Google lancia l'allarme: attenti alle app di Android preinstallate

Apr 02, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

L'azienda di Mountain View ha rilevato nel 2018 un aumento di app pericolose preinstallate sugli smartphone. Aumentano anche gli attacchi agli sviluppatori.

Se i controlli su **Google Play** per bloccare i malware sembrano (timidamente) migliorare, dalle parti di Google le preoccupazioni si stanno concentrando su forme più subdole e pericolose di infezione.

Nel report Android Security & Privacy 2018 I ricercatori di **Mountain View** segnalano un preoccupante aumento di "applicazioni potenzialmente dannose" che vengono preinstallate sugli smartphone **Android** o scaricate in seguito ad aggiornamenti del sistema operativo.

I responsabili non sono ovviamente i produttori di smartphone, ma gruppi di cyber-criminali che utilizzano tecniche di attacco rivolte alla **supply chain**, si inseriscono cioè nella filiera per infettare con malware applicazioni legittime che i produttori offrono ai loro utenti come parte degli strumenti predefiniti installati sul dispositivo.

Secondo i ricercatori, l'adozione di nuove strategie da parte dei pirati informatici è dovuta a due fattori. Il primo è l'aumento dei controlli, che secondo Google avrebbe portato a **una diminuzione del 20% del numero di app pericolose**

individuate nel corso del 2018 rispetto all’anno precedente.

Il secondo è un elemento di efficacia. Colpendo la filiera degli aggiornamenti, i cyber-criminali riescono a colpire un gran numero di utenti con il minimo sforzo.

Uno degli anelli deboli di questa catena sono gli sviluppatori, che spesso utilizzano degli **SDK (Software Development Kit)** che contengono backdoor o altre funzionalità nocive che cadono “a cascata” sulle applicazioni realizzate dagli sviluppatori stessi.

Google, si legge nel rapporto, sta cercando di arginare il fenomeno mettendo a disposizione dei suoi partner gli stessi strumenti di rilevamento e analisi che vengono utilizzati all’interno dell’azienda.

I ricercatori, però, concentrano la loro attenzione sui risultati ottenuti attraverso l’introduzione (e lo sviluppo) di **Google Play Protect**. Stando ai dati diffusi da Google, nel 2018 il software di sicurezza avrebbe bloccato l’installazione di **1,6 miliardi di applicazioni potenzialmente pericolose**.

Please follow and like us:

Il backup si sposta verso il cloud Hacking di stato italiano: il progetto Exodus spia anche i cittadini

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/02/google-lancia-lallarme-attenti-alle-app-di-android-preinstallate/

Hacking di stato italiano: il progetto Exodus spia anche i cittadini

Apr 01, 2019 Giancarlo Calzetta Attacchi, In evidenza, Malware, News, Privacy, RSS, Scenario 0

Qualche centinaio di utenti italiani sono stati inseriti per errore in un sistema per la sorveglianza di sospetti criminali sotto indagine. L'errore poteva essere facilmente evitato, ma scoperchia una situazione disastrosa nella gestione delle intercettazioni

elettroniche.

Quando si parla di hacking di stato, c'è sempre il pericolo che le cose **sfuggano al controllo** di chi dovrebbe usarle lecitamente e gli esempi non sono certo mancati in passato. Per questo non sorprende più di tanto scoprire che anche le forze dell'ordine italiane non hanno gestito in maniera impeccabile il loro sistema di intercettazione elettronica.

Come ci ha confermato qualche tempo fa un colonnello dei Carabinieri, al giorno d'oggi **una parte importantissima delle indagini viene condotta sui dispositivi elettronici dei sospettati** e le intercettazioni avvengono per lo più mettendo sotto sorveglianza lo smartphone degli indagati tramite l'uso di "captatori informatici" meglio conosciuti come spyware di Stato.

Secondo quanto riportato da un report dell'organizzazione no profit Security No Borders e dal sito Motherboard che per primo ne ha riportato i contenuti, uno dei sistemi usati dalle Forze dell'Ordine ha probabilmente spiato per errore alcune centinaia di utenti italiani che hanno scaricato delle app liberamente disponibili sul Play Store di Google.

