

proofpoint™

THE 2017

RANSOMWARE

SURVIVAL GUIDE

MANUALE DI SOPRAVVIVENZA RANSOMWARE

*Quello che ogni organizzazione deve sapere
Prima, durante e dopo un attacco*

RIEPILOGO ESECUTIVO

Il ransomware è un'antica minaccia che è tornata a ruggire con una ferocia persino maggiore. Questo tipo di malware, il cui nome deriva dal riscatto (ransom, in inglese) che richiede dopo aver bloccato i file delle vittime che ha mietuto, si è rapidamente trasformato in una delle principali tipologie di attacco cibernetico.

Più della metà delle aziende chiamate a rispondere a un recente sondaggio del Ponemon Institute ha dichiarato di aver subito un attacco ransomware. Tra queste aziende, le vittime hanno subito in media quattro attacchi ciascuna. Ogni attacco è costato in media 2500 \$.¹ Tralasciando il riscatto in sé (posto che le vittime accettino di pagare), questi attacchi richiedono un pesante tributo: interruzione dei flussi commerciali, costi legati alla risoluzione dei problemi e indebolimento del marchio.

I vettori di gran parte dei ransomware sono le e-mail di phishing, sebbene anche i dispositivi mobili e i siti Web infetti ne consentano la propagazione.

Cosa si cela dietro l'impennata dei ransomware?

Negli ultimi anni, i ransomware hanno conosciuto una rapida crescita a causa di quattro fattori principali:

- I responsabili degli attacchi vantano molteplici canali di distribuzione, la qual cosa aumenta la percentuale di buona riuscita
- I costi di costruzione sono più bassi che mai
- Identificano bersagli più redditizi altamente disposti a pagare il riscatto
- Bitcoin e altre valute digitali consentono un riscatto del pagamento agevolato

Come sopravvivere al ransomware

Gran parte delle aziende non è preparata a un attacco ransomware. Sebbene il 66% delle aziende intervistate nel sondaggio Ponemon concordi sul fatto che la gravità del ransomware sia "assai elevata", soltanto il 13% di esse ha dichiarato di essere in grado di evitarlo.²

Adesso, consideriamo i seguenti fattori come punto di partenza.

Prima dell'attacco

La strategia di sicurezza più efficace è evitare totalmente il ransomware. Questa operazione richiede una pianificazione e un lavoro di un certo tipo per evitare che si verifichi la crisi.

Backup e ripristino

La parte più importante di ogni strategia di sicurezza contro i ransomware è rappresentata dall'esecuzione di backup regolari dei dati. Sorprendentemente, solo poche organizzazioni mettono in atto routine di backup e ripristino. Entrambe le facce della medaglia sono importanti: le procedure di ripristino costituiscono l'unico modo per sapere in anticipo se il piano di backup avviato sta funzionando.

Aggiornamento e patch

È opportuno mantenere i sistemi operativi, il software di sicurezza e le patch aggiornati su tutti i dispositivi.

Addestramento e formazione per fare attenzione alle macro

La formazione e la consapevolezza dei dipendenti costituiscono due fattori imprescindibili. I dipendenti devono sapere cosa è o non è opportuno fare, come evitare i ransomware e in che modo segnalarli. In caso di ricezione di una richiesta ransomware, i dipendenti devono sapere che è necessario informare immediatamente il team addetto alla sicurezza e che non devono mai tentare personalmente il pagamento.

Investire in massicce soluzioni di sicurezza per e-mail, dispositivi mobili e social media

Persino la formazione utenti più accurata non sarebbe in grado di debellare tutti i ransomware.

Esistono soluzioni di sicurezza delle e-mail avanzate che assicurano una protezione dagli allegati, dai documenti e dagli URL maligni presenti nelle e-mail che conducono ai ransomware. Inoltre, è opportuno investire in prodotti per la protezione degli attacchi mobili allo scopo di impedire alle applicazioni mobili dannose di compromettere il proprio ambiente.

1 Ponemon Institute. "The Rise of Ransomware". Gennaio 2017..
2 ibidem.

Durante l'attacco: tornare alle proprie attività

Se da una parte la strategia di protezione dai ransomware più efficace sia evitare questi ultimi fin dall'inizio, questo consiglio lascia il tempo che trova se si è appena stati infettati.

In tal caso, sarà necessario risolvere problemi a breve termine quali riportare computer, telefoni e reti online e gestire le richieste di riscatto.

Contattare le forze dell'ordine

Il ransomware è un vero e proprio reato in quanto mette in atto furto ed estorsione. La notifica delle autorità competenti è un primo passo necessario.

Scollegarsi dalla rete

Nel preciso istante in cui i dipendenti individuano una richiesta ransomware o notano qualcosa di strano, dovranno scollegarsi immediatamente dalla rete e consegnare la macchina infetta al reparto IT.

Infatti, soltanto il team addetto alla sicurezza IT potrà tentare un ripristino, il quale andrà a buon fine esclusivamente se si tratta di uno scareware fasullo o di un malware mobile elementare.

Determinare l'entità del problema sulla base della threat intelligence

La propria risposta, la quale include la decisione di pagare o meno il riscatto, dipende da svariati fattori:

- Il tipo di attacco
- Quali soggetti sono stati compromessi nella rete
- Di che tipo di autorizzazioni di rete dispongono gli account compromessi

Pianificare una risposta

Gran parte della propria risposta è rappresentata dalla decisione di pagare o meno il riscatto. Trattandosi di una decisione complicata, potrebbe essere necessario consultare le forze dell'ordine e il proprio legale. Vi è il rischio che il pagamento sia inevitabile.

Mai affidarsi ai tool gratuiti di decodifica dei ransomware

La maggior parte dei tool gratuiti funziona soltanto per una singola fascia di ransomware o persino per una singola campagna di attacco. Dal momento che i responsabili degli attacchi aggiornano costantemente i propri ransomware, i tool gratuiti diventano presto obsoleti e aumenta così la probabilità che essi non siano efficaci sui nuovi ransomware.

Ripristino dal backup

L'unico modo per portare a termine il recupero da un'infezione ransomware è ripristinare tutti i dati dal backup. Tuttavia, pur facendo leva sui backup recenti, il pagamento del riscatto potrebbe richiedere più sforzi finanziari e operativi del previsto.

In seguito all'attacco: revisionare e consolidare

Consigliamo una valutazione di sicurezza da cima a fondo per identificare le eventuali minacce che si aggirano ancora nel proprio ambiente. Occorre esaminare attentamente i propri tool e procedure di sicurezza e le relative carenze.

Pulizia

Alcuni ransomware contengono altre minacce o trojan backdoor in grado di scatenare attacchi futuri.

Pertanto, consigliamo di avere un occhio ancora più critico per individuare eventuali minacce nascoste ignorate nel caos generale.

Analisi a posteriori

È opportuno analizzare la propria prontezza e reattività alle minacce. Se non si scopre come si è insinuato il ransomware, non sarà possibile bloccare l'attacco successivo.

Valutare la consapevolezza degli utenti

Un dipendente ben informato costituisce l'ultima linea di difesa. È pertanto fondamentale accertarsi che i dipendenti, il personale o la facoltà siano all'altezza dell'incarico.

