Usa 2020, come il Pentagono sta lavorando per proteggere le elezioni da attacchi hacker

Usa 2020 e cybersecurity, questa volta l'america non vuole trovarsi impreparata.

Per provare a scongiurare le interferenze subite durante le elezioni del 2016, il Pentagono sta portando avanti una strategia informatica per garantire che le elezioni presidenziali del 2020 siano protette al meglio da attacchi hacker.

Lo ha dichiarato il generale **Paul Nakasone**, comandante del Cyber Command degli Stati Uniti (CYBERCOM) e direttore della National Security Agency, in un recente editoriale firmato insieme al suo consigliere **Michael Sulmeyer.**

Nakasone afferma che gli Stati Uniti hanno schierato forze nell'Europa orientale per contrastare qualsiasi tentativo di interferire nelle elezioni presidenziali previste per il 3 novembre 2020.

La Election Security Group

L'anno scorso, CYBERCOM e NSA hanno formato un'unità chiamata **Election Security Group**.

Squadre di americani, le cosiddette "*hunt forward missions*", stanno lavorando per scoprire le tecniche e le tattiche degli avversari prima che attacchino i sistemi statunitensi. Come

risultato delle scoperte del nuovo gruppo, il Dipartimento per la sicurezza interna ha già "*rafforzato*" la sicurezza delle infrastrutture elettorali, mentre l'FBI sta incentivando il controllo per "*contrastare i troll stranieri sulle piattaforme dei social media*", scrive Nakasone.

Il Cybercom

Il Cyber Command degli Stati Uniti, creato nel 2009, ha svolto un ruolo più importante nelle difese elettorali dal 2018 dopo che l'amministrazione Trump ha concesso ai suoi comandanti una nuova autorità e il Congresso ha emesso silenziosamente una dichiarazione che definisce le "operazioni online" come un'attività militare tradizionale. Nello stesso anno, le forze armate statunitensi hanno schierato operatori informatici in Ucraina, Macedonia e Montenegro per contrastare i tentativi russi di interrompere le elezioni di medio termine.

"*Il Montenegro ha subito crescenti molestie dalla Russia da quando è entrato a far parte della NATO nel 2017, e il team del Cyber Command era lì per indagare sui presunti hacker, penetrati nelle reti del governo montenegrino*", scrive Nakasone nel suo editoriale. "*Lavorando fianco a fianco con i partner montenegrini, il team ha visto un'opportunità per migliorare le difese informatiche americane prima delle elezioni del 2020*".

Quella campagna, soprannominata "*Operation Synthetic Theology*", includeva l'attacco e la messa offline a una famigerata fabbrica di troll a San Pietroburgo, altrimenti nota come Internet Research Agency, che ha organizzato campagne di propaganda e disinformazione sia nelle elezioni presidenziali del 2016 che in quelle di medio termine del 2018.

Nel 2020, CYBERCOM ha istituito team informatici difensivi a chiamata, pronti a rispondere agli avversari stranieri se agenzie come DHS o FBI ne avessero bisogno.

L’allarme sulle elezioni 2020 lanciato da Microsoft

Per mesi, le agenzie di intelligence hanno avvertito che la Russia sta nuovamente tentando di interrompere le elezioni di novembre. L’ultimo monito risale ad un a settimana fa, quando Microsoft ha dichiarato pubblicamente che l’unità dell’intelligence militare russa (Gru), responsabile delle interferenze del 2016, è tornata all’attacco mettendo nel mirino collaboratori, consulenti e think tank associati sia ai dem che ai repubblicani. Gli hacker cinesi, contrariamente alla valutazione degli 007 Usa, si sono invece concentrati sulla campagna di Biden.

Mosca e Pechino hanno respinto entrambe le accuse. La Cina ha accusato l’azienda di Redmond di “*inventare*” collegamenti tra Pechino e i tentativi di attacchi informatici sulla campagna elettorale delle presidenziali Usa di novembre. “*Non abbiamo alcun interesse a interferire e non abbiamo mai interferito*“, ha dichiarato il portavoce del ministero degli Esteri **Zhao Lijian**, aggiungendo nella conferenza stampa quotidiana che “Microsoft non dovrebbe fabbricare qualcosa dal nulla e creare problemi parlando della Cina”.

“*A seguito della campagna presidenziale del 2016 negli Usa, non abbiamo visto argomenti tangibili o prove che evidenzino che un qualche tipo di organizzazione relativa alla Federazione Russa si occupi di crimini informatici”*, ha dichiarato il portavoce di **Vladimir Putin, Dmitri Peskov,** ripreso dall’agenzia Interfax. Se la dichiarazione di Microsoft “*è formulata nello stesso modo – ha proseguito Peskov – allora indica bassa qualificazione, se lì vi è un’argomentazione professionale allora vale la pena ascoltarla*“.