Da quanto si legge nel rapporto, e sfruttando l'ottimo approfondimento di Alessandro Longo su La Repubblica, capiamo che Exodus è il sistema usato da molte procure per compiere intercettazioni a tutto tondo sui dispositivi Android dei sospettati: dalle attività su Facebook alle chat di Whatsapp, tutto poteva essere dirottato sui server dei gestori del servizio, incluse conversazioni telefoniche, rubrica dei contatti e ogni altro dettaglio. Non è chiaro se lo spyware fosse in grado di intercettare anche password inserite precedentemente alla sua installazione, mentre è lecito aspettarsi che il suo modulo di keylogging potesse intercettare quelle inserite in seguito.

Come veniva inoculato lo spyware e perché dei normali cittadini sono stati spiati

Secondo quanto riporta il pezzo su *La Repubblica*, Exodus viene usato dalle procure solo dietro autorizzazione a procedere di un giudice. A quel punto, sull'indagato vengono usate delle tecniche di ingegneria sociale per indurlo a scaricare **il malware, che era presente in una ventina di versioni sullo store ufficiale di Google** (a quanto pare a insaputa del grande G). Lo spyware era camuffato da app per migliorare le prestazioni dello smartphone, aggregatore di sconti e offerte o gestore della SIM. Non dimentichiamo che le aziende di telefonia italiane sono tenute a collaborare con le Forze dell'Ordine e quindi alcune comunicazioni arrivavano direttamente dall'operatore in modo da risultare più convincenti. Una volta installata, la prima app fungeva da dropper "condizionato", inviando a server di comando e **controllo il numero di IMEI e attendendo l'eventuale payload** da installare. Purtroppo, a quanto pare, il controllo degli IMEI non era attivo e quindi **chiunque scaricasse l'app da Google Play diventava vittima** di intercettazione.

Un fenomeno tutto italiano, i numeri dell'infezione e la reazione di Google

Lo spyware a cui ci riferiamo è esclusivo del nostro Paese. Ovviamente, moltissime delle forze dell'ordine del mondo hanno a disposizione strumenti simili, ma **Exodus è stato sviluppato in Italia** da un'azienda italiana, la **eSurv** di Catanzaro, e tutti i download sono stati effettuati nel nostro Paese. Addirittura, una delle chiavi crittografiche usate all'interno del codice è "Rino Gattuso", a confermare l'orgoglio campanilistico degli sviluppatori.

I ricercatori di **Security Without Borders** hanno contattato Google per segnalare quanto avevano scoperto e **Big G ha provveduto a eliminare dallo store oltre 20 varianti** dello spyware, aggiornando le sue misure di sicurezza per riconoscere futuri software simili. Purtroppo, non è disponibile un dato certo sul numero di download effettuati, ma i ricercatori hanno stimato che **in tutto si tratti al massimo di poco più di un migliaio**.

Ovviamente, tra questi ci sono gli indagati delle procure e quindi è impossibile sapere quanti normali cittadini siano caduti per errore in questo sistema, ammettendo anche l'improbabile caso che potrebbero non essercene stati. Di sicuro, i ricercatori che hanno fatto la scoperta hanno installato la prima app e ricevuto il payload, senza che **nessuno si preoccupasse di disinfettare poi il dispositivo da remoto**.

E qui si intravede il vero problema.

Una gestione troppo allegra delle intercettazioni

I captatori informatici, o spyware, sono strumenti molto potenti ed estremamente invadenti. Per questo andrebbero usati

con molte precauzioni. In primo luogo, è **impensabile che la app non venga sottoposta a un regolare controllo di sicurezza** da parte di personale competente delle Forze dell'Ordine. Un semplice test da parte di qualcuno che sapeva come funziona il sistema avrebbe scoperto immediatamente la falla e impedito che cittadini non coinvolti diventassero potenziali oggetti di intercettazione.

