Database ElasticSearch (ancora) nel mirino dei pirati

Giu 15, 2020 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Malware, News, RSS, Scenario 0

I cyber criminali utilizzano strumenti di scansione che permettono di rilevare in tempi record i server esposti e colpiscono immediatamente.

Non si arrestano gli attacchi ai server **ElasticSearch** esposti su Internet a causa di configurazioni errate. Anzi: secondo quanto riportano i ricercatori di **Comparitech**, che hanno provato a fare un piccolo esperimento per testare la capacità di reazione dei pirati informatici.

La società di sicurezza ha messo online un honeypot, cioè un server ElasticSearch utilizzato come "esca" per registrare gli attacchi portati dai cyber-criminali. Il risultato dell'esperimento è sconcertante: il server in questione ha infatti subito **una media di 18 attacchi al giorno**.

L'elemento ancora più curioso riguarda il fatto che i pirati informatici sono istati in grado di individuare il server molto più rapidamente di qualsiasi motore di ricerca.

Gli analisti di Comparitech lo hanno messo online l'11 maggio. Mentre **Shodan** ha impiegato cinque giorni per individuarlo, **il primo attacco dei pirati è arrivato dopo solo 8 ore e 35 minuti**.

La maggior parte degli attacchi, si spiega nel report, avevano l’obiettivo di sfruttare una falla di sicurezza risalente al 2015 per installare sui server dei miner per la generazione di cripto-valuta. Altri, invece, puntavano a sfruttare la stessa vulnerabilità (CVE-2015-1427) per rubare le credenziali di accesso.

La tipologia di attacchi, in ogni caso, è stata estremamente varia e il “colpo di grazia” è arrivato il 29 maggio, quando **un bot ha individuato il server e ha cancellato tutti i file** lasciando al loro posto un messaggio con una richiesta di riscatto.

Una strategia cui abbiamo già assistito in passato (ne abbiamo parlato in questo articolo) e che, a quanto pare, non è affatto passata di moda.

Insomma: chiunque gestisca un server ElasticSearch farà meglio a predisporre tutte le misure di sicurezza possibili e immaginabili. Dopo questo esperimento, infatti, una sola cosa è certa: sarà sottoposto a un vero e proprio bombardamento di attacchi.

Condividi l’articolo

EKANS: come funziona il ransomware che ha colpito Enel e Honda

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/06/15/database-elasticsearch-ancora-nel-mirino-dei-pirati/?utm_source=rss&utm_medium=rss&utm_campaign=database-elasticsearch-ancora-nel-mirino-dei-pirati

EKANS: come funziona il ransomware che ha colpito Enel e Honda

Giu 12, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati che hanno preso di mira le due aziende utilizza un malware progettato per portare attacchi estremamente specifici.

Doppio attacco dei pirati informatici di **EKANS**, che questa volta hanno messo nel mirino due colossi industriali di caratura internazionale come **Honda** ed **Enel**, colpita domenica scorsa.

Il gruppo di cyber criminali, specializzati negli attacchi alle aziende, hanno utilizzato il solito ransomware, in grado di mettere K.O. i sistemi informatici delle aziende nel solito

schema estorsivo per cui alle imprese viene chiesto un riscatto per decodificare i dati “presi in ostaggio”.

Stando a quanto riportano le agenzie, le due aziende sono riuscite a contrastare efficacemente l’attacco e ripristinare il funzionamento delle infrastrutture IT in tempi piuttosto rapidi. L’intera vicenda, però, dimostra il livello di professionalità e specializzazione raggiunto dai pirati informatici.

L’analisi di EKANS, infatti, dimostra l’analisi condotta da come gli autori del ransomware abbiano affinato le loro tecniche per colpire con precisione millimetrica le vittime. Il malware, distribuito probabilmente attraverso la compromissione di collegamenti **RDP (Remote Desktop Protocol)** integra una serie di funzioni estremamente particolari.

Come spiegano i ricercatori di Dragos nel loro report, EKANS è pensato specificatamente per colpire sistemi industriali e unisce caratteristiche mutuate da altri malware simili. **Altri ricercatori hanno sottolineato come il malware utilizzi anche una serie di controlli incrociati, come l’analisi della rete in cui viene iniettato, per verificare di aver colpito il bersaglio giusto**.