La taglia di 10 milioni di dollari

Gli Stati Uniti hanno messo in campo un'altra tecnica per scongiurare gli attacchi informatici durante le elezioni americane. Il dipartimento di Stato Americano ha messo una taglia da 10 milioni di dollari per chi fornirà informazioni utili a identificare hacker che lavorano con governi stranieri.

La ricompensa, si legge sul sito del Dipartimento di Stato americano, è volta a ottenere "*informazioni per l'identificazione o l'ubicazione di qualsiasi persona che, mentre agisce sotto la direzione o sotto il controllo di un governo straniero, interferisce con elezioni federali, statali o locali degli Stati Uniti aiutando o favorendo una violazione della sezione 1030 del titolo 18*", cioè la legge sulle frodi e gli abusi informatici.

https://www.key4biz.it/usa-2020-come-il-pentagono-sta-lavorando-per-proteggere-le-elezioni-da-attacchi-hacker/321535/

Scuole connesse e poco sicure, crescono del +350% i cyber attacchi globali alle piattaforme di didattica online

Il mondo della scuola non è in subbuglio solamente per la ripresa delle lezioni in periodo di Covid-19 e per il problema del distanziamento sociale in classe. Un'altra minaccia si affaccia all'orizzonte: gli attacchi informatici.

L'apprendimento a distanza tramite piattaforme di didattica online è diventato una necessità per milioni di studenti in tutto il mondo, Italia compresa. Molte organizzazioni scolastiche, però, sono state costrette a gestire questa transizione con poca o nessuna preparazione.

Il conseguente forte e rapido aumento delle risorse educative online, unito a questa mancanza di preparazione, ha reso il settore dell'istruzione un bersaglio ideale per i cyber criminali.

Gli attacchi informatici alle scuole

Secondo un nuovo studio internazionale condotto da Kaspersky, a livello globale, il numero di **attacchi DDoS** (*Distributed Denial of Service Denial of Service*) **è aumentato dell'80% nel primo trimestre del 2020** rispetto allo stesso periodo dell'anno precedente.

Gli attacchi alle risorse dedicate alla didattica hanno rappresentato una parte importante di questa crescita. **Tra gennaio e giugno 2020, il numero di attacchi DDoS che hanno interessato questi obiettivi è aumentato di almeno il 350%** rispetto agli stessi mesi del 2019.

Gli attacchi DDoS (Distributed Denial of Service Denial of Service) sono particolarmente insidiosi perché sfruttano una "botnet", cioè una rete di computer infetti (detti anche "*zombie*") in grado di svolgere compiti simultaneamente e per lungo tempo.

Gli attacchi DDoS sono ritenuti molto problematici perché

possono avere una durata che va da un paio di giorni a qualche settimana, causando l'interruzione dell'attività e – nel caso delle risorse didattiche – negando l'accesso agli studenti e al personale a contenuti editoriali e/o sensibili (con conseguente pericolo per la ***privacy***, in termini di violazione di dati riservati e personali).

I casi negli Usa e in Germania

Negli Stati Uniti, in Connecticut, la Hartford Public Schools è stata oggetto di un pesante attacco informatico di tipo ransomware. Il dirigente scolastico si è visto obbligato a rinviare il ritorno in classe dopo le vacanze estive, perché un gran numero di server e device connessi in rete erano praticamente fuori uso.

Attacchi ransomware hanno riguardato anche la Clark County School di Las Vegas, la Hayward County School in North Carolina, la Ponca City School in Oklahoma, e molte altre scuole di diversi Stati.

Un risultato che secondo gli esperti ricalca le stesse dinamiche strutturali della ricerca sopra illustrata: scarsi budget per la cybersicurezza, un gran numero di contenuti online e di device connessi in rete, impreparazione di personale docente e degli stessi studenti in termini di prevenzione nella sicurezza informatica.

In Germania, in piena pandemia di Covid-19, a marzo, la piattaforma per la didattica scolastica a distanza Mebis, in Baviera, è stata bersaglio di attacchi DDoS.

> *Scuole connesse e poco sicure, crescono del +350% i cyber attacchi globali alle piattaforme di didattica online*

Smaug, come difendersi dal ransomware in vendita sul dark web

Si chiama **Smaug** il ransomware as a Service (RaaS), scoperto dai ricercatori di sicurezza Anomali in grado di infettare macchine Windows, macOS e Linux e disponibile tramite un sito Dark Web **Onion**.

Infatti è sul dark web, da sempre un punto di aggregazione per organizzazioni e criminal hacker, che anche chi non ha la capacità di sviluppare il proprio malware può trovare (nei marketplace underground) un pacchetto pronto all'uso.

Nel caso in esame le modalità risultano ancora più semplici. Per lanciare un attacco, gli acquirenti devono registrarsi, creare una campagna e quindi iniziare a distribuire il ransomware.

Sarà il servizio a gestire l'acquisto e il monitoraggio delle chiavi di decrittazione per le vittime.