Formazione e addestramento

È necessario sviluppare un programma formativo per far fronte alla vulnerabilità dei dipendenti agli attacchi cibernetici, nonché implementare un piano di comunicazione delle crisi nell'eventualità di un attacco futuro e controlli basati su esercitazioni e test di penetrazione.

Rafforzare le proprie difese

L'odierno panorama di minacce in rapida evoluzione richiede soluzioni di sicurezza in grado di analizzare, identificare e bloccare, in tempo reale, gli URL e gli allegati maligni che fungono da veicoli primari degli attacchi ransomware.

È dunque necessario cercare soluzioni di sicurezza che si adattino alle minacce nuove ed emergenti e che aiutino gli utenti a gestirle più velocemente.



INTRODUZIONE

I primi segni del problema si sono manifestati intorno all'ora di pranzo mentre alcuni dipendenti sanitari del Regno Unito provavano ad accedere ai computer ospedalieri. Quel giorno, i computer risultavano bloccati e uno strano messaggio apparve sullo schermo.

Esso recitava: “Molti dei tuoi documenti, foto, video, database e altri file non sono più accessibili in quanto sono stati crittografati. Non perdere tempo a cercare un modo per recuperare i tuoi file. Non potrai recuperare i tuoi file senza il nostro servizio di decodifica”.³

I computer furono infettati da un ransomware, un attacco cibernetico che blocca i file delle vittime fino a quando queste ultime non pagano una tassa per entrare nuovamente in possesso dei propri dati. L'attacco rese i documenti dei pazienti, i calendari degli appuntamenti, le linee telefoniche interne e le e-mail inaccessibili. Interruppe i collegamenti tra i computer e le apparecchiature mediche. Obbligò gli operatori sanitari a inviare i pazienti gravi altrove e a correre per l'ospedale con carta e penna e i propri cellulari.⁴

“Ci fu detto di spegnere i cellulari, rimuovere i cavi di rete e scollegare i telefoni”, affermò un dipendente del National Health Service del Regno Unito, citato dalla rivista inglese *The Guardian*.⁵

L'attacco, soprannominato “WannaCry” dagli esperti di sicurezza, si stava ormai diffondendo. Nel giro di poche ore, più di 40 organizzazioni nell'ambito dell'NHS erano state infettate dal ransomware.⁶ Il giorno dopo, l'attacco colpì decine di migliaia di sistemi in oltre 150 Paesi, tra cui “università cinesi, sistemi ferroviari tedeschi e persino stabilimenti di assemblaggio giapponesi”.

WannaCry fu un campanello d'allarme che fece riflettere molte persone su quanto fossero impreparate alle minacce poste dai ransomware. Più della metà degli esperti IT intervistati dal Ponemon Institute dichiarò che le proprie organizzazioni non erano pronte ad aggirare gli attacchi ransomware e che soltanto il 38% di esse aveva implementato una strategia per far fronte ai software distruttivi.⁷

Questa guida va considerata come un punto di partenza. Riveleremo le cause sottostanti il rapidissimo aumento dei ransomware e spiegheremo cosa fare quando se ne incontra uno e, cosa ancora più importante, come evitare fin dall'inizio di diventare una delle vittime.

“MOLTI DEI TUOI DOCUMENTI, FOTO, VIDEO, DATABASE E ALTRI FILE NON SONO PIÙ ACCESSIBILI IN QUANTO SONO STATI CRITTOGRAFATI. NON PERDERE TEMPO A CERCARE UN MODO PER RECUPERARE I TUOI FILE. NON POTRAI RECUPERARE I TUOI FILE SENZA IL NOSTRO SERVIZIO DI DECODIFICA”.

Nota di riscatto per WannaCry



³ Damien Gayle, Alexandra Topping et al (The Guardian). "NHS seeks to recover from global cyber-attack as security concerns resurface". Maggio 2017.

⁴ Ibidem.

⁵ Ibidem.

⁶ Nicole Perleth (The New York Times). "A Cyberattack 'the World Isn't Ready For'". Giugno 2017.

⁷ Ponemon Institute LLC. "2016 State of the Endpoint Report". Aprile 2016.

UN'ANTICA MINACCIA CHE ASSUME NUOVE FORME

Il ransomware è un'antica minaccia che, negli ultimi mesi, è tornata a ruggire ferocemente sotto forma di nuove varianti. Esso blocca l'accesso ai dati o al sistema di un computer, generalmente crittografando i file con estensioni specifiche (JPG, DOC, PPT ecc.). I file restano inaccessibili fino a quando la vittima non paga l'autore dell'attacco per ottenere un codice di decrittazione per sbloccare i file. In molti casi, la richiesta di pagamento prevede una scadenza. Se quest'ultima non viene rispettata, è possibile che l'importo del riscatto raddoppi o che i dati vengano persi definitivamente e persino distrutti.

I costi reali

Circa il 60% delle aziende intervistate dal Ponemon Institute hanno concordato sul fatto che un attacco ransomware provocherebbe "conseguenze finanziarie gravi" per le loro aziende.⁸

Tralasciando il riscatto in sé (posto che le vittime accettino di pagare), questi attacchi richiedono un pesante tributo: interruzione dei flussi commerciali, costi legati alla risoluzione dei problemi e indebolimento del marchio.

Prendiamo come esempio l'attacco WannaCry. Se da una parte il guadagno al netto per gli autori dell'attacco non ha superato quello di un giorno di paga, il ransomware è stato assai dirompente. Non avere accesso alle informazioni critiche e ai sistemi operativi può rallentare la risposta a un'emergenza e mettere a repentaglio la sicurezza pubblica.

Il settore che è stato colpito in modo particolarmente pesante è stato quello sanitario. I virus rendono inaccessibili i documenti dei pazienti, rallentano il flusso di lavoro e intaccano persino i sistemi di monitoraggio dei pazienti. Questo può rendere il debellamento dei ransomware una questione di vita o di morte.

Sfruttamento del fattore umano

La maggior parte dei ransomware si propaga tramite le e-mail di phishing. Queste e-mail ingannano gli utenti intimandoli ad aprire un allegato dannoso o cliccando un URL dannoso.

A febbraio 2016, un ceppo di ransomware ampiamente utilizzato chiamato Locky ha infettato il Methodist Hospital del Kentucky attraverso una campagna via e-mail mirata.

In seguito all'apertura di quella che appariva come una fattura insolita da parte di un dipendente, Locky si è propagato nell'intera rete interna, bloccando le stazioni di lavoro e limitando l'accesso al server centrale. La soluzione dell'ospedale: ripristinare ogni singola stazione di lavoro dal backup o sborsare la cifra relativamente modesta di quattro bitcoin (circa 1.600 \$) per sbloccare i file.

I nostri ricercatori avevano scoperto il ceppo Locky circa un mese prima. Locky viene distribuito principalmente tramite allegati Microsoft Word che, spesso, assumono le sembianze di fatture insolite. All'apertura del documento, agli utenti viene chiesto di abilitare le macro. Se gli utenti accettano di farlo, viene avviato il download di un file eseguibile noto come Troj/Ransom-CGX da un server remoto. Il processo va avanti con la crittazione dei file sensibili e si conclude con il lancio di Locky.⁹

In seguito alla crittazione, compare un messaggio popup che intima agli utenti di effettuare un pagamento, solitamente seguendo delle istruzioni che implicano l'utilizzo della rete Tor e di bitcoin. Le vittime non possono né chiudere il messaggio, né aggirarlo. Il problema non potrà essere risolto neanche ripetendo la combinazione di tasti CTRL+ALT+CANC più e più volte o riavviando il sistema.

