ABC

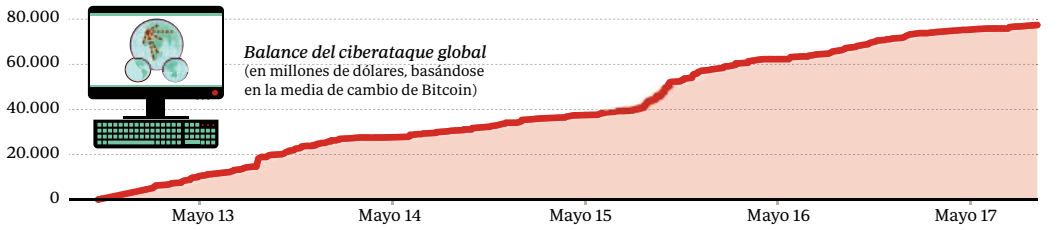
18/05/2017

Tirada: Sin auditar Categoría:
Difusión: Sin auditar Edición:
Audiencia: Sin auditar Página: 46

AREA (cm2): 774,9 OCUPACIÓN: 87,3% NOTICIAS DE ALL4SEC

Rescates pagados por virus WannaCry

El ciberataque del virus infectó a más de 200.000 equipos con sistema operativo Windows en todo el mundo, interrumpiendo operaciones en fábricas de automóviles, hospitales, comercios y escuelas. El «ransomware» encriptó los datos, exigiendo pagos de entre 300 y 600 dólares para restaurar el acceso.



Fuente: Reuters ABC

Adylkuzz, el nuevo virus que imita a WannaCry y crea dinero virtual

▸ Se cuela en el ordenador y lo usa a espaldas de su usuario para generar y robar criptomonedas

ANA I. MARTÍNEZ
MADRID

Justo cuando WannaCry está dando sus últimos coletazos, expertos en ciberseguridad han detectado un nuevo ciberataque a gran escala que afecta a cientos de miles de ordenadores en todo el mundo sin el conocimiento de los usuarios. Ha sido bautizado como Adylkuzz.

Según explicó ayer la firma de seguridad Proofpoint, con sede en California (EE.UU.) a la agencia Afp, este nuevo «malware» infectaría los ordenadores con el fin de crear y robar dinero virtual. En este caso, no se trataría de bitcoins, la más popular, sino de otra criptomoneda.

Adylkuzz es más sigiloso que el famoso WannaCry y consigue infectar los dispositivos porque utiliza la misma brecha de seguridad en Windows. Sin embargo, no actúa igual que el reciente «ramsonware» masivo.

Según explicó Robert Holmes, vicepresidente de producto en Proofpoint, «todavía no sabemos el alcance (del daño), pero cientos de miles de ordenadores pueden haber sido infectados», por lo que podría ser que este nuevo ataque resultase «mucho mayor» que WannaCry.

Equipos vulnerables

Concretamente, este «malware» se mete en equipos vulnerables para crear de forma invisible unidades de una moneda virtual llamada monero, comparable al bitcoin, «pero con capacidades mejoradas de anonimato». Como infecta a millones de ordenadores, se crea una red de dispositivos zombies, lo que se conoce como «botnet», encargada de crear la moneda digital. Los datos que utilizan estas ganancias son extraídos y enviados a direcciones cifradas.

«Varias organizaciones grandes reportaron problemas de red en la mañana del 15 de mayo que originalmente fueron atribuidos a la campaña de WannaCry (que se inició tres días antes). Sin embargo, debido a la falta de avisos de rescate, ahora creemos que estos problemas podrían estar asociados con la actividad de Adylkuzz. Cabe señalar que la campaña de Adylkuzz es significativamente anterior al ataque de WannaCry, comenzando por lo menos el 2 de mayo y posiblemente el 24 de abril. Este ataque es continuo y, aunque menos llamativo que WannaCry, es bastante grande y potencialmente bastante disruptivo», asegura la compañía en su blog, donde ha dado a conocer la nueva amenaza.

El ataque Adylkuzz es «más rentable para los cibercriminales», ya que «transforma a los usuarios infectados en participantes involuntarios que financian a sus atacantes», explica Nicolas Godier, experto en seguridad cibernética de Proffpoint.

Para el usuario, «los síntomas del ataque son (sobre todo) el rendimiento del equipo lento», asegura la compañía. «Ya ha habido amenazas de este tipo, con el "software" de creación de la moneda criptográfica, pero nunca a esta escala», aseguró Robert Holmes.

Un ataque más sigiloso

«No sabemos el alcance del daño, pero cientos de miles de ordenadores pueden haber sido infectados»

Falta de pruebas

Fuentes del Centro Nacional de Inteligencia (CNI) descartaron a este periódico que Adylkuzz suponga una amenaza mundial. De momento, es solo un estudio más de una firma de seguridad cuyas implicaciones se desconocen.

Desde All4sec, empresa española especializada en ciberseguridad, indican que «sería arriesgado afirmar que se trata de un ciberataque a nivel mundial» porque, de momento, la información es contradictoria. «Se está hablando en algunos foros de que Adylkuzz comenzó realmente el 24 de abril por lo que no se trataría de un "nuevo ataque" como tal», señaló a este periódico Alfonso Franco, CEO de la compañía española.

«Todo apunta a que es anterior a WannaCry —continúa Franco—, pero se está empezando a ver ahora y tendremos que esperar un poco para poder determinar su impacto real ya que por lo que se comenta la campaña que empezaron todavía no está acabada. Lo que sí es cierto es que muchos fabricantes de antivirus ya están incorporando las firmas de Adylkuzz en sus bases de datos».

Nace WannaCry
Telefónica, primer afectado. El virus se propaga también a Reino Unido
12 de mayo

Nuevas víctimas
La banca y el Ministerio de Interior de Rusia, trenes de Alemania y Renault
13 de mayo

Microsoft
Advirtió a los gobiernos del acopio de vulnerabilidades
14 de mayo

Lunes negro
Unas 600 empresas de Japón resultaron afectadas por el ciberataque global
15 de mayo

Autoría
EE.UU. sospecha que Corea del Norte está detrás del «ramsonware»
16 de mayo

El ciberataque masivo que paralizó al mundo durante 5 días

¿Está controlada la situación?
El Consejo Nacional de Ciberseguridad ha constatado que WannaCry ha provocado en España 1.200 «infecciones» y ha confirmado el control de su propagación, pero advierte que «no se puede garantizar de momento que no se vayan a producir nuevos incidentes de este tipo». Nuestro país ocupa la posición 18 en el ranking de países afectados.

¿Hay nuevas amenazas?
El grupo de «hackers» Shadow Brokers, que publicó un código informático que figuraba en archivos de la Agencia de Seguridad de EE.UU. (NSA) que fueron pirateados, ha amenazado con dar a conocer nuevos agujeros de seguridad a través de un modelo de pago.

¿Se podrán recuperar los datos tras el suceso?
Check Point Software Techonologies, una de las mayores empresas mundiales de seguridad informática, cree que es es «bastante improbable que los afectados recuperen sus datos aunque paguen por el rescate». «Muchas» empresas ya han pagado, pero «a día de hoy algunas no han podido volver a la normalidad».

¿Qué medidas de protección existen?
Tener un «antimalware» de nueva generación y actualizar los equipos con los parches de seguridad publicados por el fabricante. No abrir ficheros, adjuntos o enlaces de correos no confiables, ni contestar.