In secondo luogo, **è impensabile che il server di comando e controllo non sia sotto il diretto controllo di personale delle Forze dell'Ordine**. Tutti i riferimenti trovati dai ricercatori sembrano puntare a domini controllati direttamente da eServ. Come può lo Stato esser certo di come vengono gestiti i dati, estremamente sensibili, che lo spyware raccoglie?

Infine, ci si aspetterebbe che **i dati raccolti siano continuamente monitorati per riscontrare inesattezze e anomalie**, ma questo non è ovviamente accaduto dal momento il dispositivo infetto dei ricercatori è rimasto tale per diversi giorni (e probabilmente lo è ancora).

In altre parole, sembra che sebbene la gestione delle intercettazioni segua un iter corretto prima che queste avvengano, dopo l'ok **tutto accade in maniera sregolata o comunque poco appropriata**, probabilmente per una mancanza di cultura all'interno dell'organismo statale che regola queste attività.

Ci sembra urgente trovare un modo per **mettere in sicurezza questo importante strumento investigativo**, delegandone il controllo a personale competente all'interno della struttura delle Forze dell'Ordine.

Please follow and like us:

Falle critiche in VMware. Aggiornare di corsa!

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/01/hacking-di-stato-italiano-il-progetto-exodus-spia-anche-i-cittadini/

Google rende pubblica una falla zero-day nei router TP-Link

Mar 29, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Ennesimo sgarbo del Project Zero di Google: TP-Link non ha pubblicato l'aggiornamento entro i termini imposti dai ricercatori. Ora i pirati possono fare festa.

È una vulnerabilità di quelle che fanno venire i brividi e che consentirebbe a un pirata informatico di avviare l'esecuzione arbitraria di codice su un router attraverso la rete locale.

A soffrirne sono i router **TP-Link SR20 Smart Home** a causa di un processo chiamato **tddp (TP-Link Device Debug Protocol)** e che consente di inviare dei comandi al dispositivo.

La funzionalità, nel dettaglio, prevede la possibilità di inviare due tipi di comandi: il primo non richiede l'autenticazione come amministratore, il secondo invece sì.

Il problema è che uno dei comandi del primo tipo (**command 0x1f, request 0x01**) consente di inviare richieste tramite il **Trivial File Transfer Protocol (TFTP)**, che vengono elaborate da un interpreter con privilegi di root. Risultato: è possibile inviare qualsiasi tipo di comando al sistema, prendendo di fatto il controllo del dispositivo.

La vulnerabilità è stata individuata dal solito **Project Zero di Google**, che dopo averla comunicata a TP-Link ha concesso i canonici **90 giorni** all'azienda per sviluppare e distribuire la patch che la corregge. **Passata la scadenza, Matthew Garrett (il ricercatore di Google che ha individuato la falla) ha reso pubblica la falla zero-day**.

Non solo: giusto per rendere le cose più semplici ai pirati informatici che volessero sfruttarla, lo stesso Garrett ha pubblicato un Proof of Concept che permette di sfruttare l'exploit.

Non è la prima volta che il Project Zero pubblica i dettagli di vulnerabilità zero-day in seguito al mancato rispetto da

parte dei produttori delle rigide scadenze integrate nella loro policy di “responsible disclosure”.

La vittima preferita di Google, in questo senso è **Microsoft**, che ha visto pubblicare vulnerabilità relative ai suoi prodotti nel febbraio 2017 e nel febbraio 2018.

Anche se la previsione di deadline è uno strumento utile per vincere l’inerzia dei produttori nello sviluppo delle patch, una cosa è certa: i ricercatori del Project Zero non hanno molte chance di vincere il **premio simpatia** da parte dei colleghi.

Please follow and like us:

Cisco corregge 27 bug, ma due router rimangono vulnerabili

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/29/google-rende-pubblica-una-falla-zero-day-nei-router-tp-link/

Microsoft trova una voragine

di sicurezza in un driver Huawei

Mar 27, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il software di controllo della casa cinese consentiva a un utente senza privilegi di creare processi con privilegi di "super amministratore".

