Publicado en Ciudad de México el 26/10/2018

# [Avast reporta Campaña de criptominado en routers](http://www.notasdeprensa.es)

## Avast ha bloqueado más de 22.4 millones de veces direcciones URL maliciosas de criptominado en redes infectadas de routers Mikrotik

 Desde que Mikrotik distribuyó una actualización en abril para reparar el fallo CVE-2018-14847, los cibercriminales han mostrado su agilidad para explotar esta vulnerabilidad a través de ataques que van desde el criptominado hasta el espionaje. Entre el 19 de septiembre y el 15 de octubre de este año, Avast (LSE: AVST), el líder global en productos de seguridad digital, ha bloqueado más de 22.4 millones de veces direcciones URL maliciosas de criptominado relacionadas con redes infectadas de las puertas de acceso de Mikrotik – también conocidas como protocolo de vulnerabilidad WinBox. El bloqueo protegió a más de 362.616 usuarios de Avast distribuidos en 292,456 redes. La ofensiva de criptominado fue detectada como JS:InfectedMikroTik. Investigadores de Avast han determinado que Brasil es el país con más intentos de ataque (85,230), seguido de Polonia (43.677) e Indonesia (27.102). En México, se detectaron 3,817 intentos de ataque, cifra que ubica a México entre los 20 países más afectados. Después de un tweet de Bad Packets (@bad\_packets) sobre 250.000 routers de MikroTik comprometidos, el Laboratorio de Amenazas de Avast hizo recientemente un análisis más profundo del malware, lo que condujo a la identificación y remoción de dos servidores C and C. Una de las características de esta ofensiva que más impresiona a los investigadores es la larga duración del ataque, que sigue activo aun después de haberse hecho público a fines de julio. El malware emplea un conjunto de técnicas de inteligencia para controlar el poder de cómputo de cientos de miles de redes, asegurando que se mantenga operando en los routers infectados. Hay aproximadamente 314.000 routers Mikrotik en la base de datos de usuarios de Avast. De ellos, 4.89% ha sido actualizado con el último firmware de Mikrotik para reparar la vulnerabilidad. El hecho es que 85.48% de ellos es aún vulnerable a Winbox. De acuerdo con los expertos de Avast, los routers que tienen los datos de acceso por defecto o de fábrica o contraseñas débiles también pueden ser infectados. Crece el criptominadoEl aumento en el uso del criptominado, sumado a la habilidad de minar monedas digitales via javascript en un navegador, contribuyó al crecimiento de las prácticas maliciosas. Los cibercriminales ejecutaron el software para minar al usar recursos de compañías y consumidores, sin su conocimiento, minando en segundo plano. Cualquier dispositivo que pueda ofrecer poder de cálculo es atractivo para los cibercriminales, y uno de los blancos principales es el router. Esté instalado en una casa o en una entidad corporativa, los routers a menudo tienen fallas de seguridad porque cuentan con credenciales de acceso débiles o vulnerabilidades conocidas. La campaña referida usa el poder de cómputo de los routers para infectar dispositivos conectados a la red y capaces de correr en navegadores. Por ello, los computadores, teléfonos inteligentes y televisores inteligentes se encuentran en la mira. La infección inicia con la falla CVE-2018-14847. Considerada una vulnerabilidad crítica, le permite a los cribercriminales ingresar a los router sin la autorización del usuario o sin necesidad de interacción. El gran problema es que, una vez comprometido, el usuario no está seguro de cómo el router puede ser utilizado para husmear el tráfico o prestarse para páginas maliciosas, entre otros propósitos. Para determiner si hay alguna vulnerabilidad, el usuario puede usar las funciones de monitoreo de la red, como el Avast Wi-Fi Inspector. El Wi-Fi Inspector puede detectar contraseñas débiles o estándar en los routers Mikrotilk o incluso detectar la adulteración de un HTTP, llamado HNS-2018-001-MIKROTIK-HTTP-INJECTION, que puede indicar con certeza cuándo la red de un usuario ha sido infectada. En resumen, los sitios web deben ser actualizados siempre que sea posible. ¿Cómo saber si un router está infectado?Es posible que el router de un usuario esté infectado por la ofensiva, incluso si no es MikroTik. Por tanto, si el usuario detecta un JS: InfectedMikroTik, su PSI (Proveedor de Servicio de Internet) fue probablemente afectado también. Entonces, el usuario necesitará contactar a su PSI de inmediato para solucionar el problema del router. Otra forma es asegurarse si es posible conectar el router de la red interna al usar uno de los protocolos a los que el usuario está acostumbrado: WinBox, TELNET o SSH. Si el usuario no puede conectarse a través de cualquiera de esos puertos entonces tendrá que intentar puertos alternos que han sido cambiados de sitio por el hacker. Para TELNET y SSH, pueden haber sido movidos al TCP/10022. Para SSH y TCP/10023, pueden haber sido dirigidos al TELNET. Si el usuario no puede conectarse aún, la única forma de hacerlo es restableciendo el router a sus valores por defecto. Inmediatamente después de reiniciar, el usuario necesitará actualizar el firmware. Al reiniciar, todos los valores por defecto estarán seguros dado que las versiones más recientes del router MikroTik previenen el acceso de factores externos. Es fundamental revisar todas las cuentas del usuario, remover las que sean sospechosas y asignar una contraseña sólida para el resto de ellas. El usuario también puede actualizar el firmware del router con la última versión.

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-reporta-campana-de-criptominado-en](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Programación Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)