Allo stesso modo, il ransomware adotta una serie di tecniche per eliminare eventuali ostacoli alla sua attività, come terminare particolari processi attivi sulla macchina infetta,

compresi alcuni che bloccano di fatto la produzione negli impianti.

Insomma: si tratta di una sorta di “specialista” che i suoi autori utilizzano per portare attacchi attentamente pianificati. In questo caso, Honda ed Enel sono riusciti a contrastarli. L’allerta per tutte le aziende del settore industriale, però, deve rimanere ai massimi livelli.

Condividi l’articolo

Truffa su YouTube sfrutta il progetto SpaceX per raccogliere bitcoin

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/12/ekans-come-funziona-il-ransomware-che-ha-colpito-enel-e-honda/?utm_source=rss&utm_medium=rss&utm_campaign=ekans-come-funziona-il-ransomware-che-ha-colpito-enel-e-honda

---

Truffa su YouTube sfrutta il progetto SpaceX per raccogliere bitcoin

Giu 11, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS 0

I pirati hanno utilizzato tre canali YouTube per avviare una falsa raccolta fondi che ha fruttato più di 150.000 dollari in cripto-valuta.

Una truffa da 150.000 dollari (in bitcoin) portata a termine attraverso la compromissione di tre canali **YouTube** e una buona dose di inventiva. È questo lo scenario che descrive **Bleeping Computer** in un articolo in cui rivela i dettagli dell'ennesimo colpo messo a segno da un gruppo di pirati informatici.

Tra gli anglosassoni viene chiamata "giveaway" ed è una procedura (truffaldina) ormai ben conosciuta. In pratica, i cyber criminali pubblicizzano una campagna in cui verrebbero "regalati" bitcoin per le più svariate ragioni e chiedono alle vittime Peccato che per ricevere il "regalo" **è necessario inviare una prima somma che, teoricamente, dovrebbe consentire al "benefattore" di avere le coordinate per inviare la moneta virtuale**.

Il meccanismo, di solito, sfrutta il nome di qualche personaggio famoso e questa volta (non è la prima) è toccato a **Elon Musk**.

I cyber criminali, infatti, hanno "trasformato" tre canali YouTube in veicoli apparentemente collegati a **SpaceX**, l'impresa spaziale del creatore di **Tesla**, sfruttando la notorietà della recente impresa che ha portato al lancio di astronauti nello spazio.

I canali YoutTube, che fino allo scorso 8 giugno erano individuati con i nomi di “**Juice TV**”; “**Right Human**” e “**MaximSakulevich**” hanno improvvisamente cambiato nome in “SpaceX” e i follower si sono trovati davanti una serie di interviste di Elon Musk e spezzoni video relativi al progetto SpaceX.

Il trucchetto, adottato abbastanza frequentemente, è simile a quello i truffatori usano su altri social network: modificare i contenuti di un canale che ha migliaia di iscritti (quelli in questione ne avevano centinaia di migliaia) per veicolare contenuti completamente differenti rispetto a quelli originali.

In questo caso, però, i pirati informatici hanno sfruttato la tecnica per avviare una raccolta di bitcoin utilizzando lo

schema del giveaway, che (misteriosamente) sembra continuare a fare presa su un buon numero di utenti.

Il risultato, dal punto di vista della raccolta, è quasi sconcertante: sommando i tre conti bitcoin associati ai canali, i truffatori sono riusciti a intascare la bellezza di **150.000 dollari**.

Condividi l’articolo

EKANS: come funziona il ransomware che ha colpito Enel e Honda
F-Secure: ecco come cambia la protezione della mail su cloud

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/11/truffa-su-youtube-sfrutta-il-progetto-spacex-per-raccogliere-bitcoin/?utm_source=rss&utm_medium=rss&utm_campaign=truffa-su-youtube-sfrutta-il-progetto-spacex-per-raccogliere-bitcoin

---

F-Secure: ecco come cambia la protezione della mail su cloud

Giu 10, 2020 Marco Schiaffino Gestione dati, In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

La migrazione dei servizi di posta elettronica su piattaforme cloud impone un cambio di paradigma nelle logiche di cyber security. Ecco perché.

