proofpoint.

EBOOK

Guida di sopravvivenza al ransomware 2022

Cosa ogni azienda dovrebbe fare prima, durante e dopo un attacco

Sommario

Sintesi

Il ransomware è una minaccia vecchia ma ancora rilevante. Questo tipo di ransomware, così chiamato per via del riscatto (ransom in inglese) chiesto alla vittima dopo il blocco dei file, è un problema molto serio per tutte le organizzazioni moderne. È una delle forme di attacco informatico più deleterie. I principali incidenti del 2021 negli Stati Uniti ai danni dell'approvvigionamento di carburante[1], generi alimentari[2] e infrastrutture sanitarie[3], dimostrano che nessuno è al sicuro, perciò è quanto mai necessario disporre di un piano non solo per mitigare i rischi ma anche per reagire in modo efficace qualora i sistemi vengano infettati dal ransomware.

Perché il ransomware è ancora in circolazione

Il ransomware persiste a causa di quattro fattori principali:

- I soldi dei riscatti sono più facili da raccogliere rispetto ad altri tipi di frode, grazie a Bitcoin e ad altre valute digitali.
- I criminali informatici hanno molti canali di distribuzione, compresi gli ambienti già compromessi, che aumentano le possibilità di successo.
- Molte aziende hanno difese informatiche deboli o obsolete, oltre a procedure di backup e ripristino non all'altezza, per cui rappresentano un bacino enorme di obiettivi potenziali.
- I criminali informatici stanno migliorando le loro strategie di attacco e le loro tattiche.

Come la maggior parte degli attacchi informatici, solitamente il ransomware richiede spesso un'azione da parte della vittima, come aprire un allegato o fare clic su un URL.

Sopravvivere al ransomware

Il ransomware compromette dati e sistemi, ma gli attacchi che producono questo risultato prendono di mira le persone. Come la maggior parte degli attacchi informatici, solitamente il ransomware richiede spesso un'azione da parte della vittima, come aprire un allegato o fare clic su un URL. È per questo che per combattere il ransomware è necessario un approccio incentrato sulle persone.

Puoi considerare questa guida come un punto di partenza.

1 David Sanger, Clifford Krauss, Nicole Perlroth *(New York Times)* "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." (Un attacco informatico costringe alla chiusura il più grande oleodotto degli USA), maggio 2021.
2 Julie Creswell, Nicole Perlroth, Noam Schreiber *(New York Times)* "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business." (Un ransomware paralizza delle fabbriche di carne nell'ultimo attacco contro aziende critiche americane), giugno 2021.
3 Nicole Perlroth, Adam Satariano *(New York Times)* "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks." (Ospedali irlandesi tra le ultime vittime degli attacchi di ransomware), maggio 2021.

Prima dell'attacco

La migliore strategia di sicurezza è quella di evitare del tutto il ransomware. Questo richiede impegno e una pianificazione rigorosa, prima che si verifichi un incidente.

Sviluppa un piano di backup e ripristino

Un componente fondamentale di qualsiasi strategia di sicurezza contro il ransomware è l'esecuzione di backup dei dati regolari. Dato che molti ceppi di ransomware prendono di mira i backup connessi alla rete, è necessario mantenere tali backup su una rete separata oppure nel cloud, assicurandosi di disattivare l'accesso del file system a tali backup[4].

Sorprendentemente, sono poche le aziende che eseguono test di backup e ripristino. Entrambe le operazioni sono importanti; i test di ripristino sono l'unico modo per sapere in anticipo se il piano di backup funziona.

Aggiorna i sistemi e applica le patch necessarie

Mantieni aggiornati i sistemi operativi, i software di sicurezza, le applicazioni e l'hardware di rete e applica tutte le patch necessarie.

Investi in robuste soluzioni di sicurezza incentrate sulle persone

Le soluzioni avanzate per la sicurezza dell'email proteggono contro allegati, documenti e URL dannosi contenuti nelle email vettori del ransomware. Tali soluzioni proteggono anche da altri malware, tipicamente inviati tramite l'email, che possono installare il ransomware in successivi attacchi mirati.

La formazione e la sensibilizzazione dei dipendenti sono essenziali. Devono sapere cosa fare, cosa non fare, come evitare il ransomware e come segnalarlo. Se i dipendenti ricevono una richiesta dal ransomware, devono sapere di doverlo segnalare immediatamente al team della sicurezza e mai pagare di propria iniziativa.

Pianifica la tua risposta

Essere estromessi dai sistemi business critical è stressante e questo stress influenza il nostro processo decisionale[5]. Se decidi in anticipo come risponderai, in caso di attacco puoi concentrarti sul contenimento delle minacce e sul ripristino delle attività.

Contro gli attacchi di ransomware non esiste un piano di risposta universale. Gli ospedali e le altre infrastrutture essenziali devono soppesare il costo di un'interruzione dell'attività in modo molto differente rispetto alle imprese commerciali. L'esecuzione di una simulazione completa è un ottimo modo per pianificare ciascuna fase della risposta agli incidenti.

4 W. Curtis Preston *(Network World)*. "How to protect backups from ransomware." (Come proteggere i backup dal ransomware), febbraio 2021.
5 Kathleen M. Kowalski, Charles Vaught *(International Journal of Emergency Management)* "Judgement and Decision-Making Under Stress: An Overview for Emergency Managers." (Giudizio e processo decisionale sotto stress: sintesi per i responsabili dei team di intervento d'urgenza), giugno 2003.

Durante l'attacco

Anche se la migliore strategia contro il ransomware è innanzitutto quella di evitarlo, gli attacchi sempre più sofisticati contro la filiera del software hanno dimostrato che anche le aziende meglio preparate possono cadere nella trappola del ransomware[6]. Il ransomware non è sempre il primo payload a infettare i sistemi. Ora molti gruppi dediti al ransomware preferiscono comprare l'accesso a obiettivi già infettati con un trojan o un loader.

Durante un attacco ci sono problemi urgenti da risolvere, come riportare in servizio computer, telefoni e reti e gestire le richieste di riscatto.

Contatta le forze dell'ordine

Il ransomware, come qualsiasi forma di furto e di estorsione, è un reato. La notifica alle autorità preposte è un primo passo necessario.

Dovresti anche anche contattare l'assicurazione se disponi di una copertura contro i rischi informatici.

Scollegati dalla rete

Non appena un dipendente riceve una richiesta di riscatto o nota un'anomalia, deve scollegarsi dalla rete e consegnare il computer infetto al reparto IT. Solo il team della sicurezza informatica deve intraprendere un'azione come il riavvio, e in ogni caso anche una tale misura sarà efficace solo nel caso in cui si tratti di un software ingannevole o di un malware classico.

Se il ransomware ha già raggiunto un server, il team della sicurezza deve isolarlo il prima possibile e stabilire una procedura di risposta.

Ma attenzione: come accade con i parassiti domestici, un singolo dispositivo infetto è solitamente segno di un problema più grande, per cui bisogna cercare nell'ambiente altri possibili sistemi infetti.

Applica la risposta pianificata

La strategia di risposta pianificata deve essere sufficientemente flessibile in modo da includere diversi fattori:

- Il tipo di attacco, ovvero il ceppo di ransomware usato e il criminale informatico responsabile
- La presenza di precedenti payload di malware che potrebbero essere stati usati per la ricognizione o per il caricamento del ransomware
- Chi è stato compromesso nella rete
- Le autorizzazioni di rete di cui sono dotati gli account compromessi

Le infezione di ransomware sono spesso infezioni secondarie che colpiscono reti già compromesse. Ciò significa che ciascuno di questi fattori è essenziale per valutare la portata del problema e prevenire ulteriori infezioni e perdite di dati.

