Protezione contro il ransomware con Proofpoint

Impedisci al ransomware di radicarsi e diffondersi nella tua azienda.

Prodotti

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

Vantaggi principali

- Prevenzione dell'infezione iniziale
- Prevenzione di ricognizione, spostamento laterale e persistenza
- Prevenzione delle sottrazioni di dati

Il ransomware è oggi una delle forme di attacco informatico più deleterie. Causa il fallimento delle aziende, costringe gli ospedali a rifiutare i pazienti e blocca l'attività delle amministrazioni pubbliche. Oggi è una delle minacce informatiche più pericolose. Solo l'anno scorso, gli Stati Uniti hanno subito più di 65.000 attacchi di ransomware. Questa minaccia, che preoccupa molto i CISO, è diventata un problema di sicurezza nazionale. Ma quel che è peggio è che molte aziende sono del tutto impreparate per affrontare un attacco di ransomware. Solo il 13% degli esperti informatici interpellati dal Ponemon Institute afferma che la propria azienda è in grado di prevenire un attacco ransomware. Oltre il 68% si considera "vulnerabile" o "molto vulnerabile".[1]

L'email e il web sono i principali vettori degli attacchi di ransomware, la maggior parte dei quali attualmente si svolge in più fasi. La violazione di email e siti web rappresentano le fasi iniziali della catena di attacco. Il payload iniziale è spesso distribuito come un downloader di malware ed è concepito per ottenere penetrare nel sistema di un utente al fine di sottrarre le credenziali e ottenere l'accesso alla rete dello stesso. Gli operatori del ransomware usano le credenziali rubate per accedere ai servizi che sono esposti su Internet. Le tattiche più comuni sono le email di phishing delle credenziali d'accesso, gli attacchi di forza bruta per ottenere le password e le violazioni tramite download guidato.

Una volta ottenuto l'accesso iniziale, gli operatori del ransomware si stabiliscono in modo permanente, effettuano una ricognizione e si spostano lateralmente. Dall'interno, i criminali informatici non solo crittografano i file sensibili, ma possono anche trafugare informazioni sensibili per mettere in atto una doppia estorsione.

Poiché le funzionalità di backup e ripristino sono diventate più efficaci nel respingere gli attacchi di ransomware, le tattiche dei criminali informatici si sono evolute per eluderle. Oggi viene utilizzato il cosiddetto ransomware a doppia estorsione. Questa tattica comporta l'esfiltrazione dei dati sensibili e poi la crittografia dei file. Se l'azienda colpita rifiuta di pagare per far decrittografare i file, il criminale informatico ha tre opzioni per ottenere il pagamento:

1 The Ponemon Institutte, "The Rise of Ransomware" (L'ascesa del ransomware), gennaio 2017.

- Minacciare la vittima di divulgare i dati online
- Vendere i dati al miglior offerente
- Inviare email ai clienti e ai partner della vittima, minacciando di divulgare i loro dati.

L'email è il punto di infezione iniziale per la maggior parte degli attacchi di ransomware. Ecco perché un'ampia percentuale di essi inizia, in maniera diretta o indiretta, con un'email di phishing. Queste email inducono gli utenti ad aprire un allegato pericoloso o a fare clic su un URL dannoso. Servono quindi delle soluzioni avanzate per rilevare e impedire a tali minacce di compromettere le credenziali di accesso di un utente. La maggior parte dei dati di un'azienda è memorizzata nel cloud e lo stesso vale per i file delle password e i dati sensibili. È importante limitare l'esposizione dei dati nel cloud per ridurre al minimo la quantità di informazioni che possono essere condivise con i malintenzionati.

Secondo quanto osservato da Proofpoint, gli attacchi ransomware stanno diventando più mirati, più dannosi e sempre più dirompenti per le attività delle aziende. Proofpoint Advanced Threat Protection e Proofpoint Cloud Security possono aiutarti a prevenirle. Le nostre piattaforme, complete e integrate, riducono il rischio di attacco da parte di ransomware con più livelli di controllo per:

- Prevenire l'infezione iniziale
- Rilevare l'accesso iniziale e impedire la scoperta, il movimento laterale e la persistenza
- Prevenire l'esfiltrazione dei dati.