L'esplosione dei servizi cloud sta ridefinendo molti servizi e, tra questi, anche la cara vecchia posta elettronica. E non solo per quanto riguarda le modalità di utilizzo e la sua gestione. Le cose cambiano anche per quanto riguarda la sicurezza.

Prima di tutto perché lo spostamento di un servizio tradizionalmente gestito "in casa" rischia di creare qualche equivoco. "Molte aziende non mettono a fuoco i confini delle responsabilità nella gestione dei servizi" spiega **Teemu Mylykangas**, **Solution Director di F-Secure**. "Il fatto che un provider fornisca un servizio su piattaforma cloud non significa, infatti, che l'impresa possa delegargli tutto".

Dalle parti di F-Secure, che ha recentemente lanciato il suo servizio di protezione per la posta elettronica su piattaforma **Office 365**, hanno invece le idee chiare riguardo la necessità di adottare servizi di cyber security che si affianchino ai servizi mail gestititi.

Il ragionamento dell'esperto di F-Secure è semplice: se piattaforme come Office 365 prevedono una serie di strumenti di sicurezza, affidarsi solo a quelle rischia di lasciare il fianco scoperto ad attacchi mirati.

"Se un pirata informatico vuole portare un attacco via mail attraverso un servizio gestito, lo farà utilizzando strumenti tecnici in grado di aggirare le protezioni predefinite" prosegue Mylykangas. "Aggiungere un livello di sicurezza specializzato ha esattamente l'obiettivo di bloccare questo tipo di attacchi".

Il tema, in ambito aziendale, è legato particolarmente al

phishing e ad attacchi specifici che spesso prendono di mira direttamente gli amministratori dei servizi di posta elettronica, per esempio **attraverso messaggi che somigliano in tutto e per tutto agli alert di sicurezza** che la piattaforma invia ogni volta che viene rilevato un evento potenzialmente dannoso.

Nei piani di F-Secure, però, sono previsti anche strumenti specifici per la protezione dalle tecniche più comuni utilizzate dai pirati informatici specializzati negli attacchi alle aziende.

Uno di questi, chiamato Identity Protection, prevede un filtro in grado di intercettare tutti i messaggi provenienti da mittenti che risultano essere coinvolti in data breach e i cui account sono stati potenzialmente compromessi da cyber criminali.

Più specifico invece il sistema di gestione delle regole email, che sarà in grado di individuare eventuali impostazioni che indicano una possibile compromissione da parte di un hacker.

“La posta elettronica è spesso utilizzata come strumento per

l’esfiltrazione dei dati rubati” spiega Mylykangas. “**La tecnica è semplice: viene impostato un inoltro automatico di tutti i messaggi ricevuti e la cancellazione immediata delle mail dalla casella della posta inviata**. In questo modo i pirati ottengono l’accesso a tutte le comunicazioni aziendali senza troppo sforzo”

Il cambiamento, però, non riguarda soltanto gli strumenti tecnici utilizzati e le modalità di implementazione**. La “rivoluzione cloud” cambierà anche il modo di lavorare di molti soggetti che fino a oggi hanno gestito i servizi “in house” delle aziende**.

Secondo Mylykangas, quello a cui stiamo per assistere è un riposizionamento che richiederà, oltre all’utilizzo di strumenti specifici, una fase di formazione per l’acquisizione delle competenze necessarie per garantire la protezione e la gestione dei servizi di posta elettronica nella nuova declinazione. Insomma: nel settore molti operatori dovranno adattarsi a fare quello che, a tutti gli effetti, è un mestiere diverso.

Condividi l’articolo

Germania: hacker all’attacco delle aziende che producono mascherine

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/10/f-secure-ecco-come-cambia-la-protezione-della-mail-cloud/?utm_source=rss&utm_medium=rss&utm_campaign=f-secure-ecco-come-cambia-la-protezione-della-mail-cloud

Germania: hacker all’attacco delle aziende che producono mascherine

Giu 09, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS, Scenario 0

Gli attacchi hanno preso di mira i dirigenti di un’impresa coinvolta nella task force che collabora con il governo di Berlino per garantire la fornitura di PPE.

Qualcuno aveva ipotizzato che di fronte alla pandemia di **Covid-19** i pirati informatici avrebbero abbassato il livello dello scontro o, per lo meno, avrebbero scelto di risparmiare i settori collegati all’emergenza sanitaria.