Forse non rappresentano una minaccia per la sicurezza nazionale come sostiene Donald Trump, di certo però i prodotti **Huawei** qualche problema ce l'hanno. Uno lo ha individuato **Microsoft**, che ha segnalato all'azienda cinese un pericoloso bug in uno dei suoi driver.

Il rilevamento di questa vulnerabilità, spiegano i ricercatori di Microsoft, è avvenuto grazie a una nuova funzione di monitoraggio chiamata **Microsoft Defender APT**, introdotta con la versione 1809 di Windows 10.

Da un punto di vista tecnico, infatti, la falla di sicurezza individuata nel driver Huawei funziona in maniera molto simile a **DoublePulsar**, uno dei tool di hacking utilizzati dalla **National Security Agency** e resi pubblici dal leak degli **Shadow Brokers** nell'estate del 2017.

L'exploit creato dagli 007 americani sfrutta infatti una tecnica che consente l'esecuzione di codice nel corso di una sessione **Windows** avviata da un utente senza privilegi di amministratore attraverso una tecnica piuttosto elaborata.

Il codice in questione viene iniettato all'interno di un processo dotato di privilegi e la sua esecuzione viene poi "forzata" attraverso un **APC** (asynchronous procedure calls),

una funzionalità di Windows che consente di interrompere un processo e modificarne la funzione per velocizzare alcuni tipi di operazioni.

Huawei, in pratica, ha creato un driver che usa la stessa tecnica. La funzione, in realtà, rappresenta una sorta di sistema di monitoraggio che controlla il funzionamento di un servizio integrato in **PC Manager**, il software di manutenzione del produttore cinese.

Nel caso in cui il servizio venga terminato per qualsiasi motivo, il driver prevede il suo riavvio attraverso l'iniezione in un altro processo e l'uso di un APC per richiamarlo.

Una scelta piuttosto curiosa, che **apre però la strada alla possibilità che questa procedura venga avviata da un malware**, che in questo modo potrebbe eseguire codice con privilegi di amministratore sfruttando il driver di Huawei come "trampolino di lancio".

Questo comportamento anomalo, però, è stato rilevato dal sistema di analisi euristica di Microsoft Defender APT. Dopo la segnalazione da parte di Microsoft, Huawei ha corretto i suoi driver attraverso **un aggiornamento distribuito a gennaio**. Chi ha eseguito l'update, di conseguenza, può considerarsi al sicuro.

Please follow and like us:

Hackerato l'update automatico di Asus: backdoor su migliaia di PC

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/27/microsoft-trova-una-voragine-di-sicurezza-in-un-driver-huawei/

Hackerato l'update automatico di Asus: backdoor su migliaia di PC

Mar 26, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Minacce, News, RSS 0

L’attacco ha preso di mira ASUS Live Update Utility, per distribuire il malware su 500.000 computer. Ma i pirati puntavano a 600 obiettivi mirati.

Parafrasando Mao, si potrebbe dire “colpirne 500.000 per infettarne 600”. E il fatto che secondo quanto riporta **Kaspersky** i protagonisti dell’attacco si un gruppo di cyber-spioni collegato al governo cinese, non fa che rendere più calzante la citazione.

Secondo gli esperti della società russa, infatti, gli autori di questo clamoroso attacco (battezzato **Operazione ShadowHammer**) che ha preso di mira **Asus** farebbero parte del gruppo **Barium APT**, noto appunto per i suoi legami con Pechino.

L’elemento sconvolgente di tutta questa vicenda riguarda le modalità che i pirati hanno usato per portare il loro attacco, violando addirittura il sistema di aggiornamento automatico (**ASUS Live Update Utility**) di una delle più grandi aziende produttrici di computer del mondo.

Gli hacker, stando alla ricostruzione degli analisti Kaspersky, sarebbero riusciti a impossessarsi di **un certificato digitale di Asus** e avrebbero usato vecchie versioni dei driver dell’azienda taiwanese per crearne una versione contenente una backdoor.