Prevenire l'infezione iniziale

Per aiutarti a prevenire le infezioni iniziali, Proofpoint Advanced Threat Protection e Proofpoint Cloud Security:

- Rilevano e bloccano il ransomware e i downloader di malware all'origine della distribuzione del ransomware
- Prevengono la violazione delle credenziali d'accesso
- Offrono visibilità sui rischi posti dal ransomware
- Isolano i clic sugli URL in base al rischio
- Insegnano agli utenti a individuare e segnalare i messaggi pericolosi
- Automatizzano la risoluzione delle minacce che giungono via email.

Rilevamento e blocco di ransomware e downloader di malware

La piattaforma Proofpoint Advanced Threat Protection rileva e blocca sia il ransomware che viene inviato inizialmente come payload, sia il malware che lo scarica. I nostri numerosi motori basati sul machine learning permettono di rilevare il malware, il codice dannoso e le tecniche di elusione e proteggono gli utenti dai siti web dannosi e dai file infettati dal ransomware.

La piattaforma esegue anche l'analisi di reputazione e contenuti e analisi approfondite in ambiente sandbox delle minacce nascoste negli URL o negli allegati. Le funzionalità di analisi predittiva permettono di identificare e isolare nella sandbox gli URL sospetti, in base alle variazioni nelle tattiche dei criminali informatici. Per esempio, la piattaforma mette nella sandbox tutti gli URL dei siti legittimi di condivisione di file a causa del loro crescente utilizzo da parte dei criminali informatici per ospitare malware. Le soluzioni che invece si affidano solo all'analisi della reputazione non rilevano questi attacchi.

Prevenzione della violazione delle credenziali d'accesso

Per sottrarre le credenziali degli utenti, i criminali informatici hanno a disposizione tattiche diverse: phishing, attacchi di forza bruta, dark web e informazioni esposte nell'archivio cloud di un utente. Una volta ottenute le credenziali d'accesso, non è più necessario inviare un downloader. Al criminale informatico è sufficiente usare le tue credenziali per accedere alla tua VPN o ai servizi web. Dopodiché può rubare i dati confidenziali o i crittografare i file. Man mano che adottano sempre più servizi cloud, le aziende sono esposte al rischio di utenti negligenti che potrebbero caricare nel cloud i file delle password e i dati sensibili.

Proofpoint Advanced Threat Protection rileva e blocca i messaggi di phishing avvalendosi di più motori di rilevamento, compresi i classificatori basati sul machine learning che ispezionano gli URL. Proofpoint Cloud Security identifica le informazioni sensibili esposte negli account cloud che possono essere sfruttate dai criminali informatici.

Visibilità sul rischio di attacco ransomware

Proofpoint ti aiuta a identificare i tuoi VAP (Very Attacked People™ ovvero le persone più attaccate), ovvero i dipendenti della tua azienda più esposti agli attacchi. Questo ti permette di vedere i dipendenti che vengono più attaccati e le minacce cui sono soggetti. Questi dati ti permettono di adattare la tua strategia di difesa alle specifiche minacce che prendono di mira i tuoi VAP.

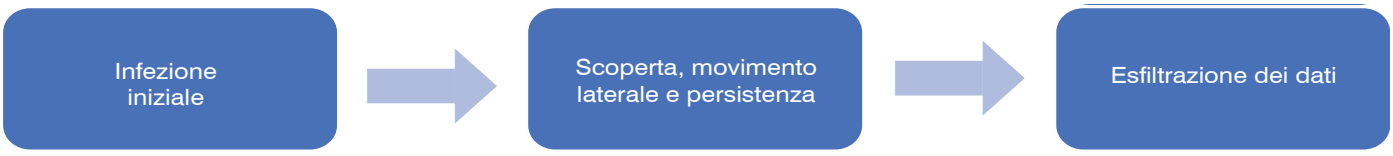

Figura 1: tre livelli di protezione.