La vendita sul forum

Risale a Maggio 2020, la prima offerta promozionale apparsa sul forum "Exploit.in". I promoter, in quella occasione, erano disposti a rinunciare addirittura alla quota di registrazione per i primi cinque acquirenti. Il post mostrava oltre che le funzionalità peculiari di Smaug:

- capacità di infettare macchine che utilizzano diversi sistemi operativi (64bit) eludendo i prodotti antivirus tradizionali;
- possibilità di attivare la “company mode”, applicando un’unica chiave a un insieme di host infetti;
- funzionalità offline;

Anche le modalità di pagamento:

- quota di registrazione 0,2 BTC (circa 2.000 dollari);
- commissioni di servizio del 20% sui guadagni.

Registrazione e funzionalità del pannello di controllo del servizio

Gli sviluppatori di Smaug hanno condiviso gli screenshot del prodotto sul loro sito Onion, offrendo alcune informazioni su come il prodotto deve essere utilizzato, e un servizio di supporto sia per l’assistenza che per richieste di funzionalità extra a pagamento.

Il sito offre un modulo per la registrazione con captcha, al termine della quale, gli utenti vengono indirizzati a pagare 0,2 BTC a un portafoglio Bitcoin specificato e solo dopo l’avvenuto pagamento attivati entro un certo lasso di tempo.

Dopo la registrazione avvenuta con successo, l’utente viene indirizzato alla dashboard di Smaug, un’interfaccia utente funzionale e molto intuitiva, con la quale l’utente può cambiare la propria password (dal menù settings) e creare campagne con messaggi di riscatto e date di scadenza personalizzabili.

Una volta creata la campagna, la dashboard consente all’utente di scaricare il payload pertinente ai target secondo i sistemi operativi scelti (Mac, Linux e Windows) e tenere traccia degli aggiornamenti circa l’evoluzione dell’infezione, delle date e dei profitti accumulati.

Solo dopo che risulti almeno un riscatto versato, l'utente può accedere alla voce di menù "Withdraw" per il prelievo su un determinato portafoglio BTC. La pagina riporta il saldo corrente (con la commissione del 20% trattenuta) e il numero di pagamenti effettuati.

Il ransomware SMAUG

Anomali Threat Research dall'analisi di alcuni campioni rilevati (esemplari Windows e Linux), ha constatato che i binari Smaug, implementati in linguaggio Golang in circa 300 righe di codice, non contengono alcun timestamp che avrebbero permesso di fissare le relative date di creazione. I ricercatori hanno potuto comunque stimare il periodo di pubblicazione basandosi sulla data di rilascio del compilatore Golang adoperato (v.1.14.2, Aprile 2020).

Gli stessi hanno appurato, inoltre (agli inizi di Agosto), ancora una bassa percentuale di rilevamento da parte dei più diffusi motori antivirus.

Crittografia e richiesta di riscatto

Dal campionamento effettuato è trapelato, altresì, che per la crittografia il malware invoca una coppia di "goroutine":

- La prima routine analizza ogni partizione alla ricerca di file con determinate estensioni predeterminate;
- la seconda routine crittografa secondo lo standard AES in modalità Cipher Block Chaining (CBC) tutti i file identificati secondo elenco.

Infine la richiesta di riscatto, archiviata nel file binario come stringa codificata Base64, viene trascritta in chiaro su un file di testo ("HACKED.txt") e salvata in tutte le cartelle contenenti i file crittografati:

“Your files have been encrypted using military grade encryption. They can never be accessed again without buying a decryption key. You can buy the decryption key at http://smaugrwmaystthfxp72tlmdbrzlwdp2pxtpvtzvhkv5ppg3difiwonad[.]onion. To access the site you need Tor Browser”.

Come difendersi

Anche se Smaug è un RaaS multipiattaforma relativamente semplice rispetto ad altri ransonware attivi (non è previsto l’arresto dei processi in esecuzione che possono bloccare la crittografia di alcuni file e non vengono eliminati i backup e i file delle copie shadow su Windows) la sua elevata fruibilità apre le porte verso un targeting potenzialmente più ampio.

Poiché al momento Smaug può essere veicolato solo mediante attacchi phishing/social engineering e/o la compromissione di siti web con tecniche “drive by download”, rimangono sempre validi gli accorgimenti di sicurezza minimi per cercare di limitarne l’impatto:

- effettuare regolarmente un backup;
- mantenere aggiornati i propri sistemi e tool di sicurezza;
- avere contezza che le insidie nascoste nel cyberspazio sempre più spesso sfruttano la complicità inconsapevole umana.

È anche recente l’alert diramato dal CSIRT – Italia, che ha reso pubblici gli IoC di un campione rilevato.

MD5

6b083c1bfd21eea2a3f18283f1f3c5f5

SHA1

929b10f78565660535a07917d144d00b0c117571

SHA256

f2363a355fe226cb2f7f1afa72daecc5edfe1cb0edc1295856fb3f874d941b6d

Malware – sample

Corporate_Detail-June.2020.exe|6b083c1bfd21eea2a3f18283f1f3c5f5

https://www.key4biz.it/smaug-come-difendersi-dal-ransomware-in-vendita-sul-dark-web/320528/

Attacco informatico all'univ. Tor Vergata, coinvolte anche le ricerche sul Covid-19

Un attacco informatico ha coinvolto l'**Università di Roma Tor Vergata**. L'ateneo, come spiega La Repubblica, è stato colpito venerdì scorso da un attacco hacker nei confronti della propria rete IT.