Avrebbero infine caricato i driver infetti sui server ufficiali di Asus che li hanno poi distribuiti come aggiornamento ad almeno 500.000 computer.

Una strategia di attacco decisamente efficace, anche perché aggiornamenti di questo tipo (relativi cioè a driver e firmware) con un certificato digitale valido e provenienza dai server ufficiali aggirano con facilità i controlli dei software antivirus.

L’obiettivo dei pirati, però, non era quello di colpire “a tappeto”, ma puntavano a una serie di obiettivi specifici. All’interno del malware che hanno distribuito, infatti, era presente un elenco di circa 600 **MAC Address**, il codice univoco che identifica un dispositivo collegato in rete.

La backdoor nascosta tra le pieghe del codice veniva attivata solo nel caso in cui il MAC Address del computer colpito corrispondeva a uno di quelli in elenco.

Insomma: i pirati sapevano esattamente quali computer volevano colpire e per raggiungerli non hanno esitato a pianificare un attacco clamoroso pur di raggiungere l’obiettivo.

D’altra parte il gruppo Barium APT è conosciuto per aver messo a segno attacchi “supply chain” anche in passato, come nel caso di **ShadowPad** (ne abbiamo parlato in questo articolo) e quello a **CCleaner** (i dettagli in questo articolo).

Resta da capire che rischi corranno gli altri utenti che sono stati colpiti dal malware. Secondo i ricercatori, infatti, potrebbe rimanere al suo posto anche se in uno stato “dormiente”. Una prospettiva per nulla rassicurante anche per chi non rientra nel selezionato gruppo di bersagli presi di mira dai pirati.

Secondo i ricercatori, il caso di Asus conferma ancora una volta il livello tecnologico di questo gruppo, che sembra essere in grado di escogitare strategie sempre più raffinate per raggiungere i suoi scopi.

Please follow and like us:

Falle di sicurezza in Java Card. A rischio anche le carte Bancomat

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/26/hackerato-lupdate-automatico-di-asus-backdoor-su-migliaia-di-pc/

Falle di sicurezza in Java Card. A rischio anche le carte Bancomat

Mar 25, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La tecnologia Oracle viene usata per consentire l'uso di applet Java su chip con memoria limitata. Vengono sfornate 6 miliardi di smart card all'anno.

SIM, carte Bancomat e centinaia di altre "smart card" contenenti chip rischiano di essere compromesse a causa di una serie di falle di sicurezza che interessano **Oracle Java Card**, una delle piattaforme più usate per consentire l'uso di applet Java.

Il sistema, progettato per garantire la massima sicurezza attraverso l'esecuzione in un ambiente virtuale (**Java Card VM**) è teoricamente protetto da una funzione di **Applet Firewall** che mantiene separate le applicazioni eseguite sul chip.

Recentemente, Oracle ha aggiornato Java Card per **poterla equipaggiare sui dispositivi IoT**, che potrebbero così godere di un maggior livello di sicurezza.

Secondo quanto riporta **Seclists.org**, però, la piattaforma contiene ben 18 vulnerabilità che consentirebbero di comprometterne il funzionamento, aprendo la strada a varie tipologie di abuso da parte dei cyber-criminali.

Sfruttando i bug della piattaforma, in particolare, sarebbe possibile accedere alla memoria delle card, ma anche **aggirare il firewall per l'esecuzione delle applet**.

Per farlo, un pirata potrebbe usare un lettore compromesso o creato ad hoc, che sarebbe in grado di avviare un programma malevolo sulla smart card.

Per fortuna, come spiegano gli stessi ricercatori, sfruttare i bug non è semplicissimo. Nel dettaglio, è necessario sapere quale firmware viene utilizzato nella smart card e conoscerne l'architettura.

Tutti i dettagli delle vulnerabilità sono state comunicate sia a Oracle, che sviluppa la piattaforma, sia a **Gemalto**, una delle società di sicurezza che utilizzano Java Card in maniera estensiva e che è coinvolta in virtù di alcuni bug relativi a due suoi prodotti: **GemXplore 3G V3.0-256K** e **3G USIMERA Prime SIM**.