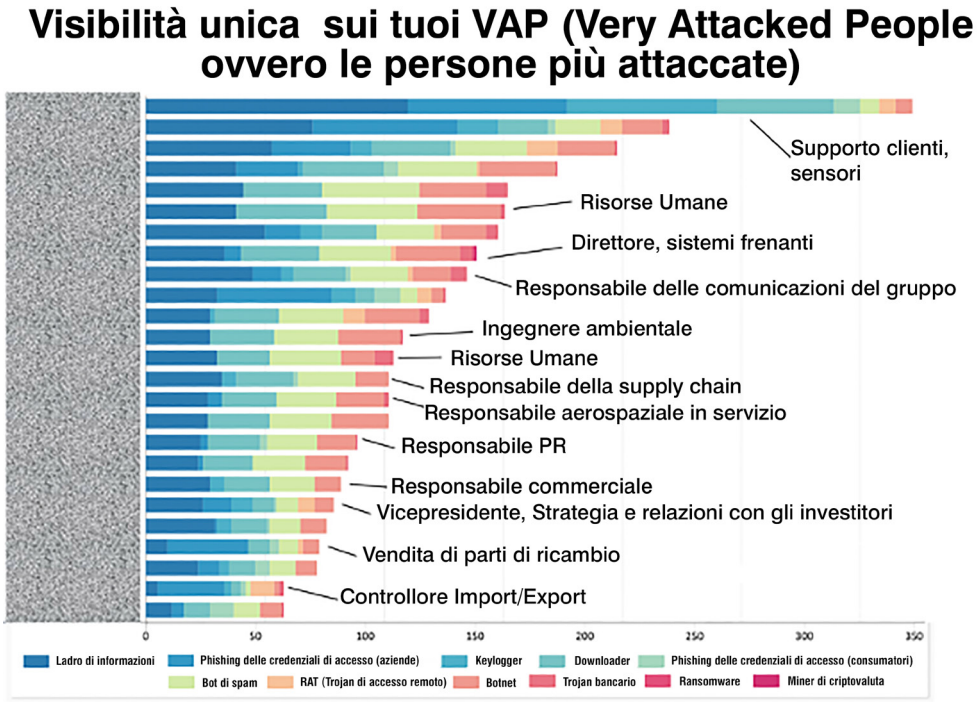

Figura 2: Proofpoint ti aiuta a identificare i tuoi VAP (Very Attacked People ovvero le persone più attaccate).

Proofpoint fornisce anche informazioni dettagliate su minacce e campagne. La dashboard Threat Insight mostra dati forensi approfonditi sui criminali informatici, i metodi di diffusione, degli esempi di messaggi, i destinatari, la progressione degli attacchi e molto altro ancora.

Riduzione dell'impatto con l'isolamento integrato delle email

I criminali informatici possono infettare gli URL dopo la consegna. Questa strategia permette di eludere il rilevamento iniziale. Proofpoint Browser Isolation riduce l'impatto dei clic degli utenti sugli URL dannosi. Fornisce una protezione in tempo reale quando si fa clic sugli URL nelle email aziendali e isola l'attività di navigazione ponendola in un contenitore sicuro che mostra agli utenti solo una versione sicura. Inoltre previene i downloader della prima fase e il furto delle credenziali d'accesso, interrompendo di fatto la catena dell'attacco.

Puoi implementare un isolamento basato sui rischi in base alle tue policy e alle informazioni sui tuoi VAP, inviare gli URL più pericolosi in sessioni di navigazione isolate del browser, definire policy più rigorose per le persone prese di mira, isolando tutti i loro clic e anche adattare la policy di isolamento al livello di rischio dell'utente e degli URL su cui fa clic.

