MITRE ATT&CK® MATRIX

TÁCTICAS DE ICS

ACCESO INICIAL

El adversario intenta entrar en tu sistema ICS.

El Acceso Inicial es cuando los adversarios encuentran maneras de entrar por primera vez en el sistema ICS. Pueden hacerlo comprometiendo dispositivos tecnológicos operativos, usando recursos de TI en la red OT o aprovechando servicios remotos externos. También podrían atacar a terceros con acceso privilegiado. En resumen, buscan puntos de entrada tanto en la red OT como en la TI. Esto podría incluir dispositivos, comunicaciones y servicios que tienen acceso y privilegios en ambos entornos.

Explotar Aplicación Expuesta al Público

Los adversarios pueden explotar software expuesto en Internet para entrar en una red industrial. Este software puede ser de diferentes tipos, como aplicaciones de usuario, implementaciones subyacentes de redes o el sistema operativo de un activo. A menudo, estos objetivos están intencionalmente expuestos para permitir la administración remota.

Los adversarios pueden dirigirse a aplicaciones expuestas públicamente para acceder directamente a un entorno de Sistemas de Control Industrial (ICS) o para moverse dentro de la red ICS. Pueden encontrar estas aplicaciones mediante herramientas en línea que escanean Internet en busca de puertos y servicios abiertos. Los números de versión del software expuesto pueden ayudar a los adversarios a identificar vulnerabilidades conocidas específicas que pueden explotar. También pueden estar interesados en los puertos de protocolo de control o de acceso remoto encontrados en Puertos Comúnmente Utilizados.

Ejemplos de Procedimientos

ID	Nombre	Descripción
G0034	Equipo Sandworm	Los actores del Equipo Sandworm aprovecharon vulnerabilidades en el software HMI de GE's Cimplicity y Advantech/Broadwin WebAccess HMI que habían sido expuestas directamente a Internet.

Activos Objetivo

ID	Activo

A0008	Servidor de Aplicaciones
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigaciones	Descripción
M0948	Aislamiento y Protección de Aplicaciones	El aislamiento de aplicaciones limitará los otros procesos y características del sistema a los que puede acceder un objetivo explotado. Ejemplos de características integradas son las políticas de restricción de software, AppLocker para Windows y SELinux o AppArmor para Linux.
M0950	Protección contra Exploits	Los Firewalls de Aplicaciones Web pueden utilizarse para limitar la exposición de las aplicaciones y prevenir que el tráfico de exploits llegue a la aplicación.
M0930	Segmentación de Redes	Separe los servidores y servicios expuestos externamente del resto de la red con una zona desmilitarizada (DMZ) o en infraestructuras de alojamiento separadas.
M0926	Gestión de Cuentas Privilegiadas	Utilice el principio de privilegio mínimo para las cuentas de servicio.
M0951	Actualización de Software	Escanea regularmente los sistemas expuestos externamente en busca de vulnerabilidades y establece procedimientos para parchar rápidamente los sistemas cuando se descubran vulnerabilidades críticas a través del escaneo y la divulgación pública.
M0916	Escaneo de Vulnerabilidades	Escanea regularmente los sistemas expuestos externamente en busca de vulnerabilidades y establece procedimientos para parchar rápidamente los sistemas cuando se descubran vulnerabilidades críticas a través del escaneo y la divulgación pública.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Log de Aplicación	Contenido del Registro de Aplicación	Detectar la explotación de software puede ser difícil dependiendo de las herramientas disponibles. Las explotaciones de software no siempre tienen éxito o pueden hacer que el proceso explotado se vuelva inestable o se bloquee. Los Firewalls de Aplicaciones Web pueden detectar entradas inapropiadas que intentan la explotación.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Utilice la inspección profunda de paquetes para buscar artefactos de tráfico de explotación comunes, como cargas útiles conocidas.

Explotación de Servicios Remotos

Los adversarios pueden aprovechar una vulnerabilidad de software para aprovechar un error de programación en un programa, servicio o dentro del propio software del sistema operativo o kernel para habilitar el abuso de servicios remotos. Un objetivo común para la explotación posterior al compromiso de servicios remotos es obtener acceso inicial y movimiento lateral en el entorno de ICS para acceder a sistemas específicos.

Los propietarios y operadores de activos de ICS han sido afectados por ransomware (o malware disruptivo que se hace pasar por ransomware) que migra de TI empresarial a entornos de ICS: WannaCry, NotPetya y BadRabbit. En cada uno de estos casos, el malware auto-propagante (gusano) infectó inicialmente las redes de TI, pero a través de la explotación (particularmente la vulnerabilidad MS17-010 que apunta a SMBv1) se propagó a las redes industriales, produciendo impactos significativos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0606	Bad Rabbit	Bad Rabbit inicialmente infectó redes de TI, pero mediante un exploit (particularmente la vulnerabilidad MS17-010 dirigida a SMBv1) se propagó a redes industriales

S0368	NotPetya	NotPetya inicialmente infectó redes de TI, pero mediante un exploit (especialmente la vulnerabilidad MS17-010 dirigida a SMBv1) se propagó a redes industriales.
S0603	Stuxnet	Stuxnet ejecuta comandos SQL maliciosos en el servidor de base de datos WinCC para propagarse a sistemas remotos. Los comandos SQL maliciosos incluyen xp_cmdshell, sp_dumpdbilog y sp_addextendedproc.
S0366	WannaCry	WannaCry inicialmente infectó redes de TI, pero mediante un exploit (especialmente la vulnerabilidad MS17-010 dirigida a SMBv1) se propagó a redes industriales.