Secondo gli esperti, l'aggiornamento di sicurezza per la

piattaforma di Oracle potrebbe essere distribuito il prossimo 16 aprile. Dal momento che stiamo parlando di smart card, però, le dinamiche sono ben diverse da quanto accade di solito e non si può certamente sperare che si possa procedere a degli update.

Insomma: è molto probabile che miliardi di smart card vulnerabili rimangano in circolazione per chissà quanto tempo.

Please follow and like us:

Attacco ai siti WordPress sfrutta uno zero-day in un plugin

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/25/falle-di-sicurezza-in-java-card-a-rischio-anche-le-carte-bancomat/

Attacco ai siti WordPress sfrutta uno zero-day in un plugin

Mar 22, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Due gruppi di pirati informatici hanno preso di mira Easy WP SMTP. Il bug nel popolare plugin consentiva di prendere il controllo totale del sito.

WordPress è di gran lunga il più popolare backend per la gestione di siti Internet. Stando ai dati di **W3Techs**, è usato per il **33,4% dei siti nel mondo**. Il Content Management System, però, ha anche un altro primato, decisamente meno entusiasmante: **il 90% dei siti hackerati nel corso del 2018 utilizzavano il CMS open source**.

La colpa sarebbe dei numerosi plugin disponibili per la piattaforma, i cui frequenti bug di sicurezza rappresentano una manna per i pirati informatici che puntano a compromettere i siti Web.

A confermare la teoria degli esperti di sicurezza arriva il caso di **Easy WP SMTP**, un plugin per WordPress che consente di configurare e gestire il servizio SMTP per l'invio delle email con più di **300.000 installazioni attive**.

Gli attacchi ai siti che utilizzano Easy WP SMTP sono stati rilevati per la prima volta venerdì scorso da **NinTechNet**, che ha pubblicato un alert sul suo sito Internet.

I cyber-criminali sfruttavano una vulnerabilità nella **versione 1.3.9 del plugin** relativa al sistema di importazione ed esportazione delle impostazioni, che in pratica consente le operazioni anche senza autenticazione.

Peggio ancora: il sistema di importazione consente di modificare la **wp_options table**, permettendo ai cyber-criminali di creare un nuovo utente con poteri di amministratore e **prendere il controllo del sito Internet**.

Gli attacchi, esaminati nel dettaglio anche dagli esperti di **WordFence** in questo report, sarebbero stati portati da due distinti gruppi di pirati informatici, che hanno utilizzato esattamente la tecnica individuata da NinTechNet nei primi attacchi.

I due gruppi, però, utilizzerebbero la falla di Easy WP SMTP per scopi diversi. Uno, infatti, si limiterebbe a inserire una backdoor che gli consente l'accesso. Il secondo, invece, utilizzerebbe i siti per **dirottare i visitatori su pagine Web contenenti malware**.

Il suggerimento, per tutti gli amministratori WordPress che utilizzano il plugin, è naturalmente quello di aggiornare immediatamente alla **nuova versione 1.3.9.1** ed eseguire una scansione e controllo del proprio sito per verificare che non sia già stato colpito.

Please follow and like us:

Attacco mirato all’Arabia Saudita. Gli esperti: “i pirati cercavano soldi”

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/03/22/attacco-ai-siti-wordpress-sfrutta-uno-zero-day-in-un-plugin/

Attacco mirato all’Arabia Saudita. Gli esperti: “i pirati cercavano soldi”

Mar 21, 2019 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS 0

L’operazione Bad Tidings attirava le vittime su un falso sito identico a quello del ministero degli interni. Ma davvero lo scopo è rubare denaro?

Leggi “Arabia Saudita” e immediatamente il pensiero va a intrighi internazionali, spionaggio e segreti militari. Invece, in questo caso, gli esperti sostengono che il movente

dei cyber-criminali che hanno preso di mira il governo saudita sia uno dei più banali: il denaro.

