Actores de amenazas vinculados al grupo de ransomware Akira han seguido enfocándose en dispositivos SonicWall como punto de acceso inicial.

La firma de ciberseguridad Rapid7 indicó que ha detectado un aumento en las intrusiones contra equipos SonicWall durante el último mes, en particular tras los reportes de una reactivación de la actividad del ransomware Akira desde finales de julio de 2025.

Posteriormente, SonicWall reveló que la actividad de SSL VPN dirigida a sus firewalls explotaba una vulnerabilidad de un año de antigüedad (CVE-2024-40766, con una puntuación CVSS de 9.3). El fallo permitía que las contraseñas de usuarios locales se mantuvieran durante la migración sin ser restablecidas.

*"Estamos observando un incremento de intentos de fuerza bruta contra credenciales de usuario por parte de actores maliciosos"*, advirtió la compañía. *"Para mitigar riesgos, los clientes deben habilitar el filtrado de botnets para bloquear actores conocidos y asegurarse de que las políticas de bloqueo de cuentas estén activadas."*

Además, SonicWall instó a los usuarios a revisar los grupos predeterminados de usuarios LDAP SSL VPN, señalando que constituyen un *"punto crítico de debilidad"* si están mal configurados en el contexto de un ataque de Akira.

Esta configuración incorpora automáticamente a todo usuario LDAP autenticado con éxito en un grupo local predeterminado, sin importar su pertenencia real en Active Directory. Si ese grupo predeterminado tiene acceso a servicios sensibles —como SSL VPN, interfaces administrativas o zonas de red sin restricciones— cualquier cuenta de AD comprometida, incluso sin necesidad legítima de esos servicios, obtiene de inmediato esos permisos.

De esta forma, se eluden los controles de acceso basados en grupos de AD, brindando a los atacantes un acceso directo al perímetro de la red tan pronto como consigan credenciales válidas.

En su alerta, Rapid7 añadió que también ha observado intentos de intrusión a través del

Virtual Office Portal alojado en equipos SonicWall, el cual, bajo ciertas configuraciones predeterminadas, puede quedar expuesto públicamente y permitir a los atacantes registrar MFA/TOTP en cuentas válidas, siempre que exista una filtración previa de credenciales.

*"El grupo Akira podría estar aprovechando una combinación de estos tres riesgos de seguridad para obtener acceso no autorizado y ejecutar operaciones de ransomware"*, señaló la compañía.

Como medidas de mitigación, se recomienda a las organizaciones rotar las contraseñas de todas las cuentas locales en SonicWall, eliminar cuentas sin uso o inactivas, configurar adecuadamente las políticas MFA/TOTP y restringir el acceso al Virtual Office Portal únicamente a la red interna.

El Australian Cyber Security Centre (ACSC) también advirtió que tiene conocimiento de ataques del grupo Akira contra organizaciones australianas a través de dispositivos SonicWall vulnerables.

Desde su aparición en marzo de 2023, Akira se ha mantenido como una amenaza constante en el panorama del ransomware, con un total de 967 víctimas hasta la fecha, según datos de Ransomware.Live. De acuerdo con cifras compartidas por CYFIRMA, el grupo estuvo detrás de 40 ataques en julio de 2025, posicionándose como el tercer grupo más activo, después de Qilin e INC Ransom.

En el segundo trimestre de 2025, de los 657 ataques de ransomware que afectaron a entidades industriales a nivel global, las familias Qilin, Akira y Play encabezaron la lista con 101, 79 y 75 incidentes respectivamente.

Akira mantuvo *"una actividad sustancial con un enfoque constante en los sectores de manufactura y transporte mediante campañas de phishing avanzadas y despliegues de ransomware multiplataforma"*, destacó la empresa de ciberseguridad industrial Dragos en un informe publicado el mes pasado.

En infecciones recientes, el ransomware Akira también ha empleado técnicas de *SEO poisoning* para distribuir instaladores troyanizados de herramientas populares de gestión de TI, utilizados posteriormente para desplegar el *loader* de malware Bumblebee.

Tras esa fase, los ataques utilizan Bumblebee como canal para distribuir el marco de post-explotación y emulación adversaria AdaptixC2, instalar RustDesk para acceso remoto persistente, exfiltrar datos y finalmente ejecutar el ransomware.

Según Palo Alto Networks Unit 42, la naturaleza modular y flexible de AdaptixC2 permite a los atacantes ejecutar comandos, transferir archivos y extraer información de los sistemas infectados. El hecho de ser de código abierto lo hace fácilmente adaptable a las necesidades de cada adversario.

La compañía también señaló que otras campañas con AdaptixC2 se han valido de llamadas en Microsoft Teams que simulaban ser del área de soporte técnico, engañando a usuarios desprevenidos para otorgar acceso remoto mediante Quick Assist, lo que permitía desplegar un script de PowerShell encargado de descifrar y cargar en memoria la *payload* de *shellcode*.

*"El grupo de ransomware Akira sigue un flujo de ataque estándar: obtener acceso inicial a través del componente SSL VPN, escalar privilegios a cuentas elevadas o de servicio, localizar y robar archivos sensibles de compartidos de red o servidores de archivos, eliminar o detener copias de seguridad y finalmente desplegar la encriptación de ransomware a nivel de hipervisor"*, explicó Rapid7.