Activos Objetivos

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Anfitrión de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Enrutadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigaciones	Descripción

M0948	Aislamiento de Aplicaciones y Entornos Controlados	Dificultar el avance de las operaciones de los adversarios a través de la explotación de vulnerabilidades no descubiertas o sin parchear mediante el uso de entornos controlados. Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto de algunos tipos de explotación. Aun así, pueden existir riesgos adicionales de exploits y debilidades en estos sistemas
M0942	Deshabilitar o Eliminar Funciones o Programas	Asegurarse de que los puertos y servicios innecesarios estén cerrados para prevenir el riesgo de descubrimiento y posible explotación.
M0950	Protección contra Explotaciones	Las herramientas de seguridad como Windows Defender Exploit Guard (WDEG) y Enhanced Mitigation Experience Toolkit (EMET) pueden ayudar a mitigar ciertos comportamientos de explotación al detectar actividades típicas de estas acciones. Otra estrategia es la verificación de la integridad del flujo de control, que permite identificar y detener posibles exploits de software. Es importante tener en cuenta que la efectividad de estas protecciones puede variar según la arquitectura y el código de la aplicación objetivo, y es posible que no funcionen en todos los casos.
M0930	Segmentación de Redes	Segmentar adecuadamente las redes y los sistemas para reducir el acceso a las comunicaciones críticas del sistema y los servicios.
M0926	Gestión de Cuentas Privilegiadas	Minimizar los permisos y el acceso de las cuentas de servicio para limitar el impacto de la explotación.
M0919	Programa de Inteligencia de Amenazas	Desarrollar una sólida capacidad de inteligencia de amenazas cibernéticas para determinar qué tipos y niveles de amenaza pueden utilizar exploits de software y vulnerabilidades 0-day contra una organización en particular.
M0951	Actualización de Software	Actualizar el software regularmente mediante la gestión de parches para los puntos finales y servidores internos de la empresa.

M0916	Exploración de Vulnerabilidades	Escanear regularmente la red interna en busca de servicios disponibles para identificar servicios nuevos y potencialmente vulnerables.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Detectar la explotación de software puede ser difícil dependiendo de las herramientas disponibles. Los exploits de software no siempre tienen éxito o pueden hacer que el proceso explotado se vuelva inestable o se bloquee, lo cual puede registrarse en el registro de la aplicación.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Utilice la inspección profunda de paquetes para buscar artefactos de tráfico de exploit común, como cargas útiles conocidas.

Servicios Remotos Externos

Los adversarios pueden usar servicios remotos externos como punto de acceso inicial a una red. Estos servicios permiten a los usuarios conectarse a recursos internos desde ubicaciones externas, como VPN o Citrix. A menudo, se usan para administrar sistemas de control desde fuera de ellos. Sin embargo, si estos servicios se comprometen, pueden ser utilizados por los adversarios para acceder y atacar la red del sistema de control. Los adversarios pueden buscar implementaciones de VPN punto a punto en redes de terceros de confianza o conexiones de empleados de soporte remoto como puntos de entrada.

Ejemplos de Procedimientos

ID	Nombre	Descripción

C0028	Ataque al Sistema Eléctrico de Ucrania 2015	Durante el Ataque al Sistema Eléctrico de Ucrania en 2015, el Equipo Sandworm utilizó Cuentas Válidas tomadas del Controlador de Dominio de Windows para acceder a la Red Privada Virtual (VPN) del sistema de control utilizada por los operadores de la red.
C0020	Violación de Maroochy Water	En la Violación de Maroochy Water, el adversario obtuvo acceso remoto a la computadora del sistema a través de la radio.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0009	Puerta de Datos
A0006	Historiador de Datos
A0012	Host de Salto
A0014	Enrutadores
A0011	Servidor de Red Privada Virtual (VPN)

Mitigaciones

ID	Mitigaciones	Descripción
M0936	Políticas de Uso de Cuentas	Configura características relacionadas con el uso de cuentas, como bloqueos de intentos de inicio de sesión, horarios de inicio de sesión específicos y requisitos de fuerza de contraseña, como ejemplos. Considera estas características en relación con los activos que pueden afectar la seguridad y la disponibilidad.
M0942	Deshabilitar o Eliminar Funciones o Programas	Considera la eliminación de servicios remotos que no se utilizan regularmente, o solo habilítalos cuando sea necesario (por ejemplo, acceso remoto de proveedores). Asegúrate de que todos los puntos de acceso remoto externo (por ejemplo, cajas de salto, concentradores VPN)
		estén configurados con la menor funcionalidad posible, especialmente la eliminación de servicios innecesarios.