A individuare l'attacco sono stati i ricercatori di **Anomali Labs**, in collaborazione con la società di telecomunicazioni saudita. Secondo la ricostruzione che si può leggere nel report pubblicato dalla società di sicurezza, **l'attività dei pirati informatici ai danni del governo saudita si sarebbe protratta per più di tre anni**.

L'operazione, battezzata con il nome di **Bad Tidings** (brutte notizie), ha preso di mira diversi siti Web del governo saudita. In particolare, nel mirino dei cyber-criminali sono finiti il ministero dell'interno, il governo, il ministero degli esteri, quello dello sviluppo sociale e la Saudi British Bank.

La tecnica è quella classica del phishing, cioè della creazione di siti clonati dagli originali e il cui scopo è quello di rubare le credenziali degli utenti che vi si collegano.

Per rendere più credibile la loro azione, i pirati hanno sfruttato il fatto che i siti in questione utilizzano Unicode per rendere i caratteri arabi originali, utilizzando una tecnica di "punycode" per registrare domini che agli occhi dei visitatori appaiono identici a quelli originali.

Il sito più bersagliato è stato quello del ministero dell'interno, noto anche come **Absher**. Si tratta di un portale che offre una serie di servizi per i cittadini sauditi, tra cui la **richiesta dei visti e la registrazione di veicoli**.

L’obiettivo, secondo i ricercatori, sarebbe quello di rubare le credenziali che poi verrebbero “monetizzate” in qualche modo. A leggere i dettagli del report, però, qualche dubbio sui reali intenti dei pirati rimane.

Prima di tutto per la tipologia dei bersagli, ma anche per alcuni indizi che si leggono qui e là nel rapporto stesso. L’analisi delle registrazioni dei domini usati per gli attacchi, infatti, sottolinea come alcuni di questi facciano riferimento allo **Yemen**.

E visto che Yemen e Arabia Saudita sono coinvolti in **un conflitto armato** che dura da qualche tempo, il dubbio che gli interessi dei pirati non siano tanto rivolti al denaro ma a informazioni di intelligence è più che legittimo.

Please follow and like us:

Un antivirus per Android? Meglio sceglierlo bene…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/21/attacco-mirato-allarabia-saudita-gli-esperti-i-pirati-cercavano-solo-soldi/

Un antivirus per Android? Meglio sceglierlo bene…

Mar 20, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario 0

Una ricerca ha analizzato le funzionalità dei software di sicurezza gratuiti disponibili su Google Play. La maggior parte sono assolutamente inefficaci.

Niente da fare: di fronte alla parola "gratis" sono pochi quelli a resistere. Anche quando avrebbero ormai dovuto capire che nel mondo degli antivirus è piuttosto difficile che qualcuno proponga un prodotto gratuito davvero valido.

A maggior ragione quando si parla di applicazioni per **Android**, cioè un settore in cui gli sviluppatori "disinvolti" sembrano essere la maggioranza anche in settori meno "delicati" di quello della sicurezza. Il rischio, infatti, è quello di ritrovarsi con un antivirus che non funziona e, per unire al danno la beffa, che si limita a visualizzare annunci o disturbare l'utente.

A dare una sveglia ai "kamikaze del gratis" ci ha pensato **AV**

Comparatives, che in un report pubblicato su Internet mette a nudo la (in)efficacia degli antivirus gratuiti per Android.

Gli esperti di AV Comparatives ne hanno testati **250**. Risultato: solo 80 di questi sono stati in grado di individuare **più del 30%** dei malware usati come base di prova senza segnalare falsi positivi. L'elenco completo è disponibile nel report a questo indirizzo Internet.

I rimanenti **170** non sono invece stati in grado di raggiungere la soglia minima del 30% (ma teniamo presente che gli antivirus commerciali per PC di solito in questo tipo di test si collocano tra il 97 e il 99%) "inciampando" spesso in **falsi positivi**, cioè nella segnalazione di applicazioni assolutamente legittime come "potenzialmente pericolose".

