

GUÍA PRÁCTICA SOBRE EL RANSOMWARE

AKIRA

UN ENFOQUE RED TEAM
VS. BLUE TEAM



INTRODUCCIÓN

El ransomware Akira representa una amenaza persistente en el panorama de la ciberseguridad.

Esta guía adopta un enfoque práctico, simulando un enfrentamiento entre un Red Team (equipo ofensivo) que intenta emular las tácticas de Akira y un Blue Team (equipo defensivo) encargado de detectar y mitigar la amenaza.

El objetivo es proporcionar a los profesionales de seguridad información accionable para fortalecer sus defensas.

HISTORIA DE AKIRA RANSOMWARE

01

Akira surgió a principios de 2023, con fuertes indicios de conexión con el desaparecido grupo Conti. Inicialmente dirigido a Windows, evolucionó para atacar también sistemas Linux y ha mostrado un interés particular en cifrar máquinas virtuales.

Sus ataques se caracterizan por la doble extorsión: cifrado de datos y exfiltración para presionar a las víctimas. La aparición de variantes con diferentes extensiones de archivo (.akira, .powerranges, .akiranew) demuestra su desarrollo continuo.

CASOS REALES DESTACADOS

02

- **Tietoevry (Enero de 2024):** Un ataque a este proveedor de servicios de TI afectó a numerosos clientes, evidenciando el impacto en la cadena de suministro. El vector inicial probablemente involucró la explotación de accesos remotos.
- **Stanford University (Octubre de 2023):** La reclamación de robo de una gran cantidad de datos subraya la capacidad de Akira para comprometer instituciones educativas y la importancia de la protección de datos sensibles.
- **Sector Salud en EE. UU.:** Múltiples incidentes resaltan la vulnerabilidad del sector salud y la criticidad de proteger la información de los pacientes. La falta de MFA en accesos remotos fue un factor común.

PERSPECTIVA OFENSIVA (RED TEAM) SIMULACIÓN DE ATAQUE AKIRA

03

El Red Team simulará las fases clave de un ataque de ransomware Akira:

Reconocimiento:

- **Objetivo:** Identificar posibles puntos de entrada y vulnerabilidades.
- **Técnicas:** Uso de herramientas de escaneo de puertos (Nmap) para identificar servicios expuestos como VPN (puertos comunes: 1723, 1194, 443) y RDP (puerto 3389). Búsqueda de información pública sobre la infraestructura del objetivo y posibles credenciales filtradas.

Acceso Inicial:

- **Objetivo:** Obtener acceso a la red del objetivo.
- **Técnicas:**
 - Explotación de VPN: Intentar explotar vulnerabilidades conocidas en dispositivos VPN sin parchar (ej. CVE-2023-20269). Uso de herramientas como Metasploit o scripts personalizados.
 - Phishing: Enviar correos electrónicos dirigidos con archivos adjuntos maliciosos (simulando un dropper que podría descargar Akira) o enlaces a páginas de inicio de sesión falsas para capturar credenciales.
 - Fuerza Bruta RDP: Si RDP está expuesto, intentar ataques de fuerza bruta o diccionario utilizando herramientas como Hydra o Medusa.

Movimiento Lateral y Escalada de Privilegios:

- **Objetivo:** Moverse a través de la red y obtener derechos de administrador.
- **Técnicas:**
 - Volcado de Credenciales: Una vez dentro, utilizar herramientas como Mimikatz (en un entorno controlado) para extraer credenciales de la memoria.
 - Explotación de Vulnerabilidades Locales: Buscar vulnerabilidades sin parchar en sistemas internos para elevar privilegios.
 - Abuso de Cuentas de Servicio: Identificar y abusar de cuentas de servicio con contraseñas débiles o permisos excesivos.

Exfiltración de Datos (Simulada):

- **Objetivo:** Simular la extracción de datos sensibles.
- **Técnicas:** Utilizar herramientas como rsync o SCP a través de canales cifrados para transferir archivos a un servidor controlado por el Red Team. Simular la creación de archivos comprimidos (.zip, .rar) de datos importantes.

Despliegue del Ransomware (Simulado):

- **Objetivo:** Simular la etapa final del ataque sin causar daño real.
- **Técnicas:** Desplegar un archivo de texto con una nota de rescate simulada en los sistemas comprometidos. Opcionalmente, desplegar un ejecutable benigno renombrado para simular el comportamiento del ransomware.