M0935	Limitar el Acceso a Recursos sobre la Red	Limita el acceso a servicios remotos a través de concentradores administrados de forma centralizada, como VPN y otros sistemas de acceso remoto gestionados.
M0932	Autenticación Multifactorial	Utiliza una autenticación multifactorial sólida para las cuentas de servicios remotos para mitigar la capacidad de un adversario para aprovechar credenciales robadas. Ten en cuenta las técnicas de intercepción de autenticación multifactorial para algunas implementaciones.
M0930	Segmentación de Redes	Niega el acceso remoto directo a sistemas internos mediante el uso de proxies de red, puertas de enlace y firewalls. Considera un servidor o host de salto en la DMZ para un mayor control de acceso. Aprovecha esta DMZ o los recursos corporativos para el acceso de proveedores.
M0927	Políticas de Contraseña	Establece y hace cumplir políticas de contraseña seguras para las cuentas.
M0918	Gestión de Cuentas de Usuario	Considera la utilización de cajas de salto para el acceso remoto externo. Además, se puede utilizar la gestión dinámica de cuentas para eliminar fácilmente las cuentas cuando no se estén utilizando

Detección

ID	Fuente de datos	Componente de datos	Detecta
DS0015	Registro de Aplicaciones.	Contenido del Registro de Aplicaciones	Cuando no se requiere autenticación para acceder a un servicio remoto expuesto, monitorea las actividades posteriores, como el uso anómalo externo de la API o la aplicación expuesta
DS0028	Sesión de Inicio de Sesión	Metadatos de Sesión de Inicio de	Sesión Monitorea los registros de autenticación y analiza patrones de acceso inusuales, ventanas de

			actividad y acceso fuera del horario laboral normal, incluido el uso de Cuentas Válidas.
DS0029	Tráfico de Red	Flujo de Tráfico de Red	Monitorea el tráfico de red que se origina desde sistemas desconocidos o inesperados.

Dispositivo Accesible por Internet

Los adversarios pueden acceder a entornos industriales a través de sistemas expuestos directamente a Internet para acceso remoto, en lugar de a través de Servicios Remotos Externos. Los Dispositivos Accesibles por Internet están expuestos a Internet de manera no intencionada o intencionada sin protecciones adecuadas, lo que puede permitir a los adversarios moverse directamente a la red del sistema de control. El acceso a estos dispositivos se logra sin el uso de exploits, los cuales estarían representados dentro de la técnica de Explotación de Aplicaciones de Cara Pública.

Los adversarios pueden aprovechar funciones incorporadas para el acceso remoto que pueden no estar protegidas o utilizar protecciones mínimas heredadas que pueden ser objetivo de ataques. Estos servicios pueden ser descubiertos mediante el uso de herramientas de escaneo en línea.

En el caso del incidente en la presa Bowman, los adversarios aprovecharon el acceso a la red de control de la presa a través de un módem celular. El acceso al dispositivo estaba protegido por autenticación de contraseña, aunque la aplicación era vulnerable a ataques de fuerza bruta.

En las operaciones de engaño manufacturero de Trend Micro, se detectó que los adversarios aprovechaban el acceso directo a Internet a un entorno de ICS mediante la exposición de protocolos operativos como Siemens S7, Omron FINS y EtherNet/IP, además de acceso VNC mal configurado.

Activos objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigaciones	Descripción
M0930	Segmentación de Red	Denegar el acceso remoto directo a sistemas internos mediante el uso de proxies de red, pasarelas y firewalls. Se deben tomar medidas para inventariar periódicamente los dispositivos accesibles por Internet para determinar si difieren de lo esperado.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0028	Sesión de Inicio de Sesión	Metadatos de Sesión de Inicio de Sesión	Monitoriza la actividad de inicio de sesión en busca de accesos inesperados o inusuales a dispositivos desde Internet.
DS0029	Trafico de Red	Contenido de Trafico de Red	Monitorear accesos inusuales a dispositivos conectados a Internet o protocolos inesperados desde/hacia Internet. El contenido del tráfico de red proporcionará información valiosa y detalles sobre el contenido de los flujos de red.
		Flujo de Tráfico de Red	Monitorear protocolos inesperados desde/hacia Internet. Mientras que el contenido del tráfico de red y los metadatos de sesión de inicio de sesión pueden identificar directamente un evento de inicio de sesión, los nuevos flujos de red basados en Internet también pueden ser un

			indicador confiable de esta técnica.

Servicios remotos

Los adversarios pueden usar servicios remotos como RDP, SMB y SSH para moverse entre activos y segmentos de red. Estos servicios permiten acceso remoto, transmisión de datos y otras funciones. Los atacantes pueden aprovecharlos para acceder a dispositivos conectados a múltiples segmentos de red y ejecutar ataques a dispositivos de control. Además, los servicios remotos como RDP y VNC pueden habilitar la ejecución de interfaces gráficas en dispositivos como IHMs. También se ha observado que actores estatales chinos comprometen canales de acceso remoto autorizados para transferir datos entre redes corporativas y de ICS.

