Trojan per iOS nascosto in 17 app disponibili sull'App Store

Ott 25, 2019 Marco Schiaffino In evidenza, Malware, News, RSS 0

Il malware sfruttava i dispositivi per garantire click pubblicitari e far incassare ai pirati informatici i proventi. Forse si tratta di un attacco supply chain.

Ancora malware all'interno di app per smartphone. Questa volta, però, le vittime non sono i (soliti) utenti Android ma i possessori di iPhone, che si sono ritrovati la bellezza di **17 app infette sullo store ufficiale di Apple**.

Come spiegano i ricercatori di **Wandera**, la società d sicurezza che ha pubblicato il report in cui è illustrata la vicenda delle app infette, il malware in questione è un trojan pensato per funzionare in background, aprendo pagine Web e simulando l'attività umana per fare click su annunci pubblicitari.

Una strategia piuttosto comune, che permette ai pirati informatici di incassare i proventi delle pubblicità truffando le aziende che pagano le inserzioni in questione.



L’elemento curioso è che, di solito, dalle parti di Apple sono piuttosto bravi a individuare e “rimbalzare” applicazioni che contengono questo tipo di malware. Tanto più che lo sviluppatore delle app (la società indiana **AppAspect Technologies Pvt**) ha qualche precedente in questo senso.

Secondo i ricercatori di Wandera, infatti, alcune app dello stesso sviluppatore erano state rimosse da **Google Play** in passato proprio a causa della presenza di codice malevolo con un comportamento simile. Di più: secondo gli esperti di sicurezza, i malware individuati in quell’occasione sfruttavano lo stesso server Command and Control a cui si collegavano le versioni per iOS.

L’episodio, che risale allo scorso agosto, aveva interessato 100 milioni di utenti Android che avevano scaricato le applicazioni in questione.

Secondo i ricercatori, non è chiaro se la backdoor inserita nelle app sia il frutto di un’azione da parte dello stesso sviluppatore o sia il risultato di un attacco **supply chain**, dovuto per esempio all’utilizzo di un Software Development Kit (SDK) che conteneva al suo interno il malware.

Questo tipo di “incidente”, infatti, si verifica con sempre maggiore frequenza a causa della pessima abitudine di

utilizzare strumenti di sviluppo di cui non è certificata l’origine o porzioni di codice sviluppati da terze parti.

Condividi l’articolo

CPDoS: la nuova tecnica di attacco prende di mira i Content Delivery Networks

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/25/trojan-per-ios-nascosto-in-17-app-disponibili-sullapp-store/

CPDoS: la nuova tecnica di attacco prende di mira i Content Delivery Networks

Ott 24, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I pirati sfruttano i sistemi di caching per impedire ai visitatori di accedere ai siti. I server non vengono sfiorati, ma gli utenti si trovano una pagina di

errore.

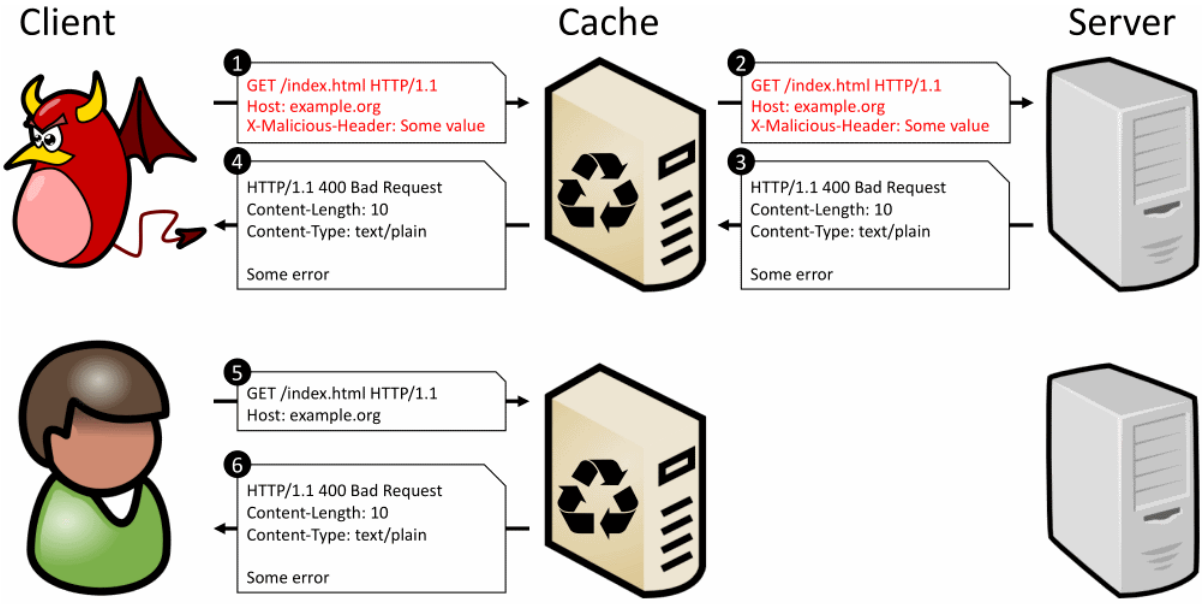
Il nome completo è **Cache-Poisoned Denial-of-Service** (per gli amici **CPDoS**) ed è una tecnica di attacco che sfrutta le caratteristiche dell'infrastruttura Web allo scopo di bloccare un sito Internet senza colpire direttamente il Web Server.

Il nuovo attacco Denial of Service sfrutta la struttura dei **Content Delivery Networks** (CDN) e, in particolare, la rete di server che forniscono servizi di caching per alleggerire il compito dei Web Server.

La rete messa in campo dai vari CDN ha lo scopo di rendere più efficiente il funzionamento del Web attraverso la distribuzione ai visitatori dei contenuti delle pagine Web senza doverle richiedere al Web Server, ma "pescandole" dalla loro memoria.

