Cyber Insights di Vodafone Business

Ebook n. 1:
IL CYBERCRIME ORGANIZZATO
Di cosa si tratta?

Scopri di più

Together we can
vodafone
business

Indice

"La visione di Vodafone Business è garantire che le organizzazioni, i dipendenti e i clienti si sentano sicuri quando utilizzano le infrastrutture digitali emergenti.

Ci adoperiamo per contribuire a rendere più resiliente la tua attività, aiutandoti ad affrontare con successo qualsiasi sfida si presenti sul tuo cammino. Nel quadro di questo impegno, abbiamo lanciato il nostro Cyber Insights eBook: uno strumento per aiutarti a tenere il passo con un mondo in continuo cambiamento, quello dei rischi informatici. L'eBook presenta tutte le ultime tendenze e offre informazioni utili e consigli pratici per un futuro della tua attività in tutta sicurezza.

La crescita del cybercrime sembra inarrestabile. Gli incidenti di sicurezza informatica causati da dipendenti interni che agiscono con negligenza o con dolo, il crimine organizzato, i nation state hacker e gli hacktivisti rappresentano una grave minaccia per le aziende che devono affrontare un percorso tutto in salita per difendersi. Tuttavia, affrontare queste sfide non deve essere necessariamente costoso, complicato o scoraggiante.

In questo primo numero, esaminiamo più da vicino alcune delle principali minacce rappresentate dal cybercrime organizzato a livello internazionale e le semplici misure a cui puoi ricorrere per difendere la tua attività."

Andrzej Kawalec
Head of Security Portfolio di Vodafone Business

Introduzione

I cyberattacchi attuali combinano diverse tattiche e gruppi

Come ti immagini un cybercriminale? Se pensi a una persona chinata su un computer in una stanza buia, allora sei rimasto indietro di cinque o dieci anni. Ora, infatti, devi immaginarti un centinaio di persone, i team HR e le collaborazioni che superano i confini nazionali.

I cybercriminali più pericolosi agiscono in modo professionale, a livello internazionale, formando coalizioni e adeguandosi a nuovi trend globali. Solo per fare qualche esempio, l'anno scorso i cybercriminali hanno sfruttato a loro vantaggio il Covid-19, il telelavoro e alcune cause di giustizia sociale come il Black Lives Matter. Di recente si è osservato un cambiamento: i gruppi organizzati, infatti, operano sempre più spesso tramite i software e i sistemi. Questa struttura fondata sulla collaborazione e sull'adattabilità conduce a un aumento costante degli attacchi. Secondo le stime di Cybersecurity Ventures, il crimine informatico costerà alle aziende quasi $10,5 trilioni l'anno entro il 2025.[1]

Una cosa è certa. Tutti i cybercriminali, anche quelli meno organizzati, perfezionano costantemente le loro tecniche. Tuttavia, coloro che possono contare su un'organizzazione, e probabilmente anche su finanziamenti, perfezionano e adattano più rapidamente le proprie strategie. Non è mai facile associare un attacco a un determinato gruppo di persone, un paese o a motivazioni specifiche, e sembra che ora stia diventando ancora più difficile. Spesso i criminali informatici combinano più metodi in un unico attacco, tra i quali:

Spesso i criminali informatici combinano più metodi in un unico attacco, tra i quali:

- Phishing: ti inviano un'e-mail fasulla per cercare di indurti a rivelare i tuoi dati;
- Controllo del computer: accedono alle impostazioni dei tuoi dispositivi e ne assumono il controllo;
- Installazione di un ransomware: bloccano i tuoi file e richiedono il pagamento di un riscatto per rilasciarli;
- Attacco alla supply chain: manomettono gli elementi meno sicuri della tua supply chain per danneggiare la tua organizzazione;
- Sfruttamento delle falle nella sicurezza: cercano le vulnerabilità dei software e dei sistemi, compresi quelli di terze parti con le quali collabori;
- Acquisto o vendita di malware: affittano un ransomware da un altro gruppo, un modello conosciuto come Ransomware-as-a-Service (RaaS);
- Uso del Distributed Denial of Service (DDoS) : cercano di indurti a pagare il riscatto minacciando un attacco DDoS , che interromperebbe l'operatività dei tuoi sistemi rendendoli inaccessibili ad altri.

Nel corso del tempo, i cybercriminali organizzati passano da un'affiliazione all'altra, si scambiano hacker e cambian nome. Non di rado, quando un gruppo introduce una nuova funzione che si rivela efficace, gli altri gruppi adottano la stessa tecnica, replicando questo tipo di attacco. È così che emergono le nuove tendenze.