Ejemplo de Procedimiento

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania de 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm utilizó un software de asistencia técnica para mover el mouse en dispositivos de control de ICS y liberar maliciosamente interruptores eléctricos.
C0025	Ataque al Suministro Eléctrico de Ucrania de 2016 Durante el	Ataque al Suministro Eléctrico de Ucrania de 2016, el Equipo Sandworm utilizó acceso a MS-SQL en una máquina pivote, permitiendo la ejecución de código en toda la red de ICS.
S1045	INCONTROLLER	INCONTROLLER puede utilizar el protocolo CODESYS para conectarse de forma remota a PLCs Schneider y realizar funciones de mantenimiento en el dispositivo INCONTROLLER puede utilizar Telnet para cargar cargas útiles y ejecutar comandos en PLCs Omron. El malware también puede utilizar scripts CGI basados en HTTP (por ejemplo, cpu.fcgi, ecat.fcgi) para

		obtener acceso administrativo al dispositivo.
S0496.	REvil	REvil utiliza el protocolo SMB para cifrar archivos ubicados en compartidos de archivos conectados de forma remota
S0603	Stuxnet	Stuxnet ejecuta comandos SQL maliciosos en el servidor de base de datos WinCC para propagarse a sistemas remotos. Los comandos SQL maliciosos incluyen xp_cmdshell, sp_dumpdbilog y sp_addextendedproc
G0088	TEMP.Veles	TEMP.Veles utilizó cajas de salto de protocolo de escritorio remoto (RDP) para moverse al entorno de ICS.

Activo Objeto

ID	Activos
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0012	Host de Salto
A0011	Servidor de Red Privada Virtual (VPN)

Mitigaciones

ID	Mitigación	Descripción

M0801	Gestión de Acceso	Las tecnologías de gestión de acceso pueden ayudar a hacer cumplir la autenticación en servicios remotos críticos, ejemplos incluyen, pero no se limitan a, servicios de gestión de dispositivos (por ejemplo, telnet, SSH), servidores de acceso a datos (por ejemplo,

		HTTP, Historiadores) y sesiones de HMI (por ejemplo, RDP, VNC).
M0800	Aplicación de Autorización	Garantizar privilegios adecuados para sesiones de GUI en operaciones de control, como modos de solo lectura o lecturaescritura en HMI. Priorizar usuarios locales sobre sesiones remotas y permitirles recuperar el control si es necesario. Evitar que sesiones de acceso remoto como RDP o VNC dominen sesiones locales, especialmente en el control de ICS, como HMI.
M0937	Filtrado de Tráfico de Red	Filtrar los mensajes de protocolo de capa de aplicación para servicios remotos para bloquear cualquier actividad no autorizada.
M0804	Autenticación de Usuario Humano	Todos los servicios remotos deben requerir una autenticación sólida antes de proporcionar acceso al usuario
M0807	Listas de Permitidos de Red	Las listas de permitidos de red pueden implementarse a través de archivos basados en host o archivos de host del sistema para especificar qué conexiones externas (por ejemplo, dirección IP, dirección MAC, puerto, protocolo) pueden realizarse desde un dispositivo.

M0930	Segmentación de Red	Segmentar y controlar el movimiento de software entre entornos comerciales y OT a través de DMZ unidireccionales. El acceso web debe estar restringido desde el entorno OT. Las estaciones de trabajo de ingeniería, incluidos los activos cibernéticos transitorios (TCAs), deben tener una conectividad mínima con redes externas, incluido Internet y correo electrónico, limitando aún más el alcance de estos dispositivos para estar conectados a múltiples redes.
M0927	Políticas de Contraseña	Hacer cumplir requisitos de contraseña sólidos para prevenir métodos de fuerza bruta de contraseñas para el movimiento lateral.
M0813	Autenticación de Proceso de Software y Dispositivo	Todas las sesiones de comunicación a servicios remotos deben autenticarse para prevenir el acceso no autorizado.
M0918	Gestión de Cuentas de Usuario	Limitar las cuentas que pueden usar servicios remotos. Limitar los permisos para las cuentas que tienen un mayor riesgo de compromiso; por ejemplo, configurar SSH para que los usuarios solo puedan ejecutar programas específicos.

Detección

ID	Fuente de datos	Componente de datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos en servicios diseñados específicamente para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. El adversario puede llevar a cabo estas acciones utilizando Cuentas Válidas.

DS0028	Inicio de sesión	Creacion de inicio de sesion	El monitoreo implica detectar cuentas de usuario accediendo a sistemas de manera inusual o con patrones anormales. Se busca correlacionar esta actividad con el uso de servicios remotos y detectar comportamientos sospechosos o maliciosos. Los adversarios suelen necesitar comprender el entorno antes de intentar moverse lateralmente. Consulte Servicios Remotos para más detalles sobre los
			procedimientos de los adversarios.
DS0011	Módulo	Carga de Módulos	Monitorear eventos de archivos DLL, específicamente la creación de estos archivos y la carga de DLL en procesos diseñados específicamente para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC.
DS0033	Compartición de Red	Acceso a Comparticiones de Red	Monitorear interacciones con comparticiones de red, como lecturas o transferencias de archivos, utilizando servicios remotos como Server Message Block (SMB). Para obtener contexto adicional sobre procedimientos de adversarios y antecedentes, consulte Servicios Remotos y sub-técnicas aplicables.