Non contare su strumenti gratuiti di decodifica del ransomware

La maggior parte degli strumenti gratuiti funziona per un solo particolare ceppo di ransomware o addirittura una sola campagna di attacco. Man mano che il ransomware viene aggiornato, gli strumenti gratuiti diventano obsoleti e non funzioneranno contro le nuove varianti.

Ripristina i dati dal backup

L'unico modo per riprendersi completamente da un'infezione di ransomware è quello di ripristinare tutto da un backup. Ma anche con backup recenti, pagare il riscatto può essere la soluzione più semplice dal punto di vista finanziario e operativo.

6 Kellen Browning *(New York Times)* "Hundreds of Businesses, from Sweden to U.S., Affected by Cyberattack." (Centinaia di aziende, dalla Svezia agli Stati Uniti, colpite da un attacco informatico), luglio 2021.

Dopo l'attacco

Una volta passata la crisi, il lavoro è lungi dall'essere finito.

Analisi e rafforzamento

Consigliamo di eseguire una valutazione di sicurezza end to end per identificare le minacce che potrebbero ancora annidarsi nell'ambiente. Bisogna guardare in maniera approfondita agli strumenti e procedure di sicurezza per trovarne le lacune.

Pulizia

Alcuni ransomware vengono distribuiti tramite altre minacce o trojan backdoor che possono condurre a futuri attacchi. Spesso l'ambiente della vittima era già compromesso, lasciando la porta aperta al ransomware.

Ricerca attivamente le minacce occulte che potrebbero esserti sfuggite nella confusione dell'attacco soprattutto se c'è il rischio che anche i backup possano essere stati compromessi.

Procedi a una revisione post-mortem

Riesamina la strategia di preparazione alle minacce, la catena degli eventi che ha condotto all'infezione e la risposta all'incidente. Se non identifichi in che modo è penetrato il ransomware, non sarai in grado di fermare il prossimo attacco.

Valuta la consapevolezza degli utenti

Un utente bene informato è la tua ultima linea di difesa. Accertati che tutti i dipendenti, di qualsiasi livello, siano all'altezza del compito. Valutazioni regolari e simulazioni di attacchi di phishing ti aiutano a identificare gli utenti più vulnerabili, e a quali esche e altre tattiche sono più suscettibili.

Educa gli utenti

Sviluppa un programma di formazione per ridurre la vulnerabilità dei dipendenti agli attacchi informatici, basandolo su campagne e tattiche di attacco osservate in ambienti reali. Redigi un piano di comunicazione di crisi nel caso di un attacco futuro e prosegui con esercizi e test di penetrazione.

Rinforza le difese tecnologiche

Il panorama delle minacce attuale, in rapido cambiamento, richiede soluzioni di sicurezza che possano analizzare, identificare e bloccare, in tempo reale, gli URL e gli allegati dannosi che fungono da punti di ingresso primari per il ransomware.

Adotta delle soluzioni di sicurezza che possano adattarsi alle minacce nuove ed emergenti e permetterti di rispondere più velocemente.

Introduzione

Il ransomware esiste ormai da più di trent'anni, durante i quali ha subito diverse evoluzioni. Quando abbiamo aggiornato l'ultima volta questo report, i numeri del ransomware erano in calo perché le aziende e i fornitori di sicurezza sono riusciti a bloccare Locky, il ransomware responsabile del ritorno della minaccia nel 2016.

AUMENTO DEL 300% SU BASE ANNUA
degli attacchi di ransomware nella prima metà del 2021, secondo le statistiche fornite dal governo degli Stati Uniti.

Ma ora la situazione è cambiata. Secondo i dati del governo statunitense, il ransomware è in aumento dall'inizio del 2021, con una crescita di questo tipo di attacchi pari al 300%[7].

Questo aumento è dovuto all'evoluzione dell'ecosistema dei criminali informatici. Gli autori degli attacchi non si affidano più a un modello di distribuzione su larga scala e a riscatti di piccola entità. Invece, le bande dedite al ransomware ora collaborano spesso con altri distributori di malware, che forniscono loro accesso a sistemi già infettati con trojan e loader a fini di ricerca delle potenziali vittime, ricognizione e attacco. Questo approccio consente ai criminali di identificare obiettivi di alto valore, che hanno più da perdere in caso di interruzione delle attività e maggiori mezzi finanziari.

Questa nuova tendenza, unita all'aumento del valore di Bitcoin e di altre criptovalute, ha creato le condizioni per un'epidemia di ransomware.

Sotto i riflettori

Gli attacchi contro distretti scolastici, dipartimenti di polizia e trasporti pubblici, dimostrano la volontà crescente, da parte delle bande dedite al ransomware, di colpire le infrastrutture pubbliche.

Nei primi sei mesi del 2021, il ransomware è passato dall'essere un problema di sicurezza informatica a una crisi discussa ai più alti livelli del governo. Gli attacchi contro distretti scolastici, dipartimenti di polizia e trasporti pubblici, dimostrano la volontà crescente, da parte delle bande dedite al ransomware, di colpire le infrastrutture pubbliche.

Nel maggio 2021, i criminali affiliati al gruppo di ransomware DarkSide hanno colpito Colonial Pipeline, i cui gasdotti riforniscono gran parte della costa orientale degli Stati Uniti. L'attacco ha causato carenze in diversi Stati poiché i cittadini, in preda al panico, cercavano di fare scorte di beni di consumo quotidiani. Alla fine, Colonial Pipeline ha scelto di pagare un riscatto di oltre 4 milioni di dollari in Bitcoin per riavere accesso ai suoi sistemi[8].

Nello stesso mese, i criminali associati alla banda REvil hanno infettato JBS Foods, un'azienda di lavorazione della carne operante in svariati paesi, fra cui Stati Uniti, Brasile e Australia. Le forniture di carne bovina e di altri prodotti a base di carne si sono interrotte finché JBS non ha accettato di pagare un riscatto pari a 11 milioni di dollari[9].

7 James Rundle e David Uberti *(The Wall Street Journal)*. "How Can Companies Cope with Ransomware?" (Come possono le aziende affrontare il ransomware?), maggio 2021.
8 Collin Eaton and Dustin Volz *(The Wall Street Journal)*. "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." (Il CEO di Colonial Pipeline spiega perché ha pagato agli hacker un riscatto di 4,4 milioni di dollari), maggio 2021.
9 Jacob Bunge *(The Wall Street Journal)*. "JBS Paid $11 Million to Resolve Ransomware Attack." (JBS ha pagato 11 milioni di dollari per risolvere un attacco ransomware), giugno 2021.

All'inizio di luglio REvil è stato anche ritenuto responsabile di aver compromesso la supply chain della società di software Kaseya[10]. Da allora, DarkSide e REvil sono scomparsi dalla scena. Ma nuovi operatori di ransomware appaiono in continuazione e non è insolito che le bande cambino nome per sfuggire ai riflettori.

