Nuevo ciberataque a gran escala está en curso

La Habana, 18 de may (RHC). Tras WannaCry, a principios de semana se detectó otro ataque informático masivo, llamado Adylkuzz, que se aprovecha de las mismas fallas de seguridad que WannaCry y enriquece a los hackers creando moneda virtual.

“Todavía desconocemos el alcance (del daño), pero cientos de miles de computadoras” podrían haber sido infectadas, dijo Robert Holmes, de Proofpoint, lo que indica que el ataque es “mucho mayor” que WannaCry y que empezó antes que este último, el 2 de mayo, o incluso el 24 de abril.

Además, Proofpoint afirma que detectó Adylkuzz al investigar WannaCry, el virus que infectó un gran número de ordenadores el fin de semana pasado, paralizando los servicios de sanidad británicos y algunas fábricas del constructor de automóviles francés Renault, entre otros.

Concretamente, este ‘malware’ se instala en equipos accesibles a través de la misma falla de Windows utilizada por WannaCry, un error ya detectado por la NSA (Agencia de Seguridad Nacional de Estados Unidos), que se filtró en internet en abril. La divulgación de los datos estuvo reivindicada por el grupo de hackers “Shadow brokers”.

Adylkuzz crea, de forma invisible, unidades de una moneda virtual ilocalizable llamada Monero, comparable al Bitcoin. Los datos que permiten utilizar este dinero son extraídos y enviados a direcciones

cifradas.

Aunque el Bitcoin, la moneda virtual más conocida garantice un fuerte anonimato a sus usuarios, sus transacciones pueden ser rastreadas. Monero va todavía más lejos en la opacidad, puesto que la cadena de transacciones queda completamente cifrada, lo que lo convierte en una codiciada herramienta de los piratas.

Con Adylkuzz, los ordenadores crean moneda, “no es dinero que se roba” a cualquiera, explicó Gér me Billois, experto del gabinete Wavestone.

El ataque es casi invisible para el usuario, explican también los diferentes expertos entrevistados por la AFP.

“Los síntomas del ataque son sobre todo un rendimiento más lento del aparato”, señaló Proofpoint en un blog, indicando que el ataque podría remontarse al 2 de mayo, o incluso al 24 de abril, y seguiría en vigor.

Paradójicamente, este ataque “es menos impactante que WananCry para las empresas, puesto que no comporta la interrupción de los servicios”, agregó Billois.

“No pone a las empresas de rodillas, como WannaCry”, que encripta los documentos exigiendo un rescate para descifrarlos, añadió.

WannaCry afectó a más de 300.000 ordenadores en unos 150 países, según las autoridades estadounidenses, y especialistas en seguridad informática estiman haber descubierto un vínculo potencial con Corea del Norte.

Además, los ataques podrían continuar, advierten.

Cuando el mes pasado se divulgaron las fallas de seguridad de Windows, y los medios para sacar provecho de ellas, los expertos en seguridad tuvieron “un fin de semana de pánico porque sabíamos que esto abría un enorme potencial” de ataques, indicó Billois.

“Dos grandes campañas de ataque están utilizando las sofisticadas ‘vulnerabilidades’ de la NSA y esperamos que otras les sigan”, avisó Nicolas Godier, experto en Proofpoint.

Además, según un texto publicado en un blog y presentado como proveniente de Shadow Brokers, estos hackers pretenden “divulgar informaciones todos los meses” a partir de junio. Unos datos que permitirían, según ellos, piratear el sistema operativo Windows 10 -que hasta ahora no se ha visto afectado por los ataques- o acceder a informaciones sobre los programas nucleares de varios países, incluido Corea de l Norte.

Por su parte, WannaCry sigue expandiéndose “rápidamente”, advirtió Maya Horowitz, encargada de análisis de amenazas en CheckPoint, fabricante de programas de seguridad, citada en un comunicado.

Según esta empresa, ya se habrían recabado 75.000 euros a través de WannaCry.

con informacion de cubadebate

Radio Habana Cuba