DS0029	Tráfico de Red	Creación de Conexiones de Red	Monitorear nuevas conexiones de red en un servicio diseñado específicamente para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. Monitorear conexiones de red que involucren protocolos comunes de gestión remota, como los puertos tcp:3283 y tcp:5900, así como los puertos tcp:3389 y tcp:22 para inicio de sesiones remotos. El adversario puede utilizar Cuentas Válidas para
			habilitar inicios de sesión remotos.
		Flujo de Tráfico de Red	Monitorear datos de red para flujos de datos inusuales (por ejemplo, hora del día, direcciones de origen/destinos inusuales) que puedan estar relacionados con el abuso de Cuentas Válidas para iniciar sesión en un servicio diseñado específicamente para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC.

DS0009	Proceso	Creación de Procesos	Monitorear procesos recién ejecutados relacionados con servicios diseñados específicamente para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. El adversario puede utilizar Cuentas Válidas para iniciar sesión y puede realizar acciones adicionales que generen procesos adicionales como el usuario.

Compromiso inalámbrico

Los adversarios pueden llevar a cabo compromisos inalámbricos como un método para obtener comunicaciones y acceso no autorizado a una red inalámbrica. El acceso a una red inalámbrica puede lograrse mediante el compromiso de un dispositivo inalámbrico. Los adversarios también pueden utilizar radios y otros dispositivos de comunicación inalámbrica en la misma frecuencia que la red inalámbrica. El compromiso inalámbrico puede realizarse como un vector de acceso inicial desde una distancia remota.

Un estudiante polaco utilizó un control remoto de televisión modificado para obtener acceso y control sobre el sistema de tranvías de la ciudad de Lodz en Polonia. El dispositivo del control remoto permitió al estudiante interactuar con la red de tranvías para modificar los ajustes de la vía y anular el control del operador. El adversario pudo haber logrado esto al alinear el control remoto con la frecuencia y amplitud de las señales del protocolo de control IR. El control remoto luego habilitó el acceso inicial a la red, lo que permitió la captura y reproducción de las señales del tranvía.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0020	Brecha en el Agua de Maroochy	En la Brecha en el Agua de Maroochy, el adversario utilizó una radio de doble vía para comunicarse y establecer las frecuencias de las estaciones repetidoras del Municipio de Maroochy.

Objetivos Específicos

ID	Activo
A0013	Entrada/Salida de Campo
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0802	Autenticidad de la Comunicación	No confiar inherentemente en la autenticidad proporcionada por la capa de red/vínculo (por ejemplo, 802.11, LTE, 802.15.4), ya que el equipamiento de la capa de vínculo puede tener largos ciclos de vida y las vulnerabilidades de protocolo pueden no ser fácilmente parcheadas. Proporcionar defensa en profundidad mediante la implementación de autenticidad dentro del protocolo de capa de aplicación asociado, o a través de una VPN de capa de red. Además, asegurar que los esquemas de comunicación proporcionen una fuerte protección contra repeticiones, empleando técnicas como marcas de tiempo o valores aleatorios criptográficos.
M0808	Cifrado del Tráfico de Red	Utilizar técnicas y protocolos criptográficos fuertes para prevenir la escucha en las comunicaciones de red.
M0806	Minimizar la Propagación de Señales Inalámbricas	Las técnicas pueden incluir (i) reducir la potencia de transmisión en las señales inalámbricas, (ii) ajustar la ganancia de la antena para evitar extensiones más allá de los límites organizacionales, y (iii) emplear técnicas de blindaje de RF para bloquear la propagación excesiva de señales.

M0813	Autenticación de Procesos de Software y Dispositivos	Asegurar que las redes inalámbricas requieran la autenticación de todos los dispositivos, y que todos los dispositivos inalámbricos también autentiquen los dispositivos de infraestructura de red (es decir, autenticación mutua). Para fines de defensa en profundidad, utilizar VPN o asegurar que los protocolos de capa de aplicación también autentiquen el sistema o dispositivo. Utilizar protocolos que proporcionen una autenticación sólida (por ejemplo, IEEE 802.1X), y hacer cumplir protecciones básicas, como el filtrado de MAC, cuando no estén disponibles técnicas criptográficas más fuertes.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicaciones	Contenido del Registro de Aplicaciones	Monitorear los registros de aplicaciones en busca de dispositivos o sesiones nuevas o inesperadas en redes inalámbricas.
DS0028	Inicio de Sesión	Creación de Inicio de Sesión	Monitorear las sesiones de inicio de sesión en busca de dispositivos o sesiones nuevas o inesperadas en redes inalámbricas.
DS0029	Trafico de Red	Flujo de Tráfico de Red	Los flujos de tráfico de red nuevos o irregulares pueden indicar dispositivos o sesiones no deseadas potencialmente en redes inalámbricas. En redes WiFi, monitorear cambios como puntos de acceso

			fraudulentos o baja intensidad de señal, lo que indica que un dispositivo está más lejos del punto de acceso de lo esperado y cambios en la señal de la capa física. El contenido del tráfico de red proporcionará un contexto importante, como direcciones de hardware (por ejemplo, MAC), cuentas de usuario y tipos de mensajes enviados.