Con gli importi delle richieste di riscatto in aumento e i criminali informatici sempre più propensi a danneggiare seriamente le infrastrutture nazionali, intenzionalmente o meno, i governi di tutto il mondo stanno prendendo coscienza della serietà della situazione. In seguito all'incidente di Colonial Pipeline, il presidente degli Stati Uniti Joe Biden ha emanato un decreto finalizzato a potenziare le difese informatiche del paese. Ha inoltre interpellato il presidente russo Vladimir Putin per l'incapacità del suo governo di assicurare alla giustizia le bande di ransomware che operano dall'interno dei suoi confini.

Funzionamento del ransomware

Il ransomware blocca l'accesso ai dati o ai sistemi informatici, solitamente crittografando i file con estensioni specifiche (JPG, DOC, PPT, ecc.). I file restano inaccessibili finché la vittima non paga un riscatto in cambio del codice di decrittazione per sbloccare i file. In molti casi la richiesta di riscatto ha una scadenza: se non viene rispettata, il riscatto può raddoppiare oppure i dati possono andare perduti per sempre, essere divulgati o anche distrutti.

In un crescente numero di casi, le vittime subiscono più di un'estorsione: prima al fine di ottenere la chiave di crittografia per sbloccare i propri dati e poi per impedire ai criminali informatici di divulgarli o di venderne copie nel Dark Web.

Il costo reale

Nel 2020, quasi l'80% delle imprese statunitensi ha subito un attacco di ransomware e il 68% di esse ha scelto di pagare il riscatto[11]. Le conseguenze finanziarie di un attacco possono essere considerevoli, poiché gli importi dei riscatti aumentano ogni anno.

Nella prima metà del 2021 sono stati confermati pagamenti pari a 4,4 milioni di dollari nel caso di Colonial Pipeline[12], 11 milioni per JBS Foods[13] e la cifra record di 40 milioni da parte di CNA Financial[14]. E questi sono solo i casi che sono diventati di dominio pubblico. Il vero costo finanziario del ransomware è probabilmente molto più alto di quanto queste cifre rivelino, dato che molte aziende inevitabilmente cercano di affrontare un'intrusione con la massima discrezione.

Ma il costo per l'azienda non si limita all'aspetto finanziario.

Secondo Coveware, una società di consulenza specializzata nella risposta agli incidenti ransomware, più di tre quarti degli attacchi ransomware della prima metà del 2021 hanno comportato la minaccia di divulgazione dei dati trafugati[15]. Nel 2020, secondo la stessa società, il 65% delle vittime cui è stata paventata la divulgazione dei dati, ha scelto di pagare il riscatto. Questo evidenzia il grave rischio per la reputazione legato alla sottrazione dolosa dei dati.

80%
delle imprese statunitensi ha subito un attacco ransomware nel 2020.

68%
ha scelto di pagare il riscatto.

10 Jonathan Vanian *(Fortune)*. "Everything to know about REvil, the group behind a big ransomware spree." (Tutto quello che c'è da sapere su REvil, il gruppo dietro un'ondata di attacchi ransomware), luglio 2021.
11 Proofpoint. "State of the Phish 2021", febbraio 2021.
12 Collin Eaton and Dustin Volz (The Wall Street Journal). "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." (Il CEO di Colonial Pipeline spiega perché ha pagato agli hacker un riscatto di 4,4 milioni di dollari), maggio 2021.
13 Jacob Bunge (The Wall Street Journal). "JBS Paid $11 Million to Resolve Ransomware Attack." (JBS ha pagato 11 milioni di dollari per risolvere un attacco ransomware), giugno 2021.
14 Kartikay Mehrotra e William Turton (Bloomberg). "CNA Financial Paid $40 Million in Ransom After March Cyberattack." (CNA Financial ha pagato un riscatto di 40 milioni di dollari dopo l'attacco informatico subito a marzo), maggio 2021.
15 Coveware. "Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority." (Gli importi dei riscatti diminuiscono nella seconda metà dell'anno mentre il ransomware diventa una priorità della sicurezza nazionale)

Forse il costo più difficile da prevedere è quello dell'interruzione delle attività, dato che le supply chain si bloccano, gli addetti commerciali non possono consultare gli elenchi di clienti esistenti e potenziali e anche gli strumenti di comunicazione più basilari diventano inaccessibili. Le conseguenze possono essere ancora più gravi in settori critici come la sanità, come ha scoperto il servizio sanitario irlandese (Health Service Executive) quando un attacco della banda di ransomware Conti ha causato ritardi nella somministrazione delle terapie e la cancellazione dei servizi ambulatoriali come le radiografie[16].

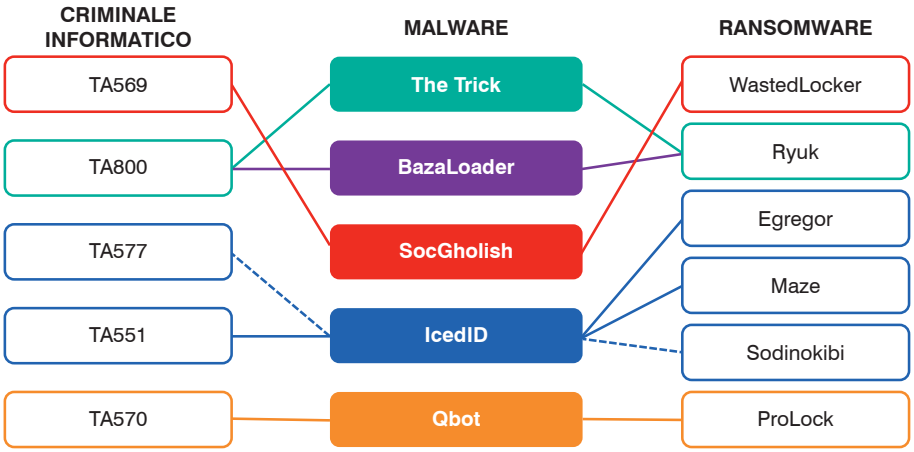
Ransomware e email

Un gran numero di attacchi ransomware inizia, direttamente o indirettamente, con un'email di phishing.

Un gran numero di attacchi ransomware inizia, direttamente o indirettamente, con un'email di phishing. Queste email inducono gli utenti ad aprire un allegato pericoloso o a fare clic su un URL dannoso.

Ma nei cinque anni successivi alla comparsa di Locky in milioni di caselle email, le cose sono cambiate. Il ransomware viene ora inviato come infezione secondaria dopo che un sistema è già stato infettato con un trojan o un loader. I gruppi che distribuiscono questi tipi di malware vendono poi l'accesso alle bande di ransomware che, fra le reti infette, vanno alla ricerca degli obiettivi più interessanti. In cambio di un punto di ingresso a una rete, I broker o facilitatori incassano una commissione forfettaria oppure una percentuale del riscatto.

Non esiste necessariamente un legame univoco tra il malware dell'accesso iniziale e il ceppo di ransomware che successivamente infetta le vittime. Tuttavia, i ricercatori di Proofpoint e altre aziende del settore hanno identificato delle interessanti associazioni.



La rete di relazioni tra i gruppi di criminali informatici è complicata, ma la sequenza di eventi in un tipico attacco di ransomware via email non lo è: l'infezione con un trojan o un loader lascia la rete vulnerabile alle bande di ransomware che cercano obiettivi di valore elevato. Quindi, per la maggior parte delle aziende, la prima linea di difesa contro il ransomware consiste nel proteggersi contro gli altri tipi di malware.

In altre parole, è necessario bloccare il loader per bloccare il ransomware.

