imperiasti®
Liderar es Cumplir

Lo que necesitas Saber del Ransomware

El ransomware es un tipo de software malicioso diseñado para bloquear el acceso a un sistema informático o a los datos que contiene hasta que se pague un rescate. Este tipo de ataque ha crecido significativamente en los últimos años, afectando tanto a individuos como a organizaciones, incluyendo empresas, hospitales, instituciones educativas y gobiernos.

Cómo cualquier ciberataque la primear fase es la preparación que se conoce como “Reconocimiento”, y el ransomware no es una excepción. Los ciberdelincuentes a menudo utilizan herramientas para escanear y examinar grandes porciones de Internet y este tipo de actividad ocurre constantemente, con el objetivo de identificar infraestructuras vulnerables

Si un ciberdelincuente escanea un rango de IP donde estamos ubicados y no encuentra vulnerabilidades, lo desestima y pasará al siguiente objetivo. Durante esta etapa, los atacantes adquieren la infraestructura de Comando y Control que pretenden usar durante el ataque, además de seleccionar el malware y herramientas necesarias.

Para minimizar los riesgos de exposición de una red o dispositivos, es crucial mantener todo el software actualizado y aplicar parches de forma continua y eficiente.

¿Cómo funciona el Ransomware?

La Infección Inicial generalmente se introduce en un sistema a través de correos electrónicos de phishing, descargas de software infectado, o vulnerabilidades en el software del sistema operativo o de las aplicaciones. Una vez que el usuario hace clic en un enlace o descarga un archivo malicioso, el ransomware se instala en su dispositivo.

Una vez instalado, el ransomware comienza a cifrar los archivos en el sistema infectado. Utiliza algoritmos de cifrado avanzados para que los archivos no puedan ser abiertos sin la clave de descifrado.

Después de cifrar los archivos, el ransomware muestra un mensaje al usuario que indica que sus archivos han sido bloqueados y exige un pago (generalmente en criptomonedas como Bitcoin) para recibir la clave de descifrado. Este mensaje puede incluir amenazas adicionales, como la eliminación de los archivos si no se paga el rescate en un tiempo determinado.

Completada la preparación, los ciberdelincuentes lanzan su ataque para obtener acceso inicial. Existen muchas tácticas para lograr esto, como comprometer la cadena de suministro o usar credenciales válidas previamente adquiridas. Una técnica común es el phishing, que sigue siendo un método popular para obtener acceso inicial. Algunos ciberdelincuentes incluso han establecido centros de llamadas y utilizan técnicas de ingeniería social para convencer a las personas de que instalen el malware inicial.

Tras obtener el acceso inicial, los ciberdelincuentes ejecutan el malware de primera etapa en el sistema de la víctima, en una fase llamada “Ejecución”. Si han identificado un servidor, dispositivo o aplicación vulnerable, utilizan el malware y las herramientas identificadas durante la fase de reconocimiento.

Es importante destacar que tanto las fases de acceso inicial como de ejecución a menudo son llevadas a cabo por actores independientes especializados en obtener acceso a una amplia variedad de víctimas. Este esquema, conocido como Acceso como Servicio (AaaS), implica que estos actores venden el acceso a las redes de las víctimas en varios foros criminales, como la “Dark Web” o de forma directa. La prima por vender acceso fresco a objetivos empresariales de alto valor puede ser de miles de dólares. Por lo tanto, varios grupos AaaS compiten para explotar y vender tantas víctimas como sea posible antes que sus competidores. Estos actores de amenazas operan de manera similar a las empresas, compitiendo por la participación de mercado y adoptando procesos automatizados para escanear y explotar dispositivos descubiertos en Internet de manera inmediata. La velocidad de explotación, junto con el tamaño e importancia de la empresa “víctima” potencial, impulsa licitaciones altas entre los actores de amenazas de ransomware.

Dependiendo del ciberdelincuente, se pueden emplear diversos métodos. La compra de acceso evita gran parte de las fases iniciales de acceso y ejecución, aunque el costo de una víctima grande con alto potencial de rescate puede ser considerable. La explotación de aplicaciones y servicios remotos externos, especialmente cuando existe una vulnerabilidad crítica, es mucho menos costosa y, para muchos actores de amenazas, es un proceso relativamente simple. Esto explica por qué esta técnica es tan ampliamente utilizada.