Come viene spiegato nel report pubblicato dai ricercatori dell'Università di Colonia, CPDoS sfrutta questo meccanismo per "avvelenare" la cache con pagine di errore. Per farlo è sufficiente inviare una serie di richieste con un http header corrotto che genera una risposta di errore del tipo "**400 Bad Request**".

Se le richieste arrivano in numero sufficiente, il CDN le memorizza fino al punto in cui tutti i visitatori del sito ricevono come risposta il messaggio di errore.



I ricercatori spiegano che l'attacco ha tre possibili varianti: **HTTP Header Oversize (HHO)**; **HTTP Meta Character (HMC)** e **HTTP Method Override (HMO)**.

Dal momento che i server usati dai CDN eseguono un refresh della cache solo periodicamente, la tecnica permetterebbe di "abbattere" un sito Internet senza dover necessariamente colpire il Web Server principale anche per lunghi periodi di tempo.

Fortunatamente, spiegano gli stessi autori del report, i sistemi per mitigare il rischio di attacchi di questo genere esistono. Basta, per esempio, modificare le impostazioni dei CDN per escludere i messaggi di errore dal sistema cdi caching.

Condividi l'articolo

La cyber immunità nei sistemi industriali.

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/24/cpdos-la-nuova-tecnica-di-attacco-prende-di-mira-i-content-delivery-networks/

MageCart e Carbanak lavorano insieme?

Ott 23, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS, Scenario 0

L'analisi degli esperti di sicurezza mette in luce un collegamento tra uno dei gruppi specializzati in skimming e la gang di cyber-criminali russa.

Il panorama della cyber-security, a volte, somiglia terribilmente a quello della criminalità organizzata degli anni '20 che abbiamo imparato a conoscere dai film di Hollywood.

Al posto di avere a che fare con personaggi come **Al Capone** e gli altri gangster resi immortali da libri e film, ci troviamo però ad avere a che fare con gang criminali la cui esistenza è certificata solo dalle ricostruzioni degli esperti di sicurezza che studiano i loro attacchi nel cyber-spazio.

Esattamente come succedeva all'inizio del secolo scorso, le connessioni tra i vari gruppi criminali hanno una certa importanza per chi cerca di comprendere le dinamiche del cyber-crimine.

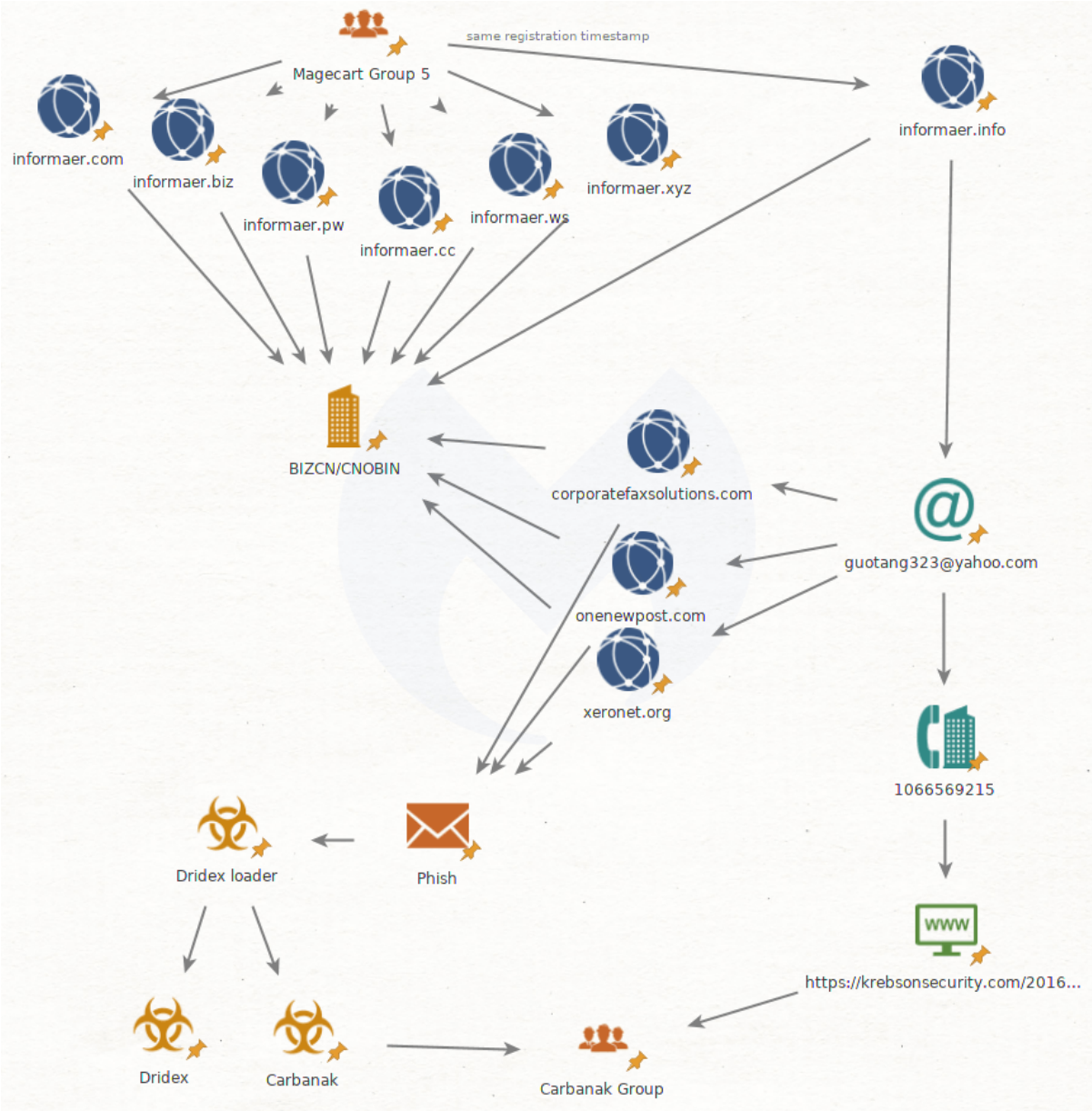
L’ultima scoperta, resa pubblica da **Kaspersky** con un report pubblicato sul blog ufficiale della società di sicurezza, riguarda un collegamento tra due dei più pericolosi gruppi di pirati informatici degli ultimi anni: **MageCart** e **Carbanak**.