16 Danny Palmer (ZDNet) "The human cost of ransomware: Disruption to Irish health service will continue for months." (Il costo umano del ransomware: i danni causati al servizio sanitario irlandese dureranno per mesi), giugno 2021

Nel 2020 a un dipendente di Tesla sono stati offerti 500.000 dollari per installare un ransomware nella rete aziendale.

La minaccia interna

Oltre alle esche inviate via email e agli exploit tecnici, i criminali informatici hanno aperto un altro fronte nella guerra del ransomware: i collaboratori complici. In un piccolo ma allarmante numero di casi, i criminali informatici cercano di reclutare i dipendenti delle aziende prese di mira affinché installino il ransomware nei loro luoghi di lavoro in cambio di denaro.

Nel 2020 a un dipendente di Tesla sono stati offerti 500.000 dollari per installare un ransomware nella rete aziendale. Il dipendente ha denunciato il tentativo, il responsabile è stato arrestato e si è dichiarato colpevole, ma non prima di essersi vantato dei propri successi altrove.

Nell'agosto del 2021 abbiamo scoperto una campagna email che offriva ai dipendenti 1 milione di dollari per installare il ransomware DemonWare nel loro luogo di lavoro. Nello stesso periodo, LockBit ha aggiornato il suo messaggio di riscatto offrendo di pagare milioni di dollari al personale interno in cambio di credenziali valide.

Nelle proprie email di reclutamento, l'autore di DemonWare non ha tentato di inviare alcun malware. Alcune soluzioni avanzate per la sicurezza dell'email sono in grado di rilevare questi tentativi di corruzione in base ad altri segnali. È comunque utile formare i dipendenti a riconoscere queste minacce e segnalarle tempestivamente.

Origini

I vettori principali per la distribuzione del ransomware sono:

- L'email, inclusi gli allegati di ransomware e gli URL che conducono a file dannosi
- La violazione delle connessioni remote di tipo RDP (Remote Desktop Protocol) e VPN (Virtual Network Protocol)
- Le vulnerabilità nelle apparecchiature di rete aziendale
- I siti web infetti o i collegamenti dannosi pubblicati nei social media e le pubblicità infettate dal malware (malvertising)
- Altri malware (come i loader e gli stealer) che possono infettare con il ransomware i sistemi già compromessi

Anche quando il ransomware nasce da altro malware, il vettore iniziale è spesso un'email, che sembra legittima e non suscita sospetti nei dipendenti che la ricevono. Spesso fingono di comunicare aggiornamenti legittimi del software, fatture non pagate o addirittura note inviate dal diretto superiore.

Perché il ransomware è ancora in circolazione

Il ransomware è un tipo di exploit che esiste da decenni, ma è diventato una minaccia sempre più critica a causa di quattro fattori principali.

Più canali di distribuzione

I criminali informatici possono aggredire migliaia di entità simultaneamente, utilizzando più vettori e aprendo la porta ad attacchi ransomware secondari.

Le difese informatiche tradizionali sono sopraffatte da minacce provenienti da tutte le direzioni:

- Campagne email massive tramite botnet
- Vulnerabilità sfruttabili nel software e nell'hardware di rete
- Malware polimorfico che supera la capacità dei fornitori di sicurezza di realizzare le nuove firme del malware
- Malvertising e siti web compromessi all'esterno del perimetro dell'azienda.

Insieme, questi fattori aumentano la probabilità di violazione, dando al ransomware maggiori opportunità di penetrazione.

Obiettivi più redditizi

Invece di lanciare attacchi ad ampio raggio, i criminali informatici stanno sempre più prendendo di mira le aziende che gestiscono dati sensibili, hanno dipartimenti IT oberati di lavoro e una forte motivazione a trovare una soluzione rapida.

A peggiorare la situazione sono le problematiche di sicurezza comuni a ospedali, servizi di polizia, scuole e altri enti pubblici nazionali e locali.

Per queste organizzazioni, un guasto alle reti non è un'opzione ammissibile. Non sorprende che molti ritengano che pagare il riscatto sia la migliore mossa dal punto di vista della gestione dell'azienda.

Una mira affinata e tattiche più sofisticate

Il ransomware una volta aveva un approccio quantitativo: attaccavano centinaia di migliaia di destinatari in campagne via email ad alto volume chiedendo riscatti contenuti, nella speranza che un numero sufficiente di vittime abboccasse.

Oggi, i criminali informatici sono sempre più selettivi in termini di obiettivi. Nella speranza di ottenere pagamenti più consistenti, cercano dati e sistemi critici e strategici che sono sia vulnerabili che assolutamente necessari per le loro vittime.

Allo stesso tempo, gli attacchi di ransomware stanno diventando sempre più sofisticati. Invece di utilizzare il ransomware nella prima fase di un attacco, i criminali informatici compromettono i sistemi con un malware più robusto e versatile.

Una volta stabilita una base all'interno, distribuiscono il ransomware sui dispositivi cui sono interessati.

Bitcoin e altre valute digitali

Fin dal suo debutto nel 2009, Bitcoin è stato una manna per chi promuove le libertà civili, ma anche per i criminali informatici. I pagamenti infatti non possono essere fatti risalire né al mittente né al destinatario, il che costituisce una modalità anonima e priva di intralci per le transazioni commerciali private.

Richiedendo il pagamento in Bitcoin, i criminali informatici ottengono l'anonimato che permette di riscuotere i riscatti facilmente come mai prima d'ora. Le precedenti forme di ransomware chiedevano l'uso di una carta di debito prepagata. Sebbene questo metodo fosse in grado di eludere le misure antifrode delle banche, era meno conveniente per entrambe le parti coinvolte nella transazione.

Tutte le principali varianti di ransomware richiedono un pagamento in Bitcoin (consultare **"La pista dei Bitcoin" a pagina 13**).

Una minaccia duratura

Per capire quanto siano insidiosi gli attacchi odierni del ransomware, e in che modo hanno un effetto diretto sui consumatori, consideriamo l'attacco sferrato a Garmin Ltd., il servizio di rete che distribuisce i dati agli smartwatch e ai fitness tracker Garmin, fra gli altri dispositivi.

Garmin Ltd. si avvale della tecnologia GPS per condividere i dati con i fitness tracker come quelli di FitBit e Apple. Questi servizi hanno subito un'interruzione il 23 luglio 2020, quando Garmin ha subito un attacco informatico che ne ha crittografato i sistemi online, compresi "assistenza clienti, applicazioni dal lato dei clienti e comunicazioni aziendali", come affermato in un comunicato stampa rilasciato dall'azienda.

Garmin non poteva più erogare molti dei suoi servizi perché questi ultimi e quelli forniti dai call center erano stati crittografati e né gli utenti né l'azienda potevano accedervi. Secondo le fonti, non è stato possibile decrittografare i servizi finché Garmin non ha pagato un riscatto di 10 milioni di dollari agli estorsori.

Il 1° agosto il sito di notizie tecnologiche BleepingComputer ha riportato che "Una fonte vicina al gruppo di risposta agli incidenti di Garmin e un dipendente di Garmin hanno confermato […] che l'attacco è stato compiuto dal ransomware WastedLocker".

> "Il team IT di Garmin ha tentato di spegnere da remoto tutti i computer in rete dopo aver rilevato che alcuni dispositivi erano stati crittografati, compresi i computer di casa connessi tramite VPN ", ha riportato BleepingComputer. "Quando l'operazione non ha funzionato, è stato chiesto ai dipendenti di spegnere qualsiasi computer in rete a cui avevano accesso".