Sensibilizzazione degli utenti ai problemi di sicurezza informatica

Per prevenire gli attacchi di ransomware i tuoi dipendenti devono essere formati. Dopo tutto, sono proprio i tuoi utenti l'ultima linea di difesa. Affinché un attacco di ransomware vada a buon fine, è necessario che un utente faccia clic su un link o scarichi un allegato. Secondo il report DBIR 2021 di Verizon, l'85% delle violazioni dell'anno scorso ha richiesto l'interazione umana[2].

La piattaforma Threat Protection include la formazione di sensibilizzazione alla sicurezza, per rendere i tuoi utenti consapevoli degli attacchi ransomware e istruirli a non fare clic sui messaggi sospetti. È possibile anche assegnare più lezioni agli utenti più colpiti e a quelli che sono stati già vittima di un attacco. Per consolidare ulteriormente la formazione degli utenti, puoi utilizzare le risorse della nostra vasta libreria di contenuti nelle tue comunicazioni con i dipendenti e negli avvisi di sicurezza. Puoi lanciare le simulazioni di attacchi con dei modelli elaborati sulla base di esche reali osservate nei miliardi di messaggi analizzati da Proofpoint. La piattaforma fornisce facili meccanismi per segnalare le email sospette, come il pulsante PhishAlarm e la visualizzazione di avvisi.

Automazione della correzione dei messaggi pericolosi

I team della sicurezza sono spesso a corto di personale e sommersi di avvisi che devono essere rapidamente ordinati per priorità e analizzati. La piattaforma Threat Protection fornisce orchestrazione, automazione e risposta agli incidenti di sicurezza contro l'email (mSOAR, Security Orchestration, Automation and Response). Automatizza l'indagine e la risoluzione delle email dannose o indesiderate segnalate dagli utenti.

2 Verizon, "DBIR: "Data Breach Incident Report" (Report d'analisi sulle violazioni dei dati), 2021.

Le credenziali di accesso degli utenti sono le chiavi del tuo regno. Con un solo nome utente e password, l'operatore del ransomware può sferrare attacchi sia dall'esterno sia dall'interno della tua azienda.

I messaggi segnalati dai tuoi utenti vengono automaticamente analizzati e arricchiti da diversi sistemi di threat intelligence e reputazione. Se un messaggio risulta essere pericoloso, viene automaticamente messo in quarantena insieme a tutti i messaggi correlati. così non è più necessario analizzare ogni singolo avviso e correggere manualmente i messaggi dannosi. Il tuo team di sicurezza risparmierà una gran quantità di tempo e ricorse. Per chiudere il cerchio, gli utenti ricevono un'email personalizzata che conferma che il messaggio era pericoloso. Questo serve a rafforzare i comportamenti virtuosi.

La piattaforma Threat Protection analizza i messaggi anche dopo che sono stati consegnati. Se un elemento pericoloso viene rilevato dopo il recapito, il messaggio viene automaticamente estratto dalla casella email dell'utente così come i messaggi inoltrati agli altri utenti oppure inviati tramite liste di distribuzione.

Rilevare l'accesso iniziale e impedire la scoperta, il movimento laterale e la persistenza

Proofpoint Cloud Security rileva le minacce ransomware:

- Monitorando e rilevando gli account cloud compromessi
- Monitorando i caricamenti di file pericolosi negli account cloud
- Proteggendo dai payload di comando e controllo (C&C) grazie a Proofpoint Web Security

Rilevamento degli account cloud di cui è stato preso il controllo

Le credenziali di accesso degli utenti sono le chiavi del tuo regno. Con un solo nome utente e password, specialmente per le applicazioni cloud come Microsoft 365 o Google Workplace, l'operatore del ransomware può sferrare attacchi sia dall'esterno sia dall'interno di un'azienda. La soluzione Proofpoint Cloud Security CASB offre controlli adattivi degli accessi in tempo reale in base al rischio, al contesto e al ruolo. I tentativi di accesso da sedi pericolose o da parte di noti criminali informatici vengono bloccati automaticamente. Proofpoint CASB utilizza inoltre dati contestuali per confermare l'identità di un utente e prevenire gli accessi a rischio, come la posizione dell'utente, il dispositivo, la rete e l'ora di accesso. Per proteggersi dagli operatori del ransomware è possibile definire delle policy di controllo dell'accesso, come l'applicazione dell'autenticazione a più fattori, oppure la limitazione dell'accesso ai dispositivi non gestiti.