Fino a oggi, infatti, le carriere criminali dei due gruppi sembravano muoversi su due binari separati. Carbanak, attivo soprattutto in Russia, è conosciuto (questo l’ultimo articolo in cui ce ne siamo occupati) per gli attacchi portati a più riprese nei confronti di **banche, bancomat, istituti di credito e gruppi commerciali**.

Più complicata la storia di MageCart. Se in un primo momento si pensava che le azioni di skimming sui siti di e-commerce (il furto di credenziali per il pagamento attraverso carte di credito – ndr) potessero essere ascrivibili a un unico soggetto, con il tempo gli esperti di sicurezza si sono resi conto che MageCart è in realtà una sorta di “community” a cui partecipano diversi gruppi. **Proprio uno di questi, identificato come “MageCart Group 5”, sembrerebbe avere dei legami piuttosto stretti con Carbanak**.

MageCart 5 è specializzato in attacchi supply-chain, cioè nella violazione di servizi utilizzati dai siti di e-commerce che permettono ai pirati informatici di colpire più siti Internet di commercio elettronico attraverso la compromissione degli strumenti utilizzati per gestire le transazioni e i pagamenti.



Il collegamento tra i due gruppi affonda le sue radici in un'analisi eseguita da un gruppo di ricercatori che hanno individuato dei domini Internet (registrati in Cina) utilizzati sia per le operazioni di MageCart, sia per la diffusione del trojan **Dridex**, un malware utilizzato dal gruppo Carbanak con grande frequenza.

L’indagine ha evidenziato come i due gruppi abbiano usato le stesse infrastrutture (registrate con la stessa email) per diverse campagne di distribuzione dei loro malware.

Difficile capire quanto sia stretto il legame tra i due gruppi, ma la scoperta dei ricercatori conferma il fatto che i cyber-criminali operano fianco a fianco nello stesso ecosistema, spesso scambiandosi (o condividendo) le infrastrutture usate per gli attacchi.

Condividi l’articolo

Server di un aeroporto europeo infettati dal crypto-miner Playerz

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/23/magecart-e-carbanak-lavorano-insieme/

Server di un aeroporto europeo infettati dal crypto-miner Playerz

Ott 21, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

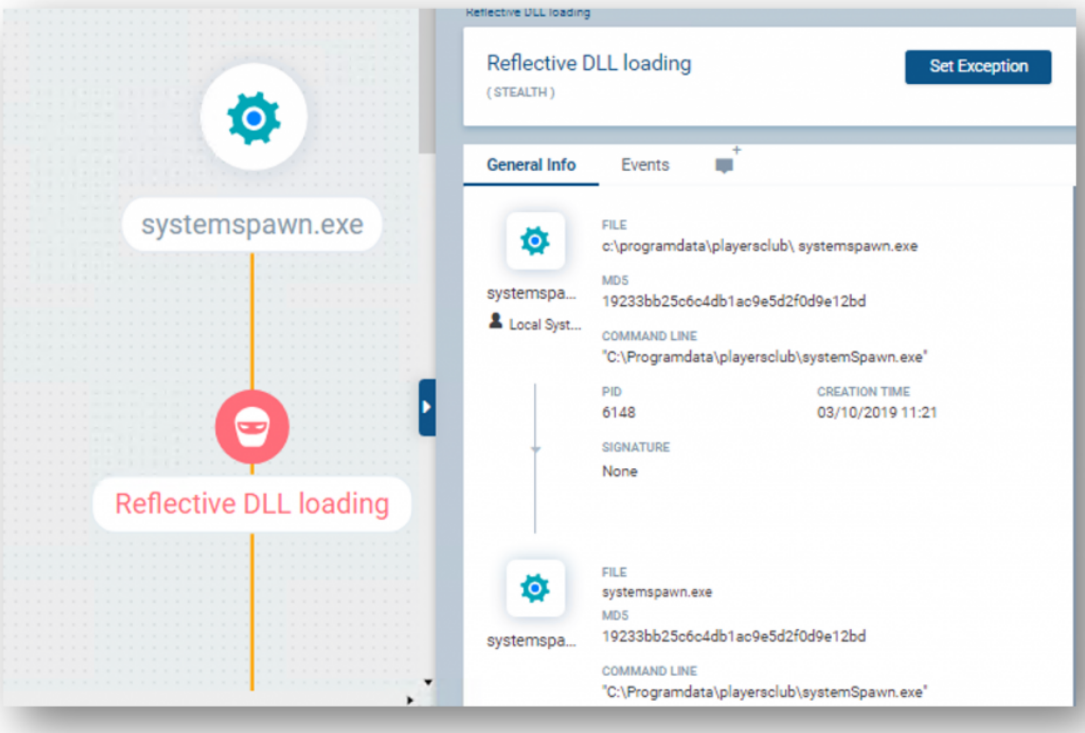
I pirati informatici hanno aggirato la protezione antivirus modificando alcuni aspetti marginali del malware. Gli esperti: "è rimasto attivo per mesi".

Sono riusciti a colpire il 50% delle workstation di un grande aeroporto europeo ma non avevano nessuna intenzione di compiere atti terroristici o azioni di sabotaggio. I pirati informatici hanno invece installato sui server una versione "modificata" di **Playerz**, un miner piuttosto conosciuto derivato da **XMRig**.

