Panoramica sulla soluzione

Sconfiggi il ransomware: assicurati che i tuoi dati non siano presi in ostaggio

Il ransomware è un malware che utilizza la crittografia asimmetrica per tenere sotto sequestro le informazioni di una vittima. La crittografia asimmetrica (pubblica-privata) è una crittografia in cui viene utilizzata una coppia di chiavi per cifrare e decifrare un file. La coppia di chiavi pubblica-privata viene generata in modo univoco dall'aggressore per la specifica vittima. La chiave privata, necessaria per decifrare i file, viene memorizzata nel server dell'aggressore stesso. Quest'ultimo mette la chiave privata a disposizione della vittima solo dopo il pagamento del riscatto, anche se non è sempre così, come si è visto in recenti campagne di ransomware. Senza l'accesso alla chiave, decifrare i file tenuti in ostaggio è pressoché impossibile.

Uno sguardo al ransomware

Per un approfondimento tecnico sul ransomware, consulta il ***Report McAfee Labs sulle minacce: maggio 2015***. Nel *Report McAfee Labs sulle minacce: novembre 2014* abbiamo previsto le nove principali minacce del 2015. Relativamente al ransomware, McAfee Labs ha affermato: "Il ransomware evolverà i suoi metodi di propagazione, di crittografia e i bersagli perseguiti". Quasi immediatamente c'è stato un picco elevato nella prevalenza del ransomware, oltre alla comparsa di nuove famiglie come Teslacrypt e di ulteriori modifiche nelle famiglie correnti come CTB-Locker, CryptoWall e TorrentLocker.

La maggior parte delle campagne di ransomware inizia con un attacco di phishing. Nel corso del tempo le campagne sono diventate più sofisticate e molte di esse ora sono specificamente e meticolosamente adattate per le impostazioni locali delle vittime prese di mira.

Le nuove tecnologie sono state adattate per rendere il ransomware più efficace.

- **Valuta virtuale:** usando la **valuta virtuale** come mezzo per far pagare i riscatti, gli aggressori non si espongono ai controlli del banking tradizionale e alla possibilità di tracciatura dei bonifici.
- **La rete Tor:** utilizzando la **rete Tor** gli aggressori possono occultare più facilmente l'ubicazione dei propri server di controllo che detengono le chiavi private delle vittime. Tor permette di mantenere a lungo un'infrastruttura criminale, che può anche essere affittata ad altri autori di attacco per svolgere le campagne affiliate.
- **Lo spostamento ai dispositivi mobili:** nel giugno 2014 i ricercatori hanno scoperto la prima famiglia di ransomware che cifra i dati contenuti nei dispositivi Android[1]. Pletor utilizza la crittografia AES, blocca i dati nella scheda di memoria del telefono e infine usa Tor, gli SMS o l'HTTP per connettersi con gli autori dell'attacco.

intel Security

- **La presa di mira dei dispositivi di archiviazione di massa:** nell'agosto 2014 Synolocker ha iniziato a colpire i dischi NAS (network-attached storage) e le stazioni rack di Synology[2]. Questo malware sfrutta una vulnerabilità presente nelle versioni non corrette dei server NAS per cifrare in remoto tutti i dati nei server, utilizzando la crittografia RSA con le chiavi a 2.048 bit o 256 bit.

Tutelarsi dal ransomware

Ecco alcune buone pratiche e policy per proteggere meglio se stessi e l'azienda contro la minaccia del ransomware.

- **Sensibilizzare continuamente gli utenti:** dato che la maggior parte degli attacchi di ransomware inizia con un'email di phishing, la sensibilizzazione degli utenti è necessaria e di fondamentale importanza. Le statistiche indicano che, per ogni dieci email inviate dagli aggressori, almeno una ha successo. Non aprire le email o gli allegati provenienti da mittenti non verificati o sconosciuti.
- **Mantenere aggiornate le patch di sistema:** molte vulnerabilità comunemente sfruttate dal ransomware possono essere protette con delle patch. Mantenere aggiornati con le patch i sistemi operativi, Java, Adobe Reader, Flash e le applicazioni. Implementare una procedura di applicazione delle patch e verificare che siano state applicate correttamente.
- **Aprire gli allegati con estrema cautela:** configurare il software antivirus per la scansione automatica di tutti gli allegati di email e della messaggistica immediata. Accertarsi che i programmi email non aprano automaticamente gli allegati o visualizzino automaticamente la grafica e disattivare il riquadro di anteprima. Non aprire mai le email indesiderate o gli allegati inattesi, anche se provenienti da persone conosciute.
- **Fare attenzione al phishing basato sullo spam:** evitare di fare clic sui link presenti nelle email o nei messaggi immediati.