Compromiso de la cadena de suministro

El compromiso en la cadena de suministro es cuando los adversarios manipulan productos o software antes de llegar al consumidor final para comprometer sistemas y datos una vez que se introducen en el entorno objetivo. Esto puede ocurrir en cualquier etapa de la cadena de suministro y puede incluir la sustitución de software legítimo por versiones maliciosas. Los dispositivos falsificados introducidos en la cadena de suministro global representan riesgos de seguridad y cibernéticos. Por ejemplo, Yokogawa encontró transmisores de presión diferencial falsificados que eran difíciles de distinguir de los genuinos. Además, los adversarios pueden colocar software troyanizado en sitios web legítimos de proveedores, infectando las computadoras de los usuarios con malware una vez descargado e instalado.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0093	Backdoor.Oldrea	El RAT Backdoor.Oldrea se distribuye a través de instaladores troyanizados plantados en sitios de proveedores comprometidos.
G0035	Dragonfly	Dragonfly troyanizó paquetes de software legítimos de proveedores de equipos ICS disponibles para su descarga en sus sitios web.
G0088	TEMP.Veles	TEMP.Veles atacó a varios proveedores y fabricantes de sistemas de control industrial (ICS).

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Servidor Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc., para identificar posibles debilidades. Realizar verificaciones periódicas de integridad del dispositivo para validar la corrección del firmware, software, programas y configuraciones. Las verificaciones de integridad, que típicamente incluyen hashes criptográficos o firmas digitales, deben compararse con los obtenidos en estados válidos conocidos, especialmente después de eventos como reinicios de dispositivo, descargas de programas o reinicios de programas.
M0945	Firma de Código	Cuando esté disponible, utilizar confianza raíz de hardware y software para verificar la autenticidad de un sistema. Esto puede lograrse a través de medios criptográficos, como firmas digitales o hashes, de software y firmware críticos en toda la cadena de suministro.

M0817	Gestión de la Cadena de Suministro	Un programa de gestión de la cadena de suministro debe incluir métodos para evaluar la confiabilidad y madurez técnica de un proveedor, junto con métodos técnicos (por ejemplo, firma de código, lista de materiales) necesarios para validar la integridad de los dispositivos y componentes recién adquiridos. Desarrollar un lenguaje de adquisición que enfatice las expectativas para los proveedores con respecto a los
		artefactos, registros de auditoría y capacidades técnicas necesarias para validar la integridad de la cadena de suministro de dispositivos.
M0951	Actualizar Software	Implementar un proceso de gestión de parches para verificar dependencias no utilizadas, dependencias no mantenidas y/o previamente vulnerables, características, componentes, archivos y documentación innecesarios.
M0916	Escaneo de Vulnerabilidades	Implementar monitoreo continuo de fuentes de vulnerabilidad. Además, utilizar herramientas automáticas y manuales de revisión de código.

EJECUCIÓN

El adversario intenta ejecutar código o manipular funciones del sistema, parámetros y datos de manera no autorizada.

La ejecución consiste en técnicas que resultan en la ejecución de código controlado por el adversario en un sistema local o remoto, dispositivo u otro activo. Esta ejecución también puede depender de usuarios finales sin conocimiento o de la manipulación de los modos de operación del dispositivo para ejecutar. Los adversarios pueden infectar objetivos remotos con ejecutables programados o archivos de proyecto maliciosos que operan de acuerdo con un comportamiento especificado y pueden alterar el comportamiento esperado del dispositivo de manera sutil. Los comandos para la ejecución también pueden ser emitidos desde interfaces de línea de comandos, APIs, GUIs u otras interfaces disponibles. Las técnicas que ejecutan código malicioso también pueden combinarse con técnicas de otras tácticas, particularmente para ayudar en el Descubrimiento y Colección de la red, impactar operaciones e inhibir funciones de respuesta.

Cambiar el Modo de Operación

Los adversarios pueden cambiar el modo de operación de un controlador con el objetivo de obtener acceso a funciones de ingeniería adicionales, como la Descarga de Programa. Los controladores programables, comúnmente utilizados en sistemas de automatización industrial, ofrecen varios modos de operación que determinan cómo se

maneja el programa del usuario y el acceso a la interfaz de programación del controlador (API).

Modo Programa: Este modo debe activarse antes de realizar cambios en el programa del dispositivo. Permite la carga y descarga de programas entre el controlador y una estación de trabajo de ingeniería. Por lo general, la lógica del PLC se detiene y todas las salidas pueden ser forzadas a apagarse para evitar interferencias durante la carga o descarga del programa.

Modo Ejecución (Run): En este modo, el programa del dispositivo se ejecuta normalmente. Las entradas y salidas se monitorean y utilizan de acuerdo con la lógica del programa. Sin embargo, las funciones de carga y descarga de programas están deshabilitadas para evitar cambios no autorizados en el programa en ejecución.

Modo Remoto: Permite realizar cambios en el modo de operación del PLC de forma remota, lo que puede ser útil en situaciones donde se requiere intervención a distancia.

