Analizando la anatomía de los ataques de Ransomware

El ransomware es un software malicioso que encripta datos valiosos y exige un rescate por su liberación, desde atacar a individuos y consumidores hasta paralizar organizaciones y gobiernos enteros. Con el paso de los años, los ataques de ransomware se han vuelto más sofisticados y devastadores: a medida que avanza la tecnología, también lo hacen las tácticas empleadas por los ciberdelincuentes.

El ataque a Colonial Pipeline en Estados Unidos en 2021 puso de relieve la vulnerabilidad de sistemas vitales. Provocó escasez de combustible y destacó el potencial del ransomware para alterar los servicios esenciales e incluso la seguridad nacional.

A medida que continúa evolucionando, plantea un desafío importante para gobiernos, organizaciones e individuos de todo el mundo. Para agravar aún más el problema, la ejecución de ataques de ransomware se ha vuelto cada vez más compleja mediante el uso de binarios y scripts (LoLBins)". Los delincuentes dependen en gran medida de estas herramientas para explorar, comunicarse, moverse, exfiltrar e impactar las redes de sus víctimas.

La mejor manera de detectar y bloquear un ataque de ransomware es comprender este comportamiento malicioso y contar con controles de seguridad que preparen a una organización para el éxito.

Abordar esta creciente amenaza requiere una defensa multifacética y un enfoque profundo, que incluya inteligencia sobre amenazas, protección del correo electrónico, MFA, EDR y XDR para estar un paso adelante del panorama en constante evolución.

Principales familias de ransomware en el último año

Estos son cinco ejemplos de las principales amenazas responsables de realizar actividades destructivas en los Estados Unidos.

- **LockBit:** en 2022 fue una de las variantes de ransomware más implementadas en todo el mundo. Conocido por el ataque contra el Hospital Francés CHSF. El grupo LockBit opera con un modelo de Ransomware como servicio (RaaS), aprovechando afiliados y socios que realizan ataques utilizando herramientas de malware LockBit y se benefician de la infraestructura y experiencia del grupo. Debido a este modelo RaaS y a las diversas preferencias y operaciones de los afiliados, los TTP específicos utilizados en los ataques pueden variar, lo que hace más difícil defenderse de ellos.
- **ALPHV (BlackCat):** el grupo de ransomware ALPHV, también llamado BlackCat, es un actor con actividad observada desde noviembre de 2021. Se dirigen principalmente a sectores como la atención médica, finanzas, manufactura y gobierno. Emplea algoritmos de cifrado avanzados para encriptar archivos y exige rescates por su liberación. Sus tácticas incluyen campañas de phishing, kits de explotación y explotación de servicios de escritorio remoto vulnerables para obtener acceso no autorizado y llevar a cabo sus ataques.
- **CL0P:** El grupo CL0P ha estado operando desde aproximadamente febrero de 2019. Son conocidos por sus técnicas sofisticadas, incluida una estrategia de doble extorsión. Se dirige a organizaciones de sectores como la atención sanitaria, educación, finanzas y el comercio minorista. Además de encriptar archivos, filtran datos confidenciales para aumentar la presión sobre las víctimas para que paguen un rescate. Sus métodos de distribución suelen implicar correos electrónicos de phishing y se han asociado con ataques de ransomware de alto perfil.

- **PYSA (Mespinoza):** el grupo PYSA, también conocido como Mespinoza, ha estado activo desde principios de 2020. Se dirige principalmente a sectores como la atención médica, educación, gobierno y manufactura. Utiliza técnicas de encriptado sólidas para bloquear archivos y, a menudo, filtra datos confidenciales antes del encriptado. Este enfoque de doble extorsión añade urgencia a las negociaciones de pago de rescate. El grupo suele emplear tácticas como campañas de phishing y explotación de vulnerabilidades para obtener acceso no autorizado y llevar a cabo sus ataques.
- **BianLian:** el grupo BianLian, atribuido al grupo de actores de amenazas WIZARD SPIDER, opera desde junio de 2022. Se dirige a organizaciones de sectores como la atención médica, energía, finanzas y tecnología. Emplea varias tácticas, incluidas campañas de phishing y explotación de vulnerabilidades, para obtener acceso no autorizado y cifrar archivos a cambio de un rescate. Sus ataques han resultado en pérdidas financieras sustanciales y perturbaciones dentro de las organizaciones objetivo.

Fases de ataque

Un ataque de ransomware típico consta de siete fases en las que un atacante pasa de la investigación pasiva o activa de la red interna a la obtención de acceso a sistemas clave y la escalada de privilegios para comprometer aún más el objetivo, el robo de datos e información valiosos, la destrucción de los mecanismos de recuperación de datos y el cifrado de la información. datos para que la víctima ya no pueda acceder a ellos y, finalmente, extorsionar a la víctima por esos datos.

1. Reconocimiento

Los atacantes recopilarán información sobre el sistema u organización objetivo, incluida la identificación de vulnerabilidades potenciales, la investigación de empleados, la recopilación de datos disponibles públicamente a través de herramientas de Business Intelligence, la visualización de qué información está disponible en la web oscura y más. Esta fase ayuda a estos actores del ransomware a comprender la infraestructura y las debilidades de su objetivo, lo que les permite planificar vías y métodos para sus ataques.