Ma non tutto è perduto. Chi vive in una zona a rischio sismico costruisce la propria casa secondo criteri diversi. Attualmente tutte le aziende si trovano nel cyberspazio. Per combattere il crimine informatico, è necessario che ogni azienda e i suoi dipendenti siano organizzati, proattivi e implacabili, proprio come i criminali. La maggior parte degli attacchi possono esser sventati mantenendo aggiornati i dispositivi, i software e i dipendenti, oltre che individuando prontamente eventual tentativi di truffa o attività sospette con l'obiettivo di bloccare le azioni criminose.

Ora esaminiamo più da vicino tre dei principali vettori di attacco usati nel cybercrime organizzato e alcune delle misure da adottare per garantire la sicurezza della tua attività.

Minacce cibernetiche in primo piano – 1

Gli attacchi ransomware e l'emergenza RaaS

Gli attacchi ransomware sono in continuo aumento tra i crimini informatici. Solo nel 2020 si è osservato un aumento del 150% negli attacchi ransomware e si prevede un ulteriore incremento nel 2021.[2] Non è difficile individuarne la ragione: a marzo 2021 il gruppo di hacker REvil ha richiesto a un produttore di computer il pagamento di un riscatto pari a circa $50 milioni; il più alto di sempre.[3] Di fatto, l'importo pagato dalle vittime di questi attacchi nel 2020 è cresciuto di oltre il 300%. [4]

Questi attacchi mirano a cancellare i tuoi backup, a creare copie dei tuoi dati e a crittografarli in modo tale che nessuno possa utilizzarli. Un altra pratica comune consiste nella minaccia da parte degli hacker di rendere pubblici o vendere i tuoi dati personali qualora non venga versato il riscatto richiesto. I cybercriminali ti inviano una nota di riscatto in cui sono riportate le informazioni sulla modalità di pagamento del riscatto e su come riottenere l'accesso ai tuoi dati. I più importanti gruppi di hacker come FIN11 sono passati di recente agli attacchi ransomware e al furto di dati a scopo di estorsione di denaro. Sono crimini che risultano particolarmente redditizi e con i quali è possibile colpire qualsiasi organizzazione.[5]

REvil è un esempio di operazione Ransomware-as-a-Service (RaaS), per cui i cybercriminali si servono degli strumenti ransomware già sviluppati da altri gruppi per i loro attacchi. Nel caso di REvil, se l'azienda vittima dell'attacco paga il riscatto, REvil guadagnerà circa il 20–30%, dividendo la differenza con i gruppi affiliati.[6]

Data la natura del RaaS, con cui i criminali con scarsa o nessuna conoscenza tecnica sono in grado di "fare affari" con il ransomware, questo tipo di crimine si è diffuso a macchia d'olio. Uno studio recente ha messo in luce che quasi due terzi degli attacchi ransomware realizzati nel 2020 proveniva da criminali che seguivano il modello RaaS.[7]

Minacce cibernetiche in primo piano – 1

Gli attacchi ransomware e l'emergenza RaaS

Studio di casi: Colonial Pipeline

A maggio 2021 è emersa la dura realtà di un attacco informatico andato a buon fine. L'azienda statunitense Colonial Pipeline, uno degli operatori di gasdotti leader su mercato statunitense, è stata costretta a interrompere temporaneamente le attività e bloccare i sistemi IT, dopo aver subìto un attacco ransomware dal gruppo DarkSide.[8]

Creata nell'agosto 2020, DarkSide è una piattaforma RaaS che i cybercriminali, una volta approvati, possono usare per condurre attacchi ransomware alle aziende. In primo luogo, gli affiliati attaccano le reti target, rubandone i dati e poi installando il codice ransomware per crittografarli.

Una volta installato il ransomware, DarkSide gestisce le negoziazioni e i pagamenti con le vittime. Dopo il pagamento del riscatto, gli affiliati ricevono una percentuale dell'importo versato.