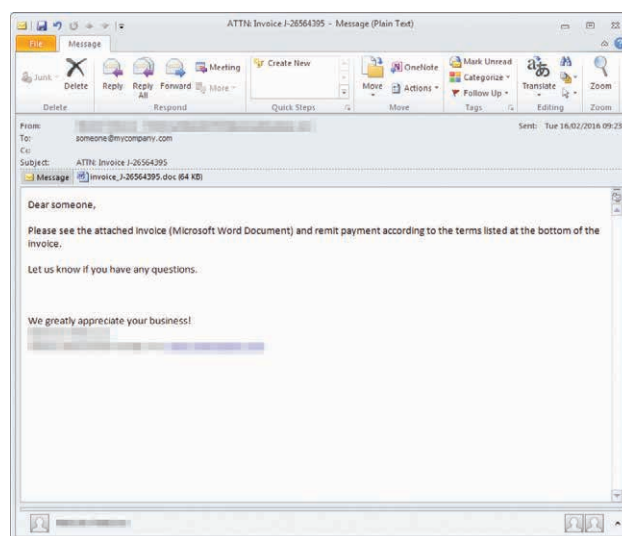
DA DOVE ARRIVA

La distribuzione del ransomware avviene tramite tre vettori di attacco principali:

- E-mail
- Dispositivi mobili
- Siti Web/link infetti sui social media e pubblicità infettate da malware (malvertising)

Le e-mail contenenti allegati o link dannosi rappresentano di gran lunga il principale vettore di minacce, con una percentuale corrispondente a circa l'85% di tutti i ransomware che abbiamo rilevato.

Queste e-mail sembrano legittime e possono ingannare i dipendenti in buona fede. Spesso, le e-mail assumono le sembianze di aggiornamenti software ufficiali, fatture insolite o persino una nota scritta dal capo a un subordinato.



Gran parte dei ransomware si propaga tramite e-mail di phishing come questa.

⁸ Ponemon Institute, "The Rise of Ransomware", Gennaio 2017.
⁹ Proofpoint, "Dridex Actors Get In the Ransomware Game With 'Locky'", Febbraio 2016.

PERCHÉ SI STA DIFFONDENDO?

Il ransomware è un exploit in circolazione da decenni. Tuttavia, negli ultimi anni abbiamo assistito alla relativa esplosione per via di quattro fattori principali:

Aumento dei canali di distribuzione

I cybercriminali possono attaccare migliaia di entità contemporaneamente utilizzando una vasta gamma di veicoli di attacco. Ne deriva che gli exploit ransomware hanno ormai una maggiore frequenza di successo.

I gateway delle e-mail tradizionali sono travolti da minacce provenienti da ogni dove:

- Campagne di e-mail di massa lanciate dai botnet
- Malware polimorfici che procedono a una velocità maggiore per impedire ai venditori nell'ambito della sicurezza di realizzare nuove firme
- URL dannosi e malvertising che non contengono alcun allegato

Nel complesso, questi fattori offrono ai ransomware una maggiore possibilità di successo.

Realizzazione più economica

Come accade in ogni attività, il successo genera successo. I creatori di ransomware hanno perfezionato la propria opera. Infatti, adesso sono ampiamente disponibili tool sofisticati che, solamente qualche anno fa, sarebbero stati accessibili esclusivamente a un'élite di cybercriminali. Tutto questo si traduce in tassi di successo più elevati e, infine, economie di scala.

Se vengono eseguiti 4.000 attacchi in un solo giorno e anche solo l'1% delle vittime paga un riscatto di 400 \$, il fatturato di un'unica giornata lavorativa risulta 16.000 \$. In un anno, i profitti possono raggiungere cifre a sei zeri.

Bersagli più redditizi

Invece di mirare ai singoli individui, i cybercriminali stanno spostando sempre più il mirino su organizzazioni in possesso di dati sensibili, reparti IT assai impegnati ed enti interessati a risolvere il problema il più rapidamente possibile. Ad aggiungere altra carne sul fuoco vi sono le configurazioni di rete di bassa qualità comunemente presenti negli ospedali, nei dipartimenti di polizia, nelle scuole e in altri uffici statali e governativi locali.

Per queste organizzazioni, i tempi di inattività della rete non rappresentano un'opzione contemplabile. Non c'è da sorprendersi se molti, dopo aver fatto un calcolo rapido, accettano di pagare il riscatto in quanto ritengono che sia la mossa aziendale migliore.

Bitcoin e altre valute digitali

Sin dal suo debutto nel 2009, Bitcoin è stato una manna per i sostenitori del libertarismo e, analogamente, per i cybercriminali. Infatti, i pagamenti non possono essere fatti risalire al mittente o al destinatario, la qual cosa assicura transazioni commerciali private anonime e prive di limitazioni.

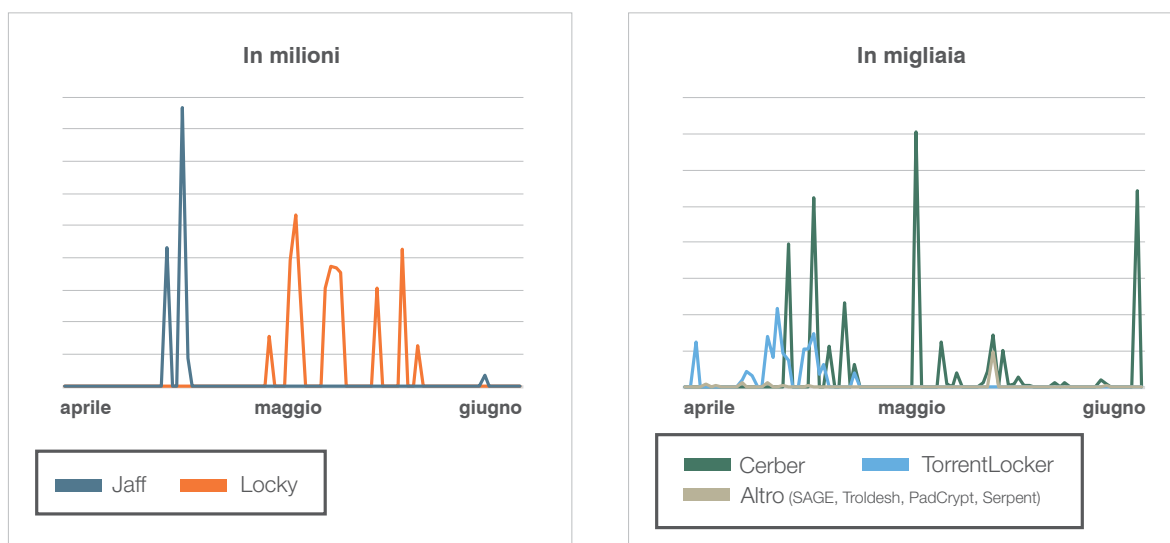
Richiedendo il pagamento in Bitcoin, i cybercriminali ottengono l'anonimato necessario a incassare il denaro del riscatto in un modo più facile che mai. Talvolta, le precedenti forme di ransomware richiedevano una carta di debito prepagata. Se da una parte questo approccio riesce ad aggirare le misure antifrode implementate dalle banche, risulta molto più scomodo per entrambe le parti della transazione.