Establecido el acceso en una red, la siguiente etapa es donde los ciberdelincuentes deben asegurar un acceso permanente y operar de manera sigilosa dentro de la red, lo que se conoce como "persistencia". Si un ataque es detectado por los controles de seguridad, persistirán en el intento ya que les permite reiniciar su ataque en otro momento.

Con un acceso el atacante comienza el reconocimiento interno. Esto implica escalar privilegios, acceder a credenciales internas, descubrir datos confidenciales y moverse lateralmente a nuevas áreas de la red. El ciberdelincuente intenta extenderse mientras evade las defensas y permanece sin ser detectado, similar a un ladrón que busca objetos de valor en una casa sin levantar sospechas. Buscan archivos críticos como documentos de recursos humanos, finanzas, bancarios, correos electrónico o seguros, que luego cifrarán para extorsionar a la víctima y presionarla a pagar el rescate.

Los ciberdelincuentes dependen de una infraestructura de comando y control estable para manipular la red accedida. Necesitan enviar y recibir comunicaciones desde y hacia los hosts comprometidos. Sin esta capacidad, no pueden conectarse a los recursos necesarios.

Cuando los ciberdelincuentes tienen un control suficiente sobre la red, implementan su carga útil de ransomware. Esto a menudo ocurre durante horas no laborables, feriados o fines de semana para dificultar una respuesta rápida e impactar a la víctima en la mayor medida posible. Los usuarios finales no pueden iniciar sesión o usar estaciones de trabajo, y muchos servicios críticos, como correo electrónico y sistemas, se vuelven inaccesibles. El ransomware muestra una nota de rescate con instrucciones para contactar a los atacantes, el monto del rescate, el período de tiempo para pagar y cómo comprar criptomonedas. Los atacantes pueden llegar a ofrecer descifrar algunos archivos como demostración de su capacidad, lo que en los secuestros de denomina “prueba de vida”.

El monto del rescate se basa en la investigación realizada dentro y fuera de la red de la víctima, incluyendo ingresos anuales y cobertura de seguro.

El cifrado generalizado de la red es la principal táctica de extorsión en los ataques de ransomware. Los ciberdelincuentes al igual que los secuestros utilizan técnicas

psicológicas para aumentar la presión sobre los tomadores de decisiones clave, como Directores, Gerentes, etc. La amenaza de filtrar documentos en sitios dedicados a filtraciones es común, y los atacantes a menudo llegan a publicar filtraciones parciales inmediatamente después del cifrado para intimidar a la víctima.

Otras técnicas de presión incluyen temporizadores de cuenta regresiva en las notas de rescate, con amenazas de aumentar el rescate si no se cumplen los plazos.

Dependiendo del tamaño y la importancia de la Organización atacada las técnicas extorsivas que pueden llegar a utilizar son:

- Amenazas de denegación de servicio (DOS) en infraestructura operativa hasta que se realice el pago.
- Amenazas de subastar datos robados a otros grupos delictivos.
- Llamadas telefónicas a la organización o terceros para ejercer presión.
- Amenazas de contactar a mercados de valores o comerciantes para colapsar las acciones.
- Entrevistas con blogueros que revelan problemas de la empresa.
- Campañas publicitarias y trolling en redes sociales.

La mayoría de los ciberdelincuentes están dispuestos a negociar el monto del rescate, utilizando servicios de chat o proporcionando una dirección de correo electrónico asociada con un proveedor cifrado como “ProtonMail”. Las negociaciones permanecen privadas a menos que la víctima se niegue a pagar. Durante la negociación, continúan ejerciendo presión psicológica para asegurar el pago.

Riesgos del pago de un rescate

Si la empresa decide pagar; puede parecer una solución rápida para recuperar el acceso y la información, pero rara vez es así. No hay garantía de que los ciberdelincuentes eliminen los datos comprometidos o se abstengan de subastarlos o lanzar otro ataque de ransomware.

