SOPHOS

Remote Ransomware

Il remote ransomware rappresenta una minaccia significativa: nel 60% degli attacchi, gli hacker utilizzano la cifratura remota[1]. Il ransomware è un business da 1 miliardo di dollari che spesso riesce a eludere i tradizionali software antivirus. Per impedire ai malware di cifrare i tuoi file, occorre una soluzione che sappia riconoscere esattamente cosa cercare e soprattutto quando entrare in azione. Leggi questa guida per scoprire di più sui pericoli dei remote ransomware e sulla protezione antiransomware in grado di bloccarli: le soluzioni leader di settore di Sophos.

Whitepaper Sophos. Giugno 2024

Che Cosa Sono I Remote Ransomware?

Un attacco “remote ransomware”, detto anche cifratura malevola eseguita da remoto, compromette un endpoint e lo usa per cifrare i dati su altri dispositivi all’interno della stessa rete.

Negli attacchi coordinati da menti umane, gli hacker cercano tipicamente di distribuire ransomware direttamente sul computer che vogliono cifrare. Se il tentativo iniziale viene bloccato (ad es. dalle tecnologie di sicurezza del dispositivo colpito), gli hacker non si perdono d’animo e optano invece per approcci alternativi, provando varie volte fino a quando non raggiungono il loro obiettivo.

Una volta violato il dispositivo, i criminali possono sfruttare l’architettura di dominio dell’organizzazione per cifrare i dati sui computer connessi a quel dominio. Tutte le attività dannose (ingresso, esecuzione del payload e cifratura) vengono svolte sul computer già compromesso e questo permette agli hacker di sfuggire al rilevamento dei moderni stack di sicurezza. L’unico indicatore di compromissione è la trasmissione di documenti da e verso altri computer.

L’80% delle violazioni tramite cifratura da remoto proviene da dispositivi non gestiti che si trovano all’interno della rete[2], sebbene alcuni attacchi abbiano inizio su computer protetti a cui mancano strumenti di difesa in grado di impedire agli hacker di accedere al dispositivo.

Perché I Remote Ransomware Sono Così Prevalenti?

Uno dei principali fattori alla base della diffusione di questo approccio è la sua scalabilità: un singolo endpoint non gestito o privo di protezione adeguata può esporre l’intero ambiente di un’organizzazione al rischio di cifratura malevola eseguita da remoto, anche se su tutti gli altri dispositivi sono installate soluzioni di sicurezza endpoint next-gen.

A complicare ulteriormente la situazione è il fatto che gli hacker hanno ben poche limitazioni in termini di varianti di ransomware che possono scegliere per questi attacchi. Sono infatti numerose le famiglie di ransomware che supportano la cifratura malevola eseguita da remoto; ecco alcuni esempi: Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk e WannaCry.

Un altro motivo importante che contribuisce alla prevalenza dei remote ransomware è il fatto che nella maggior parte dei casi i prodotti di sicurezza sono inefficaci in questi scenari, poiché si concentrano sul rilevare file e processi di ransomware dannosi solo nei computer protetti. Il problema è che, nel caso degli attacchi di cifratura da remoto, i processi si eseguono sul computer compromesso, per cui le soluzioni di protezione endpoint sono completamente ignare di questa attività pericolosa.

Sophos Intercept X protegge i tuoi sistemi con la tecnologia CryptoGuard, che blocca la cifratura non autorizzata dei file. Successivamente, ripristina i dati al loro stato originale rendendo l’attacco completamente vano.

Protezione Antiransomware con Sophos CryptoGuard

Sophos Endpoint offre vari livelli di protezione per difendere le organizzazioni dal ransomware, tra cui CryptoGuard: la nostra esclusiva tecnologia antiransomware inclusa in tutte le subscription Sophos Endpoint.

A differenza degli altri prodotti di endpoint security, che si limitano a individuare file e processi dannosi, CryptoGuard analizza i file di dati alla ricerca di attività di cifratura malevola, indipendentemente da dove vengano eseguiti i processi. Questo approccio la rende estremamente efficace nel bloccare tutte le forme di ransomware, inclusa la cifratura malevola eseguita da remoto. Se rileva un tentativo di cifratura non autorizzata, CryptoGuard blocca automaticamente l'attività e ripristina i file allo stato pre-attacco.