Tutte le principali varianti di ransomware richiedono un pagamento in bitcoin (vedere la barra laterale a pagina 9).

Carichi paganti dei malware principali per volume di messaggi

Campagne di allegati ai documenti, 2° trimestre 2017

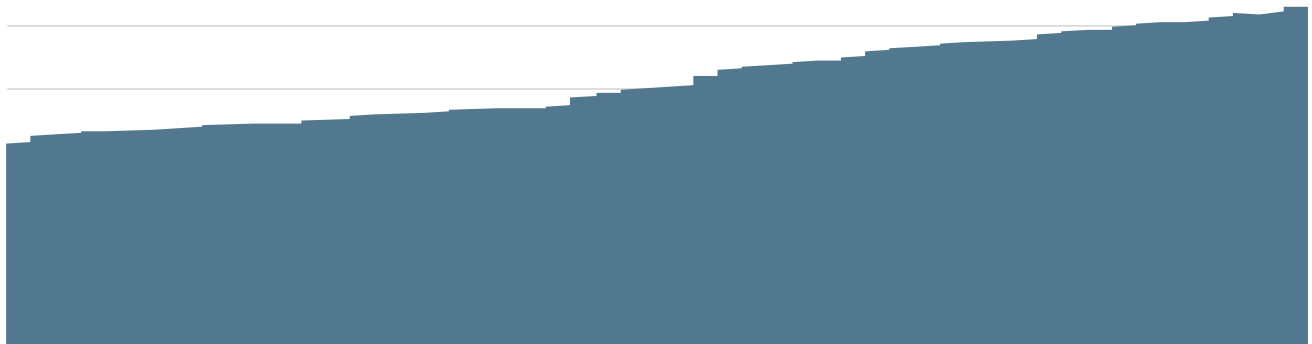
Fonte: Proofpoint, Inc.



Volume di messaggi giornalieri indicizzati dei ceppi ransomware principali, aprile-giugno 2017

Numero cumulativo di ceppi ransomware segnalati, 2017 YTD

Fonte: Proofpoint, Inc.



Dicembre 2015

Giugno 2017

IL PERCORSO DEL DENARO BITCOIN

Nel sequestro tradizionale mirato all'ottenimento di un riscatto, la sfida più grande è sempre stata incassare il denaro e fuggire col bottino. Sfortunatamente, i cybercriminali esperti di ransomware hanno davanti a sé una strada spianata.

La forma più popolare di pagamento interessa criptovalute non tracciabili, la più nota delle quali è Bitcoin. Bitcoin consente un pagamento da individuo a individuo tramite internet e non coinvolge alcuna banca o ente governativo. Esistono 21 milioni di bitcoin al mondo. Sin dai suoi esordi nel 2008, questa valuta ha subito ampie fluttuazioni di valore. Prendendo come riferimento la data della presente pubblicazione, un bitcoin vale quasi 600 \$ USA.

Per comprendere la funzione delle criptovalute, basta immaginarle come l'equivalente elettronico di una fiche del casinò. I gettoni non hanno alcun valore intrinseco nel mondo reale, ma gli utenti possono acquistarli nella loro valuta locale e utilizzarli all'interno della struttura, in questo caso internet, per poi convertirli nella valuta corrente una volta usciti dalla struttura.

Analogamente, le criptovalute possono essere acquistate online utilizzando una carta di credito o un conto bancario da fonti legittime. Nel caso dei ransomware, le vittime convertono, per esempio, la propria valuta locale in "tre bitcoin", per poi inviare questi ultimi da un portafoglio di bitcoin utilizzando l'indirizzo Bitcoin anonimo fornito dall'autore dell'attacco.

Non sempre il denaro arriva direttamente all'autore dell'attacco. Generalmente, i gettoni finiscono in un "tumbler", un servizio elettronico che unisce i bitcoin ad altri bitcoin e, in seguito, invia le monete (numerate in modo diverso, ma dotate dello stesso valore sottratte le commissioni) all'autore dell'attacco.

Proprio come accade per il riciclaggio di denaro nel mondo reale, gli autori degli attacchi possono ritrovarsi con un pagamento non tracciabile. Questo pagamento viene poi convertito nella valuta fisica locale trasformando i bitcoin (gettoni) in banconote reali.

Occorre notare che, a differenza delle valute riconosciute dal governo, le criptovalute non sono considerate "denaro". Esse sono considerate, piuttosto, come un equivalente delle fiche del poker o dei gettoni utilizzati nel gioco d'azzardo. Pertanto, il sistema di trasmissione e i tumbler non sono né regolati né considerati riciclaggio di denaro, sebbene il risultato sia presumibilmente lo stesso.

L'attrattiva di Bitcoin è più che ovvia. Infatti, mette a disposizione degli autori di attacchi informatici una cybervaluta difficile da tracciare e disponibile a livello globale che si converte direttamente nella valuta fisica locale; in altre parole, si parla di "banconote non contrassegnate".

Un tale approccio ha vantaggi evidenti rispetto all'utilizzo di carte di credito rubate, il cui valore è precipitato dal giorno in cui le istituzioni finanziarie sono diventate più esperte nel bloccare repentinamente i conti delle vittime.

RANSOMWARE MOBILI

Immaginate di prendere in mano il vostro telefono e di visualizzare, al posto della schermata iniziale, un avviso apparentemente inviato dall'FBI che vi accusa di aver preso visione di immagini illecite. Il vostro telefono è stato crittato e qualcuno vi sta minacciando di contattare le autorità se non accettate di emettere un pagamento di 300 \$ per ignorare l'accaduto.

Per un'infinità di utenti mobili, questa è una realtà purtroppo ben nota, sebbene quello appena presentato sia soltanto un esempio delle centinaia di versioni di ransomware mobili in circolazione.

Abbiamo rilevato tre vettori di attacco principali per i ransomware mobili.

Android

Sappiamo che il ransomware mirato ad Android deriva dalla stessa famiglia generica della variante di ransomware Cryptolocker. Esso potrebbe presentarsi come un aggiornamento di Adobe Flash Player che richiede delle autorizzazioni. O ancora, potrebbe collegarsi a un gioco popolare o a un'applicazione "gratuita" disponibile su un app store fasullo (la stragrande maggioranza dei ransomware Android arriva da app store terzi, e non dallo store Google Play ufficiale).

Una volta lanciato, il ransomware procede alla criptazione del dispositivo mobile e richiede un pagamento tempestivo, solitamente in Bitcoin.

Applicazioni distribuite tramite SMS

Generalmente, si tratta di applicazioni pornografiche che si

aprono sullo schermo di un dispositivo, spesso con immagini riprovevoli, e richiedono un pagamento per far scomparire tali immagini. Solitamente, esse si diffondono tramite messaggi di testo, ma si possono trovare anche sui social media, spesso nei messaggi diretti di Twitter o Instagram.