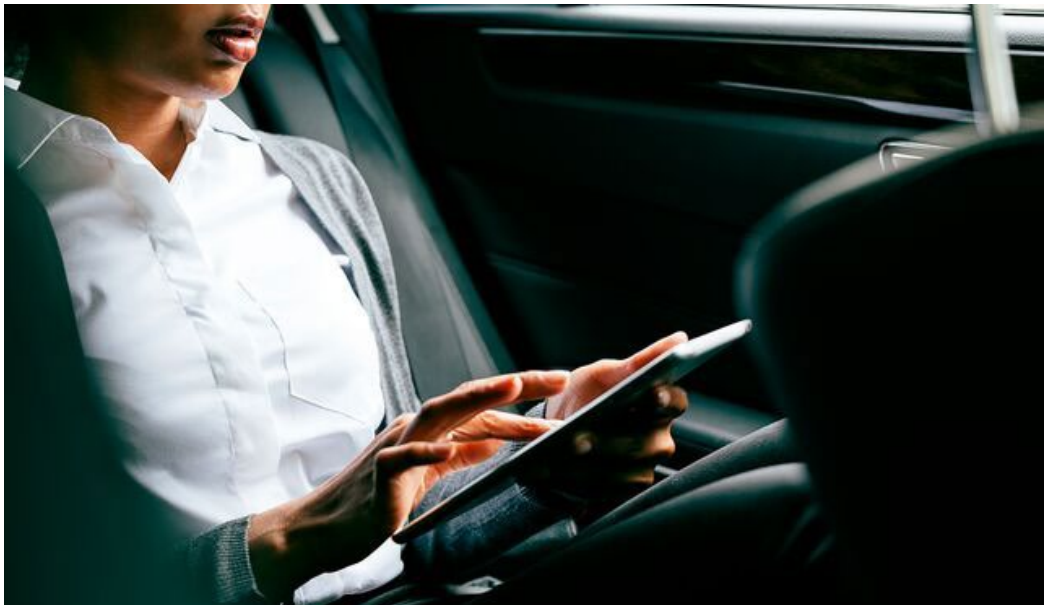
Nel caso di Colonial Pipeline, che fornisce circa il 45% del combustibile alla costa est degli Stati Uniti, gli hacker di DarkSide si sono impossessati di documenti sensibili per un volume di 100GB, minacciando di divulgarli in caso di mancato pagamento del riscatto. L'azienda ha preso la decisione di pagare il riscatto di circa $4,4 milioni al fine di riavviare il sistema di approvvigionamento in tempi rapidi e senza correre rischi.

Secondo le ultime indagini, DarkSide avrebbero ottenuto l'accesso tramite un account VPN dormiente. La password di questo account è stata trovata in un elenco di password rubate nel dark web. Un dipendente potrebbe aver utilizzato la medesima password per un altro account violato in precedenza. Questo sottolinea chiaramente l'importanza di avere una password diversa per ciascun account e di servirsi di un'autenticazione multifattoriale, se possibile.

Volere è potere

Anche se il phishing rimane il metodo più utilizzato per propagare il ransomware, gli attacchi RDP (Remote Desktop Protocol) con i quali i criminali controllano il cursore del dispositivo e le vulnerabilità del software si diffondono in misura sempre maggiore.[9]

La crescente diffusione del lavoro da remoto comporta anche un aumento delle minacce alle credenziali d'accesso. Una configurazione poco accurata dei servizi di accesso da remoto, come RDP e Virtual Private Networks (VPN), consente ai criminali di accedere facilmente alla tua rete. Non sorprende, dunque, che tra il primo e il quarto trimestre del 2020, gli attacchi RDP sono aumentati del 768%.[10]



Minacce cibernetiche in primo piano – 1

Gli attacchi ransomware e l'emergenza RaaS

Per accedere alle reti e distribuire il ransomware, le organizzazioni del cybercrime prendono di mira anche software obsoleti e privi di patch. Nell'aprile 2021, l'FBI ha scoperto una serie di attacchi su tre elementi vulnerabili e non protetti da patch in alcuni dispositivi FortiOS di Fortinet. L'obiettivo degli hacker era quello di ottenere l'accesso alla rete per rubare i dati e crittografarli.[11] A marzo 2021, almeno 10 gruppi di criminali informatici si sono serviti delle vulnerabilità del server di posta elettronica di Microsoft per condurre diversi attacchi in tutto il mondo.[12]

Le organizzazioni del cybercrime non guardano per il sottile, specialmente quando di tratta di un'attività redditizia come il ransomware, che prevede un riscatto medio di circa $170.000.[13] Queste organizzazioni hanno a disposizione una varietà di vettori di attacco tra i quali scegliere e con una ricompensa di tutto rispetto; troveranno il modo per fare affari.