Secondo i ricercatori, la maggioranza delle app in questione sono state realizzate da **programmatori amatoriali** o con il preciso e unico scopo di visualizzare sul dispositivo degli utenti pubblicità e collegamenti a siti commerciali.

Google ha già rimosso dal suo store i prodotti di 32

sviluppatori, ma secondo gli analisti di AV Comparatives **questo non basta**. Sarebbe infatti opportuno che lo stesso provvedimento fosse applicato anche agli altri antivirus farlocchi.

Al contrario di quanto frettolosamente scritto da qualche collega che ha evidentemente frainteso il senso della ricerca (sul Web abbiamo visto titoli del genere "Android, gli antivirus sono inutili") la ricerca dovrebbe in primo luogo sensibilizzare gli utenti Android riguardo **l'importanza di utilizzare un antivirus efficace e affidabile**.

Se poi aiutasse anche a evitare che qualcuno si faccia allettare dalle offerte gratuite che nascondono una fregatura (come nel caso delle tante app VPN gratis sempre per Android) potremmo pensare di aver fatto un reale passo in avanti nella sicurezza mobile.

Please follow and like us:

Nuova versione di Mirai prende di mira le grandi aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/20/un-antivirus-per-android-meglio-sceglierlo-bene/

Nuova versione di Mirai prende di mira le grandi aziende

Mar 19, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Il worm è stato aggiornato con nuovi exploit e tecniche di brute forcing alternative. Gli esperti: "punta a colpire i sistemi enterprise".

Non c'è pace per il mondo della **Internet of Things**. Come se non bastassero gli inciampi quotidiani riguardanti singole vulnerabilità e problemi di privacy, ora il settore IoT deve fare nuovamente i conti con attacchi massici portati con una vecchia conoscenza: **Mirai**.

Il worm, comparso per la prima volta **nell'autunno del 2016**, faceva leva in origine su una serie di credenziali di accesso predefinite a vari dispositivi IoT e ha permesso ai pirati informatici di creare una botnet con cui hanno portato uno degli attacchi DDoS più potenti della storia di Internet.

In seguito il worm si è evoluto, sfruttando nuove vulnerabilità ed exploit emersi nel corso dei mesi. Negli ultimi tempi, però, Mirai sembrava essere andato in letargo.

Ora un report della **Unit 42** di **Palo Alto Networks** lancia l'allarme su una nuova variante che i ricercatori hanno individuato fin dallo scorso gennaio. Il "nuovo" Mirai sfrutterebbe 27 exploit, 11 dei quali sarebbero nuovi di zecca.

In particolare, il worm prende di mira i sistemi **WePresent**

WiPG-1000 e le TV **LG Supersign**. Entrambi i dispositivi vengono utilizzati in ambito aziendale e se nel caso di LG la vulnerabilità (CVE-2018-17173) riguarda un bug che gestisce in maniera scorretta alcuni parametri e lascia aperta la via **all'esecuzione di codice in remoto**, per i sistemi WePresent si parla invece di una classica **iniezione di comandi**. Gli altri dispositivi presi di mira sono in maggioranza router e, tanto per cambiare, videocamere di sorveglianza.

Accanto ai nuovi exploit, sembra che i pirati abbiano trovato altre **credenziali predefinite** che non erano presenti nel "catalogo" originale di Mirai.

Le preoccupazioni degli esperti, però, si concentrano sulla natura dei device che Mirai compromette. Dal momento che le botnet Mirai vengono utilizzate principalmente per portare attacchi DDoS, il fatto che i dispositivi in questione siano collocati all'interno di reti aziendali è piuttosto preoccupante.

I bot controllati dai pirati, infatti, **avrebbero a**

disposizione collegamenti a banda larga che gli utenti domestici non hanno e l’efficacia degli attacchi DDoS portati con una botnet con queste caratteristiche potrebbe essere decisamente superiore a quanto abbiamo visto finora. ,

Please follow and like us:

Raffica di attacchi sfruttano WinRAR. Utilizzati più di 100 exploit

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/19/nuova-versione-di-mirai-prende-di-mira-le-grandi-aziende/