La presenza del codice malevolo sarebbe passata inosservata per mesi, fino a quando non è stata individuata dai ricercatori di **Cyberbit**, che in un report pubblicato sul loro blog illustrano come sia avvenuta la scoperta dell'attacco.

Gli analisti, nel dettaglio, spiegano che hanno rilevato l'attività "clandestina" grazie all'utilizzo di un sistema di algoritmi che eseguono un'analisi comportamentale a livello di kernel, notando un uso anomalo di **PAExec**. Lo strumento permette di avviare l'esecuzione di programmi per Windows su sistemi virtuali senza che sia necessaria la loro installazione.

Qualcosa che ai pirati informatici viene molto utile e che, in questo caso, è stato usato in abbinata a **Reflective DLL Loading**, una tecnica di iniezione di una libreria all'interno di un processo esistente.



Come sottolineano gli stessi ricercatori, l'uso di due tecniche di offuscamento come quelle citate lascia pochi dubbi sul carattere malevolo del programma avviato. Ma la parte surreale di tutta la vicenda è che i cyber-criminali sono riusciti ad aggirare i controlli degli antivirus installati sui server attraverso un trucchetto piuttosto banale: **modificare l'hash MD5 del file usato dagli antivirus come signature per identificarlo**.

Peggio ancora: i pirati non si sono nemmeno preoccupati di cambiare il nome del file originale (Player.exe) contando evidentemente sul fatto che le modifiche a livello di MD5 sarebbero state sufficienti a ingannare i software di protezione.

Una scommessa vinta, visto che secondo Cyberbit, l'analisi del file stesso attraverso gli strumenti di VirusTotal (la piattaforma che consente di eseguire una scansione dei file utilizzando tutti i motori di ricerca antivirus disponibili) avrebbe dato esito positivo solo in 16 casi su 73. **In altre parole: solo il 21% dei programmi di protezione erano in grado di rilevare un malware che aveva subito una modifica tutto**

sommato marginale.

Fortunatamente l'impatto di Playerz sui sistemi dell'aeroporto (nel report non viene specificato di quale si tratti) sono stati minimi e hanno provocato soltanto una degradazione delle prestazioni a livello di server.

Tutta la vicenda, però, è un sintomo preoccupante di quanto possa impattare l'uso di sistemi di protezione legacy, soprattutto se si considera che stiamo parlando di infrastrutture decisamente "sensibili".

Condividi l'articolo

Scoperto un malware "invisibile" che colpisce Apache

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/21/server-di-un-aeroporto-europeo-infettati-dal-crypto-miner-playerz/

Scoperto un malware "invisibile" che colpisce Apache

Ott 18, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

È stato battezzato p0sT5n1F3r= e consente di rubare tutti i dati che vengono inseriti dai visitatori senza lasciare alcuna traccia.

Un modulo persistente nascosto nella piattaforma Apache e in grado di memorizzare ed esfiltrare le informazioni sensibili inviate dai visitatori in un sito Web. È questa la sintesi del report con cui **Yarix** ha rivelato al mondo l'esistenza di **p0sT5n1F3r=**.

Il malware, che la società di sicurezza definisce un **APT** ma che sembra agire più che altro come uno **skimmer**, ha caratteristiche estremamente particolari che lo rendono difficilissimo da individuare.

Come spiegano i ricercatori, p0sT5n1F3r= è inserito in un modulo per **Apache** e agisce a livello server per sniffare le informazioni una volta che queste sono state decodificate dal Web Server. Le informazioni vengono memorizzate e poi trasmesse in modo da non destare sospetti negli amministratori.

La trasmissione, infatti, non avviene in maniera autonoma, ma in seguito a un collegamento avviato dall'esterno dai pirati informatici che, agli occhi di qualsiasi strumento di controllo, sembra del tutto legittimo.

Allo stesso modo, l'attività di sniffing non lascia alcuna traccia nei log di sistema e lo stesso codice del malware, che i ricercatori hanno sottoposto a scansione su **VirusTotal**, sfugge ai motori antivirus in commercio.



Insomma: p0sT5n1F3r= è in pratica uno sniffer quasi invisibile, che dale parti di Yarix hanno individuate dopo una complessa analisi che ha richiesto il superamento di **numerosi livelli di offuscamento** utilizzati dai pirati per nascondere la presenza del modulo.

Nel caso specifico, il malware è stato utilizzato per rubare informazioni sulle credenziali di pagamento inserite dai visitatori, ma la stessa tecnica potrebbe essere utilizzata per intercettare anche altri tipi di informazioni.

“È un testa a testa senza esclusione di colpi, quello tra hacker ed esperti di cyber security: ad ogni passo avanti nello sviluppo dei sistemi di protezione si contrappone una minaccia nuova. In questa logica si inserisce l’individuazione di un APT mai rilevato in precedenza a livello internazionale” commenta **Mirko Gatto**, CEO di **Yarix**.

“Averne identificato la comparsa ci dice molto sulla capacità offensiva ed organizzativa del cyber crime, ma al tempo stesso ci conforta rispetto alla possibilità di aver spuntato alcune delle armi degli hacker, per quanto riguarda questo inedito e pericoloso strumento di attacco”.

Condividi l’articolo

Il worm Graboid fa strage di Docker vulnerabili

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/18/scoperto-un-malware-invisibile-che-colpisce-apache/

Il worm Graboid fa strage di Docker vulnerabili

Ott 17, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Si installa e sfrutta i server per generare cripto-valuta utilizzando un sistema di attivazione casuale che lo rende più difficile da individuare.