Cosa può fare Intel Security per aiutarti a proteggerti dal ransomware

McAfee Web Gateway

Malvertising, download guidati e URL pericolosi incorporati in siti web affidabili sono solo alcuni dei metodi di attacco utilizzati per distribuire il ransomware. **McAfee Web Gateway** è un prodotto efficace con cui potrai ottimizzare la protezione della tua azienda da questo tipo di minaccia.

- **McAfee Gateway Anti-Malware Engine:** l'analisi senza firma degli intenti filtra in tempo reale i contenuti dannosi dal traffico web. L'emulazione e l'analisi del comportamento proteggono in modo proattivo contro gli attacchi mirati e zero-day. McAfee Gateway Anti-Malware Engine ispeziona i file e ne blocca il download nel caso in cui siano pericolosi.
- **Integrazione con McAfee Global Threat Intelligence (McAfee GTI):** i feed di intelligence in tempo reale sulla reputazione di file e siti web e la classificazione dei siti di McAfee GTI garantiscono protezione dalle minacce più recenti perché McAfee Web Gateway blocca i tentativi di connessione ai siti Web di cui è nota la pericolosità o ai siti che utilizzano reti pubblicitarie malevole.

McAfee Email Gateway

Il fatto che un'apparentemente innocua email nella casella di posta di un utente possa essere invece un attacco di phishing è fonte di notevole preoccupazione per le aziende. **McAfee Email Gateway** offre protezione con diverse funzioni che contrastano questi tipi di attacchi di phishing sempre più sofisticati.

- **ClickProtect:** elimina le minacce che si annidano negli URL incorporati nei messaggi email con la scansione degli URL al momento del clic dell'utente. L'ispezione prevede il controllo della reputazione dell'URL e l'emulazione proattiva da parte di Gateway Anti-Malware Engine.
- **Integrazione con McAfee Advanced Threat Defense:** rileva il malware sofisticato e sfuggente con l'analisi approfondita del codice, statica e dinamica, eseguita sui file sospetti allegati alle email, bloccando i file pericolosi prima ancora che giungano in una casella di posta.

- **Integrazione con McAfee GTI:** combina le informazioni delle reti locali e i dati di intelligence globali sulla reputazione forniti da McAfee Global Threat Intelligence per garantire la forma di protezione più completa contro minacce, spam e malware in ingresso.

McAfee Advanced Threat Defense
McAfee Advanced Threat Defense è una soluzione multilivello per il rilevamento del malware che riunisce molteplici motori di verifica che applicano controlli basati su firme e reputazione, emulazione in tempo reale, analisi completa del codice statico e sandboxing dinamico. McAfee Advanced Threat Defense protegge contro i ransomware prevalenti come CTB-Locker, CryptoWall e altri.

- **Rilevamento basato sulle firme:** rileva virus, worm, rootkit, trojan, buffer overflow e attacchi misti. La sua knowledge base completa, creata e aggiornata da McAfee Labs, contiene attualmente oltre 150 milioni di firme, comprese quelle di CTB-Locker, CryptoWall e delle loro varianti.
- **Rilevamento basato sulla reputazione:** controlla la reputazione dei file mediante il servizio McAfee GTI per rilevare le minacce emergenti.
- **Analisi statica ed emulazione in tempo reale:** consentono di individuare rapidamente minacce zero-day e malware non identificati dalle tecniche basate su firma o secondo la reputazione.
- **Analisi completa del codice statico:** decompila il codice dei file per valutarne tutti gli attributi e i set di istruzioni e analizzare in modo approfondito il codice sorgente senza eseguirlo. Le funzioni esaustive di decompressione aprono tutti i tipi di file compressi e di archivi per abilitare l'analisi completa e la classificazione del malware, consentendo alla tua azienda di comprendere la minaccia posta dallo specifico malware.
- **Analisi dinamica nella sandbox:** esegue il codice del file in un ambiente di runtime virtuale e osserva il comportamento che ne risulta. Gli ambienti virtuali si possono configurare in modo da riprodurre gli ambienti host della tua azienda e supportano immagini personalizzate dei sistemi operativi Windows 7 (a 32 o 64 bit), Windows XP, Windows Server 2003, Windows Server 2008 (64 bit) e Android.

McAfee Threat Intelligence Exchange
Disporre di una piattaforma di intelligence in grado di adattarsi nel tempo alle esigenze del tuo ambiente è importante. **McAfee Threat Intelligence Exchange** riduce considerevolmente l'esposizione a questi tipi di attacchi grazie all'individuazione delle minacce immediate come file o applicazioni sconosciute in esecuzione nell'ambiente. Il blocco degli eseguibili nuovi o sconosciuti assicura una protezione proattiva contro il ransomware.

