ALERTA

Campaña de Ciberespionaje

[COLCERT AL 0612-032]

TLP:CLEAR

Fortigate

Campaña de ciberespionaje china utiliza diferentes herramientas mediante vulnerabilidad crítica en los sistemas FortiGate para implementar malware, infectando 20.000 sistemas en todo el mundo en una campaña de ciberespionaje dirigida a gobiernos.

”China que utilizó la vulnerabilidad CVE-2022-42475 en dispositivos FortiGate”

Técnicas utilizadas

Explotación de la vulnerabilidad CVE-2022-42475 en dispositivos FortiGate. Implementación del malware Coathanger para el ciberespionaje y la persistencia remota.

Impacto en la seguridad digital

El malware Coathanger era difícil de detectar y eliminar.

Los ataques se basaron en la explotación de día cero de la vulnerabilidad CVE-2022-42475. El Servicio de Inteligencia y Seguridad Militar holandés (MIVD) descubrió el malware en su red. La campaña es indicativa de las sofisticadas capacidades de ciberespionaje de China.

Para protegerse contra estas vulnerabilidades

Aplique parches de seguridad para la vulnerabilidad CVE-2022-42475 inmediatamente. Implemente medidas de seguridad adicionales para detectar y prevenir ataques. Esté atento a las comunicaciones de las agencias de seguridad sobre nuevas amenazas.

NIVEL DE RIESGO

MEDIO

FUENTES:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080
2. https://www.thestack.technology/20-000-fortinet-devices-breached-by-chinese-hackers-reboots-firmware-updates-no-defence/
3. https://www.crn.com/news/security/2024/fortinet-hacks-led-to-20-000-fortigate-devices-breached-report