TIC

ALERTA

Ransomware AKIRA

COLCERT AL-0908-038

TLP:CLEAR

Descripción

Desde marzo de 2023, el ransomware Akira ha afectado a una amplia gama de empresas y entidades de infraestructura crítica en América del Norte, Europa y Australia. Al 1 de enero de 2024, ha impactado a más de 250 organizaciones, obteniendo aproximadamente 42 millones de dólares (USD) en ganancias. También se han monitoreado ataques en México, Argentina y algunos países de Centroamérica.

En junio de 2024, se descubrió que un grupo de amenazas utilizando el ransomware Akira estaba atacando a una aerolínea latinoamericana, demostrando su actividad creciente en América Latina. Aunque inicialmente se dirigía a empresas en Estados Unidos y Canadá, ahora también afecta significativamente a esta región. Su sitio de filtración en la red TOR tiene un aspecto retro único que recuerda a las consolas de pantalla verde de los años 80 y se navega mediante comandos específicos.

El ransomware Akira ha impactado a una amplia gama de negocios y entidades de infraestructura crítica en múltiples regiones, subrayando la necesidad urgente de fortalecer las medidas de seguridad cibernética.

Indicadores de Compromiso (IoC)

Extensiones de Archivos Cifrados:

- akira
- powerrangers

Herramientas Utilizadas:

AdFind, Advanced IP Scanner, AnyDesk, LaZagne, PCHunter64, PowerShell, Mimikatz, Ngrok, RClone, SoftPerfect, WinRAR, WinSCP

Notas de Rescate:

Archivos de texto con nombres como "README.txt" que contienen instrucciones para el pago del rescate y contacto a través de URLs .onion.

Modo de Operación Métodos de Distribución:

- Correos electrónicos de phishing con archivos adjuntos maliciosos.
- Explotación de vulnerabilidades en software sin parchear.
- Acceso a través de servicios RDP expuestos.

COLCERT

TIC

ALERTA

Ransomware AKIRA

COLCERT AL-0908-038

TLP:CLEAR

Proceso de Infección:

- Acceso Inicial: Los actores de Akira obtienen acceso inicial a través de servicios VPN sin autenticación multifactor (MFA) configurada y utilizando vulnerabilidades conocidas en Cisco (CVE-2020-3259 y CVE-2023-20269).
- Persistencia y Descubrimiento: Crean nuevas cuentas de dominio para establecer persistencia. Utilizan herramientas como Kerberoasting para extraer credenciales.
- Cifrado: Utilizan un cifrado híbrido de flujo ChaCha20 y RSA para bloquear datos. Los archivos cifrados tienen extensiones .akira o .powerrangers.
- Exfiltración de Datos: Utilizan herramientas como FileZilla, WinRAR, WinSCP y RClone para exfiltrar datos, y herramientas de escritorio remoto como AnyDesk y MobaXterm para control y comando.

Impacto en la Operación:

Pérdida de acceso a archivos críticos, interrupciones operacionales, potencial pérdida de datos y costos financieros asociados al pago del rescate.

Sectores Afectados:

Empresas y entidades de infraestructura crítica en múltiples sectores, incluyendo tecnología, salud, educación y finanzas.

Recomendaciones de Mitigación

Prevención:

- Mantener sistemas y software actualizados con las últimas actualizaciones de seguridad.
- Implementar autenticación multifactor (MFA) para servicios críticos, especialmente VPN y RDP.
- Realizar copias de seguridad regulares de datos críticos y almacenarlas fuera de línea.
- Capacitar a los empleados sobre cómo reconocer correos electrónicos de phishing y otros métodos de ingeniería social.
- Desplegar herramientas de seguridad robustas como antivirus, firewalls y sistemas de detección de intrusiones.

COLCERT

TIC

ALERTA
Ransomware AKIRA

COLCERT AL-0908-038

TLP:CLEAR

NIVEL DE RIESGO

ALTO

Respuesta a la Infección:

- ❑ Desconectar los sistemas infectados de la red para evitar la propagación del ransomware.
- ❑ No pagar el rescate, ya que no garantiza la recuperación de los datos y financia actividades delictivas.
- ❑ Restaurar los archivos cifrados desde copias de seguridad limpias.
- ❑ Contactar a las autoridades competentes y reportar el incidente.

IMPACTO PARA COLOMBIA Y LA REGIÓN

El ransomware ha tenido un impacto significativo en Colombia, afectando tanto a entidades públicas como privadas. En el sector público, se han reportado interrupciones en servicios esenciales, comprometiendo la seguridad y disponibilidad de datos críticos en organismos gubernamentales y entidades de salud. En el sector privado, diversas empresas de finanzas, tecnología y manufactura han enfrentado pérdidas económicas considerables y tiempos de inactividad operativa prolongados.

La táctica de doble extorsión, que implica tanto el cifrado de datos como la amenaza de su divulgación, ha aumentado la vulnerabilidad de las organizaciones colombianas, subrayando la necesidad urgente de fortalecer las medidas de ciberseguridad e invertir en infraestructura de protección de datos.

Aunque no hay evidencia clara de que el ransomware Akira haya afectado directamente a Colombia, la creciente amenaza de este tipo de ataques destaca la importancia de estar preparados y adoptar medidas preventivas robustas.

FUENTES:

- Cybersecurity and Infrastructure Security Agency. (n.d.). Alertas y asesorías de ciberseguridad. Recuperado de https://www.cisa.gov
- Federal Bureau of Investigation. (n.d.). Alertas de seguridad cibernética. Recuperado de https://www.fbi.gov
- Europol - European Cybercrime Centre. (n.d.). Informes de ciberamenazas. Recuperado de https://www.europol.europa.eu
- Centro Nacional de Seguridad Cibernética de los Países Bajos. (n.d.). Alertas y reportes de seguridad. Recuperado de https://www.ncsc.nl
- Microsoft Security Response Center. (n.d.). Blog de seguridad de Microsoft. Recuperado de https://www.microsoft.com/security/blog
- Kaspersky. (n.d.). Reportes de seguridad. Recuperado de https://www.kaspersky.com
- Symantec Threat Intelligence. (n.d.). Informes de inteligencia de amenazas. Recuperado de https://www.broadcom.com/products/cyber-security
- Trend Micro Security News. (n.d.). Noticias y análisis de seguridad. Recuperado de https://www.trendmicro.com/vinfo/us/security/news.
- Fortinet Threat Intelligence Insider. (n.d.). Blog de investigación de amenazas. Recuperado de https://www.fortinet.com/blog/threat-research.

COLCERT