Publicado en Ciudad de Mexico el 26/05/2017

# [Adylkuzz, el malware de minería de criptomoneda que se propaga usando la misma vulnerabilidad que WannaCry](http://www.notasdeprensa.es)

## Avast bloquea Adylkuzz, el sigiloso malware de minería de monedas virtuales que infecta las computadoras usando la misma vulnerabilidad aprovechada por el ransomware WannaCry, el peor ataque de ransomware de la historia, captó la atención de los medios de comunicación, pero no es la única cepa de malware que se propaga a gran escala. Una de ellos es Adylkuzz, una forma de minería de monedas virtuales que ha infectado computadoras en todo el mundo, al igual que WannaCry

 Aunque este programa maligno no es totalmente nuevo, su última campaña se lanzó en grande. Lo detectamos por primera vez alrededor de la medianoche del 23 de abril, cuando detuvimos un ataque en Ucrania. Desde entonces, las estadísticas preliminares muestran que bloqueamos más de 92.000 intentos de ataque a nuestra base de usuarios. Si bien este número no es tan elevado como la cantidad de ataques de WannaCry que bloquemos, que hasta el momento llega a más de 250.000, sigue siendo una cantidad importante. Propagado como WannaCryAdylkuzz infecta las computadoras de la misma manera que WannaCry: aprovecha la vulnerabilidad de Windows en el protocolo Server Message Block (SMB) descrita en el boletín de seguridad MS17-010 a través de la vulnerabilidad llamada EternalBlue/DoublePulsar de Windows. El ataque de Adylkuzz es más insidioso que si se propagara por medio de correos electrónicos con phishing, porque no requiere la interacción del usuario para infectar un sistema. Lo nuevo es que, a diferencia de WannaCry, Adylkuzz trata de bloquear otras amenazas que buscan infectar la computadora mediante la vulnerabilidad MS17-010. La PC estará infectada con Adylkuzz, pero este programa maligno la protegerá de otras cepas de malware que tratan de aprovechar la misma vulnerabilidad. Qué curioso, ¿no? Tal como sucedió con WannaCry, los principales objetivos de Adylkuzz fueron Rusia, Ucrania y Taiwán en primer lugar, seguidos por Brasil e India, que también fueron víctimas importantes de WannaCry. Consumir en silencio la capacidad de procesamientoA los que se preguntan si Adylkuzz es un ransomware, como WannaCry, le decimos que no. Adylkuzz no secuestra datos ni equipos, como WannaCry y otros de programas de ciberchantaje. En vez de eso, explota los recursos de la computadora infectada para alimentar la operación de minería de moneda virtual del autor, de modo que solo se centra en la minería de la criptomoneda, Monero. La minería de monedas virtuales es una actividad legal. Pero escalarla lo suficiente para maximizar las ganancias requiere una gran capacidad de procesamiento. Por este motivo, algunos mineros ejecutan granjas de servidores enormes para minar Bitcoins u otras monedas virtuales como Litecoin, Ethereum o Monero. Construir y mantener la infraestructura y acceder a la electricidad necesaria para usarla requiere una gran inversión económica. Los autores de Adylkuzz quieren evitar estos costos haciendo que computadoras aleatorias en todo el mundo hagan el trabajo por ellos, sin pagar. Por lo tanto, cada instancia de infección por Adylkuzz consume capacidad de procesamiento del equipo infectado, para ejecutar el trabajo de los ciberdelincuentes. No es la primera vez que ocurre un ataque para minar monedas virtuales; en 2014, fuimos testigos del secuestro de grabadoras de video digital (DVR) efectuado mediante malware, con el objetivo de minar Litecoin. Los autores de Adylkuzz buscan obtener tanta energía como puedan, durante tanto tiempo como sea posible, de cada computadora, motivo por el cual el malware está diseñado para ejecutarse en segundo plano. La mayoría de los usuarios, aparte de notar que el sistema está un poco más lento que lo habitual, no detectará este tipo de programa maligno. Esto es una gran diferencia con WannaCry, cuyas víctimas saben, sin lugar a dudas, que su computadora está infectada. Títeres que escuchan a su amoLas máquinas infectadas por Adylkuzz forman un gran botnet de minería, controlado por su amo mediante servidores de comando y control (C and C). Sin entrar en detalles, los servidores C and C dan instrucciones a los bots a los que Monero se dirije (imagine que son como cuentas bancarias) para que las monedas minadas se transfieran a: Es más, los servidores C and C también pueden instruir a los bots para que descarguen y ejecuten las aplicaciones que quieran en las computadoras infectadas. De este modo, los operadores de los botnet tienen el control total de la computadora infectada con Adylkuzz y pueden instalar cualquier tipo de código malicioso. Curiosamente, el control se lleva a cabo ejecutando scripts en lenguaje LUA, lo que no es lo habitual para malware. ¿Qué podemos esperar?Si bien Avast detecta todas las versiones conocidas de Adylkuzz y las ha estado bloqueando desde hace algún tiempo, recomendamos a todos los usuarios de Windows que mantengan sus sistemas al día con las últimas actualizaciones disponibles. Ya sabemos que existe otra cepa de malware que trata de obtener su propia tajada aprovechándose de la vulnerabilidad que ya mencionamos, MS17-010. Se denomina “UIWIX” y también es ransomware. Continuaremos monitoreando estos ataques y actualizaremos el blog cuando tengamos más detalles.

**Datos de contacto:**

F

Marketing Q S

56152196

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

Categorías: Telecomunicaciones Programación Hardware Software Ciberseguridad Dispositivos móviles



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