Consiglio 1: "Patch" significa rammendo, ma questa volta non servono ago e filo

È importante che tutti i cellulari, i tablet, i computer e i software che usano i tuoi dipendenti vengano aggiornati regolarmente dal produttore. Gli aggiornamenti, oltre ad aggiungere funzionalità, riparano le vulnerabilità che il produttore ha individuato e che potrebbero comportare dei rischi per la sicurezza.

Una delle cose più importanti da fare per migliorare la sicurezza è installare questi aggiornamenti non appena vengono rilasciati[14]. E se un dispositivo, un sistema operativo, un'app o un software non viene più supportato? In questo caso è necessario sostituirlo con una versione supportata. Ove possibile, è opportuno impostare l'aggiornamento automatico sia per l'hardware che per il software. Questo è quanto: niente puntaspilli o codici complicati, la patch consiste nell'aggiornare e migliorare costantemente i tuoi sistemi.

Consiglio 2: Password sicure per un RDP sicuro

Esistono diversi modi per proteggere il tuo RDP dagli attacchi di forza bruta. Solitamente sono causati da una scarsa igiene informatica, ad es. password deboli o non esistenti per i punti d'accesso. Si consiglia di non pubblicare mai desktop remoti privi di protezione su Internet e di assicurarsi che i punti d'accesso siano protetti da un'autenticazione multifattoriale in modo che solo gli utenti autorizzati possano accedere al desktop remoto.

L'uso di un Remote Desktop Gateway tra l'Internet pubblico e i tuoi dispositivi interni RDP può altresì contribuire a mitigare gli attacchi.

Minacce cibernetiche in primo piano – 2

L'aumento del phishing, vishing, smishing e situazione attuale, BEC

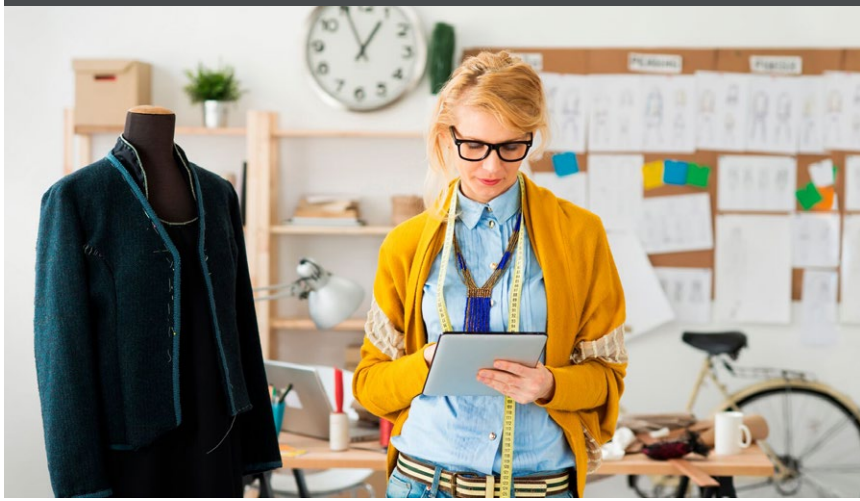
Il 57% delle aziende a livello internazionale ha subito nel 2020 un attacco di phishing andato a buon fine[15]. Con le campagne di phishing, i cybercriminali inviano e-mail ai dipendenti delle aziende per cercare di indurli a rivelare dati tramite una pagina web fittizia. Si servono poi delle informazioni ottenute per accedere alla rete aziendale. Rispetto al ransomware, il phishing rappresenta un tipo di truffa che consente di fare soldi facili. I criminali non devono preoccuparsi di scrivere codici o di diffondere virus. A loro basta inviare un'e-mail che sembri autentica. Una nuova tattica consiste nell'inviare queste e-mail dopo una vacanza, quando la casella di posta in entrata è piena di messaggi non letti che l'utente potrebbe aprire inavvertitamente.

Secondo il Rapporto sulla trasparenza di Google e i dati analizzati da Atla VPN, Google ha registrato più di due milioni di siti web di phishing nel 2020, che equivale a una media di oltre 46.000 nuovi siti a settimana. Forbes ha affermato che questa cifra "rappresenta un aumento del 19,91% su base annuale rispetto al 2019, una percentuale che indica l'incremento delle opportunità delle truffe online dovuto alla pandemia di Covid-19."[16]

Come si traducono questi dati in termini pratici? Uno studio di Cybersecurity Insiders su piccola scala condotto da 317 professionisti del settore IT e della cybersicurezza negli Stati Uniti ha rilevato che nel 2020 le aziende hanno subito una media di 1.185 attacchi di phishing ogni mese. Il 53% degli intervistati ha affermato che la sua organizzazione ha osservato un incremento degli attacchi di phishing per e-mail durante la pandemia di Covid-19 e il 36% ha espresso incertezza in merito alla capacità dei propri dipendenti di riconoscere ed evitare un attacco di phishing.[17]

