Malware sin antecedentes ataca a sistemas de seguridad industrial en Medio Oriente

Desde que *Stuxnet* por primera vez seleccionó y destruyó centrifugadoras de enriquecimiento de uranio en Irán durante la década pasada, el mundo de la ciberseguridad estuvo esperando el próximo paso en aquella carrera de armas digital: otra pieza de software malicioso diseñado específicamente para provocar daño o destrucción de equipamiento industrial. Aquel tipo raro de malware reapareció ahora en Medio Oriente. Y en este momento, parece tener la intención de desarmar los sistemas de seguridad industrial que protegen a la vida humana.

Andy Greenberg

Fuente: ***https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east***

Artículo publicado originalmente en la revista *Wired*, traducido especialmente para *AADECA Revista*

La empresa de seguridad *FireEye* reveló la existencia de *Triton,* también conocida como *Trisis*, una familia de malware construida para comprometer los sistemas de control industrial. Si bien no es claro en qué tipo de instalación industrial —o incluso en qué país— apareció el sofisticado malware, tiene como blanco el equipamiento vendido por la empresa *Schneider Electric*, en general en instalaciones de gas y petróleo, también, algunas veces, en instalaciones de energía nuclear o plantas de fabricación. Específicamente, el malware *Triton* está diseñado para corromper o incluso inhabilitar los productos *Triconex*, de *Schneider*, conocidos como "sistemas instrumentados de seguridad", así como "sistemas de control distribuido", fabricados por una empresa separada, y utilizado por operarios humanos para monitorear procesos industriales.

Los componentes SIS están construidos para funcionar de forma independiente de otros equipos en una instalación y monitorear condiciones peligrosas potenciales, enviando alertas o paradas para prevenir accidentes o sabotajes. Al posicionarse en el DCS, los hackers podrían usar *Triton* para crear una situación que podría causar daño físico, una explosión o pérdida. Y dado que el código de *Triton* también puede desarticular las medidas de protección de

Triconex, los resguardos que existen para apagar el equipo en tal situación no podrían responder. Esto permite tácticas de hackers con escaladas más peligrosas que alcanzan infraestructura crítica.

"Recientemente, *Mandiant* [filial de *FireEye*] respondió a un incidente en una organización de infraestructura crítica en donde un atacante desplegó malware diseñado para manipular sistemas de protección industriales", dice el reporte de *FireEye* en sus nuevas lecturas sobre malware. "Declaramos con confidencia moderada que el atacante estaba desarrollando la capacidad de causar daño físico y operaciones de parada inadvertidas".

A prueba de falla

Triton actúa como una "carga explosiva" luego de que los hackers hayan alcanzado un acceso profundo a la red de una instalación, declara Rob Lee, el fundador de la empresa de protección *Dragos Inc*. *Lee* dice que *Dragos* observó el malware operando en Medio Oriente un mes antes, y que desde entonces lo había estado analizando, antes de que *FireEye* hiciera pública su existencia. Cuando se instala *Triton* en un sistema de control industrial, el código busca el equipamiento *Triconex* de *Schneide*r, confirma que se pueda conectar a él, y luego comienza a inyectarle comandos nuevos en sus operaciones. Si tales comandos nos son aceptados por los componentes *Triconex*, pueden romper el sistema de protección. Al respecto, *Schneider Electric* dijo que "en este caso, tales comandos fueron aceptados exitosamente por los componentes *Triconex*, y la planta se apagó de forma segura".

Desde que los sistemas *Triconex* se diseñan "a prueba de falla", eso podría conducir a otros sistemas a apagarse como medida de seguridad, interrumpiendo las operaciones de la planta. "Si el sistema de seguridad se apaga, todos los otros sistemas se paralizan", dice Lee.

De hecho, eso es exactamente lo que pasó; *FireEye* descubrió a *Triton* respondiendo a un incidente en el que el SIS de una compañía había entrado en un estado seguro a prueba de fallas —una parada automática de procesos industriales— sin razón clara. Hultquist cree que la manipulación de SIS fue accidental. Un uso intencional más probable habría mantenido al SIS en funcionamiento, mientras manipulaba el DCS hacia el desastre. "Si los atacantes hubieran tenido la intención de hacer un ataque real, parece que tenían mejores opciones, porque también controlaban el DCS", declara Hultquist. "Podrían haber causado mucho más daño".

