RaaS: Ransomware-as-a-Service

La democratización de la Ciberdelincuencia.

Para comprender mejor el alcance del problema empecemos por definirlo: un servicio que ofrece kits de malware con instrucciones detalladas de uso, que permite desplegar ataques de ransomware a cualquiera que lo adquiera. Es decir, pone a disposición de individuos que tal vez no tengan las habilidades ni los medios técnicos necesarios, las herramientas para llevar a cabo este tipo de ataques de forma económica y en unos pocos clics.

¿Cómo se desarrollan estos ataques?

Existen personas con conocimientos avanzados de informática, redes corporativas y desarrollo de malware, que elaboran este tipo de programas maliciosos y los venden en el mercado negro, la Dark Web. A partir de ese momento, cualquier individuo u organización con malas intenciones puede adquirirlo y perpetrar un ataque de ransomware contra su objetivo.

Una vez adquirido, lo siguiente será buscar la puerta de entrada a su objetivo. Habitualmente requieren de ayuda humana de la propia víctima y el phishing (a través del correo electrónico) sigue siendo el vector de ataque más utilizado; con técnicas de ingeniería social engañan a los usuarios e infectan uno o varios equipos de la víctima. A partir de ahí, el propio malware hará el resto: el ataque se extenderá por la red, identificando y exfiltrando información confidencial, encriptando archivos y bloqueando accesos legítimos a los sistemas, dejándolos totalmente inoperativos.

En ese punto, el atacante tratará de sacar un beneficio económico utilizando la extorsión. Normalmente se ponen en contacto con la víctima, habitualmente con miembros del Comité de Dirección, y les informan que para recuperar su información y la operativa de sus sistemas deberán pagar un rescate.

No se trata del pago del rescate, sino del impacto económico asociado a la pérdida de operativa del negocio durante el tiempo que tarden en recuperarse, sumado al impacto negativo que el ataque pueda tener en la imagen de marca y en sus clientes, las multas o sanciones regulatorias incurridas...

Las empresas víctimas de estos ataques **nunca** deberían plantearse ceder al chantaje. Primero, porque estarían contribuyendo a fomentar este nuevo tipo de amenazas y podrían incurrir en un delito de blanqueo de capitales, y por otro lado porque nadie puede asegurar que los criminales vayan a cumplir su parte del trato.

Consecuencias

El impacto sobre las compañías afectadas es difícil de calcular. No se trata del pago del rescate, sino del impacto económico asociado a la pérdida de operativa del negocio durante el tiempo que tarden en recuperarse, sumado al impacto negativo que el ataque pueda tener en la imagen de marca y en sus clientes, las multas o sanciones regulatorias incurridas...

El impacto es especialmente relevante cuando el objetivo son instituciones o servicios públicos, ya que la ciudadanía en general también puede verse afectada. Hemos sufrido ataques a instituciones como el SEPE, que afectó a miles de ciudadanos que no podían cobrar sus pensiones en plena pandemia. También ayuntamientos, universidades e incluso hospitales han sido víctimas de estos ataques.

Por tanto, la proliferación de este tipo de servicios supone una verdadera amenaza tanto para el sector privado como para los servicios públicos, en ocasiones críticos para la sociedad.

¿Cómo prepararse frente a estas amenazas?

1. **Adoptar una estrategia de seguridad Zero-Trust**

Zero-Trust supone un cambio en la mentalidad de las empresas, eliminando los conceptos de "zona segura" en la red interna y "zona insegura" en el exterior.

Con la proliferación del cloud y el uso de servicios descentralizados, el perímetro se ha difuminado y las empresas deben asumir la brecha del mismo y reforzar la seguridad de las identidades, por ejemplo, con políticas de acceso condicional o el uso de **MFA**.

Especialmente se deben proteger las cuentas privilegiadas, otorgando los accesos mínimos tanto en privilegios como en duración. El rotado frecuente de este tipo de credenciales es también fundamental.

Por Javier Castro
Director Asociado
Líder Área
Ciberseguridad
stratesys

Mantener la plataforma tecnológica al día significa detectar y gestionar de forma continua sus vulnerabilidades. Esto es esencial para evitar que los atacantes puedan detectarlas y explotarlas.

2. **Entrenamiento frente a ataques de Ingeniería Social**
El personal es la primera barrera de protección de las empresas, su "firewall-humano". Es clave realizar actividades de concienciación en ciberseguridad, particularmente en **Ingeniería Social** (ataques dirigidos a las personas).

3. **Mantener actualizados los sistemas y ponerlos a prueba con servicios de RED-TEAM**
Mantener la plataforma tecnológica al día significa detectar y gestionar de forma continua sus vulnerabilidades. Esto es esencial para evitar que los atacantes puedan detectarlas y explotarlas.

Por otro lado, los ejercicios de seguridad ofensiva son necesarios para poner a prueba y entrenar tanto las herramientas de seguridad como a los equipos de detección y defensa de las empresas.

4. **Diseñar un plan de recuperación**
El nivel de preparación y trabajo previo a sufrir un ataque de ransomware determinará el tiempo de recuperación de los sistemas y por tanto el impacto en la Organización.

Es fundamental contar con una estrategia de recuperación ante desastres y herramientas de respaldo-recuperación que se ajusten a las necesidades del negocio (RTO, RPO): realizar copias de los datos importantes en diferentes soportes y almacenar algunas de ellas en servicios cloud de forma que pueda levantarse la infraestructura necesaria de rápidamente si son afectados los servicios principales.

¿Cómo podemos ayudarte?

Desde Stratesys podemos ayudarte con nuestros servicios de consultoría especializados en ciberseguridad, pregúntanos en **ciberseguridad@stratesys-ts.com**:

- Servicios de seguridad ofensiva: Red-Team
- Campañas de concienciación de empleados
- Planes estratégicos de Ciberseguridad
- Servicios IaaS y Disaster-Recovery
- Servicios de seguridad gestionados en Microsoft Azure □

Javier Castro, Director Asociado de Ciberseguridad, Stratesys.

Más información en
www.stratesys-ts.com