El Mundo – 17.01.2022

Ángel Jiménez de Luis

Microsoft alerta de un sofisticado ciberataque dirigido a Ucrania

Microsoft попереджає про потужну кібератаку, спрямовану на Україну

Центр розвідки загроз (MSTIC), один із підрозділів Microsoft, що займається виявленням кібератак і вразливостей мережі, попереджає про потужну атаку спрямовану на українські компанії та організації. У Microsoft зазначили, що це шкідливе програмне забезпечення вперше з'явилося в Україні 13 січня 2022 р. і воно нагадує інші програми-вимагачі. Інженери MSTIC виявили це програмне забезпечення на більш ніж дюжині комп'ютерів у декількох державних організаціях, неурядових організаціях та компаніях, які базуються в Україні.

https://www.elmundo.es/tecnologia/2022/01/17/61e549ecfc6c8389508b4575.html

Se parece a otros ataques de ransomware, pero, a diferencia de estos, no busca el pago de un rescate, sino simplemente inhabilitar los equipos.

El Centro de Inteligencia para Amenazas (MSTIC), una de las divisiones de Microsoft dedicada a la detección de ciberataques y vulnerabilidades en redes, ha alertado de un sofisticado ataque en los últimos días dirigido a empresas y organizaciones ucranianas.

"Este malware apareció por primera vez en los sistemas de víctimas en Ucrania el 13 de enero de 2022", explican desde la compañía. "Está diseñado para parecerse a otros programas de ransomware (programas que bloquean o cifran los datos de un ordenador hasta que la víctima paga un rescate) pero carece de un mecanismo de rescate, **su objetivo es destruir e inhabilitar dispositivos**", añaden.

Los ingenieros del MSTIC han detectado este software en más de una docena de equipos que abarcan múltiples organizaciones gubernamentales, ONG y empresas de tecnología, todas con sede en Ucrania. El número de infectados, en cualquier caso, podría ser mucho mayor, ya que se trata de una amenaza reciente que aún están investigando.

El ataque se suma a otros actos de sabotaje electrónico que Ucrania ha sufrido en el último mes, con el telón de fondo de una creciente tensión militar con Rusia. El pasado domingo, fuentes del Gobierno ucraniano afirmaron contar con pruebas de la implicación de Rusia en **un ciberataque contra varias web gubernamentales**. Este ataque tuvo lugar durante la madrugada del pasado viernes y no está directamente relacionado con la amenaza descubierta por Microsoft, pero ocasionó que las páginas web de varios ministerios ucranianos fueran inaccesibles durante varias horas.

El malware descubierto por Microsoft se instala en el sector de arranque de los ordenadores que logra infectar y muestra un aviso similar a los de otros programas de ransomware, exigiendo el pago de 10.000 dólares en bitcoin para recuperar los archivos del equipo.

Pero, según Microsoft, aquí es donde esta amenaza diverge sobre de los casos clásicos de ransomware. Un segundo programa, que se ejecuta justo después de la infección, sobrescribe la mayoría de archivos en el disco duro de la máquina, haciendo imposible recuperarlos. Después de sobrescribir el contenido, el software cambia también el nombre de cada archivo con una extensión de cuatro bytes aparentemente aleatoria.

Otra pista de que este ataque no trata de recaudar fondos sino de destruir la información almacenada en el dispositivo es que el aviso en pantalla **no incluye una forma de contacto con el atacante**, que sería lo habitual en un ataque convencional para guiar a la víctima en los pasos a seguir para recuperar su información.

El MSTIC no ha señalado a Rusia como fuente del ataque, pero asegura ser consciente de la situación geopolítica en la que se encuentra Ucrania. "De momento no hay muchos elementos comunes entre las características únicas del grupo detrás de estos ataques y los grupos que tradicionalmente hemos rastreado", explica Tom Burt, vicepresidente de seguridad de Microsoft.

La empresa ha notificado el ataque a las organizaciones afectadas y varias agencias de seguridad de los Estados Unidos. Nuevos filtros en algunas de las herramientas de seguridad de la empresa protegen ya también a los sistemas de este ataque. Desde Microsoft, en cualquier caso, recomiendan como medida de seguridad **redoblar la vigilancia a organizaciones gubernamentales y empresas ucranianas** y activar funciones adicionales de protección como la autenticación en dos pasos.