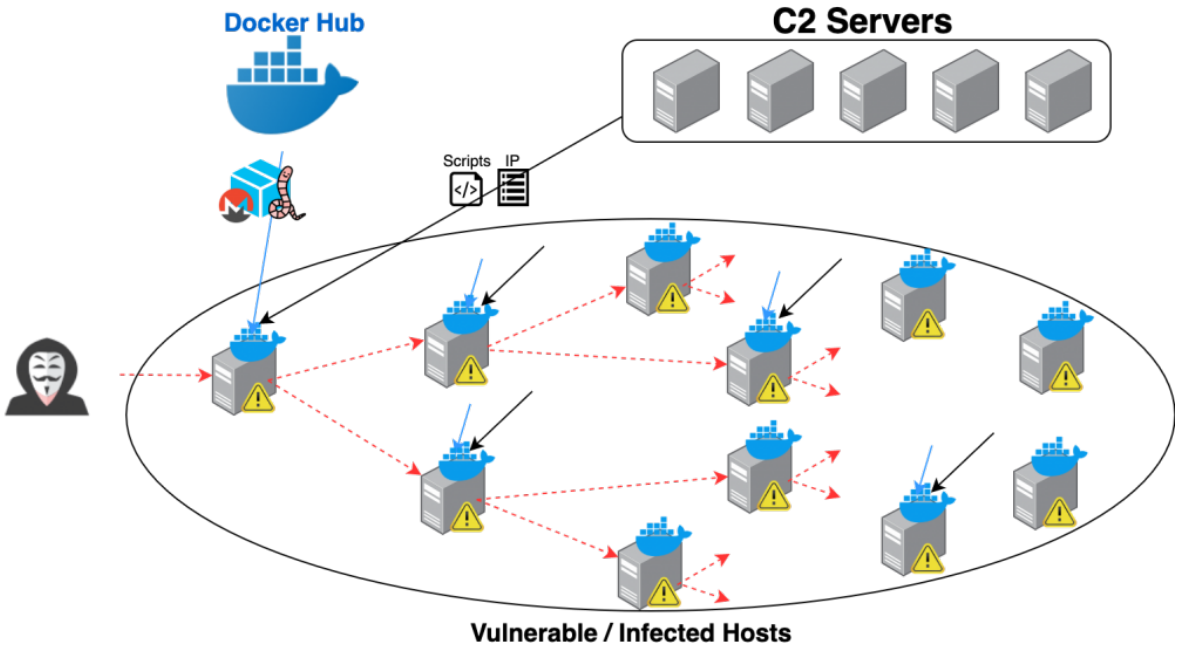
L'ennesimo attacco che prende di mira la piattaforma **Docker** questa volta vede come protagonista un worm. Si tratta di **Graboid**, un cryptominer che è stato scoperto dal team **Unit 42** di **Palo Alto Networks**.

Docker è una piattaforma estremamente diffusa, che permette di creare dei "pacchetti" chiamati container al cui interno ci sono applicazioni in grado di girare su cloud come se fossero su una macchina virtuale, ma senza che sia necessaria la presenza di un vero e proprio sistema operativo. **Negli ultimi mesi, però, Docker è diventata il bersaglio preferito dei pirati informatici**.

Nel caso di Graboid, l'attacco prende di mira le installazioni

Docker che non hanno protezione, cioè quelle per cui gli amministratori **non hanno predisposto un sistema di autenticazione per il caricamento dei pacchetti**. Stando a quanto raccontano i ricercatori nel report pubblicato sul blog di Palo Alto Network, in circolazione ce ne sarebbero almeno 2.000.

Il container usato dai cyber-criminali contiene due moduli. Il primo è programmato per diffondere il worm individuando nuovi bersagli attraverso le indicazioni che provengono dal server Command and Control. Il secondo contiene invece un miner **xmrig** che sfrutta la potenza del server compromesso per generare **Monero**, la cripto-valuta preferita dai pirati informatici.



L'attacco avviene in sei passaggi:

1 Il pacchetto **pocosow/centos:7.6.1810** viene installato utilizzando dei comandi in remoto sull'host vulnerabile. Al suo interno è presente uno strumento che permette di comunicare con gli altri host Docker.

2 In seguito viene avviato lo script **/var/sbin/bash**, che scarica quattro script shell (**live.sh**, **worm.sh**, **cleanxmr.sh**, **xmr.sh**) dal server Command and Control (c2) e li esegue uno per uno.

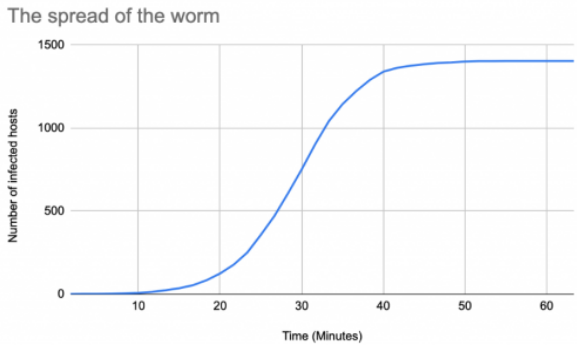
3 Lo script **live.sh** invia al server C2 informazioni sul numero di CPU disponibili sull'host compromesso.

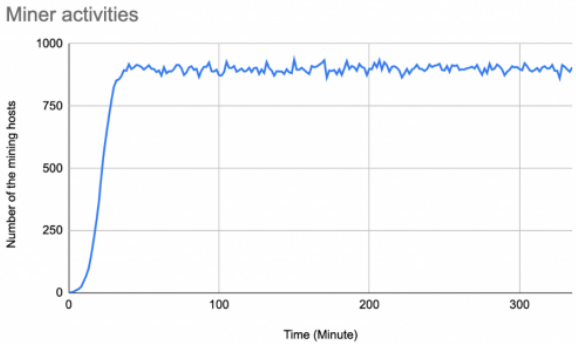
4 L'esecuzione di **worm.sh**, invece, avvia il download di un elenco con oltre 2.000 indirizzi IP. Si tratta degli host Docker vulnerabili all'attacco. Lo script comincia a inviare i comandi in remoto per installare il pacchetto infetto su ogni host indicato nell'elenco.

