SOPHOS

Ransomware remoto

El cifrado remoto malicioso es una técnica de ransomware popular que se utiliza en el 60 % de los ataques de ransomware perpetrados por humanos[1]. La mayoría de las soluciones de seguridad para endpoints más utilizadas tienen dificultades para protegerle de esta amenaza y, si no usa Sophos Endpoint, es muy probable que su organización esté expuesta. Lea esta guía para informarse sobre el riesgo del ransomware remoto y sobre la protección antiransomware líder del sector que ofrece Sophos para detenerlo.

¿Qué es el ransomware remoto?

El ransomware remoto, también conocido como cifrado remoto malicioso, explota un endpoint comprometido para cifrar datos en otros dispositivos de la misma red.

En los ataques perpetrados por humanos, los adversarios suelen intentar desplegar el ransomware directamente en los equipos que desean cifrar. Si este intento inicial es bloqueado (por ejemplo, por parte de tecnologías en los dispositivos objetivo), rara vez cejan en su empeño y, lejos de ello, cambian de estrategia para seguir intentándolo una y otra vez.

Cuando los atacantes consiguen comprometer un dispositivo, pueden utilizar la arquitectura de dominios de la organización para cifrar datos en los equipos administrados unidos al dominio. Toda la actividad maliciosa (entrada, ejecución de cargas y cifrado) se produce en el equipo ya comprometido, eludiendo por tanto las pilas de seguridad modernas. El único indicador de peligro es la transmisión de documentos a otros equipos y desde ellos.

El 80 % de los ataques con cifrado remoto se originan en dispositivos no administrados de la red[2], aunque algunos se inician en equipos mal protegidos que carecen de las defensas necesarias para impedir que los atacantes se infiltren en el dispositivo.

¿Por qué está tan extendido el ransomware remoto?

Un factor clave tras el uso generalizado de este enfoque es su escalabilidad: un único endpoint no administrado o mal protegido puede dejar expuesta toda la infraestructura de una organización al cifrado remoto malicioso, incluso cuando los demás dispositivos ejecutan una solución de seguridad para endpoints next-gen.

Por si esto fuera poco, los adversarios no se ven limitados por la variante de ransomware que hayan elegido para estos ataques. Hay una gran variedad de familias de ransomware muy conocidas compatibles con el cifrado remoto malicioso, como Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk y WannaCry.

Otro motivo importante del predominio del ransomware remoto es que la mayoría de los productos de seguridad para endpoints no son efectivos en esta situación, porque se centran en detectar archivos y procesos de ransomware maliciosos en el endpoint protegido. Sin embargo, con los ataques de cifrado remoto, los procesos se ejecutan en el equipo comprometido, de modo que la actividad maliciosa pasa desapercibida para la protección de endpoints.

En cambio, Sophos proporciona la solución de protección de endpoints sin intervención más sólida contra el ransomware remoto, respaldada por nuestra tecnología de protección CryptoGuard líder en el sector.

Protección hermética contra el ransomware con Sophos CryptoGuard

Sophos Endpoint contiene múltiples capas de protección que defienden a las organizaciones frente al ransomware, entre ellas, CryptoGuard, nuestra tecnología antiransomware exclusiva, incluida en todas las suscripciones a Sophos Endpoint.

A diferencia de otras soluciones de seguridad para endpoints que únicamente buscan archivos y procesos maliciosos, CryptoGuard analiza los archivos de datos para detectar indicios de cifrado malicioso independientemente de dónde se ejecuten los procesos. Esta estrategia es muy efectiva para detener cualquier tipo de ransomware, incluido el cifrado remoto malicioso. Si detecta cifrado malicioso, CryptoGuard bloquea automáticamente la actividad y revierte los archivos a su estado previo al cifrado.