- **Informazioni complete sulle minacce:** personalizza facilmente le informazioni complete sulle minacce provenienti dalle fonti dislocate in tutto il mondo. Queste ultime possono essere costituite da feed McAfee GTI oppure di terze parti, contenenti le informazioni locali sulle minacce derivanti da eventi passati o in fase di svolgimento, inviate tramite endpoint, gateway e altri componenti della sicurezza.
- **Prevenzione dell'esecuzione e remediation:** McAfee Threat Intelligence Exchange può intervenire e impedire l'esecuzione di applicazioni sconosciute nell'ambiente. Se un'applicazione ammessa all'esecuzione viene in seguito giudicata dannosa, McAfee Threat Intelligence Exchange disattiva in tutto l'ambiente i processi in esecuzione a essa associati, grazie alle potenti capacità di gestione centralizzata e di imposizione delle policy.
- **Visibilità:** McAfee Threat Intelligence Exchange può rilevare tutti i file eseguibili compressi e la loro esecuzione iniziale all'interno dell'ambiente, oltre a tutte le modifiche che si verificano in seguito. Tale visibilità sulle azioni di un'applicazione o processo, dall'installazione fino al momento contingente, velocizza risposta e remediation.
- **Indicatori di compromissione (IoC):** importate gli hash dei file nocivi in McAfee Threat Intelligence Exchange per immunizzare l'ambiente da questi file di pericolosità nota mediante l'imposizione di policy. Se nell'ambiente viene attivato uno degli IoC, McAfee Threat Intelligence Exchange può interrompere tutti i processi e le applicazioni associati a quell'IoC.

McAfee VirusScan Enterprise

Con **McAfee VirusScan® Enterprise** è semplice rilevare ed eliminare il ransomware. McAfee VirusScan Enterprise utilizza il premiato motore di scansione McAfee per proteggere i file da virus, worm, rootkit, trojan e altre minacce avanzate.

- **Protezione proattiva contro gli attacchi:** integra la tecnologia antimalware e la prevenzione delle intrusioni per proteggere dagli attacchi che sfruttano gli exploit da overflow del buffer indirizzati alle vulnerabilità delle applicazioni.
- **Rilevamento ed eliminazione del malware imbattibili:** protegge da minacce come rootkit e trojan con l'analisi avanzata dei comportamenti. Blocca il malware sul nascere impiegando tecniche tra cui il blocco delle porte, dei nomi file, delle cartelle o directory e delle condivisioni dei file, rintracciando e risolvendo le infezioni.
- **Sicurezza in tempo reale tramite l'integrazione di McAfee GTI:** protegge contro le minacce note ed emergenti su tutti i vettori – file, web, email e rete – grazie al supporto della piattaforma di informazioni sulle minacce più esaustiva del mercato.

McAfee Network Security Platform

McAfee Network Security Platform è studiato per eseguire ispezioni approfondite del traffico di rete. McAfee Network Security Platform combina le tecniche di ispezione più avanzate – analisi completa del protocollo, reputazione delle minacce, analisi comportamentale e analisi avanzata del malware – per rilevare e prevenire gli attacchi, ad es. il caso del ransomware che cerca di comunicare tramite i protocolli di rete quali Tor, IRC e altri.

- **Difesa completa contro il malware:** combina la reputazione dei file di McAfee GTI, l'analisi approfondita dei file con ispezione di JavaScript e l'analisi avanzata e senza firma del malware per rilevare e neutralizzare le minacce zero-day, il malware personalizzato e altri attacchi di virus occulti.
- **Sfrutta le tecniche di ispezione avanzata:** analisi completa del protocollo, reputazione delle minacce e analisi comportamentale per rilevare e prevenire nella rete sia gli attacchi noti che quelli di tipo zero-day.
- **Integrazione con McAfee GTI:** combina la reputazione in tempo reale dei file, la reputazione degli indirizzi IP e la localizzazione geografica con il contesto dettagliato costituito da utenti, dispositivi e applicazioni. Ciò consente una risposta rapida e accurata agli attacchi che si originano dalla rete.
- **Security Connected:** grazie all'utile integrazione fra i due prodotti, McAfee Network Security Platform può inviare i file sospetti scoperti nel traffico monitorato a McAfee Advanced Threat Defense e negarne o consentirne l'esecuzione a seconda dei risultati ottenuti da McAfee Advanced Threat Defense.

Fare in modo che i preziosi dati di un'organizzazione non siano delle facili prede può sembrare un'impresa ardua, soprattutto con la costante crescita del ransomware quale vettore dell'attacco. La tecnologia Intel Security aiuta la tua azienda a proteggersi in modo proattivo da minacce come il ransomware sia sugli endpoint, sia sulla rete.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com