I criminal hacker, spiega il quotidiano, si sono introdotti nella rete attraverso un server e hanno iniziato a rendere inutilizzabili importanti documenti, come quelli sulle ricerche e le terapie per contrastare il Covid-19.

L'attacco a tutto il sistema ha colpito i file presenti nei dischi rigidi, mettendo a rischio tutte le analisi sul Coronavirus, si legge nell'articolo, e sarebbero stati cifrati

tutti i documenti di studenti e professori che usufruivano del sistema cloud, compresi i dati sensibili.

Compromessi oltre 100 computer del personale. Da quanto si apprende, si era bloccata anche la didattica a distanza che ha permesso di far sostenere 71mila esami.

"*Per ora non è stato chiesto alcun riscatto* – ha spiegato a Repubblica il rettore **Orazio Schillaci** – *e non sappiano ancora cosa abbiano sottratto, ma siamo riusciti subito ad avviare contromisure circoscrivendo il danno e attivando il ripristino dal backup, così da non perdere dati, ricerche e assicurare il proseguimento della didattica*".

La corsa al vaccino sul Coronavirus: la partita cyber

In Italia non è la prima volta che criminali informatici attaccano una struttura sanitaria specializzato nella lotta al coronavirus. Un caso analogo si era avuto con l'attacco informatico l'**Ospedale Spallanzani di Roma** a fine marzo. Ma per fortuna i criminal hacker non hanno avuto successo.

Nel mondo invece secondo Stati Uniti, Regno Unito e Canada, dall'inizio della pandemia, ci sono stati numerosi tentativi di **cyber spionaggio industriale** tesi a rubare studi, ricerche e test dei vari vaccini sperimentati sin qui, tutti coordinati da Mosca e Pechino. Gli Usa non hanno dubbi e puntano il dito sulla Cina, accusandola di aver rubato una ricerca americana.

A prova dell'elevato rischio che sta correndo il Paese, lo scorso luglio il leader repubblicano alla Camera, **Kevin McCarthy**, ha presentato un disegno di legge per fermare e sanzionare i cyber criminali stranieri che tentano di sottrarre informazioni riservate in questo settore.

https://www.key4biz.it/attacco-informatico-a-tor-vergata-coinvolte-anche-le-ricerche-sul-covid-19/320340/

Cos’e’ il ransomware? Come si diffonde? La guida su come difendersi

Cos’è il ransomware? Come si diffonde? Come liberarsene? A queste domande cerchiamo di dare delle risposte con questa breve guida su una delle attività più diffuse e dannose in ambito di cybersecurity.

Cos’e’ il ransomware?

Il ransomware è un programma informatico dannoso (“malevolo”) che può “infettare” un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, “ransom”) da pagare per “liberarli”.

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All’utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

Ci sono due tipi principali di ransomware:

• i cryptor (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);

• i blocker (che bloccano l’accesso al dispositivo infettato).

Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

• sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);

• contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

Ransomware: 'occhio' al gratis

In altri casi, il ransomware può essere scaricato sul dispositivo quando l'utente:

• clicca link o banner pubblicitari su siti web (un canale molto usato è rappresentato dai siti per adulti) o social network;

• naviga su siti web creati ad hoc o "compromessi" da hacker per diventare veicolo del contagio ransomware.

Il ransomware può essere diffuso da malintenzionati anche attraverso software e app (giochi, utilità per il PC, persino falsi anti-virus), offerti gratuitamente per invogliare gli utenti al download e infettare così i loro dispositivi.

E' bene ricordare che ogni dispositivo "infettato" ne può "contagiare" altri.

Il ransomware può diffondersi sfruttando, ad esempio, le sincronizzazioni tra dispositivi, i sistemi di condivisione in cloud, oppure può impossessarsi della rubrica dei contatti e utilizzarla per spedire automaticamente ad altre persone messaggi contenenti link e allegati che diventano veicolo del ransomware.

Come difendersi?

La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ognora il contenuto.

Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze.

Ad esempio:

- non aprire mai allegati con estensioni “strane” (ad esempio, allegati con estensione “.exe” sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
- scaricare preferibilmente app e programmi da market ufficiali, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;
- se si usa un pc, si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso

nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).

E' inoltre utile:

- installare su tutti i dispositivi un antivirus con estensioni anti-malware;
- mantenere costantemente aggiornati il sistema operativo oltre che i software e le app che vengono utilizzati più spesso;
- utilizzare dei sistemi di backup che salvino (anche in maniera automatica) una copia dei dati (sono disponibili soluzioni anche libere e gratuite per tutti i sistemi operativi). Con un corretto backup, in caso di necessità, si potranno così ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio.