De acuerdo a Lee, la extensión de tal daño potencial —causado por un ataque de malware o físico— podría ser bastante serio. "Podría aparecer todo como aún funcionando, pero sin una red protegida", dice Lee. "Podrías tener explosiones, derrames de petróleo, destrozos en equipos de fabricación y matar gente, fugas de gas que matan gente. Depende de qué proceso industrial se esté llevando a cabo, pero tranquilamente se pueden tener docenas de muertes".

Esa orientación de los sistemas de protección hace a *Triton*, en algunos aspectos, el malware más peligroso jamás encontrado, argumenta Lee. "Por su impacto potencial, es el más escandaloso que hemos visto", dice Lee, "Incluso la insinuación de hacerlo es horrible".

En una declaración a *Wired, Schneider Electric* dice que está advertida de la situación, y está investigando. "*Schneider Electric* está advertida de un incidente dirigido que tenía por objetivo el sistema de protección de un solo cliente", dice la empresa. "Estamos trabajando muy cerca con nuestro cliente, con organizaciones independientes de ciberseguridad e ICS-CERT para investigar y mitigar los riesgos de este tipo de ataques. Si bien la evidencia sugiere que este fue un caso aislado y no se debió a la vulnerabilidad del sistema *Triconex*, o a su código de programación, seguimos investigando si existe algún otro vector para el ataque. Es importante

notar en esta instancia que el sistema *Triconex* respondió apropiadamente, deteniendo de forma segura las operaciones de la planta. No se produjo ningún daño, ni al cliente, ni a al ambiente".

Daño en el mundo real

Triton es el tercer tipo de malware focalizado en dañar o corromper equipamiento físico. El primero fue *Stuxnet,* ampliamente asumido como diseñado por NSA junto a los servicios de inteligencia israelíes. Y a fines de 2016, un tipo de malware sofisticado conocido como *Industroyer*, o *Crash Override*, tuvo como blanco los sistemas de energía de Ucrania, generando un pequeño apagón en Kiev, la ciudad capital. Se cree ampliamente que el ataque fue responsabilidad de un equipo de hackers del gobierno ruso, conocido como *Sandworm*, que llevaba adelante una ciberguerra contra Ucrania desde 2014.

Sin embargo, Hultquist considera que *Triton* escala más alto que los ataques previos. "La diferencia más grande es que la herramienta que estamos viendo fue construida para controlar los sistemas de seguridad", dijo. "Dado que son los resguardos para proteger instalaciones y a la gente, meterse con esos sistemas podría tener consecuencias graves. No estamos hablando solo de apagar las luces. Estamos hablando de potenciales accidentes físicos en la planta".

Ni *FireEye*, ni *Dragos* quisieron aventurar ideas sobre quién habría creado *Triton*, ni mencionar las motivaciones de los hackers. Pero entre los sospechosos más habituales, Irán tiene una larga historia de ejecución de ciberataques en Medio Oriente. En 2012, un malware iraní conocido como *Shamoon* destruyó decenas de miles de computadoras de Saudi Aramco, un movimiento entendido en su momento como una represalia en contra de Occidente por el sabotaje de *Stuxnet* a las ambiciones nucleares iraníes. Más tarde ese año, emergió una nueva variante de Shamoon, orientada a los sistemas de computadoras de Arabia Saudita y de otros por el Golfo Pérsico. Y más recientemente, *FireEye* siguió de cerca a algunos grupos de hackers iraníes patrocinados por el Estado que han sondeado infraestructura crítica e incluso infectado objetivos con software "dropper" aparentemente preparado para ataques destructores de datos.

Tanto Lee, como Hultquist, dicen que esta implementación de *Triton* fue como un sondeo o reconocimiento. Esto origina la posibilidad de que se podría usar otra vez en contra de objetivos en Occidente, apunta Lee. Esa reutilización del malware requeriría un rediseño significativo, ya que *Triconex* está diseñado muy a la medida de las instalaciones industriales en donde presta servicio. Pero Lee, no obstante, argumenta que la creación de *Triton* podría significar una nueva era de hackers apuntando a los sistemas de protección industriales, con todos los riesgos de destrucción e incluso de muertes que implica. "No espero que esto aparezca en Europa o Norteamérica, pero el adversario ha creado un plano para atacar sistemas de protección", declara Lee, "Eso es lo que están probando. Y de eso deberíamos preocuparnos". ❖

Reporte adicional por Brian Barrett
Esta historia fue actualizada para incluir comentarios de *Schneider Electric*. Luego se agregaron datos para esclarecer que el DCS impactado no era un producto de *Schneider Electric*, y para incluir las apreciaciones de *Schneider Electric* sobre cómo el malware interactúa con el sistema *Triconix*.