A differenza della maggior parte dei ransomware, generalmente i dati non vengono crittati. Comunque, per gli utenti, l'effetto è sempre lo stesso: il blocco dei dispositivi. Aggirare questo tipo di minaccia è possibile, ma anche molto complicato. Per questo, molti utenti optano per il pagamento del riscatto.

Browser iOS

Generalmente, il ransomware che colpisce i dispositivi iOS si presenta sotto forma di ransomware basato sul browser. Spesso, avvisa le vittime che hanno scaricato immagini illegali o dichiara che il loro dispositivo è stato infettato. Per sbloccare o "riparare" il dispositivo, la vittima viene reindirizzata a un sito per effettuare il pagamento tramite Bitcoin o una carta di debito prepagata.

Questi siti di ransomware fraudolenti si propagano per lo più tramite annunci dannosi di siti Web per adulti. Il tasso di conversione di questi siti per il pagamento fornito dalle vittime è basso. Ma quando centinaia di migliaia o milioni di vittime vengono infettate ogni settimana, le cose cambiano.

Al momento della presente pubblicazione, non abbiamo ancora assistito a una criptazione diffusa dei dispositivi iOS. La maggior parte degli schemi utilizzati si limita a bloccare l'accesso delle vittime ai relativi browser Web.

GLI INCIDENTI O I COMPROMESSI PIÙ GRAVI

Fonte: Ponemon

71%

Attacchi zero day

68%

DDoS

53%

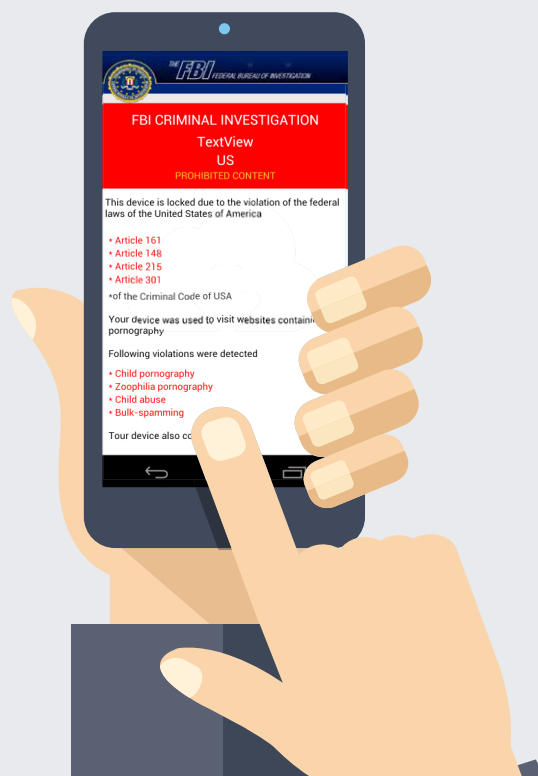
Exploit di vulnerabilità software esistenti
(attive da più di 3 mesi)

51%

Ransomware

47%

Attacchi malware generati dal Web





PRIMA DELL'ATTACCO

PREVENZIONE DEI RANSOMWARE

La migliore strategia di sicurezza consiste nell'evitare totalmente questo tipo di estorsione. Si tratta di una strategia attuabile dalla maggior parte delle aziende, ma che richiede una pianificazione e un lavoro non indifferenti prima che la crisi colpisca.

Backup e ripristino

La parte più importante di ogni strategia di sicurezza contro i ransomware è rappresentata dall'esecuzione di backup regolari dei dati. Questo viene fatto da gran parte delle aziende ma, sorprendentemente, solo poche di esse mettono in atto routine di backup e ripristino. Entrambi i processi sono importanti: le procedure di ripristino costituiscono l'unico modo per sapere in anticipo se il piano di backup avviato sta funzionando.

Probabilmente, occorrerà occuparsi di alcuni cavilli prima che la crisi possa insinuarsi. Se i test di backup e ripristino vengono eseguiti regolarmente, l'impatto dell'infezione da ransomware non sarà devastante; in tal modo, si avrà un punto di ripristino sicuro e aggiornato.

Ancora una volta, si noti che gran parte delle aziende e degli individui esegue i backup. Tuttavia, l'esecuzione di test regolari di un ripristino completo risulta cruciale.

Aggiornamento e patch

È opportuno mantenere i sistemi operativi, il software di sicurezza e le patch aggiornati su tutti i dispositivi. Potrebbe sembrare scontato, ma stando a un sondaggio recente, circa la metà dei professionisti IT ammette di avere difficoltà a rimanere al passo con l'enorme volume di patch rilasciate ogni mese. Inoltre, i soggetti intervistati hanno dichiarato che gli aggiornamenti variano incredibilmente in termini di complessità e date di rilascio.

Le difficoltà incontrate dai team riguardano anche l'aggiornamento di determinate applicazioni, come ad esempio Adobe Flash, che potrebbero compromettere altre funzionalità interne basate sul software. Gli hacker sanno bene che questi e altri fattori possono portare a una "stanchezza da patch", così sviluppano gli exploit di conseguenza.⁹

Addestramento e formazione per fare attenzione alle macro

Il più delle volte, l'attacco inizia da un unico dipendente che, in buona fede, apre quella che appare come un'e-mail di lavoro.

Questo è il motivo per cui la formazione e la consapevolezza dei dipendenti sono fattori cruciali. I dipendenti devono sapere cosa è o non è opportuno fare, come evitare i ransomware e in che modo segnalarli. In caso di ricezione di una richiesta ransomware, i dipendenti devono sapere che è necessario informare immediatamente il team addetto alla sicurezza e che non devono mai tentare personalmente il pagamento (infatti, il pagamento potrebbe comportare conseguenze nefaste per la reputazione e la sicurezza del marchio).

Le nostre ricerche mostrano che i cybercriminali fanno attivamente leva sulla curiosità e sugli errori umani. La recente ondata delle e-mail di ransomware riflette la tendenza dei cybercriminali a ingannare gli individui chiedendo loro di diventare complici inconsapevoli del tentativo di blocco di informazioni e della richiesta di un pagamento.¹⁰

Questi attacchi fanno leva sulla disinformazione dell'utente e, generalmente, portano questi ultimi ad aprire allegati di documenti Word o allegati JavaScript dannosi e ad attivare le macro. Una volta che gli utenti fanno clic sul pulsante "Abilita contenuto" per attivare le macro, la macro dannosa scarica il ransomware e dà inizio al processo di attacco. Un'opzione possibile è disattivare gli script delle macro da file di Office trasmessi per e-mail. Tuttavia, alcune macro possono essere utili, e disattivarle completamente potrebbe penalizzare la produttività.

Investire in massicce soluzioni di sicurezza per e-mail, dispositivi mobili e social media

Persino la formazione utenti più accurata non sarebbe in grado di debellare tutti i ransomware. Le e-mail di phishing odierne sono sofisticate e altamente mirate. Gli autori degli attacchi eseguono un'attenta ricerca dei propri bersagli per creare e-mail dalle sembianze legittime e ingannano le vittime per fare in modo che facciano clic.