Garmin ha affermato di aver iniziato il riavvio dei propri servizi online quattro giorni dopo.

Secondo BleepingComputer il ransomware WastedLocker è stato fatto risalire al gruppo di criminali informatici russi Evil Corp. Anche se il nome sembra evocare il cattivo di un cartone animato, nel dicembre 2019 Evil Corp è stato accusato dal Dipartimento della Giustizia statunitense di aver giocato un ruolo nel caso del malware Dridex e di aver usato il ransomware in altri attacchi, fra cui il ransomware Locky e il loro proprio ceppo chiamato BitPaymer.

La pista dei Bitcoin

Nei tradizionali rapimenti a scopo di estorsione, la maggiore difficoltà è sempre stata quella di raccogliere il riscatto senza intoppi. Purtroppo i criminali informatici che utilizzano il ransomware hanno vita molto più facile.

La forma più diffusa di pagamento è l'uso di criptovalute, che non sono tracciabili, come la notissima Bitcoin. Bitcoin consente pagamenti fra persone tramite Internet, senza il coinvolgimento di banche o governi.

Un modo semplice per comprendere le criptovalute è quello di immaginarle come l'equivalente elettronico di una fiche del casinò. Le fiche non hanno un valore intrinseco nel mondo reale, ma gli utenti possono acquistarle nella loro valuta locale e usarle nell'ambiente stabilito, in questo caso Internet, e convertirle in valuta all'uscita.

Analogamente, le criptovalute sono acquistabili online con una carta di credito o un conto corrente, da fonti legittime. Nel caso del ransomware, una vittima può, per esempio cambiare la propria valuta in Bitcoin e inviarli a un portafoglio di criptovalute anonimo, messo a disposizione dal ricattatore informatico.

Non sempre gli importi vengono inviati direttamente all'estorsore. Normalmente i Bitcoin raggiungono un "tumbler", un servizio elettronico che mescola i Bitcoin di diverse transazioni e poi li paga all'estorsore (con una numerazione differente, ma di pari valore al netto della commissione).

Come nel caso del riciclaggio nel mondo fisico, i criminali informatici ricevono così un pagamento non tracciabile, che poi cambiano nella propria valuta fisica locale vendendo i Bitcoin in cambio di contanti.

A differenza delle valute ufficiali, le criptovalute non sono riconosciute ovunque come strumenti finanziari, ma sono invece considerate alla stregua delle fiche del poker o dei gettoni. Pertanto, il sistema di trasmissione e i tumbler di criptovalute non sono regolamentati ma non sono considerati un sistema di riciclaggio del denaro, anche se il risultato è fondamentalmente lo stesso.

L'attrattiva dei Bitcoin è ovvia: fornisce ai criminali una valuta informatica internazionale difficile da tracciare che può essere convertita direttamente in una valuta fisica locale, l'equivalente delle "banconote non segnate" dei riscatti tradizionali.

Un tale approccio ha dei chiari vantaggi rispetto all'uso delle carte di credito rubate, il cui valore crolla da un giorno all'altro poiché le istituzioni finanziarie sono ora in grado di congelare tempestivamente i conti delle vittime.

E dato che il valore del Bitcoin è aumentato negli ultimi anni, con un picco di quasi 65.000 dollari per Bitcoin, si aggiunge un ulteriore incentivo finanziario per i criminali informatici.

A seguito dell'attacco a Colonial Pipeline, l'FBI ha rivelato di aver recuperato circa metà del riscatto pagato in Bitcoin. L'agenzia federale non ha però rivelato come e non è chiaro se un tale recupero possa essere ripetibile[17],

17 Katie Brenner, Nicole Perlroth *(New York Times)* "U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack." (Gli Stati uniti sequestrano una parte del riscatto pagato agli hacker nell'attacco a Colonial Pipeline), giugno 2021.

Prima dell'attacco

La migliore strategia di sicurezza è quella di evitare del tutto l'estorsione. Ciò è possibile per la maggior parte delle aziende, ma richiede impegno e un'attenta pianificazione prima di essere colpiti da qualsiasi incidente.

Elabora un piano di backup e ripristino

Il componente più importante di qualsiasi strategia di sicurezza contro il ransomware è l'esecuzione di backup dei dati regolari. La maggior parte delle aziende ha dei backup, ma sorprendentemente sono poche quelle che eseguono test di backup e ripristino. Entrambi sono importanti e le esercitazioni di ripristino sono l'unico modo per sapere in anticipo se il piano di backup funziona,

Può essere necessario correggere alcune procedure prima che si verifichi un incidente. Se i test di backup e ripristino vengono svolti regolarmente, un'infezione di ransomware non avrà un impatto devastante perché si disporrà di un punto di ripristino recente e sicuro.

Aggiorna i sistemi e applica le patch necessarie

Assicurati che i sistemi operativi, il software di sicurezza, le applicazioni e l'hardware di rete siano aggiornati con tutte le patch applicate. Può sembrare ovvio, ma secondo un recente sondaggio più della metà delle aziende afferma che non esiste un modo facile per capire se le vulnerabilità vengono coperte dalle patch in modo tempestivo. I manager interpellati affermano che gli aggiornamenti variano notevolmente in termini di complessità e tempi di rilascio[18].

Esistono però dei punti di riferimento per la gestione delle patch, come il CIS (Center for Internet Security), un'organizzazione no profit che promuove e condivide le best practice per la gestione della sicurezza informatica, comprese le minacce ransomware.

Quando si tratta di patch, è fondamentale non abbassare la vigilanza, perché il rigore in questo settore è essenziale per mantenere un ambiente sicuro. Correggere le falle di sicurezza dei protocolli di accesso remoto o nelle connessioni VPN può essere la soluzione per bloccare punti di accesso da cui i criminali informatici possono sferrare attacchi di ransomware.

Pianifica la tua risposta

Stabilisci in anticipo come reagirai, in modo da concentrarti sul contenimento delle minacce e sul ripristino in caso di un attacco. Subire un attacco ransomware sul momento è un'esperienza stressante e ogni secondo è prezioso per impedire ai criminali informatici di penetrare sempre di più nella rete, aggravando i danni.

18 Ponemon Institute. "Today's State of Vulnerability Response: Patch Work Demands Attention." (Report sulla correzione delle vulnerabilità: le patch hanno bisogno di attenzione da parte delle aziende), aprile 2018.

È più difficile rispondere in tempo reale a domande quali: chi deve essere informato, come preservare le comunicazioni, quanto si è disposti a pagare e se si è disposti a pagare un riscatto. Questa pressione crea potenzialmente dei colli di bottiglia nel processo decisionale e può portare a costosi ritardi. Se si decide di pagare il riscatto, è necessario stilare un piano appropriato, che include i dirigenti esecutivi chiave, il personale operativo e i consulenti legali.

Contro gli attacchi di ransomware non esiste un piano di risposta universale. Gli ospedali e le altre infrastrutture essenziali valuteranno il costo di un'interruzione dell'attività in modo molto differente rispetto alle imprese commerciali. L'esecuzione di una simulazione completa è un ottimo modo per pianificare ciascuna fase della risposta agli incidenti.