Ecco alcuni degli oggetti dei messaggi e-mail più comunemente usati dai gruppi di cybercriminali per gli attacchi di phishing nel quarto trimestre 2020, secondo il Phishing By Industry Report (it. report sul phishing per settore) di KnowBe4.[18] Nella maggior parte dei casi è evidente come i gruppi sfruttino questa situazione particolare in cui milioni di persone lavorano da casa.

- **Twitter:** Allerta sicurezza: login nuovo o inconsueto a Twitter
- **Amazon:** Azione richiesta | La tua richiesta di iscrizione ad Amazon Prime è stata rifiutata
- **Zoom:** Errore nella pianificazione del meeting
- **Google Pay:** Pagamento inviato
- **Microsoft 365:** Azione richiesta: aggiorna l'indirizzo per la console del tuo Xbox Game Pass
- **Workday:** Reminder: è necessario eseguire un importante aggiornamento di sicurezza
- **DHL:** il tuo pacco è in arrivo, traccialo qui



Minacce cibernetiche in primo piano – 2

L'aumento del phishing, vishing, smishing e situazione attuale, BEC

Il tuo settore è a rischio? Le dimensioni della tua azienda fanno di te una preda facile?

KnowBe4 ha osservato che i settori attualmente più esposti al rischio di phishing sono il settore, manifatturiero, dell'istruzione, delle costruzioni, dei servizi per le imprese e delle tecnologie. Expert Insights, che ha pubblicato questi risultati, aggiunge che le piccole e medie imprese sono a rischio di attacchi informatici nella stessa misura delle grandi imprese. Di fatto, proprio perché di frequente non dispongono dell'infrastruttura o delle risorse per una protezione adeguata da eventuali attacchi, proprio le aziende di piccole dimensioni sono considerate facili prede.[19]

I criminali del vishing ora possono chiamarti "dal" numero della tua banca

Per gli attacchi di phishing i criminali di servono di e-mail e telefonate, mentre per il vishing, che è una combinazione di "voice" e "phishing", utilizzano i servizi di telefonia Internet (VoIP). Tramite un messaggio registrato o contattando personalmente la vittima, i visher si presentano come operatori professionali e ricorrono alla manipolazione emotiva con l'obiettivo di ottenere determinate informazioni. Inoltre, tramite una tecnica conosciuta come ID spoofing, i truffatori sono in grado di effettuare la telefonata dal numero verde dell'istituto di credito. Attualmente, infatti, il bersaglio di questo tipo di attacchi sono i clienti bancari.

Consegne a domicilio: il target dei furti di identità

Lo smishing è una forma di phishing che si serve di messaggi di testo (SMS) inviati al cellulare, i quali rimandano a un sito web fasullo, che sembra però identico a quello reale. Attualmente, le gang sfruttano il fatto che durante la pandemia le consegne a domicilio si sono moltiplicate. I messaggi di testo assomigliano, infatti, a quelli inviati dall'ufficio postale o da un servizio postale. Ti informano che è arrivato un pacco per te e che per ritirarlo devi versare una piccola somma tramite una pagina web. Il pagamento dell'importo, in realtà, non è che un espediente che consente ai cybercriminali di impadronirsi dei tuoi dati. I truffatori spesso dispongono già di informazioni personali su di te, ottenute da LinkedIn o dalla tua pagina Facebook.

Studio di casi: FluBot e Android

La truffa denominata Flubot si basa su un messaggio di testo che infetta i cellulari Android su tutte le reti. I cybercriminali inviano un SMS (smishing), simulando la provenienza da una società di spedizioni come FedEx e DHL. Questo SMS informa gli utenti dello stato di consegna di un pacco con un link per tracciare l'ordine. Il link in realtà contiene un malware.

Facendo clic sul link indicato, l'utente scarica app dannose (che contengono il modulo FluBot in forma criptata). Il malware assume il controllo del dispositivo dell'utente e invia SMS infetti agli altri contatti dell'utente. Oltre a tracciare le app aperte sul dispositivo, sovrascrive le pagine di login delle app di finanza con versioni malevole, progettate per impossessarsi delle credenziali di accesso e delle liste dei contatti, dei messaggi, delle chiamate e delle notifiche.

