DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092**	**Fecha: 19-04-2023** **Página 5 de 14**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña patrocinadas por el estado Ruso dirigido a la infraestructura de red global		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Investigadores de Cisco Talos, han indicado que los actores de amenazas patrocinados por el estado Ruso están apuntando sus ciberataques a enrutadores y firewalls a nivel mundial. Cisco señalo que hay actores extremadamente sofisticados que se dirigen cada vez más a dispositivos de infraestructura de red de una variedad de fabricantes. La falta de concienciación y los parches insuficientes, la dependencia de equipos al final de su vida útil y la necesidad de conectividad permanente, hacen que múltiples dispositivos de infraestructura sean vulnerables. La explotación exitosa de estas vulnerabilidades podría permitir a un actor de amenazas realizar actividades delictivas que afecten a la seguridad nacional.

2. **Detalles:**

- El Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido ha publicado un informe sobre una campaña sostenida de una agencia de inteligencia rusa dirigida a una vulnerabilidad en los enrutadores para los que Cisco había publicado un parche en el 2017. Esta campaña, denominada "**Jaguar Tooth** (Diente de jaguar)", es una muestra de una tendencia mucho más amplia de sofisticados actores de amenazas que dirigen sus ataques a la infraestructura de redes para promover objetivos de espionaje o para futuras actividades delictivas.

- Los ataques Jaguar Tooth son en realidad una secuencia de ataques, el primero busca cadenas de comunidad SNMP mal seleccionadas. Una vez que se encuentra una cadena comunitaria, el atacante explota la vulnerabilidad CVE-2017-6742, que se anunció por primera vez el **29 de junio de 2017**, después de lo cual se liberó un parche de software.

- Cisco Talos indicó que estos ataques sostenidos contra la infraestructura de red probablemente tengan como objetivo el equipo de Cisco, pero los ataques no se limitan de ninguna manera al hardware de Cisco, sino que se apuntaría a cualquier marca de infraestructura, con un componente de escaneo dirigido a casi 20 fabricantes diferentes de enrutadores y conmutadores.

- Por otro lado, CISA ha informado sobre adversarios chinos que apuntan a equipos de red de un conjunto igualmente amplio de fabricantes. Ciertamente, estas no son las únicas campañas dirigidas a equipos de red, ni los únicos actores. Es razonable concluir que cualquier operación de inteligencia nacional suficientemente capaz desarrollaría y usaría la capacidad para comprometer la infraestructura de comunicaciones de sus objetivos preferidos.

- Cisco señalo que, en las investigaciones, han observado la manipulación de tráfico, copia de tráfico, configuraciones ocultas, malware de enrutadores, reconocimiento de infraestructura y debilitamiento activo de las defensas por parte de adversarios que operan en equipos de red. Los adversarios, han demostrado un nivel muy alto de comodidad y experiencia trabajando dentro de los límites de los equipos de red comprometidos.

- Por último, Cisco dijo, que las agencias nacionales de inteligencia y los actores patrocinados por el estado Ruso en todo el mundo han atacado la infraestructura de la red como un objetivo de preferencia principal.

3. **Productos afectados:**

- Múltiples marcas de enrutadores y conmutadores de infraestructura de red.

4. **Solución:**

- Actualizar tanto el hardware como el software que ejecuta su dispositivo de red. No solo porque aplica los parches de seguridad elimina las vulnerabilidades conocidas, sino que las actualizaciones también introducen nuevas capacidades y controles de seguridad que antes no estaban disponibles. Cisco ha introducido una serie de tecnologías y protocolos que han mejorado la seguridad de sus productos.

- Las organizaciones que no actualicen su hardware y software tendrán más probabilidades de ser víctimas de vulnerabilidades de seguridad sin parches, pero también tendrán menos herramientas para combatir a los adversarios.

Fuentes de información	▪ hxxps://blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/