Investi in soluzioni di sicurezza robuste, incentrate sulle persone, per proteggere i tuoi ambienti email, web e cloud

Le email di phishing attuali sono sofisticate ed estremamente mirate. Gli hacker studiano attentamente i propri obiettivi per manipolarli con email apparentemente legittime.

L'email: il vettore più critico

I gateway email, i filtri web e i software antivirus tradizionali devono essere aggiornati e funzionanti su tutte le reti, ma da soli non sono in grado di contrastare la minaccia del ransomware. Un'efficace soluzione per la sicurezza dell'email deve andare oltre.

Dato che l'email è il punto dell'infezione iniziale per la maggior parte degli attacchi ransomware, servono soluzioni avanzate che proteggano questo vettore critico.

Ciò significa, per esempio, analizzare gli URL incorporati e gli allegati per assicurare che nessun contenuto dannoso violi il sistema. I criminali informatici sono sempre un passo avanti e le configurazioni tradizionali per la sicurezza email si affidano troppo a firme obsolete.

Le soluzioni avanzate per la sicurezza dell'email proteggono contro allegati, documenti e URL dannosi contenuti nelle email vettori del ransomware. L'autenticazione dell'email basata sullo standard DMARC aiuta a bloccare gli attacchi che si affidano allo spoofing del dominio per ottenere la fiducia degli utenti. La tua soluzione per la sicurezza dell'email deve proteggerti anche contro altri tipi di frode dell'identità, come lo spoofing del nome visualizzato e i domini fotocopia.

Proteggi i tuoi account cloud

Gli account email cloud sono un altro importante vettore per la diffusione del malware. I criminali informatici possono assumere il controllo di alcuni account cloud per colpire altri utenti all'interno della stessa azienda. Gli account email possono essere compromessi in vari modi, fra cui:

- Attacchi di forza bruta automatizzati (tentativi di connessione con innumerevoli combinazioni di nome utente/password fino a trovarne una che funziona)
- Furto delle credenziali di altri account dello stesso utente (sfruttando il fatto che gli utenti spesso riutilizzano le stesse password per diversi account)
- Malware per il furto delle credenziali d'accesso
- Controlli cloud malfunzionanti

Proteggere gli account cloud è una componente critica di una strategia di protezione contro gli attacchi ransomware.

Infine, è importante richiedere agli utenti remoti di connettersi a Internet tramite una VPN aziendale, in modo che siano protetti dalle difese di sicurezza informatica dell'azienda ovunque si trovino.

Trasforma i dipendenti nella tua ultima linea di difesa

La maggior parte delle infezioni di malware inizia con un singolo dipendente in buona fede che apre un'apparente email di lavoro.

È per questo che la formazione e la sensibilizzazione dei dipendenti sono essenziali. Devono sapere cosa fare, cosa non fare, come evitare il ransomware e come segnalarlo. Un programma di formazione che si basa su attacchi reali e fornisce un sistema di segnalazione dei messaggi sospetti aiuta gli utenti a individuare i messaggi dannosi e rafforza i comportamenti positivi.

Se un dipendente riceve una richiesta dal ransomware, deve sapere di doverlo segnalare immediatamente al team della sicurezza e mai pagare di propria iniziativa. Il pagamento può avere gravi ripercussioni sulla reputazione di un marchio e sulla sicurezza e, in alcuni casi, potrebbe contravvenire alle normative in vigore. Questa decisione deve essere ponderata attentamente dalla dirigenza con un consulente legale.

Le nostre ricerche mostrano che i criminali informatici sfruttano attivamente gli errori e la curiosità umana. Questo approccio fa parte di una tendenza più ampia del crimine informatico: manipolare gli utenti per renderli inconsapevolmente complici degli attacchi per bloccare i dati e richiedere un riscatto per il loro rilascio.

Questi attacchi sfruttano la mancanza di conoscenza degli utenti. Spesso richiedono agli utenti di eseguire diverse azioni, come aprire i documenti allegati dannosi, scaricare e aprire o eseguire documenti o script. L'attivazione di macro in un documento dannoso, per esempio, può portare al download del ransomware e lanciare il processo di attacco.

La formazione più efficace spiega agli utenti le tecniche e le campagne di attacco del mondo reale e include anche le più recenti informazioni sulle minacce, in modo che gli utenti abbiano familiarità con le minacce che hanno le maggiori probabilità di affrontare. Le simulazioni di phishing possono aiutare a identificare gli utenti particolarmente inclini a cadere vittima del ransomware e di altre tattiche di attacco.

Raccomandazioni tecniche delle autorità statunitensi

Oltre alla strategia generale esposta nella presente guida, l'FBI raccomanda inoltre le seguenti misure tecniche per scongiurare gli attacchi di ransomware.

Verifica e gestisci i privilegi degli utenti

Adotta un approccio di minimo privilegio per le autorizzazioni legate a file, cartelle e condivisioni di rete.

Gli utenti che non hanno bisogno di modificare un file, per esempio, dovrebbero avere accesso in sola lettura. In molti casi, gli utenti non dovrebbero avere alcun accesso. Un addetto alle casse non ha bisogno di accedere ai libri contabili dell'azienda. Allo stesso modo, l'amministratore di un ospedale non ha necessità di consultare le cartelle cliniche dei pazienti.

Dai agli utenti solo il livello di accesso di cui hanno bisogno per svolgere il proprio lavoro.

Blocca l'esecuzione del codice in determinati punti

Definisci controlli software per impedire l'esecuzione di codice nei punti comunemente usati dal ransomware. Questi includono le cartelle temporanee create dai browser web e le directory dei file compressi nella cartella AppData/LocalAppData di Windows.

Blocca i software sconosciuti

È consigliata l'adozione di una policy di liste di autorizzazione che consentano l'esecuzione nei sistemi dei soli programmi noti e verificati. Tale policy dovrebbe impedire l'esecuzione della maggior parte dei ransomware, ma può non essere applicabile in tutti gli ambienti di lavoro.

Utilizza macchine virtuali

Le macchine virtuali consentono di eseguire applicazioni e addirittura interi sistemi operativi in un ambiente isolato.

La si può immaginare come una "camera di detonazione" per il software. L'esecuzione di un codice sensibile o non verificato all'interno di un ambiente o contenitore VM assicura che, nel caso in cui insorgano dei problemi di sicurezza, restino confinati a tale ambiente virtuale, lasciando le altre parti del sistema intatte.

Segmenta dati e sistemi

Mantieni separati dati e sistemi critici, cosicché un problema di sicurezza non influisca sugli altri sistemi. Per esempio, i dati sensibili di ricerche o informazioni aziendali non dovrebbero risiedere sullo stesso server e segmento di rete dell'ambiente email di un'azienda.

Le raccomandazioni complete del governo statunitense sono reperibili sul sito **fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf.**

Durante l'attacco

Sei stato colpito dal ransomware. Cosa fare?

Anche se la migliore strategia contro il ransomware è innanzitutto quella di evitarlo, gli attacchi sempre più sofisticati contro la filiera del software hanno dimostrato che anche le aziende meglio preparate possono cadere nella trappola del ransomware.
Il ransomware non è sempre il primo payload a infettare i sistemi: molte bande di ransomware preferiscono acquistare l'accesso a obiettivi già infettati con un trojan o un loader.

Durante un attacco ci sono problemi a breve termine da risolvere, come riportare in servizio computer, telefoni e reti e gestire le richieste di riscatto.