FluBot è stato individuato per la prima volta negli ultimi mesi del 2020 in seguito a campagne che hanno infettato il cellulare di più di 60.000 utenti in Spagna. A quanto pare, il virus ha raggiunto più di 11 milioni di numeri di telefono, ovvero il 25% della popolazione totale della Spagna. Secondo una nuova analisi di Proofpoint, gli attori della minaccia FluBot (alias Cabassous) hanno esteso la loro azione oltre i confini della Spagna per prendere di mira il Regno Unito, la Germania, l'Ungheria, l'Italia e la Polonia.[20]

Secondo le previsioni di Proofpoint, "FluBot continuerà a diffondersi rapidamente, muovendosi in modo metodico da paese e paese, potendo contare sull'azione consapevole degli autori di crimini informatici. Fino a quando gli utenti saranno disposti a fidarsi di un messaggio SMS e a seguire le istruzioni e i suggerimenti dei cybercriminali, le campagne come questa sono destinate ad andare a segno".

Minacce cibernetiche in primo piano – 2

L'aumento del phishing, vishing, smishing e situazione attuale, BEC

Il mittente di questa e-mail è davvero il mio capo?

La tecnica del Business Email Compromise (BEC) indica l'invio di un'e-mail di phishing che all'apparenza sembra provenire dall'azienda per cui lavori, forse anche dal CEO. Le ultime campagne BEC hanno preso di mira i vaccini contro il Covid-19 e i laboratori nei quali vengono sviluppati. Quest'anno le campagne di phishing e BEC continueranno a diffondersi e i cybercriminali perfezioneranno le loro tattiche.

La gang Cosmic Lynx di recente è passata dal malware agli attacchi BEC, un settore molto più lucrativo. Dal luglio 2020, la gang russa ha partecipato a più di 200 campagne BEC rivolte a dirigenti senior in 46 paesi. Rispetto ai consueti scammer che si servono della tattica BEC, il gruppo russo si contraddistingue per l'invio di e-mail molto ben scritte e scenari riguardanti le attività di fusione e acquisizione, che risultano poi fasulli, al fine di impossessarsi di ingenti somme di denaro.[21]

Consiglio 3: Diffondi consapevolezza e tienila sempre viva

È sufficiente che un tuo dipendente faccia clic su un link sospetto, usi una password facile da indovinare oppure dimentichi di aggiornare il dispositivo o il software, per consentire a un hacker di infiltrarsi nei tuoi sistemi. Accertati di informare con regolarità i dipendenti sulle ultime minacce e sulle misure da attuare per proteggersi. Basta lasciare una "finestra aperta" ... e i criminali si sono già infiltrati.

Insegna ai dipendenti la differenza tra un'e-mail legittima e uno scam. Insegna ai dipendenti a diffidare di tutto e a verificare qualsiasi elemento sospetto prima di fare clic, controllando ulteriormente su un altro canale come Google, ad esempio. Se vuoi, puoi fare anche un test: prova a inviare un'e-mail fasulla ai tuoi dipendenti, magari chiedendo aiuto al tuo partner per la sicurezza IT. Crea un'e-mail che sia veramente sospetta e difficile da identificare. Se i dipendenti cadranno nel tranello, e succederà, spiega loro cosa avrebbero dovuto fare.

I cybercriminali cambiano tattica di frequente, dunque è importante prestare attenzione a nuovi tipi di attacchi. Aggiorna costantemente il materiale che usi per la formazione con le ultime truffe individuate e includi nuove linee guida che specifichino cosa fare in caso di violazione. Ricorda di controllare le segnalazioni dei tuoi fornitori di sistemi tecnologici in merito a tutte le vulnerabilità nei sistemi che usi.

Minacce cibernetiche in primo piano – 3

L'aumento notevole dell'APT e gli attacchi zero-day

A dicembre 2020, SolarWinds (una grande azienda tecnologica americana) ha scoperto un attacco ai clienti del suo sistema di gestione della rete: Orion. Alcune delle più grandi organizzazioni del mondo si servono del software Orion, tra cui la maggioranza delle aziende incluse nella lista US Fortune 500 e molti dipartimenti del governo federale (anche se le ultime indagini rivelano che il Pentagono ne è uscito illeso.) Brad Smith, Presidente di Microsoft, ha descritto la violazione della supply chain di SolarWinds come "l'attacco più grande e sofisticato mai osservato prima d'ora."[23]