PERSPECTIVA DEFENSIVA (BLUE TEAM)

DETECCIÓN Y DEFENSA CONTRA AKIRA

04

El Blue Team implementará estrategias para prevenir, detectar y responder a un ataque simulado de Akira:

Prevención:

- Implementación Robusta de MFA: Asegurar que la autenticación multifactor esté habilitada en todos los accesos remotos (VPN, RDP) y cuentas críticas.
- Gestión de Parches Rigurosa: Establecer un proceso para aplicar parches de seguridad de manera oportuna a todos los sistemas operativos, aplicaciones y dispositivos de red, especialmente para vulnerabilidades conocidas explotadas por ransomware.

- **Políticas de Contraseñas Fuertes:** Implementar políticas que requieran contraseñas complejas, únicas y que se cambien periódicamente. Educar a los usuarios sobre la importancia de no reutilizar contraseñas.
- **Segmentación de Red Efectiva:** Implementar una segmentación de red que limite el movimiento lateral de los atacantes en caso de compromiso. Utilizar firewalls internos y listas de control de acceso (ACLs).
- **Estrategia de Copias de Seguridad Sólida:** Implementar una estrategia de copias de seguridad regular, automatizada y probada, almacenando las copias fuera de línea o en un entorno aislado para protegerlas del cifrado.
- **Principio de Privilegio Mínimo:** Asignar a los usuarios solo los permisos necesarios para realizar sus tareas. Auditlar y revocar permisos innecesarios.

Detección:

- **Monitoreo de Logs de VPN:** Supervisar los logs de los servidores VPN en busca de intentos de inicio de sesión fallidos, inicios de sesión desde ubicaciones inusuales o actividad sospechosa después de una conexión exitosa.
- **Detección de Conexiones RDP Anormales:** Monitorear las conexiones RDP en busca de inicios de sesión desde direcciones IP desconocidas o fuera del horario laboral habitual. Implementar restricciones geográficas si es apropiado.
- **Detección de Volcado de Credenciales:** Implementar reglas en el SIEM (Security Information and Event Management) o en soluciones EDR (Endpoint Detection and Response) para detectar patrones de comportamiento asociados con herramientas de volcado de credenciales como Mimikatz.

- **Monitoreo del Tráfico de Red:** Analizar el tráfico de red en busca de patrones de comunicación sospechosos, como conexiones a servidores de comando y control conocidos o transferencias de grandes cantidades de datos a destinos desconocidos.
- **Detección de Comportamiento de Ransomware:** Utilizar soluciones EDR con capacidades de detección de comportamiento para identificar procesos que intentan cifrar una gran cantidad de archivos o eliminar copias de sombra de volumen. Implementar honeypots o archivos señuelo para detectar actividad de cifrado temprana.

Respuesta:

- **Plan de Respuesta a Incidentes Específico para Ransomware:** Tener un plan de respuesta a incidentes bien definido y probado para ataques de ransomware, que incluya roles y responsabilidades claras.
- **Aislamiento Rápido:** En caso de detección, aislar inmediatamente los sistemas afectados de la red para evitar la propagación del ransomware.
- **Análisis Forense:** Realizar un análisis forense para comprender el alcance del ataque, identificar el vector inicial y determinar qué datos se vieron comprometidos.
- **Comunicación:** Establecer un plan de comunicación interna y externa para mantener informadas a las partes interesadas.
- **Restauración desde Copias de Seguridad:** Restaurar los sistemas y datos afectados desde copias de seguridad limpias y verificadas. Asegurarse de que los sistemas estén completamente parcheados y seguros antes de volver a ponerlos en producción.

CONCLUSIÓN

Este ejercicio práctico desde la perspectiva del Red Team y el Blue Team destaca la importancia de una estrategia de seguridad en capas para defenderse contra el ransomware Akira.

La prevención, la detección temprana y una respuesta eficaz son cruciales para minimizar el impacto de un posible ataque.

RECURSOS PRÁCTICOS

- **Herramientas de Red Team:** Nmap, Metasploit, Hydra, Mimikatz (para entornos de prueba controlados).
- **Herramientas de Blue Team:** SIEM (ej. Splunk, ELK Stack), Soluciones EDR (ej. CrowdStrike, SentinelOne), herramientas de análisis de logs.
- **Alertas de Seguridad:** Suscribirse a las alertas de seguridad de organizaciones como CISA y CERTs.
- **Plataformas de Inteligencia de Amenazas:** Utilizar plataformas para mantenerse actualizado sobre las últimas TTPs de ransomware

**Sígueme
para más**

Información

**y recursos
como este.**