2. Acceso inicial

La segunda fase después de la investigación inicial es aprovechar esa información para lograr un punto de apoyo inicial en el sistema objetivo. Esto se puede hacer a través de una variedad de medios, desde explotar una vulnerabilidad, usar credenciales de acceso y de inicio de sesión robadas, o incluso ejecutar un ataque de phishing exitoso contra los empleados. El objetivo es obtener acceso a la red interna para poder establecer una presencia y una puerta trasera en un dispositivo para prepararse para la siguiente fase del ataque.

3. Escalamiento y movimiento lateral

Después de obtener acceso inicial a la red, los actores de amenazas explorarán la red y los dispositivos conectados a su punto original de compromiso para ver si hay más vulnerabilidades que puedan explotar o credenciales que puedan aprovechar para obtener acceso a sistemas y recursos adicionales. Esta fase permite a los atacantes afianzarse en la red de una organización, profundizando su presencia y ampliando su nivel de control y acceso. Es a través de este proceso que los grupos de ransomware obtienen acceso a los datos que finalmente buscan robar.

4. Recopilación y exfiltración de datos

El siguiente paso es identificar, recopilar y extraer datos valiosos en todos los sistemas y dispositivos que ha comprometido. Estos datos podrían ser en forma de información confidencial, propiedad intelectual, detalles financieros o registros personales. Lo que importa

es si el atacante cree que la organización pagaría para que le devuelvan los datos y si esos datos también podrían venderse para obtener mayores ganancias en la dark web.

Los datos recopilados luego se filtran, a menudo a través de canales encubiertos, a servidores externos bajo el control del atacante. Esto permite conservar copias de los datos para pedir un rescate y/o venderlos.

5. **Degradación de los sistemas de recuperación**

Después de extraer todo lo de valor que puedan, el objetivo de los ataques de ransomware es atacar y comprometer los mecanismos de recuperación de datos y los sistemas de seguridad presentes dentro de la red. Deshabilitarán o alterarán los sistemas de respaldo, los sistemas de detección de intrusiones, los firewalls o cualquier otra medida de seguridad que pueda obstaculizar sus actividades o alertar a los defensores.

6. **Despliegue del ransomware, ejecución y encriptación**

En esta fase, cuando los atacantes comprueban que han extraído activos o datos valiosos de la red interna, implementan el ransomware y, finalmente, inician contacto con la víctima para afirmar su control sobre los sistemas comprometidos. Habiendo adquirido copias de archivos confidenciales y posiblemente deshabilitado los mecanismos de recuperación, avanzan a la etapa de implementación, donde se pueden explotar herramientas como Microsoft Group Policy Objects (GPO), Microsoft System Center Configuration Manager (SCCM) y herramientas de administración remota como Admin Arsenal. Al utilizar estas herramientas, los atacantes ejecutan su ransomware en sistemas comprometidos, cifrando de manera efectiva archivos y datos cruciales, volviéndolos inaccesibles para la organización víctima. Posteriormente, se presenta una demanda de rescate, estipulando un pago a cambio.

7. **Recuperación y retrospectiva**

La última fase ocurre después de que se ha producido el ataque de rescate, cuando la organización víctima se concentra en los esfuerzos de recuperación y se concentra exclusivamente en minimizar el daño y prevenir futuros ataques de ransomware. Esto incluye investigar la exposición de la red interna para intentar aislar los sistemas comprometidos, eliminar malware en los dispositivos infectados, restaurar sistemas a partir de copias de seguridad y fortalecer las medidas de seguridad. La organización víctima también debe realizar un análisis exhaustivo del ataque para identificar las vulnerabilidades que fueron explotadas y mejorar su postura general de seguridad.

Conclusión

Es evidente que en el panorama actual de ciberseguridad, depender únicamente de la protección tradicional de endpoints es insuficiente para proteger eficazmente a las organizaciones de las amenazas de ransomware en todas las fases de ataque.

Es imperativo complementarla con tecnologías como EDR, XDR y el uso extensivo de Threat Intelligence. La sinergia entre estas tecnologías fortalece las defensas y la postura de seguridad de una organización, aprovechando el análisis de comportamiento en tiempo real, la detección de anomalías y la inteligencia de amenazas para identificar rápidamente y detener al actor de la amenaza.

Al integrar XDR en los controles de seguridad, las organizaciones obtienen una plataforma unificada y centralizada que combina seguridad de endpoints, monitoreo de redes e inteligencia sobre amenazas. Este enfoque integral permite a los equipos de SecOps correlacionar y analizar eventos de seguridad en múltiples puntos finales y capas de red, descubriendo patrones de ataque sofisticados que pueden pasar desapercibidos para las defensas tradicionales.

Este documento es un resumen de la investigación realizada por el Centro de Investigación Avanzada (ARC) de Trellix, que cuenta con un equipo de élite de investigadores y profesionales de la seguridad, para producir inteligencia profunda y accionable, en tiempo real, para mejorar los resultados de los clientes y de la industria en general.

Todos estos conocimientos e investigaciones se ofrecen por delante del mercado, y se brindan además asesorías a organizaciones de todo el mundo. El grupo detrás de estos esfuerzos está apoyado por expertos que impulsan las investigaciones, hablan en eventos de la industria y educan a personas influyentes en los medios, el mundo académico, analistas, creadores de políticas y el sector público global.