# 500 mil routers afectados con malware

Talos, la división de inteligencia de ciberseguridad de la compañía Cisco, reveló que **un grupo de cibercriminales logró infectar con malware a más de 500 mil routers y dispositivos de almacenamiento en la nube en 54 países.**

Según los investigadores, se trata de un sofisticado sistema de **malware modular, llamado 'VPNFilter',** con el que sería posible realizar un ataque de gran escala.

"El malware tiene una capacidad destructiva al poder **dejar inservible a un dispositivo infectado,** que puede activarse en máquinas de víctimas individuales o en masa. Además tiene el potencial de cortar el acceso a internet para cientos de miles de víctimas en todo el mundo", resalta el informe.

La investigación apunta que la campaña se estaría orquestando desde Ucrania, teniendo en cuenta que el código de este malware "se superpone con versiones del **malware BlackEnergy**, que fue responsable de múltiples ataques a gran escala dirigidos a equipos en Ucrania".

Los dispositivos que hasta el momento han resultado afectados por **VPNFilter son routers de Linksys, MikroTik, NETGEAR y TP-Link,** utilizados tanto en oficinas como en hogares.

**Sin seguridad**

El documento también detalla que este tipo de dispositivos son difíciles de proteger, pues se encuentran en el perímetro de la red, sin un sistema de protección y **sin capacidades antimalware integradas.**

"No estamos seguros de la vulnerabilidad específica utilizada en este caso, pero la mayoría de los dispositivos dirigidos, especialmente en versiones anteriores, tienen exploits públicos conocidos o contraseñas predeterminadas que hacen que el compromiso sea relativamente sencillo", dice la división de Cisco.

La compañía recomendó a los usuarios **resetear los dispositivos a los valores predeterminados de fábrica** y reiniciarlos para eliminar el malware potencialmente destructivo y no persistente de las etapas 2 y 3.

Si alguna empresa o negocio tiene alguno de estos routers, **Cisco señala que es importante que se comunique con el fabricante para asegurarse de que su dispositivo esté actualizado con las últimas versiones de parches de seguridad**.

Según Cisco, el crecimiento de **esta amenaza se ha realizado silenciosamente desde 2016**. Hasta el momento la compañía de ciberseguridad señaló que ningún otro proveedor ha sido infectado, pero que continuarán investigando para revelar más hallazgos. El gobierno de Estados Unidos dijo

el pasado miércoles que buscaría liberar los cientos de miles de enrutadores infectados.

Por otro lado, el **servicio de seguridad estatal ucraniano SBU** advirtió de un posible ciberataque sobre entes públicos y empresas privadas antes de la final de la **Liga de Campeones del fútbol** europeo que se realizará este sábado.

El SBU está especialmente preocupado por el hecho de que infraestructuras críticas parecen ser un objetivo y cree que Rusia está detrás del posible ataque.