Niente di più sbagliato: dopo i numerosissimi episodi in cui i cyber criminali hanno sfruttato il Coronavirus come esca, adesso arriva un attacco diretto alle aziende che stanno lavorando al contrasto dell’epidemia.

Succede in **Germania**, dove il governo ha creato una task force coinvolgendo aziende e società multinazionali per garantire un adeguato approvvigionamento di mascherine PPE ai cittadini. Una di queste, denunciano i ricercatori di **IRIS** (**IBM X-Force Incident Response and Intelligence Services**) è finita nel mirino di un gruppo di hacker.

Stando a quanto scrivono gli analisti di IRIS nel loro report, i pirati informatici avrebbero avviato **una massiccia campagna**

di spear phishing nel tentativo di compromettere i computer di numerosi dirigenti (gli analisti parlano di 100 bersagli) di una multinazionale che fa parte della task force.

I ricercatori non citano il nome dell'azienda, ma specificano che la suddetta task force sarebbe composta da grandi imprese che possono vantare "entrature" con i produttori cinesi di mascherine PPE e che avrebbero in pratica offerto i loro servigi per rendere più facile ed efficace il loro reperimento.

Ma quale sarebbe l'obiettivo dei pirati? Le ipotesi sono numerose, ma partono tutte dal presupposto che si tratti di un gruppo collegato al governo di una nazione "concorrente" che potrebbe voler ottenere una posizione di vantaggio a livello commerciale per aggiudicarsi i materiali sanitari.

Qualcuno, però, ha fatto notare che l'attacco potrebbe anche provenire dalla Cina. **I gruppi APT legati a Pechino, infatti, agiscono spesso in sinergia con le aziende cinesi allo scopo di fornire loro informazioni riservate sui partner commerciali occidentali**.

Insomma: non è da escludere che gli hacker abbiano l’obiettivo di fornire sottobanco le comunicazioni interne delle aziende tedesche ai produttori di mascherine per consentire loro di spuntare condizioni di vendita migliori.

Condividi l’articolo

La cybersecurity raccontata con i “fumetti”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/09/germania-hacker-allattacco-delle-aziende-che-producono-mascherine/?utm_source=rss&utm_medium=rss&utm_campaign=germania-hacker-allattacco-delle-aziende-che-producono-mascherine

---

La cybersecurity raccontata con i “fumetti”

Giu 08, 2020 Anna Vaccarelli Approfondimenti, In evidenza, Scenario 0

Registro.it (www.registro.it) è l’anagrafe dei domini italiani che svolge la propria attività all’interno dell’Istituto di Informatica e Telematica del Cnr di Pisa (Iit-Cnr) ed è da sempre impegnato nella diffusione della cultura di Internet,

anche attraverso la Ludoteca del Registro.it. Dal 2011 svolgiamo laboratori ludico didattici nelle scuole primarie per i bambini da 8 a 11 anni, per spiegare come funziona la rete e come usarla con competenza e in sicurezza. Dal 2017, grazie alla presenza nello Iit-Cnr di un gruppo di ricerca in Sicurezza Informatica molto attivo, abbiamo **inserito la Cybersecurity a pieno titolo nei nostri laboratori**.

La sfida era trovare una chiave divertente per spiegare la Cybersecurity ai bambini e **abbiamo pensato di usare i fumetti**. Il protagonista dei nostri “comics”, Nabbovaldo, esordisce in un primo albo pubblicato nella collana Comics&Science del Cnr: è un ragazzo sprovveduto (il Newbie) che va a vivere nella città della rete (Internetopoli) dove affronta difficoltà del

tutto nuove. Nel secondo albo, “Nabbovaldo contro i pc Zombie”, il protagonista affronta a Internetopoli una nuova serie di avventure legate alla Cybersecurity.

La storia, illustrata da Gabriele Peddes e sceneggiata da Giovanni Eccher, è stata **analizzata e validata dai ricercatori dello Iit-Cnr**, conferendo autorevolezza alla pubblicazione. L’albo, oltre alla storia a fumetti, **contiene articoli di approfondimento a beneficio degli adulti** che, auspicabilmente, accompagnano i bambini in questo percorso. Nel fumetto, scaricabile gratuitamente come pdf dal sito della Ludoteca del Registro, vengono affrontati i temi della sicurezza delle password, degli antivirus, dei troll, della privacy, del furto di dati personali, dei cookie, dei malware.