Come liberarsi dal ransomware?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in "liste di pagatori" potenzialmente soggetti a periodici attacchi ransomware.

La soluzione consigliata è quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.

Un'alternativa efficace è quella di formattare il dispositivo: ma in questo caso, oltre ad eliminare il malware, si perdono tutti i dati in esso contenuti. Per questo è fondamentale (come suggerito) effettuare backup periodici dei contenuti (che è sempre una buona prassi) in modo da non perderli in caso di incidenti (es: danneggiamento del dispositivo, ecc.) o

attacchi informatici che necessitano di interventi di ripristino.

E’ sempre consigliabile segnalare o denunciare l’attacco ransomware alla **Polizia postale** anche per aiutare a prevenire ulteriori illeciti.

https://www.key4biz.it/cose-il-ransomware-come-si-diffonde-la-guida-su-come-difendersi/319639/

Trojan bancari, dopo 10 anni QBot continua a fare vittime in ambito cyber

QBot, noto anche con i nomi di Qakbot e Pinkslipbot, è un trojan bancario prolifico e in attività da oltre dieci anni (identificato in origine nel 2008). Si stima che abbia causato migliaia di vittime a livello globale, grazie alle sue molteplici capacità (altamente strutturato, multistrato e in continuo aggiornamento) e attitudini, agendo non solo da infostealer ma anche come distributore di malware (inclusi i temuti ransomware), che lo rendono ancora, a tutti gli effetti, una minaccia pericolosa e persistente.

QBot: ancora in attività

Secondo un nuovo rapporto una nuova campagna malspam veicolante il trojan QBot è ripresa all’inizio del mese di agosto, diffondendosi globalmente in particolare su obiettivi

statunitensi ed europei tra enti governativi, militari e di manufactoring (di cui il 7% in Italia).

Già presente quest'anno in campagne svolte da marzo a fine giugno, a luglio è ricomparso con una variante e un rinnovato impianto di comando, controllo e funzionalità utilizzando per la sua diffusione infrastrutture d'infezione di terze parti come il framework Emotet che nello stesso mese ha avuto un notevole impatto sulle organizzazioni di tutto il mondo (circa il 5%, affermano i ricercatori di Check Point).

I principali e nuovi moduli individuati includono:

- un modulo utilizzato per comunicare con i server di comando e controllo;
- un modulo di raccolta email per rubare thread di posta elettronica dal client Outlook;
- un modulo di aggancio per iniettare moduli web e codici javascript malevoli nelle sessioni di navigazione;
- un modulo che scarica l'open source Mimikatz per cercare di carpire credenziali e password;
- un plug-in che consenteil controllo della macchina vittima tramite una connessione VNC remota (un attaccante esterno potrebbe eseguire transazioni bancarie all'insaputa dell'utente, anche se lo stesso risulterebbe contemporaneamente connesso al computer);
- un modulo per la cattura di cookie di autenticazione, utilizzabili per dirottare le sessioni dei browser (**Internet Explorer, Edge, Chrome e Firefox);**
- un modulo per l'aggiornamento dell'eseguibile corrente con una versione o con un elenco bot più recente;
- un modulo proxy, per anonimizzare l'indirizzo IP del server di comando e controllo.

La catena di infezione

Le più recenti catene di infezione QBot sono cambiate rispetto al passato e le email di spam non utilizzano più allegati con

macro malevole ma piuttosto includono link URL che puntano a file .zip, ospitati su siti WordPress compromessi (https://factory-hot[.]com/bafmxby/ CcdEhoQGHq.zip) e contenenti un downloader VBScript. Questo script estrae il carico utile .exe da ulteriori sei indirizzi URL hardcoded (crittografia XOR con chiavi dinamiche), evadendo il controllo sandbox tramite l'esecuzione di opportune routine.

Anche se il VBS è un linguaggio di scripting sviluppato da Microsoft, che è stato deprecato lo scorso anno, i criminal hacker scommettono sul fatto che molte aziende continuino a adoperare versioni Windows e di Internet Explorer (la cui fine assistenza è stata annunciata per Agosto 2021) prive degli aggiornamenti di sicurezza più recenti.

Una volta che una macchina viene compromessa può diventare essa stessa una potenziale minaccia per altri computer nella rete locale, divenendo un bot con capacità di spostamento laterale.

Il modulo "Hijacked Email Threads"

La catena di infezione che inizia dunque con l'invio di email appositamente allestite, presenta degli attributi aggiuntivi che ne migliorano l'efficacia. Uno di questi è rappresentato dal modulo "**Hijacked Email Threads"** che estrae tutti i thread di posta elettronica dal client Outlook target e li carica su un server remoto codificato. Queste email rubate vengono quindi utilizzate per future campagne di malspam, inducendo così più facilmente gli utenti a cliccare sui link dando l'impressione di continuare una conversazione legittima già esistente.

