Incidente ID:	0013
Fecha del reporte:	06/11/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Ransomware Akira y los ataques a Microsoft 365
Herramienta de detección	N/A
Activo involucrado:	VPN SonicWall y Cuentas de Microsoft 365
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la campaña activa del grupo de ransomware "Akira", que está explotando vulnerabilidades en dispositivos VPN SonicWall y comprometiendo cuentas de Microsoft 365.

Descripción:

El grupo de ransomware como servicio (RaaS) Akira continúa realizando ataques dirigidos contra organizaciones de diferentes sectores mediante la explotación de dispositivos VPN de SonicWall vulnerables.

Los actores de amenaza están aprovechando la vulnerabilidad CVE-2024-40766, descubierta en 2024 y ya corregida por el fabricante, pero que sigue siendo explotada en entornos donde no se ha aplicado el parche de seguridad correspondiente.

Además, se ha identificado que los atacantes utilizan credenciales robadas previamente a la aplicación del parche, lo que les permite interceptar contraseñas de un solo uso (OTP) y generar tokens de sesión válidos, eludiendo así la autenticación multifactor (MFA) incluso en sistemas que ya han sido actualizados.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Una vez obtenido el acceso inicial, Akira despliega su ransomware cifrando los sistemas comprometidos y exfiltrando información sensible para extorsionar a las víctimas.

Productos afectados:

Los productos afectados son los dispositivos VPN SonicWall con versiones vulnerables al CVE-2024-40766 y las Cuentas corporativas de Microsoft 365, utilizadas como vector de movimiento lateral o para robo de credenciales.

Modo de explotación y cadena de infección

Los atacantes obtienen el acceso inicial aprovechando appliances SSL-VPN (principalmente SonicWall) explotando la vulnerabilidad CVE-2024-40766 o utilizando credenciales válidas obtenidas por técnicas como credential stuffing, password-spraying o filtraciones previas; en varios incidentes los atacantes han reutilizado credenciales y seeds de OTP para generar códigos válidos y así eludir la autenticación multifactor. Una vez dentro, buscan establecer persistencia creando cuentas administrativas tipo itadm o en algunos casos instalando herramientas de acceso remoto legítimas como AnyDesk, RustDesk o túneles tipo Ngrok para mantener control a largo plazo.

Con el acceso persistente realizan un reconocimiento y movimiento lateral usando herramientas legítimas como, utilidades de red, scripts y escáneres como SoftPerfect/Advanced IP Scanner para descubrir controladores de dominio, listar recursos y mapear discos, al mismo tiempo ejecutan técnicas de evasión y preparación del impacto deshabilitando o eludiendo defensas (incluyendo técnicas BYOVD y terminación de procesos AV/EDR), volcando credenciales en memoria con herramientas tipo Mimikatz o mediante dumps de LSASS y exfiltrando datos mediante RClone, WinSCP, o archivadores como WinRAR mientras establecen canales de mando y control (C2).

Finalmente despliegan el payload de cifrado que es el binario asociado a Akira o algunas de sus variantes y luego eliminan copias de volumen para impedir la recuperación, cifran masivamente con

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

extensiones características como .akira y ejecutan la doble extorsión: cifrado de sistemas más la amenaza de publicar o vender los datos exfiltrados si no se satisface el pedido del grupo atacante.

Indicadores de Compromiso

A continuación, se presentan los hashes relacionados con Akira

Nombre	Indicador
Akira	e57340a208ac9d95a1f015a5d6d98b94
Akira	e8139b0bc60a930586cf3af6fa5ea573
Akira	a1f4931992bf05e9bff4b173c15cab15
Akira	08bd63480cd313d2e219448ac28f72cd
Akira	4aecef9ddc8d07b82a6902b27f051f34
Akira	ab9e577334aeb060ac402598098e13b9

- Archivos cifrados con extensión *. Akira
- Akira_readme.txt (nota de rescate)
- patrón de log creado por el ransomware (Log-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.txt)

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Técnicas MITRE ATT&CK Detectadas:

ID	Nombre
T1190	Explotar la aplicación de cara al público
T1133	Servicios remotos externos
T1078	Cuentas válidas
T1018	Detección de archivos y directorios
T1082	Descubrimiento de información del sistema
T1564.002	Ocultar artefactos: Usuarios ocultos
T1564.006	Ocultar artefactos: Ejecutar instancia virtual
T1021.001	Servicios remotos: Protocolo de escritorio remoto
T1003	Volcado de credenciales del sistema operativo
T1560	Datos recopilados del archivo
T1219	Software de acceso remoto
T1020	Exfiltración automatizada
T1486	Datos cifrados para minimizar el impacto

Recomendaciones de mitigación:

- Aplicar inmediatamente los parches/firmware recomendados por SonicWall (corrección de CVE-2024-40766) y por otros fabricantes; aislar appliances VPN expuestos hasta verificar integridad.
- Forzar el reset de credenciales de cuentas VPN administrativas y de usuario, rotar secrets y, si existe sospecha de seeds comprometidos, forzar re-registro MFA (OTP seeds).
- Detectar los inicios de sesión VPN desde ASN hosting, patrones de SMB/Impacket; alertar y contener en minutos (dwell time suele medirse en horas).
- Segmentar las redes de gestión y servidores críticos; limitar acceso administrativo desde redes externas.
- Asegurar copias offline/air-gapped e inmutables y probar restauración.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Aplicar políticas de bloqueo, detección de drivers sospechosos y control de instalación de drivers (BYOVD mitigations).

Fuentes:

- https://cybersecuritynews.es/el-ransomware-akira-y-los-ataques-a-microsoft-365-entre-las-principales-amenazas/
- https://www.sonicwall.com/support/notices/gen-7-and-newer-sonicwall-firewalls-sslvpn-recent-threat-activity/kA1VN0000000RDG0A2?utm_source

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570