Investigación demuestra que un ataque remoto estilo Stuxnet es posible con malware de PLC basado en web

Publicación original de Segu Info

Lectura recomendada por Diego Romero
Miembro del Consejo Editorial
romero.diego.m@gmail.com

Un equipo de investigadores ha desarrollado malware diseñado para atacar controladores lógicos programables (PLC) modernos en un esfuerzo por demostrar que se pueden lanzar ataques remotos estilo Stuxnet contra dichos sistemas de control industrial (ICS).

Los investigadores son del Instituto de Tecnología de Georgia y han publicado el artículo "Compromising Industrial Processes using Web-Based Programmable Logic Controller Malware", que detalla este proyecto de seguridad de ICS. Los autores son Ryan Pickren, Tohid Shekari, Saman Zonouz, Raheem Beyah.

En el caso de los PLC tradicionales, un atacante puede apuntar a la capa lógica de control o a la capa de firmware. Los ataques de firmware pueden proporcionar un alto nivel de control del dispositivo y son difíciles de detectar, pero el malware puede ser difícil de implementar. El malware de lógica de control es más fácil de implementar, pero también de detectar. Ambos escenarios requieren que el atacante tenga acceso privilegiado a la red industrial de la organización objetivo.

En el caso de los PLC modernos, muchos incluyen un servidor web y se pueden configurar, controlar y monitorear de forma remota a través de API dedicadas y un navegador web normal que sirve como interfaz humano-máquina (HMI).

Si bien estos PLC modernos pueden proporcionar muchos beneficios a las organizaciones, los investigadores advierten que también pueden ampliar significativamente la superficie de ataque de los ICS.

El malware puede abusar de las API web legítimas del PLC para interrumpir los procesos industriales o dañar la maquinaria

Nota del editor

Artículo original escrito por Eduard Kovacs para SecurityWeek, publicado el 4 de marzo de 2024, disponible en https://www.securityweek.com/remote-stuxnet-style-attack-possible-with-web-based-plc-malware-researchers/

Versión en español disponible en Segu-Info, en https://blog.segu-info.com.ar/2024/03/investigacion-demuestra-que-ataque.html

Para demostrar los riesgos, los investigadores desarrollaron lo que llaman "malware PLC basado en web", que reside en la memoria del controlador, pero que los dispositivos equipados con navegador presentes en el entorno ICS ejecutan en el lado del cliente. El malware puede abusar de las API web legítimas del PLC para interrumpir los procesos industriales o dañar la maquinaria.

Este nuevo malware para PLC puede ser fácil de implementar y difícil de detectar. La infección inicial se puede realizar a través del acceso físico o de red a la HMI basada en web de destino, pero el malware también se puede implementar directamente a través de Internet secuestrando la HMI y utilizando vulnerabilidades de origen cruzado.

Para lograr persistencia, este nuevo tipo de malware de PLC aprovecha los trabajadores de servicios, que permiten que el código JavaScript se introduzca en la memoria caché del navegador y se ejecute independientemente de la página web que lo instaló. Además, seguirán ejecutándose hasta 24 horas después de que el archivo haya sido eliminado del servidor. Con este método, el malware puede sobrevivir a actualizaciones de firmware, nuevas HMI basadas en web e incluso reemplazos de hardware.

El malware puede sobrevivir a actualizaciones de firmware, nuevas HMI basadas en web e incluso reemplazos de hardware

Una vez que se ha implementado, las capacidades del malware dependen del poder de las API legítimas basadas en web que se utilizan, y algunas de estas son muy poderosas. Por ejemplo, se pueden aprovechar para sobrescribir directamente valores de entrada/salida, abusar de las entradas HMI, cambiar puntos de ajuste y configuraciones de seguridad, falsificar la pantalla HMI, actualizar configuraciones del administrador e incluso para la filtración de datos en tiempo real.

Los investigadores afirmaron que el malware también puede tener una conexión de comando y control (C&C), incluso si el PLC objetivo está en una red aislada.

Los investigadores afirmaron que el malware también puede tener una conexión de comando y control (C&C), incluso si el PLC objetivo está en una red aislada

Una vez que el actor de la amenaza lleva a cabo las tareas deseadas, puede cubrir sus huellas haciendo que el malware se destruya a sí mismo, sobreescriba la carga útil maliciosa con una carga útil benigna, cancele el registro de todos los trabajadores del servicio y, potencialmente, incluso realice un restablecimiento de fábrica del dispositivo.

Los investigadores demostraron su trabajo desarrollando un malware llamado "IronSpider", que diseñaron para atacar los PLC de Wago. El ataque simulado implicó la explotación de vulnerabilidades previamente desconocidas para implementar el malware cuando el operador objetivo mira un báner publicitario especialmente diseñado. El malware puede sabotear un motor industrial para causar daños mientras falsifica la pantalla HMI para que muestre valores normales y evite levantar sospechas.

Algunas de las vulnerabilidades de Wago PLC fueron descritas en otro artículo (https://www.securityweek.com/critical-vulnerabilities-allow-hackers-to-take-full-control-of-wago-plcs/) luego de una conversación con Ryan Pickren, uno de

los investigadores involucrados en este proyecto de malware para PLC.

IronSpider ha sido comparado con el notorio malware Stuxnet, que atacó el programa nuclear de Irán hace más de una década. "Stuxnet saboteó las instalaciones nucleares iraníes modificando la señal de salida analógica a unidades de frecuencia variable que controlaban las centrifugadoras de enriquecimiento de uranio. Un resultado directo de este sabotaje fue la destrucción física de más de mil centrífugas y una reducción del 30% en la capacidad operativa de las instalaciones", dijeron los investigadores en su artículo.

Stuxnet atacó los PLC mediante malware de lógica de control que implementó a través de estaciones de trabajo de ingeniería comprometidas […]. IronSpider, sin embargo, utilizó malware basado en web que implementó utilizando un sitio web malicioso sin necesidad de comprometer ningún sistema periférico

Agregaron: "Nuestro prototipo de malware, IronSpider, pudo lograr un ataque fundamentalmente similar utilizando un enfoque drásticamente diferente. Stuxnet atacó los PLC mediante malware de lógica de control que implementó a través de estaciones de trabajo de ingeniería comprometidas […]. IronSpider, sin embargo, utilizó malware basado en web que implementó utilizando un sitio web malicioso sin necesidad de comprometer ningún sistema periférico".

Si bien el ataque se demostró contra un producto Wago, los investigadores determinaron que este tipo de malware de PLC también se puede utilizar contra PLC de Siemens, Emerson, Schneider Electric, Mitsubishi Electric y Allen Bradley. Los ataques contra estos controladores implican la explotación de vulnerabilidades recién descubiertas o conocidas previamente. En algunos casos, para un ataque se requieren contraseñas FTP, protocolos inseguros o información privilegiada.

Los expertos han creado un marco independiente del proveedor que se puede utilizar para crear y analizar malware de PLC basado en web.

"Este marco explora cada etapa con estrategias ampliamente aplicables que pueden usarse contra la mayoría de los modelos de PLC modernos y presenta una descripción general de cómo el código frontal malicioso puede subvertir la integridad de los entornos ICS al comprometer metódicamente las propiedades web de los PLC. Este marco se puede utilizar como punto de referencia en estudios futuros en cualquier proveedor y modelo de PLC", explicaron los investigadores. ❖