Gli esperti ritengono che dietro l'attacco a SolarWinds ci sia un gruppo russo come Cozy Bear o APT29. Matthieu Faou, ricercatore esperto di cybercrime, ritiene che Cozy Bear, che a suo avviso non è l'autore dell'attacco a SolarWinds, sia composto da diversi gruppi più piccoli. "Credo che [Cozy Bear] sia composto da diversi sottogruppi con diversi obiettivi e strumenti." Faou aggiunge che il gruppo "non è assolutamente monolitico".[24]

Gli hacker raggiungono nuovi livelli di furtività e pazienza

Le indagini riguardanti l'attacco a SolarWinds stanno mostrando i primi segni di compromissione risalenti già al settembre 2019. I cybercriminali sono rimasti invisibili e tranquilli per molti mesi, spiando l'azienda. È una strategia conosciuta come APT (Advanced Persistent Threat). Di frequente accade di vedere gruppi identificati con una APT e un numero, con cui vengono classificati dal governo degli Stati Uniti.

Minacce cibernetiche in primo piano – 3

L'aumento notevole dell'APT e gli attacchi zero-day

Il pericolo degli attacchi zero-day

La violazione di SolarWinds comprende una combinazione di metodi, tra cui il tentativo di usare una password utente comune su più account (password spray) e camuffare il codice in altri file (trojan).[25] Il metodo più preoccupante, però, è l'attacco zero-day o "zero-day malware".

Questo tipo di attacco viene effettuato prima che il fornitore di sistemi tecnologici abbia rilasciato una soluzione correttiva (patch) per porre rimedio a una carenza o "vulnerabilità" nella sicurezza. Di solito, quando scopriamo una vulnerabilità in un'infrastruttura, siamo in grado di rimediare. Gli attacchi zero-day, però, sono particolarmente pericolosi, proprio perché non lasciano il tempo di agire e di porre rimedio a una vulnerabilità con una patch che il fornitore non ha ancora rilasciato.

Nel 2019, il 50% dei malware identificati era stato classificato come minacce zero-day[26] e non ci sono segnali di rallentamento. In un contesto in cui i gruppi di criminali informatici si servono di strumenti sempre più sofisticati, gli attacchi diventano più audaci e assumono una portata di volta in volta più ampia. Gli esperti ritengono che gli attacchi zero-day avverranno una volta al giorno nel 2021, mentre nel 2015 si verificavano una volta a settimana.[27]

Consiglio 4: Ripeti frequentemente i tuoi processi di sicurezza

Anche se non è sempre possibile bloccare le violazioni, è essenziale identificarle e reagire immediatamente. Solo scoprendo tempestivamente gli attacchi, potrai ridurre i danni alla tua attività. Non farti prendere dal panico. Se un criminale si è introdotto nei tuoi sistemi, è possibile fermarlo. Se te ne accorgi.

Assicurati dunque di pianificare l'installazione regolare di patch di sicurezza e la formazione specifica e regolare dei dipendenti in modo da renderli consapevoli delle minacce. E soprattutto, non ci stancheremo mai di ripeterlo, esegui i processi di sicurezza con frequenza. Non solo di tanto in tanto.

E dopo?

Non perdere il prossimo Cyber Insights eBook oppure contattaci

Noi di Vodafone Business offriamo servizi e analisi a tutti i tipi di aziende: piccole, medie e grandi. Collaboriamo anche con agenzie di security intelligence leader di mercato come SecurityScorecard e Recorded Future, e aziende come Accenture, Lookout, Trend Micro e IBM, con l'obiettivo di garantire alla tua azienda i migliori risultati.

Indipendente dalla dimensione della tua organizzazione, noi di Vodafone Business ti offriamo assistenza in quattro semplici passi: **verifica, proteggi, scopri e rispondi.** In questo modo potrai proteggere i tuoi sistemi e garantire la sicurezza del tuo personale, i tuoi spazi, i tuoi beni e i tuoi dati: Se non vuoi farti sfuggire nessun pericolo, non perdere il prossimo numero di Cyber Insights eBook. Inoltre, se hai bisogno di aiuto in merito a uno dei nostri consigli o desideri ulteriori informazioni su come possiamo aiutarti a rendere la tua attività più resiliente, visita il nostro **sito web**. (Oppure, dal momento che non ci si deve mai fidare di un link, cerca Vodafone Business Security.)