5 Qui le cose si fanno strane: cleanxmr.sh è infatti programmato per scegliere casualmente un host dall'elenco e bloccare il miner attivo al suo interno.

6 L'ultimo script (**xmr.sh**) seleziona casualmente un host dall'elenco e installa il container **gakeaws/nginx** che contiene il miner.

Questa strana procedura fa in modo che il funzionamento del modulo di crypto-jacking sia molto particolare. Si attiva per periodi di tempo limitati e lo fa in modo apparentemente casuale. **Dalle simulazioni effettuate dai ricercatori, i miner sono attivi solo per il 65% del tempo per periodi di tempo che in media non superano i 4 minuti**.





Probabilmente la tecnica punta a rendere più difficile l'individuazione del miner, che solitamente viene effettuata attraverso l'analisi dei carichi di lavoro delle CPU. Non solo: visto che l'attività di mining non comincia subito dopo l'installazione, l'analisi dei log non mostra un'immediata corrispondenza tra il download di un pacchetto e l'aumento dell'attività della CPU.

Il loro attacco, però, è decisamente efficace. **Secondo la Unit 42, i pirati hanno a disposizione 1.400 processori e una potenza di calcolo complessiva di circa 900 CPU**. Tradotto in parole povere: stanno intascando un mucchio di soldi.

Condividi l’articolo

I pirati attaccano i programmi fedeltà

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/17/il-worm-graboid-fa-strage-di-docker-vulnerabili/

Uno strano bug di Linux consente l’invio di comandi root

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

Basta inserire un ID particolare per elevare i privilegi di un utente a root. Per fortuna la falla

riguarda solo i sistemi con (improbabili) impostazioni personalizzate.

Secondo i ricercatori di sicurezza, il bug individuato in **Linux** non dovrebbe creare troppi problemi a livello globale. Nonostante riguardi una tecnica che permette di elevare i privilegi di un utente, infatti, la falla di sicurezza (CVE-2019-14287) è stata infatti classificata da **Red Hat** con uno score di "solo" **7.8** su 10.

Il motivo? Un eventuale exploit funziona solo se l'amministratore ha impostato la funzione Sudo (quella che consente di avere privilegi di super utente – ndr) per consentire a qualsiasi utente all'interno di un gruppo l'esecuzione di comandi come se fosse un altro utente.

L'impostazione, che può essere inserita nel file **sudoers** che regola l'uso di Sudo, consente in pratica di concedere a tutti gli utenti la possibilità di controllare gli altri utenti (con l'eccezione del super user) utilizzando **RunAs**.



Nelle intenzioni, quindi, una impostazione di questo genere consente un ampio campo di azione, ma esclude i privilegi di

root. **Peccato che le cose non funzionino esattamente così**.

Se un utente esegue un comando impostando l'ID utente con il valore -1 (il comando completo è **sudo -u#-1**), infatti, acquisisce automaticamente i privilegi di root. Il valore -1, infatti, viene interpretato come "non cambiare l'ID dell'utente". **E visto che Sudo viene avviato come root, il sistema esegue il comando con i massimi privilegi**.

L'elemento curioso è che lo stesso accade se si usa il comando **-u#4294967295**, che in 32 bit corrisponde proprio a -1. Il bug è stato prontamente corretto con il rilascio di Sudo **1.8.28**. Ci si aspetta, quindi, che tutti gli aggiornamenti per le varie distro lo includano.

La speranza, in ogni caso, è che i sistemi potenzialmente vulnerabili siano pochi, se non pochissimi. La stessa idea di permettere a qualsiasi utente di eseguire qualsiasi comando come se fosse un altro, da un punto di vista logico, è piuttosto bizzarra.

Condividi l'articolo

Apple aiuta la Cina a tracciare gli utenti? No, però…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/16/uno-strano-bug-di-linux-consente-linvio-di-comandi-root/

Apple aiuta la Cina a tracciare gli utenti? No, però…

Ott 15, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Scenario 0

L'azienda di Tim Cook smentisce le voci riguardanti rischi per la privacy legati all'uso della navigazione sicura su Safari in Cina. Nessun tracciamento, ma c'è il rischio censura.

Ogni volta che si parla di **Apple** e della sua attività in **Cina**, spuntano puntualmente polemiche e accuse. L'azienda di Cupertino, in particolare, viene considerata da molti un po' troppo accondiscendente con le richieste del governo di Pechino.

Per rimanere solo ai casi più recenti, ad Apple viene rinfacciato per esempio di aver rimosso le app con servizi di VPN per gli utenti cinesi, di aver eliminato dal suo store l'applicazione usata dai manifestanti a **Hong Kong** per tracciare i movimenti della polizia e di aver assecondato l'eliminazione di ogni riferimento a **Taiwan** (come l'emoticon la bandiera taiwanese) sui suoi dispositivi.

L'ultima polemica in ordine di tempo riguarda **Safari** e la funzionalità di navigazione sicura, che sul browser Apple è impostata come opzione predefinita.

Si tratta di una funzione presente in tutte le versioni di Safari e che ha come scopo quello di bloccare la navigazione e inviare una segnalazione all'utente quando si sta per collegare a un sito Internet potenzialmente pericoloso.

Nel resto del mondo, Apple utilizza a questo scopo un database gestito da **Google**. In Cina, dove Google è bloccato, utilizza però il servizio di **Tencent**, azienda cinese molto “vicina” al governo di Pechino.



L’accusa, ripresa da molti siti di news generalisti, è che in questo modo Apple permetta alle autorità cinesi di tracciare la navigazione degli utenti Apple sul territorio della Repubblica Popolare.

L’azienda di Tim Cook, però, respinge ogni accusa. La funzione di navigazione sicura (nelle impostazioni è indicata come “Avvisi siti web fraudolenti”) funzionerebbe infatti attraverso un meccanismo che non comporta la condivisione di alcuna informazione con il soggetto che gestisce il database dei siti considerati pericolosi.