I ricercatori di sicurezza hanno campionato diversi thread di posta elettronica mirati e dirottati verso i file .zip dannosi, con argomenti relativi a Covid-19, reclutamento di lavoro (ricerca di sviluppatori C #, Java e PowerShell) e solleciti di pagamento.

QBot: il metodo d’infezione

Il metodo d’infezione basato su VBS, che da aprile 2020 è una novità per QBot, offre la possibilità di utilizzare diversi metodi di offuscamento e decodifica. Ad esempio per evadere i controlli delle sandbox, le dimensioni di uno script VBS possono essere maggiorate di un certo numero di byte nulli per superare le soglie di guardia standard (35 MB), oppure può essere adeguatamente ritardata la sua esecuzione tramite una chiamata API sleep.

Il modulo di comunicazione

L’impianto di comunicazione prevede un metodo collaudato per nascondere l’indirizzo IP del server di comando e controllo. L’host vittima infatti comunica indirettamente con il server C2 oppure con un proxy di secondo livello (46.228.199.235:443, 93.88.75. 176:443, 207.244.112. 112:443) contattando un determinato bot, scelto tra un pool di 150 indirizzi IP, che si occupa di inoltrare il flusso dati.

I messaggi, crittografati con un valore di inizializzazione casuale, vengono inviati tramite POST all’URL del bot scelto (https://[IPbot]:[portabot/]) e in formato JSON.

Nuove funzionalità

Almeno fino a quando i criminal hacker mostreranno interesse a sviluppare e aggiornare nuove funzionalità e attributi, QBot continuerà a rappresentare una minaccia duratura nel tempo.

Anche per QBot, definito da Check Point Research “*l’equivalente malware di un coltellino svizzero*”, occorre prestare la massima attenzione, soprattutto perché può essere adoperato (alla stregua del famigerato Emotet) come testa di ponte per la distribuzione nelle reti colpite di ulteriori malware.

Il team ha pubblicato, nel suo rapporto, gli indici di compromissione di molti dei campioni QBot e VBS analizzati durante la ricerca, una regola YARA e degli script Python per l'estrazione degli URL malevoli.

https://www.key4biz.it/trojan-bancari-dopo-10-anni-qbot-continua-a-fare-vittime-in-ambito-cyber/319575/

La Norvegia sotto attacco informatico. Hackerato il Parlamento

Il parlamento norvegese ha subito un attacco hacker, con la violazione degli account di posta elettronica di diversi ministri, deputati e dipendenti.

Lo ha reso noto il servizio stampa dell'assemblea nazionale e l'agenzia di controspionaggio della Norvegia, ripresa dai media locali. "*La nostra analisi mostra che sono state scaricate varie quantità di dati*", si legge nella dichiarazione. I mandanti e le conseguenze di tale attacco sono ancora tutti da valutare, anche se l'autorità per la sicurezza nazionale norvegese (Nsa) ha dichiarato di avere contrastato l'attacco intervenendo in modo immediato.

"S*iamo stati coinvolti per alcuni giorni*", ha detto il portavoce della Nsa, **Trond Oevstedal.** "*Stiamo assistendo il parlamento con analisi e assistenza tecnica*", ha aggiunto.

Non solo il parlamento, attacco hacker a Hedmark IKT

Poche ore dopo che il parlamento norvegese aveva annunciato un attacco ai propri sistemi è avvenuto l'hack ai lavoratori del settore pubblico dell'azienda **Hedmark IKT**.

Secondo fonti locali, questa mattina, 10,000 dipendenti di Hedmark IKT, azienda pubblica che offre servizi informativi a diverse amministrazioni sul territorio, si sono svegliati senza poter più accedere alle proprie caselle di posta elettronica.

I dipendenti municipali di **Hamar**, situato sulla riva del più grande lago norvegese Mjøsa, sono stati tra coloro che sono stati colpiti dall'attacco ai sistemi di posta elettronica del settore pubblico nella regione di Hedmark. Hamar ha recentemente combattuto un nuovo focolaio di Coronavirus, per questo l'attacco alle comunicazioni è stato considerato particolarmente grave.

Non è ancora chiaro se i due attacchi, siano correlati, ma entrambi sono stati descritti dalle autorità norvegesi come "*estremamente gravi* e *sofisticati*".

https://www.key4biz.it/la-norvegia-sotto-attacco-informatico-hackerato-il-parlamento/319526/

Fortnite è una miniera d'oro per i criminal hacker. Gli

account rubati valgono 1 miliardo

Decine di migliaia gli account di **Fortnite** rubati ai legittimi proprietari e venduti sul dark web generano nelle tasche dei criminali informatici 1 miliardo di dollari all'anno.

Lo riporta **Bloomberg** secondo cui, nel nuovo rapporto degli analisti di **Night Lion Security**, il popolare videogioco è al centro di un mercato illegale.