Modo Parada (Stop): Detiene la ejecución del programa y fuerza todas las salidas a apagarse. Este modo se utiliza para detener temporalmente el funcionamiento del sistema.

Modo Reinicio (Reset): Restablece las condiciones del PLC a su estado original. Un reinicio cálido puede conservar parte de la memoria, mientras que un reinicio en frío restablecerá todas las configuraciones, incluidos los registros de entrada/salida y los datos del programa.

Modo de prueba / Monitorización: Similar al modo de ejecución, pero permite realizar operaciones de monitorización, forzar salidas, realizar reinicios y realizar ajustes o depuraciones en el sistema. A menudo se utiliza como una herramienta de diagnóstico o para probar el sistema antes de la implementación completa.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede establecer una conexión HTTP remota para cambiar el modo de operación de los PLCs de Omron.
S1006	PLC-Blaster	PLC-Blaster detiene la ejecución del programa de usuario en el objetivo para permitir la transferencia de su propio código. El gusano luego se copia a sí mismo en el objetivo y posteriormente vuelve a iniciar el PLC objetivo.
S1009	Triton	Triton tiene la capacidad de detener o ejecutar un programa a través del protocolo TriStation. TsHi.py contiene instancias de funciones de detener y ejecutar siendo ejecutadas.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autenticar todo acceso a los controladores de campo antes de autorizar el acceso o la modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en todo el sistema de control industrial (ICS).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir los cambios de modo de operación solo a usuarios autenticados requeridos (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles. Además, se pueden utilizar mecanismos físicos (por ejemplo, llaves) para limitar los cambios de modo de operación no autorizados.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para prevenir cambios no autorizados en el sistema.
M0804	Autenticación de Usuarios Humanos	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario
M0807	Listas de Permitidos de Red	Utilizar listas de permitidas basadas en el host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingenierías conocidas
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicaciones	Contenido del Registro de Aplicaciones	Monitorear los registros de aplicaciones de dispositivos que pueden contener información relacionada con cambios en el modo de operación, aunque no todos los dispositivos producen tales registros.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitorear los protocolos de gestión de ICS en busca de funciones que cambien el modo de operación de un activo.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitorear alarmas para obtener información sobre cuándo se cambia un modo de operación, aunque no todos los dispositivos producen tales registros.

Interfaz de Línea de Comandos

Los adversarios pueden utilizar interfaces de línea de comandos (CLI) para interactuar con sistemas y ejecutar comandos. Las CLIs proporcionan un medio de interacción con sistemas informáticos y son una característica común en muchos tipos de plataformas y dispositivos dentro de entornos de sistemas de control. Los adversarios también pueden utilizar CLIs para instalar y ejecutar nuevo software, incluidas herramientas maliciosas que pueden ser instaladas durante el transcurso de una operación.

Las CLIs suelen ser accedidas localmente, pero también pueden ser expuestas a través de servicios como SSH, Telnet y RDP. Los comandos que se ejecutan en la CLI lo hacen con el nivel de permisos actual del proceso que ejecuta el emulador de terminal, a menos que el comando especifique un cambio en el contexto de permisos. Muchos controladores tienen interfaces CLI para fines de gestión.

Ejemplos de Procedimientos

ID	Nombre	Descripción

C0025	Ataque al Suministro Eléctrico de Ucrania 2016	Durante el Ataque al Suministro Eléctrico de Ucrania en 2016, el Equipo Sandworm suministró el nombre del archivo DLL de la carga útil a Industroyer a través de un parámetro de línea de comandos.
S0604	Industroyer	El nombre del archivo DLL de la carga útil de Industroyer es suministrado por los atacantes a través de un parámetro de línea de comandos proporcionado en uno de los principales backdoors para ejecutar comandos de shell.
G0034	Equipo Sandworm	El Equipo Sandworm utiliza el comando xp_cmdshell del servidor MS-SQL y PowerShell para ejecutar comandos.
S0603	Stuxnet	Stuxnet almacenará y ejecutará código SQL que extraerá y ejecutará Stuxnet desde el archivo CAB guardado utilizando xp_cmdshell con el siguiente comando: set @s = master..xp_cmdshell extrac32 /y +@t+ +@t+x; exec(@s).

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0012	Servidor Puente
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0942	Deshabilitar o Eliminar Característica o Programa	Considerar eliminar o restringir características que no son necesarias para la función prevista de un activo dentro del entorno de control.
M0938	Prevención de Ejecución	La prevención de ejecución puede bloquear software malicioso para acceder a recursos protegidos a través de la interfaz de línea de comandos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicaciones	Contenido del Registro de Aplicaciones	Monitorear los registros de aplicaciones instaladas (por ejemplo, registros del historiador) en busca de comandos inesperados o abuso de características del sistema.
DS0017	Comando	Ejecución de Comandos	En sistemas Windows y Unix, monitorear los comandos ejecutados y los argumentos que pueden usar comandos de shell para la ejecución. En dispositivos de red y sistemas integrados CLI, considerar revisar el historial de comandos si se usaron comandos no autorizados o sospechosos para modificar la configuración del dispositivo.
DS0009	Proceso	Creación de Procesos	Monitorear procesos generados desde aplicaciones de shell de comando conocidas (por ejemplo, PowerShell, Bash). La actividad benigna deberá ser incluida en la lista blanca. Esta información puede ser útil para obtener información adicional sobre las acciones de los adversarios a través de cómo utilizan procesos nativos o herramientas personalizadas.