Peddes ed Eccher hanno realizzato delle **tavole ad hoc, che raccontano brevi storie incentrate sui temi della cybersecurity**. Per esempio, quelle del Cyberquiz illustrano situazioni potenzialmente pericolose: **il sexting, la privacy nostra e degli altri, gli sconosciuti (di cui non fidarsi), il bullismo, il furto di dati personali, i malware, i virus, la sicurezza delle reti wifi, le “catene”**, ecc.. Per ogni situazione sono proposti tre possibili comportamenti, uno solo dei quali è corretto: ragioniamo con i bambini sulla storia raccontata (spesso decidono di “sceneggiarla”) e facciamo

scegliere il comportamento che secondo loro è quello giusto, motivandolo. Nel gruppo nasce una discussione che viene condotta alla spiegazione sulla “soluzione” giusta”.

Insieme al Cyberquiz ci sono **altri giochi basati sui fumetti**, che vengono proposti nei laboratori nelle classi, come i classici “trova le differenze“, “trova l’errore” e il memory, tutti scaricabili liberamente dal sito della Ludoteca del Registro .it. Ciascuno di essi ha per tema un aspetto della cybersecurity e costituisce lo spunto per ragionare su quel tema con i piccoli “navigatori”.

La lettura del fumetto, o meglio la sua “messa in scena” fatta in classe con i bambini, assegnando loro i ruoli dei personaggi, **risulta molto efficace stimolando la curiosità e la creatività e favorendo la riflessione insieme al divertimento**. È, quindi, uno strumento efficace con i bambini ma anche con gli adulti, dato che i comics abbracciano un pubblico trasversale. I laboratori, i più “gettonati” dagli insegnanti, confermano che conoscere meglio questi argomenti è un’esigenza molto sentita da tutti.

Condividi l’articolo

Zorab promette di decodificare gratis i file infetti ma è… un

ransomware!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/08/la-cybersecurity-raccontata-con-i-fumetti/?utm_source=rss&utm_medium=rss&utm_campaign=la-cybersecurity-raccontata-con-i-fumetti

---

Tempo di aggiornamenti per Firefox e Zoom

Giu 05, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Per i due software sono disponibili in queste ore gli update di sicurezza che correggono falle critiche. Zoom propone la crittografia, ma non per tutti.

Aggiornamenti importanti per **Firefox** e **Zoom**. Per entrambi le nuove versioni contengono correzioni di bug che mettono a rischio la sicurezza degli utenti.

Per quanto riguarda la versione 77 di Firefox, gli aggiornamenti risolvono, in particolare, alcuni bug che avrebbero permesso l'esecuzione di codice in remoto sulle macchine equipaggiate con il browser di Mozilla.

Le falle di sicurezza in questione sono tre e riguardano la gestione dei JavaScript (CVE-2020-12406) e vari bug che possono portare alla corruzione di memoria identificati come CVE-2020-12410 e CVE-2020-12411.

Le vulnerabilità sono state classificate ad alto rischio e avrebbero consentito l'esecuzione di codice in seguito al semplice caricamento di una pagina Web contenente un eventuale exploit.

Come d'abitudine, l'aggiornamento di Firefox è automatico, pertanto la nuova versione del browser verrà scaricata e installata al momento del primo riavvio.

Diverse le cose per Zoom, per il quale è invece necessario il download e l'esecuzione dell'installer. I dettagli delle vulnerabilità individuate nel software di videoconferenza sono stati pubblicati dai ricercatori di **Talos** e si tratta di bug di una certa importanza.

Nel dettaglio, gli analisti hanno individuato un bug che avrebbe consentito di **avviare l'esecuzione di codice in remoto** attraverso l'invio in chat di una GIF animata (CVE-2020-6109) o di un messaggio di testo specifico (CVE-2020-611).

Entrambe le vulnerabilità avrebbero consentito di portare l'attacco a tutti i partecipanti alla conferenza video, consentendo quindi a un eventuale pirata informatico di fare una vera strage di PC in pochissimo tempo.

Qualche polemica, invece, riguarda la scelta degli sviluppatori di Zoom di limitare la protezione crittografica end to end agli utenti che hanno un account a pagamento.