Proofpoint ti offre la visibilità necessaria per far emergere la diffusione laterale o il rischio posto ai tuoi dati in seguito alla violazione di un account. Puoi anche determinare se una connessione sospetta è correlata a un account che invia email dannose, oppure se un criminale informatico ha cercato di installare un accesso persistente tramite l'impostazione di regole di inoltro e delega dell'email o l'utilizzo di token OAuth. Hai inoltre visibilità sul tipo di attività dei file sospetti.

Prevenzione della distribuzione del ransomware dalle applicazioni cloud

Il ransomware può diffondersi attraverso la condivisione di file infetti e la sincronizzazione automatica, con ripercussioni potenzialmente gravi per la tua azienda, i tuoi partner e i tuoi clienti. Proofpoint Cloud Security monitora attivamente le condivisioni dei file nel cloud e ti avvisa quando trova un file sospetto. Con lo strumento di analisi sandbox di Proofpoint e l'analisi dei file nelle applicazioni cloud, è possibile confinare questi file dannosi nel cloud tramite la quarantena automatica e altre misure di mitigazione.

Protezione contro i payload di comando e controllo grazie a Proofpoint Web Security

Un dispositivo compromesso invia un segnale ai server del criminale informatico, il quale quindi invia la successiva serie di istruzioni. Grazie al controllo del dispositivo, l'operatore del ransomware può eseguire una serie di azioni, che vanno dalla distribuzione del ransomware al trafugamento dei dati.

Le funzionalità Web Security e Browser Isolation di Proofpoint Cloud Security bloccano le connessioni ai siti compromessi, impedendo così al gestore del ransomware di controllare il dispositivo e causare ulteriori danni. La threat intelligence è alimentata dal grafico sulle minacce Nexus di Proofpoint che combina in tempo reale migliaia di miliardi di punti dati su molteplici vettori delle minacce in tutto il mondo, con l'intelligenza artificiale avanzata, il machine learning e un gruppo di ricercatori globale per tenere testa alle minacce informatiche più pericolose.

Prevenire l'esfiltrazione dei dati

Proofpoint Advanced Threat Protection e Proofpoint Cloud Security prevengono l'esfiltrazione dei dati:

- Monitorando i segni precoci di esfiltrazione dei dati
- Rilevando e prevenendo i movimenti dei dati non autorizzati

Le funzionalità Web Security e Browser Isolation di Proofpoint Cloud Security proteggono i dati tenendo conto dei rischi e prevenendo le perdite di dati (DLP) in tempo reale. Utilizzate insieme, le funzionalità Browser Isolation e Web Security forniscono controlli granulari dei dati come l'accesso in sola lettura e autorizzano o bloccano le applicazioni cloud e il web. Proofpoint Browser Isolation protegge l'accesso degli utenti ai dati e alle applicazioni isolando le sessioni del browser in un contenitore sicuro.

Inoltre, Proofpoint CASB ti aiuta a ottenere una visibilità immediata sulle attività sospette dei file che possono essere correlate con delle connessioni sospette. I team della sicurezza possono rapidamente distinguere le attività sui file iniziate dai criminali informatici da quelle avviate dagli utenti e reagire in modo tempestivo.

Oltre a proteggere i dati sensibili nelle app del cloud, Proofpoint è in grado di bloccare l'esfiltrazione di contenuti sensibili tramite payload di comando e controllo, il download dei contenuti su dispositivi non gestiti (appartenenti all'operatore del ransomware) e il loro invio tramite email.

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.

0203-004-01-03 12/21