CryptoGuard esamina attivamente i contenuti di tutti i documenti al momento della lettura e della scrittura. Si serve di analisi matematiche per stabilire i file se sono stati cifrati. Questo approccio universale e unico nel suo genere permette a Sophos Endpoint di bloccare gli attacchi ransomware che sfuggono alle altre soluzioni, incluse le violazioni da remoto e le varianti di ransomware mai viste prima.

CryptoGuard è una delle funzionalità esclusive di Sophos Endpoint ed è inclusa in tutte le subscription Sophos Intercept X Advanced, Sophos XDR e Sophos MDR. Inoltre, è attivata per impostazione predefinita, per garantire alle organizzazioni protezione immediata e completa contro gli attacchi ransomware locali o remoti, senza bisogno di alcuna ottimizzazione o configurazione aggiuntiva. **È la strategia di protezione endpoint zero-touch più efficace contro i remote ransomware.**

- **Rileva la cifratura malevola analizzando i contenuti dei file**

  A differenza di altre soluzioni, che analizzano il ransomware solo basandosi sulle proprie capacità antimalware, ovvero concentrandosi sul rilevare il codice dannoso, CryptoGuard individua i tentativi di cifratura dei file in blocco effettuati in rapida successione, grazie all'uso di potenti algoritmi matematici.

- **Blocca gli attacchi ransomware locali e remoti**

  Poiché CryptoGuard esamina i contenuti dei file, è in grado di rilevare i tentativi di cifratura dei ransomware anche quando il processo dannoso non viene eseguito sul dispositivo della vittima.

- **Ripristina automaticamente i file cifrati allo stato pre-attacco**

  CryptoGuard crea backup temporanei dei file modificati e annulla automaticamente le modifiche quando rileva attività di cifratura in blocco. Sophos adotta una strategia esclusiva e completamente innovativa. Diversamente, gli altri prodotti si basano sul Windows Volume Shadow Copy che, come tutti sanno, per gli hacker è molto facile da eludere. CryptoGuard ripristina qualsiasi file, senza alcun limite di tipologia o di dimensioni. Il risultato è un impatto minimo sulla produttività aziendale.

- **Blocca automaticamente i dispositivi remoti**

  Quando è in corso un attacco remote ransomware, CryptoGuard blocca automaticamente l'indirizzo IP del dispositivo remoto che cerca di cifrare i file sul computer della vittima.

- **Protegge il record di avvio principale (MBR)**

  CryptoGuard protegge i dispositivi anche dai ransomware che cifrano il record di avvio principale (impedendo l'avvio) e dagli attacchi di formattazione dell'hard disk.

Individuazione dei Dispositivi Non Protetti

Un singolo endpoint non protetto può esporre la tua azienda a un attacco di cifratura eseguita da remoto. Quando installi Sophos Endpoint, puoi contare su una protezione antiransomware potente e universale, che difende i tuoi sistemi dalla cifratura malevola. Ma come puoi fare per sapere se nella tua rete sono presenti dispositivi non protetti?

È proprio nel trovare risposta a questa domanda che Sophos Network Detection and Response (NDR) si rivela fondamentale. Sophos NDR monitora il traffico di rete, individuando flussi sospetti e identificando eventuali dispositivi non protetti, nonché risorse non autorizzate, presenti nell'ambiente informatico.

Per assicurarti la protezione più potente contro gli attacchi remote ransomware, installa Sophos Endpoint su tutti i computer del tuo ambiente e distribuisci Sophos NDR per sapere se all'interno della tua rete ci sono dispositivi non protetti.

Eleva Subito la Tua Protezione Contro i Remote Ransomware

La cifratura malevola eseguita da remoto è una tecnica di ransomware molto diffusa, che la maggior parte delle soluzioni di protezione endpoint non è in grado di bloccare. Se non usi Sophos Endpoint, è molto probabile che i tuoi sistemi siano a rischio.

Per scoprire di più su Sophos Endpoint e per sapere come possiamo aiutare la tua organizzazione a proteggersi meglio contro i moderni attacchi avanzati (inclusi i remote ransomware), parla con un consulente Sophos o con il tuo Partner Sophos di fiducia. Puoi anche osservare il prodotto in azione nel tuo ambiente informatico, con una prova gratuita di 30 giorni senza obbligo di acquisto.

1 Report sulla difesa digitale Microsoft. https://www.microsoft.com/it-it/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (5 ottobre 2023). Espionage fuels global cyberattacks (Lo spionaggio alimenta gli attacchi informatici). Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

2024-14-06 (WP-NP)

SOPHOS