La dichiarazione del CEO di Zoom **Eric Yuan** secondo cui la scelta punta a **consentire alle forze di polizia di poter agire nei confronti di chi usa la piattaforma per scopi illegali** fa infatti acqua da tutte le parti. Vista la valanga di critiche piovuta sull'azienda, è possibile che le cose cambino in un prossimo futuro.

Condividi l'articolo

Crescono gli attacchi di phishing su mobile nei confronti delle imprese

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/05/tempo-di-aggiornamenti-per-firefox-e-zoom/?utm_source=rss&utm_medium=rss&utm_campaign=tempo-di-aggiornamenti-per-firefox-e-zoom

Crescono gli attacchi di phishing su mobile nei confronti delle imprese

Giu 04, 2020 Marco Schiaffino In evidenza, News, Phishing, RSS, Scenario 0

Con l'adozione dello smart working in tutte le maggiori aziende, i pirati puntano ad attaccare i dipendenti sulle piattaforme mobili. Più 37% in tre mesi.

Nessuno dica di non essere stato avvisato: l'introduzione precipitosa dello smart working legata all'emergenza Covid-19 è stata da subito indicata da tutti gli esperti di sicurezza come un problema a cui prestare attenzione.

Una conferma, adesso, arriva da una ricerca pubblicata da **Lookout**. Nello studio (consultabile a questo indirizzo) viene evidenziato un aumento esponenziale degli attacchi di phishing diretti ai dipendenti di grande aziende sui loro dispositivi mobili.

Lo scenario in cui si inserisce il fenomeno è quello di un lavoro in remoto (di "smart" per la verità ha ben poco) che ha costretto tutti i lavoratori a spostare buona parte delle comunicazioni su strumenti digitali e in particolare su smartphone.

Un'occasione che i cyber criminali hanno colto al volo, attrezzandosi immediatamente per sfruttare la situazione attraverso campagne di phishing mirate.

Rispetto ai “normali” attacchi rivolti ai computer, quelli che prendono di mira gli smartphone, spiegano gli esperti di Lookout, sono più insidiosi. Sfruttano infatti una pluralità di vettori come SMS, messaggi su varie piattaforme e su social network che possono facilmente trarre in inganno le potenziali vittime.

La portata di questi attacchi è spaventosa: nello studio viene stimato un aumento del 37% dall’ultimo trimestre 2019 al primo trimestre 2020.

Uno degli elementi di criticità è anche il fatto che i dispositivi mobili, tipicamente adibiti a un uso “promiscuo” che mescola le attività professionali con quelle private, rappresentano uno strumento che gli utenti usano con una maggiore leggerezza rispetto a quelli aziendali.

A peggiorare la situazione, c’è il fatto che il lavoro in remoto pone i lavoratori al di fuori di quel perimetro “protetto” che in azienda consente di intercettare e bloccare sul nascere attacchi di questo genere.

Insomma: secondo i ricercatori, il rischio aumenta anche a causa del fatto che gli strumenti di protezione che di solito preservano i dipendenti finiscono per abbassare la percezione del livello di minaccia.

Condividi l’articolo

Tempo di aggiornamenti per Firefox e Zoom Estorsioni online: ora i pirati di Maze e LockBit fanno cartello

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/04/crescono-gli-attacchi-di-phishing-su-mobile-nei-confronti-delle-imprese/?utm_source=rss&utm_medium=rss&utm_campaign=crescono-gli-attacchi-di-phishing-su-mobile-nei-confronti-delle-imprese

---

Estorsioni online: ora i pirati di Maze e LockBit fanno cartello

Giu 03, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario 0

Diversi gruppi di cyber-criminali specializzati in ransomware stanno unendo le loro forze per "spremere" al massimo le vittime.

Il mondo del cyber-crimine continua a evolversi seguendo una logica che ricorda molto da vicino quella del mondo del business legittimo. Se da tempo esiste una filiera della pirateria informatica e da qualche anno si è imposto il modello del "malware as a service", adesso arrivano le partnership.

A darne notizia è Bleeping Computer, che in un articolo spiega come il gruppo **Maze**, specializzato in attacchi ransomware, abbia creato una sorta di piattaforma attraverso la quale gestire forme di collaborazione con altre gang di cyber-criminali.

