankirk, Chief Revenue Officer della società di sicurezza. “Tra qualche tempo ci troveremo a fronteggiare attacchi che sfruttano queste tecniche per fare leva sulle vulnerabilità hardware dei processori”.

Uno scenario che, secondo Vankirk, va di pari passo con l’evoluzione delle tecniche di attacco utilizzate dai governi nella cyber-warfare, come dimostrano i recenti attacchi portati dagli Stati Uniti nei confronti dell’Iran.

“Per fronteggiare minacce come queste è necessario usare strumenti alternativi rispetto ai tradizionali antivirus” prosegue Vankirk. “Quello che serve è un sistema di analisi in tempo reale che permetta di individuare e bloccare gli attacchi automaticamente”.

Un percorso, questo, che SonicWall ha intrapreso l’anno scorso attraverso una tecnologia battezzata con il nome di **Real-Time Deep Memory Inspection (RTDMI)**. “L’uso dell’Intelligenza Artificiale ci permette di individuare i malware direttamente a livello di memoria” spiega **Luis Fisas** di SonicWall. “Un sistema molto più efficiente delle classiche sandbox sia in termini di accuratezza, sia in termini di rapidità nel rilevamento e nel contrasto all’attacco”.

La logica, spiegano Fisas e Vankirk, è piuttosto semplice: **lo stesso aumento del numero di attacchi, che genera una maggiore mole di dati da dare in pasto ai sistemi di AI, permette di migliorare le prestazioni del motore di scansione**.



A dimostrarlo, proseguono, è il numero (oggettivamente impressionante) di nuove tecniche di attacco individuate attraverso RTDMI nel corso del 2018.

Dalle parti di SonicWall, però, ritengono che l'approccio automatizzato "in tempo reale" sul quale stanno lavorando abbia un altro importante vantaggio. **Il sistema, infatti, permetterebbe di reagire agli attacchi anche in contesti che non possono contare su strutture dedicate**.

"Le piccole e medie aziende sono quelle che rischiano di più in questo scenario" puntualizza Vankirk. "Non potendo contare su risorse dedicate al contrasto degli attacchi informatici, hanno infatti bisogno di sistemi che possano bloccarli automaticamente".

Condividi l'articolo

Raffica di vulnerabilità nell'infrastruttura server Lenovo

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/02/affidarsi-allintelligenza-artificiale-si-puo-e-si-deve-fare/