Dal momento che gran parte dei ransomware viene trasmessa tramite e-mail, dispositivi mobili e social media, sono necessarie soluzioni avanzate per poter fermare queste minacce in tempo reale. Secondo le nostre ricerche, il volume degli attacchi ransomware è aumentato enormemente. Solo nel canale e-mail, i ransomware rappresentano circa il 70% di tutti i messaggi dannosi.¹¹

I gateway delle e-mail legacy, i filtri web e i software antivirus tradizionali dovranno pertanto essere aggiornati ed essere eseguiti su tutte le reti. Tuttavia, tali strumenti non riescono a contrastare la minaccia ransomware da soli. Risulta infatti necessaria una soluzione di sicurezza delle e-mail più efficace. Questo significa analizzare gli URL e gli allegati incorporati per assicurarsi che nessun contenuto dannoso comprometta il sistema. I ladri informatici sono sempre un passo avanti rispetto a noi, e le configurazioni di sicurezza delle e-mail tradizionali si affidano troppo spesso a firme obsolete.

Esistono soluzioni di sicurezza delle e-mail avanzate che assicurano una protezione dagli allegati, dai documenti e dagli URL maligni presenti nelle e-mail che conducono ai ransomware. Contemporaneamente, è necessario investire in prodotti per la protezione dagli attacchi mobili per impedire alle applicazioni mobili dannose di compromettere il proprio ambiente.

⁹ Tripwire, Inc. "Tripwire 2016 Patch Management Study". Marzo 2016.

¹⁰ Proofpoint. "The Human Factor 2016". Febbraio 2016.

¹¹ Proofpoint. "The Human Factor 2016". Febbraio 2016.

RANSOMWORM SOTTO I RIFLETTORI, MA IL BERSAGLIO PRINCIPALE RIMANE L'E-MAIL

L'epidemia di minacce ransomware ad alto profilo quali WannaCry e Petya, le quali si diffondono sotto forma di un worm informatico piuttosto che tramite e-mail, ha portato i ransomware sotto i riflettori globali. Tuttavia, i cosiddetti "ransomworm" rimangono l'eccezione alla regola. La maggior parte degli attacchi ransomware, proprio come gran parte delle minacce informatiche nel complesso, viene inviata tramite e-mail.

Prendiamo Jaff, un ceppo di ransomware che ha eclissato rapidamente e silenziosamente le più grandi campagne di malware del 2017. Già a metà anno, Jaff si è rivelato il carico di malware di gran lunga più pesante per volume di messaggi negli spiegamenti Proofpoint di tutto il mondo. Infatti, complessivamente, ha rappresentato il 72% delle e-mail contenenti ransomware e quasi la metà di tutte le e-mail cariche di malware.

Le campagne Jaff a volumi elevati si sono fermate non appena è stato pubblicato uno strumento di decriptazione a metà giugno. Tuttavia, l'autore delle campagne di attacco Jaff si è convertito nuovamente a Locky e ha continuato a inviare un altro ceppo di ransomware chiamato The Trick. Questa rapida svolta evidenzia l'incredibile facilità con cui gli autori degli attacchi rispondono a nuove difese.

Molti altri ceppi di ransomware vengono inviati impiegando sforzi minori e maggiormente mirati. Il bersaglio di Cerber, per esempio, è rappresentato dalle aziende statunitensi. TorrentLocker mira piuttosto all'Europa. Serpent, invece, ha colpito il Belgio e i Paesi Bassi.

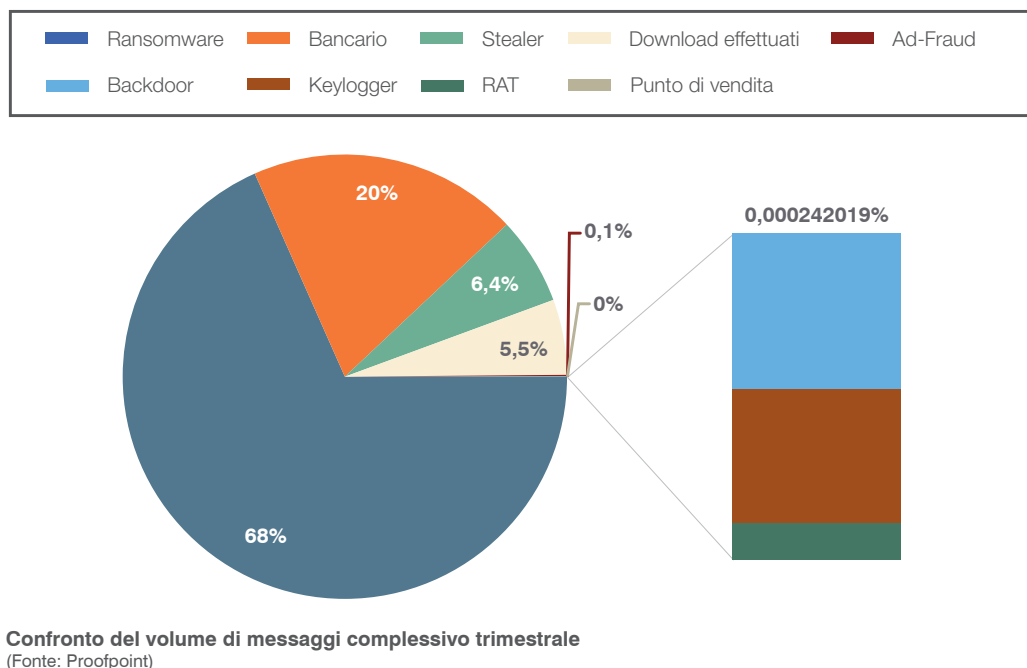
Alcuni ceppi di ransomware, quali il maneggevole e personalizzabile Philadelphia, mirano persino ad aziende specifiche.

WannaCry e Petya rimangono l'eccezione alla regola per un'altra ragione fondamentale: sembrano focalizzarsi sul gettare scompiglio piuttosto che ottenere un vero e proprio riscatto.

"Direi, con una certezza quasi assoluta, che [Petya] è stato un attacco ponderato, dannoso e distruttivo", ha affermato Nicholas Weaver, un ricercatore nell'ambito della sicurezza presso l'International Computer Science Institute rivolgendosi al giornalista Brian Krebs. "O forse un test travestito da ransomware".¹²

Per gli attacchi ransomware verificati, l'e-mail è la fonte di gran lunga più comune.

Malware divisi per categoria, primo trimestre 2017



12 Brian Krebs (Krebs sulla sicurezza). "Petya" Ransomware Outbreak Goes Global". Giugno 2017



DURANTE L'ATTACCO

RITORNO ALLE BASI

Siete stati colpiti da un ransomware. E ora?

Se da una parte la migliore strategia contro i ransomware è evitarli completamente, questo consiglio perde valore se si è appena stati infettati. In tal caso, sarà necessario risolvere problemi a breve termine quali riportare computer, telefoni e reti online e gestire le richieste di riscatto.

Tuttavia, una risposta presa in preda al panico non sarà d'aiuto e potrebbe persino peggiorare le cose.

Contattare le forze dell'ordine

Il ransomware è un vero e proprio reato in quanto mette in atto furto ed estorsione. Nessuno ha il diritto di sequestrare dispositivi, reti o dati, né certamente di esigere un riscatto per poterli riottenere. La notifica delle autorità competenti è un primo passo necessario.