250 dollari a profilo rubato

Ogni profilo è venduto in media a 200-250 dollari ma ce ne sono alcuni con "skin" – cioè personalizzazioni dell'avatar – di particolare valore, che fanno crescere il prezzo di un account fino a qualche migliaio di dollari.

E Fortnite, che conta 350 milioni di videogiocatori registrati nel mondo, non è l'unico videogame ricercato sul mercato nero degli account. Ad essere gettonati sono anche Minecraft, RuneScape e Roblox. Insieme, i quattro giochi danno vita a compravendite per 700 milioni di dollari.

Un mercato redditizio

Quelli dei videogame "sono tra gli account hackerati più redditizi sul mercato nero", evidenziano gli esperti, secondo cui la compravendita di questi profili "si è evoluta in un'industria clandestina da un miliardo di dollari all'anno, con una sua catena di approvvigionamento perfettamente funzionante".

In questo contesto “la pandemia di Covid-19 in corso sembra accelerare la richiesta di account, con le persone che non sono al lavoro e hanno tutto il tempo per usare i videogiochi”, evidenziano gli analisti, mentre gli sviluppatori dei videogame “ad oggi non hanno ancora avuto successo nel rallentare quest’economia sommersa, che agli hacker e ai venditori più bravi frutta entrate annuali a sei o sette cifre”.

I numeri di Fortnite

Fortnite conta ad oggi oltre 3.5 milioni di utenti registrati, di questi il 53% tra i 10 e 25 anni e, dai 18 anni in su, il 62,7% tra i 18 e i 24. Tra il 70 e l’80% di questi, sono maschi. Vette raggiunte anche grazie alle ore di gioco che risultano essere 3.2 miliardi solo nel mese di aprile. Il tempo medio speso da ogni giocatore è tra le 6 e le 10 ore a settimana.

https://www.key4biz.it/fortnite-e-una-miniera-doro-per-i-criminal-hacker-gli-account-rubati-valgono-1-miliardo/319163/

TeamTNT, il nuovo worm che batte criptomoneta attraverso il cloud di Amazon

Un nuovo worm di cryptomining, si sta diffondendo attraverso il cloud **AWS** (Amazon Web Services) per ottenere accessi multipli non autorizzati e estrarre criptovaluta **Monero** tramite lo strumento di mining XMRig.

Questo è quanto emerge dalla pubblicazione dei ricercatori di Cado Security secondo cui il worm distribuirebbe anche ulteriori malware e tool di sicurezza offensivi:

- punk.py, uno strumento di post-exploitation SSH;
- log_clean.c, uno strumento di pulizia registro;
- il Rootkit Diamorphine;
- la backdoor Tsunami IRC

Attraverso questo malware i criminal hacker riescono, oltre che prendere di mira specificamente AWS per scopi di cryptojacking, a carpire credenziali locali e eseguire scansioni Internet alla ricerca di piattaforme Docker e Kubernetes pericolosamente esposte in rete.

TeamTNT: analisi del codice malevolo

Il team di Cado Security ha attribuito il worm al gruppo TeamTNT (gruppo altamente prolifico apparso all'inizio dell'anno e di cui precedenti ricerche Trend Micro, Malware Hunter Team e r3dbU7z hanno fornito evidenze), trovando diversi riferimenti all'interno del codice malware.

Tra questi, in particolare, spicca il dominio chiamato teamtnt [.] Red che ospita il payload e che presenta una home page intitolata "TeamTNT RedTeamPentesting" con un elenco indirizzi di diverse sandbox pubbliche.

Come noto AWS CLI (l'interfaccia a riga di comando di AWS link https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html) archivia le credenziali ed ulteriori dettagli di configurazione (per gli account e la stessa infrastruttura AWS) in file non crittografati contenuti rispettivamente nelle

sottocartelle / .aws / credentials e / .aws / config presenti nella directory home oppure root del sistema AWS.

Pertanto il codice malevolo procede, utilizzando il comando curl, a scaricare dai sistemi compromessi i suddetti file (.credentials e .config) predefiniti di AWS, archiviandoli sul server criminale, presidiato ed in ascolto all'indirizzo sayhi.bplace [.] Net.

- Lo script malware TeamTNT, che contiene del codice copiato da un altro worm Kinsing osservato in precedenti campagne (è solito per il cryptomining copiare il codice della concorrenza, dicono i ricercatori) e progettato per arrestare gli strumenti di Alibaba Cloud Security, prevede anche delle routine:
- per eseguire la scansione (tramite il port scanner masscan) delle API Docker aperte, per poi successivamente avviare l'installazione del payload;

• per utilizzare il miner XMRig ed estrarre la criptovaluta Monero generando profitti illeciti. A tal proposito i ricercatori hanno scoperto almeno 119 sistemi compromessi e due wallet Monero collegati al gruppo hacker.

