Publicado en CDMX el 07/10/2022

# [Detectar el parásito silencioso del cryptojacking para evitar las infecciones: SonicWall](http://www.notasdeprensa.es)

## Cuando el dispositivo de un usuario sufre un ataque de cryptojacking, el equipo se comporta como un parásito que vive de la energía del dispositivo anfitrión

 La criptominería es una de las formas legítimas de conseguir criptomonedas, pero para conseguir beneficios hace falta tener paciencia (y una gran cantidad de recursos), ya que se tarda alrededor de 10 minutos para procesar un solo bloque de la moneda. Para conseguir mucho dinero, los «mineros» deben completar el procesamiento de datos más deprisa que sus competidores, y para eso necesitan grandes cantidades de energía, computadoras con una gran potencia y varios servidores. Ha surgido un tipo de minero que, a diferencia de las personas que se dedican a minar criptomonedas utilizando sus propios servidores y suministro de energía, actúa de mala fe y utiliza servidores ajenos, sin el consentimiento de sus propietarios. A esa práctica se le llama cryptojacking. Cuando el dispositivo de un usuario sufre un ataque de cryptojacking, el equipo se comporta como un parásito que vive de la energía del dispositivo anfitrión. Como sucede con muchos parásitos, es difícil detectarlo, ya que el dispositivo infectado apenas muestra síntomas; como mucho, un pequeño retardo en la velocidad de procesamiento.  La forma en que entra el parásito, es que un atacante infecta los endpoints de un equipo con un malware de cryptojacking, tal vez mediante un correo de phishing o un anuncio pop-up que, al pulsar en ellos, introducen un script de minería en el dispositivo. También la nube es un objetivo muy buscado, debido a su elasticidad, lo que significa que, cuando se quedan sin capacidad de CPU, la instancia del virus puede seguir expandiéndose.  Según cómo consigan el acceso inicial y el tipo de endpoints al que accedan, los hackers pueden ser capaces de acceder al contenido total del endpoint y, en el peor escenario, pueden tener acceso a una red corporativa en la que infiltrarse más profundamente.  El aumento de los ataques de cryptojacking de los últimos años afectó de forma desproporcionada a las instituciones educativas de todo el mundo, y muchas fueron víctimas de esos ataques. Los recientes hallazgos sobre amenazas indican que el cryptojacking subió un 68 % desde 2018 hasta 2021, y que el mayor aumento de los ataques en una misma región se produjo en Europa, con un 60 %. Instituciones como escuelas y hospitales se convirtieron en los principales objetivos de los delincuentes, ya que esas organizaciones dependen de servidores que a su vez permiten a los hackers acceder a una red con gran número de servidores conectados.  Afortunadamente, existe un remedio. Asegurar los firewalls puede proteger las redes y sus dispositivos frente a esos parásitos del cryptojacking, para proporcionar una capa defensiva perimetral que los detenga a las puertas. Los firewalls pueden detectar ataques potenciales de malware, al analizar las variantes existentes y los ingredientes de su firma, así como al detener cualquier elemento relacionado con ellos. La segunda capa defensiva utiliza técnicas avanzadas de sandboxing y tecnología de inspección de memoria profunda en tiempo real (RTDMI) para ejecutar diagnósticos profundos, con el fin de detectar y minimizar el peligro del malware.

**Datos de contacto:**

Carlos Soto

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/detectar-el-parasito-silencioso-del](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Programación Software Ciberseguridad Criptomonedas-Blockchain



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