L'evoluzione del gruppo, negli ultimi mesi, è stata simile a quella di altri operanti nello stesso settore, che sono passati dalla semplice diffusione di ransomware agli attacchi che puntano al furto di dati in prospettiva di una richiesta di riscatto per evitare la loro divulgazione pubblica.

A questo, scopo, i membri di Maze hanno creato un sito

dedicato, che adesso verrebbe utilizzato come punto di riferimento per collaborare con altri gruppi che utilizzano la stessa strategia. **Il loro obiettivo, confermato ai colleghi di Bleeping Computer in uno scambio di messaggi, è quello di condividere risorse e informazioni.**

I primi affiliati sarebbero i pirati di **LockBit**, anche loro specializzati in ransomware, e altri dovrebbero aggiungersi nei prossimi giorni. I toni usati dai pirati, così come riportati nell'articolo, ricordano da vicino quelli utilizzati di solito in ambito commerciale: "Trattiamo gli altri gruppi come partner e non come competitor".

Insomma: se le sporadiche collaborazioni tra gruppi di cyber-criminali hanno già creato qualche grattacapo in passato, adesso che ci si trova di fronte ad alleanze strutturate la situazione rischia di peggiorare ulteriormente.

Condividi l'articolo

GitHub avvisa gli sviluppatori: "attenti al malware Octopus Scanner"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/03/estorsioni-online-ora-i-pirati-di-maze-e-lockbit-fanno-cartello/?utm_source=rss&utm_medium=rss&utm_campaign=estorsioni-online-ora-i-pirati-di-maze-e-lockbit-fanno-cartello

---

Allarme dell’NSA: hacker russi di Sandworm all’attacco dei server email

Mag 29, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, Scenario, Vulnerabilità 0

I servizi segreti USA sollecitano ad aggiornare i server per eliminare ua vulnerabilità utilizzata dai pirati informatici e smantellare la loro rete.

Si è mossa direttamente la **National Security Agency** e non è un caso. Per il governo USA, infatti, quando si ha a che fare con **Sandworm** le mezze misure non sono accettabili.

Il gruppo, conosciuto anche come **TeleBots**, sarebbe in realtà la **Unità 74455**, parte integrante della sezione di cyber-spionaggio del **GRU**, i servizi segreti russi che hanno raccolto il testimone del più famoso **KGB**.

Nel curriculum dei pirati informatici al soldo di Mosca, ci sarebbero attacchi di primo piano come quelli portati con il malware **BlackEnergy**, che ha colpito l’Ucraina nel 2015 e 2016, nonché la creazione di NotPetya, il “finto ransomware” che ha fatto tremare il mondo nel giugno 2017.

Ora i cyber-spioni al servizio di Putin sarebbero impegnati in una campagna che sfrutta una vulnerabilità che affligge i server che utilizzano il Mail Transfer Agent **Exim**. Il componente, usato su sistemi Unix, aveva già avuto problemi qualche tempo fa e adesso è interessato da una nuova falla di sicurezza.

Il nuovo bug (CVE-2019-10149) viene sfruttato dai pirati di Sandworm per avviare il download e l'esecuzione di uno **shell script** che consente loro di disabilitare le impostazioni di sicurezza, ottenere elevati privilegi sul server e avviare ulteriori script sulla macchina. **In poche parole: un attacco devastante che permette agli hacker di prendere il controllo del server**.

L'obiettivo del rapporto a firma NSA è quello di sensibilizzare gli amministratori IT e spingerli a eseguire l'aggiornamento (rilasciato nel febbraio 2019) che blocca l'attacco. Il problema è che meno della metà dei server che usano Exim sono aggiornati. **Questo significa che circa il 25% dei server email nel mondo (la metà usa Exim) sono vulnerabili agli attacchi.**

La speranza dell'agenzia statunitense è anche quella di fare in modo che gli amministratori rimuovano le backdoor eventualmente installate dal gruppo Sandworm per "depotenziare" la botnet sotto il loro controllo.

Condividi l'articolo

Quando i rischi più gravi provengono dall’interno

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/29/allarme-dellnsa-hacker-russi-di-sandworm-allattacco-dei-server-email/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-dellnsa-hacker-russi-di-sandworm-allattacco-dei-server-email