La lista degli indirizzi a rischio, infatti, verrebbe invece inviata al browser sotto forma di hash e confrontata in locale con quelli che l’utente visita. **Insomma: in questo caso**

Tencent non avrebbe alcun modo per tracciare la navigazione degli utenti su iOS o macOS.

“Apple tutela la privacy degli utenti e protegge i dati con Avvisi siti web fraudolenti, una funzione di sicurezza che individua i siti Web noti per essere pericolosi” spiegano dalle parti di Cupertino con un comunicato.

“Quando la funzione è attiva, Safari controlla l’URL del sito confrontandola con un lista di siti Internet conosciuti e visualizza un avviso se l’indirizzo corrisponde a una pagina che può contenere contenuti fraudolenti. Per farlo, Safari riceve una lista da Google e, per i dispositivi che risultano essere in Cina, da Tencent. L’URL non viene mai condivisa con il soggetto che fornisce la lista e la funzione”.

Resta, naturalmente, il problema della possibile censura di siti Internet che vengono indicati come pericolosi quando la loro colpa è solo quella di proporre contenuti sgraditi al governo. Nell’ecosistema dell’Internet cinese, però, non si tratta certo di una novità e, come ricorda la stessa Apple nel comunicato, la funzione di navigazione sicura può essere disabilitata dalle impostazioni di Safari.

Insomma: se i problemi legati alla presenza di Apple in Cina rimangono, per questa volta si è trattato della classica tempesta in un bicchier d’acqua.

Condividi l’articolo

Per l’Italia Simjacker è un problema

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/15/apple-aiuta-la-cina-a-tracciare-gli-utenti-no-pero/

Per l'Italia Simjacker è un problema

Ott 14, 2019 Marco Schiaffino Attacchi, In evidenza, News, Privacy, Vulnerabilità 0

Nuovo rapporto sulla vulnerabilità che permette di spiare i telefoni attraverso la SIM. I paesi interessati sono solo 29 e l'Italia è tra questi.

Buone notizie (per il mondo) sulla vicenda **Simjacker**. Stando a un nuovo report di **AdaptiveMobile Security**, infatti, la vulnerabilità individuata lo scorso settembre dai ricercatori della società di sicurezza impatterebbe solo 61 operatori mobile in 29 paesi. **La cattiva notizia (per l'Italia) è che il nostro paese rientra nell'elenco**.

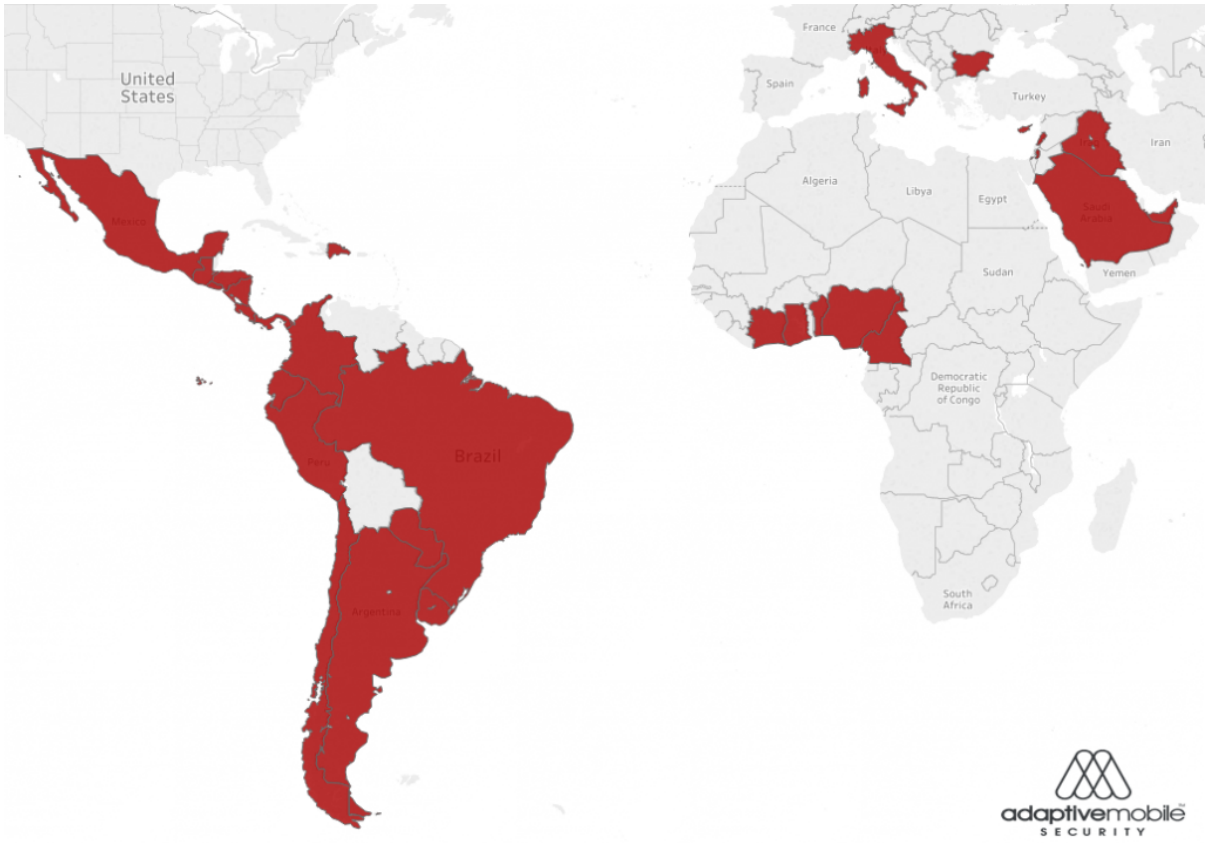
Come abbiamo spiegato in questo articolo, Simjacker è una falla di sicurezza che fa leva su un'applicazione integrate nelle SIM che non riceve alcun aggiornamento dal 2009 e può essere sfruttata per inviare comandi tramite degli SMS contenenti un particolare codice.