Además, los pagos de rescate incentivan a los ciberdelincuentes a continuar con sus actividades, contribuyendo al crecimiento constante de las operaciones de ransomware.

¿Qué tipo de Ransomware se conocen?

Existen varios tipos de ransomware, cada uno con características y métodos de ataque específicos. Aquí están los más comunes:

1. Crypto Ransomware

   Este tipo de ransomware cifra archivos en el sistema de la víctima, haciendo que sean inaccesibles. (CryptoLocker, WannaCry).

2. Locker Ransomware

   Bloquea la interfaz de usuario del dispositivo, impidiendo el acceso al sistema, pero sin cifrar archivos. (Police Locker, Winlocker).

3. Scareware

   Intenta asustar a la víctima con falsas alertas de virus o problemas en el sistema, incitándola a pagar para resolver problemas inexistentes. (Rogue security software).

4. Doxware (Leakware)

   Amenaza con publicar información sensible de la víctima a menos que se pague el rescate. Ransomware dirigido a empresas que manejan datos confidenciales.

5. RaaS (Ransomware as a Service)

   Una modalidad donde desarrolladores de ransomware alquilan su software a otros ciberdelincuentes, compartiendo las ganancias del rescate. (Cerber, Satan).

6. Fileless Ransomware

   Opera en la memoria del sistema y utiliza herramientas legítimas del sistema operativo para ejecutar el ataque, dejando pocos rastros. (Sorebrect).

7. Mobile Ransomware

   Apunta a dispositivos móviles, bloqueando el acceso o cifrando datos en teléfonos inteligentes y tabletas. (Svpeng, Fusob).

8. IoT Ransomware

   Dirigido a dispositivos del Internet de las Cosas (IoT), como cámaras de seguridad, dispositivos domésticos inteligentes y routers. (BrickerBot).

Cada tipo de ransomware utiliza diferentes métodos para infectar sistemas y extorsionar a las víctimas, pero todos comparten el objetivo común de obtener un pago a cambio de restaurar el acceso o evitar la divulgación de información.

¿Qué hacer si eres víctima de un ransomware?

Desconectar el dispositivo infectado para evitar la propagación del ransomware a otros dispositivos en la red.

Nunca pagar el rescate, aunque puede ser tentador, pagar el rescate no garantiza la recuperación de los archivos y financia más actividades criminales.

Buscar Ayuda Profesional consultando a especialistas en ciberseguridad para intentar recuperar los datos y asegurar que el sistema esté limpio.

Restaurar desde copias de Seguridad si están disponibles, analizando previamente que esas copias no estén cifradas, dado que muchas veces sigilosamente comienzan a cifrar las copias de seguridad y luego los archivos principales, para asegurarse los ciberdelincuentes que no se pueda restaurar una copia. Luego de certificar que las copias de Seguridad no están infectadas, restaurar los archivos desde esa copia limpia y actualizada.

Analizar la vulnerabilidad que detectaron

El ransomware es una amenaza significativa en el panorama actual de ciberseguridad, pero con medidas preventivas adecuadas y una respuesta rápida y adecuada, sus efectos pueden ser mitigados.

Prevención y Mitigación

Mantener copias de seguridad regulares y actualizadas de los datos importantes, almacenadas de manera segura y desconectada del sistema principal. Efectuar pruebas que aseguren la Integridad, la disponibilidad y versionado de los datos.

Mantener el sistema operativo y todas las aplicaciones actualizadas con los “Patchings” publicados por los fabricantes, haciéndolo de forma continua y eficiente para evitar vulnerabilidades que los atacantes puedan explotar.

Utilizar software antivirus y antimalware actualizado, así como implementar firewalls y otras medidas de seguridad en la red.

Educar y capacitar a los usuarios sobre los riesgos del phishing y cómo identificar correos electrónicos sospechosos.

La seguridad de la información no es solo una cuestión de tecnología y políticas empresariales; es una responsabilidad que comienza y termina con cada uno de nosotros. En un mundo cada vez más digitalizado, cada acción individual cuenta para proteger la integridad, confidencialidad y disponibilidad de los datos.

Héctor M. Amodeo
Socio
Gerente Comercial