CryptoGuard examina activamente el contenido de todos los documentos a medida que se leen y escriben los archivos, sirviéndose de análisis matemáticos para determinar si se han cifrado o no. Este enfoque universal es único en el sector y permite a Sophos Endpoint detener los ataques de ransomware que otras soluciones pasan por alto, como los ataques remotos y las variantes de ransomware desconocidas.

CryptoGuard es una de las funcionalidades exclusivas de Sophos Endpoint y se incluye en todas las suscripciones a Sophos Intercept X Advanced, Sophos XDR y Sophos MDR. Además, esta funcionalidad está activada por defecto para garantizar que las organizaciones estén totalmente protegidas desde el primer minuto frente a los ataques de ransomware tanto locales como remotos, sin necesidad de realizar ajustes ni modificar configuraciones. **Es la solución de protección de endpoints sin intervención más sólida contra el ransomware remoto.**

- **Detecta el cifrado malicioso al analizar el contenido de los archivos**

  A diferencia de otras soluciones que analizan el ransomware desde una perspectiva antimalware y se centran en detectar código malicioso, CryptoGuard analiza el contenido mediante algoritmos matemáticos para detectar el cifrado de archivos rápido y masivo.

- **Bloquea los ataques de ransomware tanto locales como remotos**

  Puesto que CryptoGuard se centra en el contenido de los archivos, puede detectar los intentos de cifrado del ransomware incluso cuando el proceso malicioso no se ejecuta en el dispositivo de la víctima.

- **Revierte automáticamente el cifrado malicioso**

  CryptoGuard crea copias de seguridad temporales de los archivos modificados y revierte automáticamente los cambios cuando detecta un cifrado masivo. Sophos utiliza un enfoque propio, a diferencia de otras soluciones que utilizan el Servicio de instantáneas de volumen de Microsoft, que se sabe que los adversarios burlan. No hay límites de tamaño ni de tipo de archivo para la recuperación, lo que minimiza el impacto en la productividad empresarial.

- **Bloquea automáticamente dispositivos remotos**

  En un ataque de ransomware remoto, CryptoGuard bloquea automáticamente la dirección IP del dispositivo remoto que intenta cifrar archivos en el equipo de la víctima.

- **Protege el registro de arranque maestro (MBR)**

  CryptoGuard también protege el dispositivo contra el ransomware que cifra el registro de arranque maestro (lo que impide el inicio) y los ataques que borran el disco duro.

Detecte dispositivos desprotegidos

Un solo endpoint desprotegido puede dejar a su organización expuesta a un ataque de cifrado remoto. El despliegue de Sophos Endpoint le proporciona una protección antiransomware robusta y universal frente al cifrado remoto, pero ¿cómo puede saber si tiene dispositivos desprotegidos en la red para empezar?

Aquí es donde puede ayudarle Sophos Network Detection and Response (NDR). Sophos NDR supervisa el tráfico de la red para detectar flujos sospechosos y, al hacerlo, identifica dispositivos desprotegidos y recursos no autorizados en el entorno.

Para contar con la máxima protección contra los ataques de ransomware remoto, instale Sophos Endpoint en todos los equipos del entorno y despliegue Sophos NDR para detectar dispositivos desprotegidos en su red.

Refuerce hoy su protección contra el ransomware remoto

El cifrado remoto malicioso es una técnica de ransomware popular difícil de detener para la mayoría de las soluciones de seguridad para endpoints más utilizadas. Si no utiliza Sophos Endpoint, es muy probable que su organización esté expuesta.

Para obtener más información sobre Sophos Endpoint y cómo puede ayudar a su organización a defenderse mejor de los ataques avanzados de hoy día, incluido el ransomware remoto, hable con un asesor de Sophos o con su Partner de Sophos hoy mismo. También puede probarlo en su propio entorno con una evaluación gratuita de 30 días sin ningún compromiso.

1 Informe de protección digital de Microsoft. https://www.microsoft.com/es-es/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (5 de octubre de 2023). El espionaje alimenta los ciberataques globales. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2024-14-06 (WP-NP)

SOPHOS