È opportuno recarsi nella succursale più vicina. Non abbiate paura di prendere il telefono e contattare le autorità. Esse saranno pronte ad aiutarvi.

Scollegarsi dalla rete

Nel preciso istante in cui i dipendenti individuano una richiesta ransomware o notano qualcosa di strano, come ad esempio la perdita improvvisa dell'accesso ai propri file, dovranno scollegarsi immediatamente dalla rete e consegnare la macchina infetta al reparto IT.

Sconsigliamo di far effettuare un riavvio del sistema ai dipendenti. Infatti, soltanto il team addetto alla sicurezza IT potrà tentare un ripristino, il quale andrà a buon fine esclusivamente se si tratta di uno scareware fasullo o di un malware mobile elementare.

In questi casi, quello che appare come un ransomware è meglio descritto come "scareware". Esso può bloccare lo schermo dell'utente con una richiesta di riscatto e istruzioni di pagamento, senza tuttavia coinvolgere la crittazione dei dati. In questi scenari, per risolvere il problema basta eseguire la combinazione di tasti CTRL+ALT+CANC, aprire il "Task Manager" di Windows e chiudere il browser.

Determinare l'entità del problema grazie alla threat intelligence

Se da una parte tutti i ransomware sono dannosi, alcuni attacchi sono più distruttivi di altri. La risposta delle vittime, ivi compresa la decisione di pagare o meno il riscatto, dipende da svariati fattori.

Occorre chiedersi quanto segue:

- Di che tipo di attacco si tratta? I ransomware lasciano i propri biglietti da visita, pertanto la vostra risposta può basarsi sull'autore dell'attacco e sugli strumenti colpiti.
- Quali soggetti sono stati compromessi nella rete?
- Di che tipo di autorizzazioni di rete dispongono gli account compromessi?

Le vostre risposte potranno aiutare gli amministratori di rete a identificare la portata del problema, ideare un piano d'azione e, possibilmente, limitare i danni.

Pianificare una risposta

In base alla configurazione di rete, potrebbe essere possibile limitare la diffusione dell'attacco a una singola stazione di lavoro.

Scenario migliore: la macchina infetta viene scambiata con un nuovo computer e viene completato un ripristino dal backup. Scenario peggiore: tutte le macchine di rete sono infette. In tal caso, sarà necessario effettuare un rapido calcolo dei costi e dei benefici che confronti le ore-uomo necessarie a risolvere il problema con la possibilità di pagare semplicemente il riscatto.

Gran parte della propria risposta è rappresentata dalla decisione di pagare o meno il riscatto. Trattandosi di una decisione complicata, potrebbe essere necessario consultare le forze dell'ordine e il proprio legale. Per molte vittime, vi è il rischio che il pagamento sia inevitabile (vedere pagina 16).

Mai affidarsi ai tool di decodifica dei ransomware gratuiti

Alcuni venditori di prodotti di sicurezza offrono programmi gratuiti di decodifica dei ransomware. In alcuni casi, questi ultimi possono aiutare le vittime a recuperare i propri dati senza pagare il riscatto.

Tuttavia, la maggior parte dei tool gratuiti funziona soltanto per una singola fascia di ransomware o persino per una singola campagna di attacco. Dal momento che i responsabili degli attacchi aggiornano costantemente i propri ransomware, i tool gratuiti diventano presto obsoleti e aumenta così la probabilità che essi non siano efficaci sui nuovi ransomware.

Potreste essere fortunati nel veder funzionare uno strumento di decodifica gratuito, ma non contemplatelo come piano di risposta all'incidente.

Ripristino dal backup

L'unico modo per portare a termine il recupero da un'infezione ransomware è ripristinare tutti i dati dal backup (i backup dovrebbero essere eseguiti giornalmente). Questa dovrà essere l'ultima spiaggia in termini di misure da prendere una volta infettati, ma dovrà essere la prima scelta in termini di prevenzione.

Anche sfruttando i backup recenti, comunque, il pagamento del riscatto potrebbe richiedere sforzi dal punto di vista finanziario e operativo. Il ripristino dai backup richiede tempo e sforzi. Alcune aziende potrebbero non essere in grado di concedersi tempi di inattività.

PAGARE O NON PAGARE: IL DILEMMA MORALE DEI RANSOMWARE

Il ransomware è già dannoso se considerato singolarmente. Tuttavia, uno dei suoi aspetti particolarmente abominevoli consiste nel fatto che obbliga le vittime a fare sia una "scelta di Hobson", sia una scelta morale. Spesso, quando si è sotto il mirino di una minaccia ransomware, non ci si può prendere il lusso di ponderare attentamente la correttezza morale del pagamento del riscatto. Il problema va risolto il prima possibile.

Finora, gli exploit malware hanno richiesto per lo più una linea d'azione trasparente: rilevamento della frode, archiviazione dei rapporti e risoluzione. Ma ora, i ransomware aggiungono una scelta morale all'equazione.

Accettare di pagare il riscatto è una decisione tanto riprovevole quanto necessaria. Infatti, finanzia attivamente l'autore dell'attacco che si è appena introdotto nella vostra rete rubando i vostri dati. Vi fa automaticamente apparire come persone che possiedono una rete vulnerabile e che, per questo motivo, hanno un incentivo a pagare. Inoltre, consente ai cybercriminali di finanziare attacchi futuri.

I recenti attacchi evidenziano, comunque, un fatto scomodo: non c'è sempre una risposta "bianco o nero" quando non si sa se pagare o meno.

Nessuna organizzazione desidera essere vittima di estorsione, né tantomeno finanziare gruppi criminali. Tornando all'esempio precedente, quali erano le scelte a disposizione dell'ospedale? In un certo qual modo, è il prezzo da pagare per aver finanziato in modo insufficiente i reparti IT, i quali utilizzavano software privi di patch o obsoleti. Negli Stati Uniti, vi sono ancora ospedali che lavorano su Windows XP. E 17.000 \$ è una cifra relativamente contenuta quando sono a rischio delle vite.

Persino l'FBI ha consigliato alle vittime di "pagare semplicemente il riscatto", a detta di Joseph Bonavolonta, agente speciale responsabile del programma Cyber and Counterintelligence nella sede dell'FBI di Boston.¹³ Eppure, ufficialmente, l'agenzia sconsiglia il pagamento. Infatti, anche accettando di pagare, si rischia comunque di non rientrare in possesso dei propri dati.¹⁴

Le organizzazioni devono prendere in considerazione tutte le possibilità prima di scegliere la linea d'azione migliore. Questi fattori possono includere:

- Tempo e ore-uomo necessari a tornare online
- Responsabilità di mantenimento delle attività in esecuzione nei confronti degli azionisti
- Sicurezza dei clienti e dei dipendenti
- Quale attività criminale potrebbe finanziare il pagamento.

Proprio come accade nelle situazioni più ostili, due organizzazioni diverse non risponderanno mai allo stesso modo.

ACCETTARE DI PAGARE IL RISCATTO È UNA DECISIONE TANTO RIPROVEVOLE QUANTO NECESSARIA. INFATTI, FINANZIA ATTIVAMENTE L'AUTORE DELL'ATTACCO CHE SI È APPENA INTRODOTTTO NELLA VOSTRA RETE RUBANDO I VOSTRI DATI.