Attività di contrasto

Nonostante l'importo sino adesso racimolato ammonti a 3 XMR (circa 300 $) e che queste tipologie di attacchi non siano particolarmente sofisticate, resta alta la probabilità che il numero dei sistemi compromessi possa aumentare ulteriormente, considerando anche il trend crescente nell'utilizzare ambienti cloud e container da parte delle aziende, aprendo di fatto una nuova superfice di attacco per i criminal hacker. Non sono nemmeno da escludere prossime iniziative fotocopia.

I ricercatori di sicurezza consigliano alle aziende come attività di contrasto:

- di identificare i propri e eventuali sistemi che archiviano i file di credenziali AWS eliminandoli se non necessari;
- utilizzare strumenti firewall per limitare gli accessi alle API Docker;
- monitorare il traffico di rete delle connessioni ai pool di mining e di quelle che inviano credenziali AWS via HTTP;
- di implementare gli IoC pubblicati sugli apparati di sicurezza.

IoC

Monero Wallets
88ZrgnVZ687Wg8ipWyapjCVRWL8yFMRaBDrxtiPSwAQrNz5ZJBRozBSJrCYffurn1Qg7Jn7WpRQSAA3C8aidaeadAn4xi4k
85X7JcgPpwQdZXaK2TKJb8baQAXc3zBsnW7JuY7MLi9VYSamf4bFwa7SEAK9Hgp2P53npV19w1zuaK5bft5m2NN71CmNLoh

Domain Names
6z5yegpuwg2j4len.tor2web[.]su
dockerupdate.anondns[.]net
teamtntisback.anondns[.]net
sayhi.bplaced[.]net
teamtnt[.]red
healthymiami[.]com (Compromised)
rhuancarlos.inforgeneses.inf[.]br (Compromised)

IP Addresses
129.211.98[.]236
85.214.149[.]236
203.195.214[.]104

File-Hashes
3a377e5baf2c7095db1d7577339e4eb847ded2bfec1c176251e8b8b0b76d393f
929c3017e6391b92b2fbce654cf7f8b0d3d222f96b5b20385059b584975a298b

705a22f0266c382c846ee37b8cd544db1ff19980b8a627a4a4f01c1161a71cb0

https://www.key4biz.it/teamtnt-il-nuovo-worm-che-batte-criptomoneta-attraverso-il-cloud-di-amazon/318639/

Cybersecurity per i veicoli connessi in rete, spesa mondiale oltre i 3 miliardi di dollari nel 2025

Tutto ciò che è connesso in rete potrebbe essere esposto ad attacchi informatici di varia natura. È un assioma ed è valido anche per i **veicoli connessi in rete**, con altri veicoli, con le infrastrutture e le reti di distribuzione energetiche, i cosiddetti **V2X** o *Vehicle-to-everything*.

Esistono soluzioni tecnologiche *software* dedicate alla protezione informatica e digitale di tali veicoli e delle reti a cui sono connessi, sia interne al mezzo, sia esterne, cioè ***cloud based***.

Cyber sicurezza e guida connessa

La spesa mondiale in tecnologie di ***cybersecurity*** applicate all'industria V2X dovrebbe arrivare a sfiorare il miliardo di euro entro la fine del 2020, secondo nuove stime Research and

Markets.

Nei prossimi anni, la crescita delle reti **5G** e il moltiplicarsi dei loro impieghi, renderà la mobilità connessa in rete sempre più una realtà per un gran numero di aree urbane nel mondo, ma anche per le stesse reti autostradali, come nel caso del progetto europeo "***5G Carmen***", a cui partecipa anche l'Italia.

La spesa mondiale in tecnologie *cybersecurity* dedicate all'industria V2X è attesa raggiungere entro il 2025 il valore di 3,06 miliardi di dollari, ad un tasso di crescita media annua del +26,8% (Cagr 2020-2025).

Comunicazione veicoli a cloud (V2C)

Particolarmente rilevante in questo mercato è la tecnologia c*loud*. Nello specifico, il ***vehicle-to-cloud*** o V2C consente di archiviare un grande flusso di dati, anche sensibili, cioè relativi al conducente, quindi personali, come il tipo di guida, il comportamento al volante, la posizione di guida, i comandi più azionati e molto altro attinente al modo in cui portiamo un veicolo.

Il V2C è quindi sia una miniera di dati per le aziende della *cybersecurity*, sia una priorità in termini di attenzione e tutela, perché tutti i dati raccolti diventano poi informazioni preziose per migliorare la qualità dei servizi offerti.

V2X in Cina

La **Cina** è il Paese che per primo dovrebbe arrivare a lanciare entro il 2021 servizi V2X, in particolare V2C e veicolo verso l'infrastruttura (*vehicle-to-infrastructure* o V2I), proprio grazie all'attivazione di numerose reti 5G dedicate alla mobilità connessa.

Non è un caso che gli esperti automotive si attendono un boom delle vendite della Mercedes-Benz E-Class, automobile equipaggiata proprio con tecnologie V2X, V2C, V2I e relative misure di cybersecurity.

Per saperne di più: 5G

Cybersecurity per i veicoli connessi in rete, spesa mondiale oltre i 3 miliardi di dollari nel 2025