Verifica

Esegui una verifica completa di tutti i dispositivi e software collegati alla tua rete. Ricorda che qualsiasi dispositivo connesso a Internet è una potenziale porta d'accesso. I criminali informatici possono usare il metodo forza bruta per impadronirsi della password, indovinare migliaia di possibilità al minuto o aggirare il problema usando un bug nel codice. Presta attenzione a qualsiasi falla. I dispositivi sono configurati correttamente? Le password sono sicure e casuali? I tuoi fornitori hanno accesso ai tuoi dati? Se sì, i loro sistemi sono sicuri? Memorizzano le tue password in un documento qualsiasi, conservato senza particolari precauzioni?

Proteggi

Mantieni i tuoi dispositivi e i software aggiornati alle ultime versioni. Rimuovi o disabilita programmi che non usi e serviti dell'autenticazione multifattoriale, ove possibile. Assicurati anche di fare il backup dei dati. In questo modo, non correrai il rischio di pagare un riscatto. Esegui il backup regolarmente, fai più copie e conserva almeno una copia in un'altra sede e offline per impedire che gli hacker la cancellino.

Scopri

Usa servizi come i firewall, IPS (Intrusion Prevention Systems) e IDS (Intrusion Detection Systems). Questi programmi monitorano la tua rete e ti avvisano circa potenziali intrusioni o attività insolite. Invia tutti i log a un server centrale e assicurati di monitorare e verificare i log per escludere attività sospette.

Rispondi

Se subisci un attacco, devi essere in grado di rispondere immediatamente per limitare il più possibile il danno. Se individui una violazione, disconnettiti dalla rete e fai riferimento al tuo piano di risposta agli incidenti (IR - Incident Response) per intraprendere le misure appropriate. Disconnetti i server dalla rete. Poi esegui una scansione e accertati che non ci siano codici malevoli nei dati. Aggiorna tutti i tuoi sistemi per assicurarti che usino la versione più recente e modifica tutte le password. È importante collaborare con una società esperta nella cybersicurezza affidabile che, in caso di violazione, potrà aiutarti a reagire e ripristinare i sistemi. Potrebbe essere opportuno anche stipulare un'assicurazione a copertura dei rischi informatici.

Riferimenti

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybersecurity Ventures, 2020

2. Ransomware Attacks Are Spiking. Is Your Company Prepared?, Harvard Business Review, 2021

3. $50m ransomware demand on Acer is highest ever, ComputerWeekly, 2021

4. Ransomware Attacks Are Spiking. Is Your Company Prepared?, Harvard Business Review, 2021;

5. This major criminal hacking group just switched to ransomware attacks, ZDNet, 2020

6. REvil ransomware explained: A widespread extortion operation, CSO, 2020

7. Ransomware Uncovered 2020/2021, Group-IB, 2021

8. Colonial Pipeline attack: Everything you need to know, ZDNet, 2021

9. Top 3 Attack Vectors Ransomware Loves to Exploit, Digital Defense

10. RDP Attacks Persist Near Record Levels in 2021, Dark Reading, 2021

11. FBI: Unpatched Fortinet Flaws Remain Under Attack by APT Actors, 2021

12. At least 10 hacking groups using Microsoft software flaw: researchers, Reuters, 2021

13. The average ransomware demand is now $170K. Here's how we can fight back, World Economic Forum, 2021

14. Cyber security for your organisation starts here, National Cyber Security Centre UK

15. Phishing attack victimization among businesses worldwide 2020, Statista, 2020

16. Google Registers Record Two Million Phishing Websites In 2020, Forbes, 2020

17. 2020 Phishing Attack Landscape Report [Greathorn], Cybersecurity Insiders, 2020

18. 2020 Phishing By Industry Benchmarking Report, KnowBe4, 2020

19. 50 Phishing Stats You Should Know In 2021, Expert Insights, 2021

20. FluBot Android Malware Spreading Rapidly Through Europe, May Hit U.S. Soon, Proofpoint, 2021

21. First-Ever Russian BEC Gang, Cosmic Lynx, Uncovered, Threat Post, 2020

22. Pentagon believes it escaped unscathed from SolarWinds, Microsoft hacks, Federal News Network, 2021

23. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president, Reuters, 2021

24. How the Russian hacking group Cozy Bear, suspected in the SolarWinds breach, plays the long game, CyberScoop, 2020

25. FBI, CISA Uncover Tactics Employed by Russian Intelligence Hackers, The Hacker News, 2021

26. As malware and network attacks increase in 2019, zero day malware accounts for 50% of detections, HelpNetSecurity, 2019

27. Zero Day Report 2017, Cybersecurity Ventures, 2017

Together we can

vodafone business