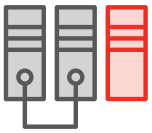
Ma reagire in preda al panico non è certamente una soluzione e può peggiorare la situazione.

Contatta le autorità

Il ransomware, come qualsiasi altra forma di furto e di estorsione, è un reato. Nessuno ha il diritto di bloccare l'accesso a dispositivi, reti o dati, tanto meno di chiedere un riscatto per essi. Avvisare le autorità preposte è un primo passo necessario.

Contatta immediatamente le forze dell'ordine locali o nazionali. Non aver paura di alzare il telefono e chiamarle, poiché è il loro compito.

Dovresti anche contattare l'assicurazione se disponi di una copertura contro i rischi informatici. Può aiutarti a coordinare la risposta agli incidenti e le indagini.



Isola i sistemi infettati

Non appena un dipendente riceve una richiesta di riscatto o nota un'anomalia (come non avere più accesso ai propri file, per esempio), deve scollegarsi dalla rete e consegnare il computer infetto al reparto IT.

Non è consigliabile che i dipendenti riavviino i propri sistemi. Solo il team della sicurezza informatica deve intraprendere un'azione come il riavvio, e in ogni caso anche una tale misura sarà efficace solo nel caso in cui si tratti di "scareware" o falso ransomware.

In tali casi quello che sembra ransomware è in realtà un software progettato per spaventare l'utente, ma è innocuo. Può bloccare lo schermo con una richiesta di riscatto e le istruzioni per il pagamento, ma senza in realtà crittografare i dati. In questi casi sono d'aiuto i normali strumenti antimalware.

Notare la differenza tra i due non è sempre facile. Determina la portata del problema in base alla threat intelligence. Tutto il ransomware è pericoloso, ma alcuni attacchi sono più aggressivi di altri. La risposta, compreso l'eventuale pagamento del riscatto, dipende da vari fattori.

Le domande da porsi sono le seguenti:

- **Di che tipo di attacco si tratta?** Questo attacco è un'infezione secondaria? Proviene da downloader, trojan di accesso remoto (RAT) oppure altro malware installato nel computer infettato o altri computer in rete?
- **Chi è stato compromesso nella rete?** Quanto sono diffuse le infezioni? Si tratta di un malintenzionato che sta sondando la rete, trafugando i dati o che è pronto a rilasciare il ransomware su altri dispositivi?
- **Quali autorizzazioni di rete possiedono gli account o i dispositivi compromessi?** Il ransomware potrebbe essere stato installato solo dopo che i criminali informatici si erano già spostati lateralmente nella rete oppure avevano sottratto credenziali e altri dati.

Le risposte a queste domande dovrebbero aiutare gli amministratori di rete a determinare la portata del problema, a stilare un piano di azione e possibilmente a bloccare la diffusione.

Ricorda che il ransomware si diffonde rapidamente e spesso deriva da altre minacce. Se trovi un'infezione, probabilmente ce ne sono altre che non si vedono, per cui devi cercare attivamente altri problemi nel tuo ambiente.

Applica il tuo piano di risposta

A seconda della configurazione della rete, potrebbe essere possibile limitare la diffusione a una sola postazione.

Nel migliore dei casi, si può cambiare il computer infettato con uno nuovo ed effettuare un ripristino dal backup. Nel peggiore, tutti i computer in rete sono infetti e in questo caso bisognerà calcolare i costi e benefici, valutando il tempo e le risorse necessarie per ripristinare i dati anziché semplicemente pagare il riscatto.

Se il ransomware ha già raggiunto i server, vanno isolati i sistemi colpiti. È qui che le attività di segmentazione della rete aiutano a contenere la minaccia.

Una parte importante della tua risposta consiste nel decidere se pagare o meno il riscatto. Dare una risposta è complicato e può essere necessario chiedere il consiglio delle forze dell'ordine e una consulenza legale. Per alcune vittime il pagamento può essere inevitabile (consultare la sezione **"Pagare o non pagare: il dilemma morale e legale del ransomware" a pagina 21**).

Non contare su strumenti gratuiti di decodifica del ransomware. Alcuni fornitori di sicurezza offrono programmi gratuiti per la decrittografia del ransomware, che in alcuni casi aiutano a recuperare i dati senza pagare il riscatto.

Tuttavia la maggior parte funziona per un solo particolare ceppo di ransomware o addirittura una sola campagna di attacco. Man mano che il ransomware viene aggiornato, gli strumenti gratuiti diventano obsoleti e non funzioneranno contro le nuove varianti.

Potresti essere fortunato e uno strumento di decrittografia gratuito potrebbe aiutarti, ma è bene non includerlo nel tuo piano di risposta agli incidenti.

Ripristina i dati dal backup

L'unico modo per riprendersi completamente da un'infezione di ransomware è quello di ripristinare tutto da un backup, che deve essere effettuato ogni giorno. Anche se questo è l'ultimo passaggio da compiere dopo un'infezione, è il primo per quanto riguarda la prevenzione.

Ma anche con backup recenti, pagare il riscatto può essere la soluzione più semplice dal punto di vista finanziario e operativo. Il ripristino dei backup è un'operazione lunga e laboriosa e alcune aziende non possono permettersi interruzioni delle attività.

Pagare o non pagare: il dilemma morale e legale del ransomware

Il ransomware è un problema serio di per sé, ma uno dei suoi aspetti più sgradevoli è che forza le vittime a compiere una scelta delicata dal punto di vista morale. Quando un attacco ransomware ti punta una pistola alla tempia, spesso non hai il lusso di poter soppesare attentamente le implicazioni morali di un pagamento. Devi agire senza indugi.

Il pagamento del riscatto può essere un male tanto detestabile quanto necessario. Arricchisce l'aggressore che è appena penetrato nella tua rete per rubare i dati. Ti rende una vittima, che possiede una rete vulnerabile e non ha altra scelta che cedere al ricatto. E consente al criminale informatico di finanziare gli attacchi futuri.

Gli attacchi recenti hanno però svelato una verità scomoda: la decisione di pagare o meno il riscatto non è una questione ovvia.

Va da sé che nessuna azienda vuole essere ricattata, tanto meno finanziare il crimine organizzato, però molte vittime sentono di non avere scelta. In un certo senso è il prezzo che si paga per avere dei dipartimenti informatici sottofinanziati e del software privo di patch od obsoleto. Negli Stati Uniti ci sono ancora degli ospedali che utilizzano terminali obsoleti con Microsoft Windows XP e quando ci sono in gioco delle vite umane, il riscatto è spesso un prezzo relativamente piccolo da pagare.

A volte perfino l'FBI ha consigliato alle vittime di pagare il riscatto. Ufficialmente l'agenzia federale sconsiglia il pagamento, ma di recente si è dichiarata contraria alla proibizione dei pagamenti da parte del Congresso americano.[19]. Anche se si paga, sottolinea l'agenzia, non è detto che si riabbiano indietro i dati.

Ma nel 2020, il Dipartimento del Tesoro statunitense ha emesso un avviso per ricordare a imprese e cittadini che il pagamento di un riscatto potrebbe comportare la violazione di normative o portare a sanzioni finanziarie.

Le ramificazioni di questo avviso sono ancora al vaglio da parte di assicuratori e di negoziatori della risposta agli incidenti, ma i possibili rischi legali complicano un processo decisionale già difficile.