¹³ Tess Danielson (Business Insider). "The FBI says you may need to pay up if hackers infect your computer with ransomware". Ottobre 2015.

¹⁴ FBI. "Ransomware". Aprile 2016.



DOPO L'ATTACCO

ESAMINARE E CONSOLIDARE

Indipendentemente dai danni causati dal ransomware, l'attacco rivela uno scarso livello di sicurezza che ha provocato la compromissione di un dispositivo o di una rete. Quando tutto sarà tornato alla normalità, avrete l'opportunità di imparare dagli errori commessi in termini di sicurezza al fine di evitare attacchi futuri.

Consigliamo di ricorrere a una valutazione di sicurezza da cima a fondo, ancora meglio se eseguita da un'azienda di servizi esterna, per identificare le eventuali minacce che si aggirano ancora nel proprio ambiente. Inoltre, è arrivato il momento di esaminare i vostri strumenti e le vostre procedure di sicurezza e, soprattutto, le relative carenze.

Pulizia

Alcuni ransomware contengono altre minacce o trojan backdoor in grado di scatenare attacchi futuri. Questo è il motivo per cui ripulire internamente ogni dispositivo e ripristinarlo da un backup risulta fondamentale. Consigliamo di avere un occhio più attento per rilevare eventuali minacce nascoste ignorate nel caos generale.

Analisi a posteriori

È opportuno analizzare la propria prontezza e reattività alle minacce. In che modo è stato eseguito il piano di risposta alla crisi? Possiamo migliorare le configurazioni di rete per contenere eventuali attacchi futuri? Possiamo implementare una soluzione di sicurezza delle e-mail più massiccia?

Controllate le misure di sicurezza attuali e chiedetevi se siano sufficienti a combattere le minacce odierne. Trasformate questa esperienza in una lezione appresa: infatti, è assai probabile che vi ricapiti in futuro. Se non si scopre come si è insinuato il ransomware, non sarà possibile bloccare l'attacco successivo.

Valutazione della consapevolezza degli utenti

La maggior parte dei ceppi di ransomware fa leva sull'interazione umana per dispiegare carichi paganti. Nel caso in cui, a causa di misure di sicurezza vigenti scarse, si dovesse ricevere una "fattura insoluta" infettata tramite e-mail, un dipendente ben informato rappresenta l'ultima linea di difesa da cui dipenderà il futuro di un'azienda, un ospedale o una scuola: rimanere online oppure apparire sull'ennesima statistica ransomware. Assicuratevi che i dipendenti, il personale o le facoltà siano all'altezza dell'incarico.

Potrebbe inoltre essere utile investire in aziende specializzate nei test di penetrazione, la cui missione è aumentare la consapevolezza dei dipendenti e incrementare la sicurezza aziendale. Replicando gli attacchi reali tramite gli exploit di spear phishing, ingegneria sociale e social media, i "pen tester" possono analizzare e identificare le vulnerabilità in termini di sicurezza giocando in anticipo rispetto agli attacchi effettivi.

Formazione e addestramento

Dopo aver analizzato la consapevolezza degli utenti, è necessario sviluppare un programma formativo che si proponga di ridurre la vulnerabilità dei dipendenti agli attacchi informatici, facendo leva sulle lezioni apprese dalle esperienze precedenti, nonché implementare un piano di comunicazione delle crisi nell'eventualità di un attacco futuro e controlli basati su esercitazioni e test di penetrazione.

Investire in difese moderne

Gli hacker e altri cybercriminali sono stati sempre un passo avanti alle misure di sicurezza endpoint e alle forze dell'ordine.

Se da un lato la maggior parte delle reti è esperta nel blocco delle minacce note, l'odierno scenario di minacce 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 veicoli principali degli attacchi ransomware.

Pertanto, è necessario cercare soluzioni di sicurezza che possano adattarsi a minacce nuove ed emergenti e aiutarvi a rispondere più velocemente a esse.

CONCLUSIONE

Il ransomware è tornato in modo ancora più imponente e con intenti maggiormente redditizi. Queste linee guida possono mostrarvi la strada giusta per combattere i ransomware prima, durante e dopo un attacco effettivo.

Naturalmente, il modo più efficace per farlo è bloccarne l'accesso, il che richiede una soluzione anti-minaccia avanzata in grado di rilevare i ransomware propagati tramite e-mail, dispositivi mobili e social media.

Una cybersicurezza massiccia identifica ed elimina i ransomware prima che possano metter piede nel vostro ambiente. Questo include la capacità di analizzare gli allegati e i link delle e-mail in tempo reale, scardinare le minacce in un ambiente virtuale e aggiornare repentinamente le politiche. Inoltre, viene ridotto il fattore umano, il collegamento più debole nella maggior parte delle infrastrutture di sicurezza.

Per maggiori informazioni su come bloccare gli attacchi ransomware, visitare www.proofpoint.com/targeted-attack-protection.

CHECKLIST DI SOPRAVVIVENZA RANSOMWARE

Segue una rapida checklist utile a valutare se si è pronti a evitare e gestire le minacce ransomware.

Prima: prevenire l'arrivo dei ransomware

- ☐ Backup e ripristino
- ☐ Aggiornamento e patch
- ☐ Formazione e addestramento degli utenti
- ☐ Investire in massicce soluzioni di sicurezza per e-mail, dispositivi mobili e social media

Durante: ritorno alle attività

- ☐ Contattare le forze dell'ordine
- ☐ Scollegarsi dalla rete
- ☐ Determinare l'entità del problema sulla base della threat intelligence
- ☐ Pianificare una risposta
- ☐ Mai affidarsi ai tool di decodifica dei ransomware gratuiti
- ☐ Ripristino dal backup

Dopo: esaminare e consolidare

- ☐ Pulizia
- ☐ Analisi a posteriori
- ☐ Valutazione della consapevolezza degli utenti
- ☐ Formazione e addestramento
- ☐ Investire in difese moderne



INFORMAZIONI SU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), società di sicurezza informatica di nuova generazione, consente alle aziende di proteggere la modalità di lavoro odierna dei propri dipendenti dalle minacce avanzate e dai rischi di conformità. Proofpoint aiuta i professionisti della sicurezza informatica a proteggere i propri utenti dagli attacchi avanzati che li prendono di mira (tramite e-mail, app mobili e social media), a proteggere le informazioni importanti create dai dipendenti e a dotare i team dell'intelligenza e degli strumenti giusti per rispondere rapidamente quando insorgono problemi. Aziende leader di tutte le dimensioni, tra cui oltre il 50 per cento di quelle presenti in Fortune 100, si affidano alle soluzioni di Proofpoint, che sono create per gli ambienti IT odierni mobili e social e sfruttano sia la potenza del cloud sia una piattaforma di analisi basata su big data per combattere le moderne minacce avanzate.

proofpoint[™]

www.proofpoint.com

©Proofpoint, Inc. Proofpoint è un marchio di Proofpoint, Inc. negli Stati Uniti e in altri Paesi. Tutti gli altri marchi contenuti nel presente documento sono di proprietà dei rispettivi titolari.