I messaggi, la cui ricezione non viene notificata in alcun modo al proprietario del telefono, permettono di eseguire numerose operazioni, come "estrarre" la posizione del telefono

attraverso il GPS, avviare telefonate o aprire collegamenti nel browser.

In altre parole, Simjacker può essere usato per monitorare gli spostamenti di una persona, mettere a segno truffe telefoniche "forzando" chiamate verso numeri a pagamento o **installare un malware attraverso una pagina Web infetta**.

L'approfondimento dei ricercatori si è concentrato sulla mappatura degli operatori telefonici mobili che usano ancora **S@T Browser**, l'applicazione che consente l'invio dei comandi in remoto. Il risultato è piuttosto sorprendente.



I 29 paesi a rischio, infatti, sono per la maggior parte in Sud America, mentre sono esclusi Stati Uniti e la stragrande maggioranza dei paesi europei. **Nel vecchio continente le nazioni a rischio sono solo tre: Bulgaria, Cipro e Italia**.

Il report di AdaptiveMobile Security non specifica quali siano le compagnie telefoniche interessate, ma fa una stima complessiva sul numero di SIM vulnerabili all'attacco. **I**

ricercatori parlano di un numero variabile tra i 500 e gli oltre 800 milioni di SIM.

L’approssimazione è dovuta al fatto che anche gli operatori che usano S@T Browser, in molti casi lo hanno dismesso e, di conseguenza, il problema potrebbe essere presente soltanto sulle vecchie SIM.

Per il momento, nessuno ha registrato ondate di attacchi che sfruttano Simjacker. Gli unici episodi si sarebbero verificati in Messico, Colombia e Perù.

Condividi l’articolo

Apple aiuta la Cina a tracciare gli utenti? No, però… Red Team o Blue Team? Adesso c’è anche il Purple Team… ed è una macchina

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/14/per-litalia-simjacker-e-un-problema/

Red Team o Blue Team? Adesso c’è anche il Purple Team… ed

è una macchina

Ott 10, 2019 Giancarlo Calzetta Approfondimenti, In evidenza, RSS, Software, Tecnologia 0

Le operazioni di Red Teaming sono importantissime, ma costano molto. FireEye ha appena lanciato una soluzione efficace e moderna che costa molto meno.

Le operazioni di **Red e Blue teaming** dovrebbero essere il pane quotidiano per i responsabili di sicurezza delle grandi aziende, ma troppo spesso non è così. Sebbene tutti gli esperti di sicurezza ne riconoscano l'efficacia, hanno il difetto di costare molto perché si basano sull'intervento diretto di una squadra che si mette al lavoro per testare o affinare le difese. Il risultato è che **diventano operazioni sporadiche**, comunque molto utili ma che non garantiscono una efficacia nel tempo.



“Sebbene l’efficacia del red teaming sia riconosciuta e apprezzata” – ci dice Grady Summers di FireEye – “la rete non resta immutata per lunghi periodi di tempo. Basta aggiungere un componente o cambiare la configurazione di un altro per rischiare di escludere appliances o contromisure dal flusso di dati aziendali”.

Per questo **servirebbe un sistema più snello**, ma ugualmente efficace, per testare più spesso, se non addirittura in maniera continua, la resistenza delle difese.

Il nuovo servizio di FireEye, Purple Team, fa proprio questo, fornendo **un assessment red team e blue team per lo più automatizzato**, basato sull’infrastruttura di Verodin.

“Sul framework Verodin” – “continua Summers – “viene impostata la simulazione di una serie di attacchi a cui l’azienda deve rispondere in maniera continua. Dove dovessero risultare delle falle, il nostro sistema è già pronto a passare a una operazione di blue teaming per suggerire al personale dell’azienda quali contromisure mettere in atto”.

Sebbene le operazioni completamente automatizzate facciano alzare ben più di un sopracciglio agli esperti, in questo caso gli **attacchi simulati** possono contare su di un elemento che li rende molto interessanti: la connessione continua con il database centrale di FireEye.

“Le operazioni di attacco simulato” – conferma Summers – “vengono elaborate dal nostro sistema centrale, basandosi sugli indicatori di compromissione e sui pattern che rileviamo negli attacchi che coinvolgono i nostri clienti. Questo significa che quando identifichiamo un tipo di attacco, viene automaticamente creato lo scenario che Purple Team poi mette in esecuzione negli ambienti aziendali. In questo modo, c’è una risposta velocissima all’evoluzione degli attacchi e si è in grado di capire se l’infrastruttura aziendale sarebbe vulnerabile o no”.

L’offerta del **Purple Team Assessment** è già disponibile ed è declinata in due versioni: una versione “one shot”, simile per approccio a quelle di red e blue team tradizionali e una più sensata denominata “Continous Purple Team Assessment” che si estende sue periodi da tre a sei mesi.

“In Italia” – dice Marco Riboli di FireEye – “tendiamo a suggerire la versione continuous de Purple Team assessment perché è quella economicamente più vantaggiosa. Sfruttare le potenzialità del framework Verodin su una operazione continuata nel tempo è molto più efficiente rispetto a una operazione one shot”.

La tipologia di azienda che può essere interessata alle operazioni di Purple Team Assessment è di grandi dimensioni, dato che l’investimento è comunque significativo, ma val la pena di pensare a una visione d’insieme più vasta in cui questa iniziativa possa fare da “testa di ponte” per testare l’utilità di Verodin nel nostro ambiente informatico.

Condividi l’articolo

Analisi UE dei rischi legati al 5G, ma l’obiettivo è Huawei

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/10/red-team-o-blue-team-adesso-ce-anche-il-purple-team-ed-e-una-macchina/