Un'altra campagna che chiede alle persone di rifiutare il pagamento dei riscatti proviene da Europol, la polizia dell'Unione Europea. La sua iniziativa "No More Ransom" (Basta riscatti), lanciata cinque anni fa, è una collaborazione pubblico-privato per aiutare le vittime di attacchi informatici a ricostruire i loro dati e a decrittografarli senza pagare.

L'iniziativa ha aiutato 6 milioni di vittime del ransomware a recuperare i loro file, evitando di pagare quasi 1 miliardo di euro in riscatti (gli strumenti di No More Ransom sono a disposizione di chiunque, non solo dei residenti nell'Unione Europea).

Per scegliere il modo migliore di procedere, le aziende devono soppesare i pro e i contro. Tra i fattori conflittuali da prendere in considerazione:

- Tempo e risorse necessari per tornare operativi
- Responsabilità verso gli azionisti in relazione all'interruzione delle attività aziendali
- Sicurezza dei clienti e dei dipendenti
- Tipo di attività criminale che il pagamento potrà finanziare
- Qualsiasi responsabilità legale che potrebbe derivare dal versamento di fondi a un individuo o Stato condannato per un crimine

La questione è complessa, non ci sono due aziende che risponderebbero allo stesso modo.

I recenti attacchi hanno però svelato una verità scomoda: la decisione di pagare o meno il riscatto non è una questione ovvia.

19 Maggie Miller *(The Hill)* "Top FBI Official Advises Congress Against Banning Ransomware Payments." (Un dirigente dellI'FBI consiglia al Congresso degli Stati Uniti di non vietare il pagamento del riscatto in caso di un attacco ransomware), luglio 2021.

Dopo l'attacco

A prescindere dal danno causato dal ransomware, un attacco riuscito rivela una falla nella sicurezza che si traduce nella violazione di un dispositivo o di una rete. Dopo che le cose sono tornate alla normalità, si ha l'opportunità di imparare dalla violazione subita per evitare attacchi futuri.

Consigliamo di eseguire una valutazione di sicurezza end to end, possibilmente da parte di un fornitore esterno, per identificare le minacce che potrebbero ancora annidarsi nell'ambiente. Questo è anche il momento giusto per rivedere gli strumenti e le procedure di sicurezza e identificarne le lacune.

Pulizia

Alcuni ransomware contengono altre minacce o trojan backdoor che possono condurre a futuri attacchi. In altri casi, si tratta di una violazione preesistente a spalancare le porte all'infezione del ransomware. Ecco perché è indispensabile cancellare i dati di ogni dispositivo e ripristinarli da un backup pulito. Cerca più approfonditamente le minacce occulte che, nella confusione dell'attacco, potrebbero essere passate inosservate.

Revisione post-mortem

Valuta la tua preparazione e risposta agli incidenti. Come è stato eseguito il piano anticrisi? È possibile migliorare le configurazioni di rete per limitare la diffusione di futuri attacchi? Si può implementare una soluzione per la sicurezza dell'email più robusta? In generale, si dovrebbe adottare un approccio totalmente nuovo alla cybersecurity?

Esamina le misure di sicurezza attuali e chiediti se sono sufficienti per combattere le minacce odierne. Trasforma quanto accaduto in un'esperienza di apprendimento, poiché potrebbe accadere di nuovo.

Se non identifichi in che modo è penetrato il ransomware, non sarai in grado di fermare il prossimo attacco.

Valuta la consapevolezza degli utenti

Molti ceppi di ransomware richiedono l'interazione umana per distribuire i loro payload, che si tratti di un'infezione diretta o attraverso una trasmissione successiva da parte di un altro tipo di malware. Se le misure di sicurezza sono inefficaci e un messaggio fraudolento che riporta una "fattura non pagata" raggiunge il server email, un utente ben informato è l'ultima linea di difesa che impedisce a un'azienda, ospedale o scuola di diventare un'altra vittima del ransomware. Assicurati che tutti i tuoi dipendenti, di qualsiasi livello, siano all'altezza del compito.

Può valere la pena investire in strumenti di simulazione del phishing per aumentare la sensibilizzazione dei dipendenti, identificare gli utenti che sono particolarmente vulnerabili e migliorare la sicurezza complessiva. Ricreando gli attacchi reali e le ultime tecniche di social engineering e i metodi di attacco, le simulazioni di attacchi di phishing aiutano ad analizzare e identificare le vulnerabilità incentrate sulle persone, prima che si verifichi un attacco.

Educa gli utenti

Dopo aver analizzato la consapevolezza degli utenti, sviluppa un programma di formazione per ridurre la vulnerabilità dei dipendenti agli attacchi informatici, comprese le lezioni apprese dai casi precedenti. Includi una formazione continua per gli utenti più vulnerabili, quelli che più probabilmente saranno presi di mira oppure dispongono di privilegi elevati per dati sensibili, sistemi e altre risorse.

Inoltre, il programma di formazione deve integrarsi con le altre difese informatiche per aiutare gli utenti non solo a identificare gli attacchi ma anche a segnalarli tempestivamente.

Investi in difese moderne

Gli attacchi informatici attuali sono diretti contro le persone e non contro le infrastrutture. Scegli soluzioni di sicurezza che adottano un approccio incentrato sulle persone, per mantenerle protette.

I criminali informatici non hanno una visione del mondo in termini di topologia di rete. Va pertanto adottata una soluzione che permetta di identificare le vittime degli attacchi, i metodi utilizzati e se l'attacco è andato a segno. Bisogna considerare il rischio individuale rappresentato da ogni utente, includendo il modo in cui viene colpito, i dati a cui ha accesso e se tende facilmente a farsi trarre in inganno.

Allo stesso tempo, impedisci che i contenuti web rischiosi entrino in contatto con il tuo ambiente. La tecnologia di isolamento dell'ambiente web può eseguire il rendering delle pagine web provenienti da URL sospetti e non verificati in un contenitore protetto all'interno del normale browser web dell'utente. L'isolamento del web può fornire una protezione critica per gli account email condivisi, che sono difficili da proteggere tramite l'autenticazione a più fattori. La stessa tecnologia può isolare la navigazione personale degli utenti e i servizi di webmail, garantendo loro libertà e privacy senza compromettere l'azienda.

Per gestire gli attacchi altamente mirati è necessario disporre di informazioni avanzate sulle minacce. Affidati quindi a una soluzione che combina tecniche statiche e dinamiche per rilevare nuove caratteristiche di attacco (ovvero strumenti, tattiche e obiettivi) e fai tesoro di tali informazioni.

Passi successivi

Finché il ransomware permetterà di ottenere un guadagno esisterà in una forma o l'altra. I consigli contenuti nella presente guida hanno lo scopo di aiutarti ad affrontare il ransomware prima, durante e dopo un attacco.

Ovviamente il modo migliore per combattere il ransomware è quello di impedire che si infiltri nel tuo ambiente e per questo sono necessarie difese informatiche concepite per le minacce di oggi.

Una sicurezza informatica efficace è quella incentrata sulle persone, che renda gli utenti più resilienti tramite dei corsi di sensibilizzazione basati sulle tecniche di attacco del mondo reale, identifichi e distrugga il ransomware che prende di mira i tuoi dipendenti. E che neutralizzi le minacce e aiuti a reagire in modo rapido ed efficace agli incidenti.

Per saperne di più su come bloccare gli attacchi ransomware, visita il sito **www.proofpoint.com/it**.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0501-006-01-01 11/21