¿Qué es EVilPLC?

EvilPLC es una forma de ataque enfocada a infectar los procesos industriales.

Normalmente, un actor malicioso buscaría irrumpir en un PLC para infectarlo y así lograr cambiar su funcionamiento normal, lo cual conlleva riesgos asociados, ya que, al lograr controlar el PLC, pueden controlar aquello que el PLC controle, como ser un mecanismo o un proceso dentro del entorno industrial, y generar disrupciones potencialmente peligrosas, por ejemplo desactivando una compuerta y causando desbordamientos, o infectando una reserva de agua con cloro como ocurrió en Israel.

La lógica del Evil PLC, sin embargo, consiste en que el actor malicioso logre acceder al PLC, pero en vez de afectar su comportamiento, modifique el código fuente de este para introducir en él algún código o archivo malicioso y utilizará ese PLC para infectar otras terminales.

Esto se consigue normalmente causando que el código del PLC sea descargado por un ingeniero:

Una vez que el código malicioso está subido al PLC, el actor malicioso suele causar un desperfecto en el dispositivo para llamar la atención del ingeniero y forzar a este a realizar un diagnóstico. El truco está en que el ingeniero debe descargar todo el código fuente del PLC en su estación de ingeniería, la cual tiene accesos y privilegios más altos y probablemente pueda acceder a muchos dispositivos en la empresa, y cuando descarga el código malicioso, infecta su propia estación. Ahora el actor malicioso tiene acceso a todo aquello que el ingeniero también.

Otra variante de este ataque es buscar específicamente una localización remota donde el atacante sepa (gracias a un sondeo previo de la empresa) que no existe un ingeniero in-situ, y en vez de eso, se subcontrata a un ingeniero que solo viene cuando hay algo que revisar. Estos ingenierons freelance suelen estar contratados por varias empresas a la vez, con lo que lograr infectar su estación de trabajo (su laptop probablemente), lograrían eventualmente tener acceso a varias empresas distintas a medida que el ingeniero se moviera por ellas.

Para prevenir o mitigar esto, tenemos que primero lograr un aislamiento de los plcs, tanto virtualmente como físicamente, de manera que podamos evitar que el actor malicioso obtenga acceso a este PLC, ya que modificar el código de este es el primer paso para esta táctica.

Luego debemos asegurarnos de que se necesite autenticación para modificar cada uno de estos dispositivos (una de las vulnerabilidades más comunes en dispositivos IoT es que no piden autenticación).

Además, el cifrado mediante el uso de claves públicas puede ayudar a encriptar el tráfico de entrada y salida, dificultando así que el actor malicioso logre descubrir cómo entrar al PLC en cuestión.

Finalmente, debido a que este ataque comprende una carga maliciosa y anormal de datos en el PLC, deberíamos monitorizar el flujo de datos entrante y saliente del dispositivo, puesto que podríamos ver en ese caso que se ha producido un flujo sospechoso de datos (obviamente, cualquier herramienta de monitoreo e incluso de prevención sería buena para esto, como ser un IDR/IPS).

Como última medida, debido a que todo esto se da subiendo el código a la máquina del ingeniero, esta también debería ser reforzada, y quizá abrir el código en una *sandbox*, para evitar que este se propague.