Ejecución a través de API

Los adversarios pueden intentar aprovechar las Interfaces de Programación de Aplicaciones (APIs) utilizadas para la comunicación entre el software de control y el hardware. La funcionalidad específica suele estar codificada en las APIs, las cuales

pueden ser invocadas por el software para activar funciones específicas en un dispositivo u otro software.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1009	Triton	Triton utiliza un protocolo TriStation reconstruido dentro de su marco para activar APIs relacionadas con la descarga de programas, la asignación de programas y los cambios de programa.

Activos Objetivo

ID	Activo
A0009	Puerta de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Las tecnologías de Gestión de Acceso pueden ser utilizadas para hacer cumplir políticas y decisiones de autorización, especialmente cuando los dispositivos de campo existentes no proporcionan capacidades para admitir la identificación y autenticación de usuarios. Estas tecnologías típicamente utilizan un dispositivo de red en línea o un sistema de puerta de enlace para evitar el acceso de usuarios no autenticados, mientras se integran con un servicio de autenticación para verificar primero las credenciales de usuario.
M0800	Aplicación de Autorización	Todas las APIs utilizadas para realizar ejecuciones, especialmente aquellas alojadas en controladores integrados (por ejemplo, PLCs), deben proporcionar una aplicación de autorización adecuada para el acceso de usuarios. Minimizar el acceso del usuario a solo las llamadas de API requeridas.

M0938	Prevención de Ejecución	Minimizar la exposición de llamadas de API que permitan la ejecución de código.
M0804	Autenticación de Usuarios Humanos	Todas las APIs en sistemas remotos o procesos locales deben requerir la autenticación de usuarios antes de ejecutar cualquier código o cambios en el sistema.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0009	Proceso	Ejecución de API del SO	Los dispositivos que proporcionan acceso de usuario al sistema operativo subyacente pueden permitir la instalación de software personalizado para monitorear la ejecución de API del SO. Monitorear las llamadas de API puede generar una cantidad significativa de datos y puede que no sea útil para la defensa a menos que se recolecten bajo circunstancias específicas, ya que el uso benigno de las funciones de API es común y puede ser difícil de distinguir del comportamiento malicioso. La correlación de otros eventos con el comportamiento que rodea las llamadas de funciones de API mediante el monitoreo de API proporcionará contexto adicional a un evento que puede ayudar a determinar si se debe a un comportamiento malicioso.

Interfaz Gráfica de Usuario

Los adversarios pueden intentar obtener acceso a una máquina a través de una Interfaz Gráfica de Usuario (GUI) para mejorar las capacidades de ejecución. El acceso a una GUI permite a un usuario interactuar con una computadora de manera más visual que con

una interfaz de línea de comandos (CLI). Una GUI permite a los usuarios mover un cursor y hacer clic en objetos de la interfaz, utilizando un ratón y un teclado como los principales dispositivos de entrada, en lugar de solo usar el teclado.

Si el acceso físico no es una opción, entonces el acceso podría ser posible a través de protocolos como VNC en sistemas operativos basados en Linux y Unix, y RDP en sistemas operativos Windows. Un adversario puede utilizar este acceso para ejecutar programas y aplicaciones en la máquina objetivo.

Ejemplos de procedimiento

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania en 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm utilizó interfaces gráficas de usuario (GUI) HMI en el entorno SCADA para abrir interruptores.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0012	Servidor Salto
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0816	Mitigación Limitada o No Efectiva	Una vez que un adversario tiene acceso a una GUI remota, pueden abusar de las funciones del sistema, como las funciones HMI requeridas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos relacionados con servicios específicamente diseñados para aceptar conexiones gráficas remotas, como RDP y VNC. Los Servicios Remotos y Cuentas Válidas pueden ser utilizados para acceder a la GUI de un host.
DS0028	Sesión de Inicio Sesión	Creación de Inicio de sesion	Supervisar las cuentas de usuario conectadas a sistemas a los que normalmente no accederían o patrones de acceso anormales, como múltiples sistemas en un período relativamente corto de tiempo. Correlacionar el uso de la actividad de inicio de sesión relacionada con servicios remotos con comportamientos inusuales u otras actividades maliciosas o sospechosas. Los Servicios Remotos pueden ser utilizados para acceder a la GUI de un host.
DS0011	Módulo	Carga de Módulos	Monitorear eventos de archivos DLL, específicamente la creación de estos archivos binarios, así como la carga de DLL en procesos asociados con conexiones gráficas remotas, como RDP y VNC. Los Servicios Remotos pueden ser utilizados para acceder a la GUI de un host.
DS0009	Proceso	Creación de Procesos	Monitorear procesos recién ejecutados relacionados con servicios específicamente diseñados para aceptar conexiones gráficas remotas, como RDP y VNC. Los Servicios Remotos y Cuentas Válidas pueden ser utilizados para acceder a la GUI de un host.

Modificar la asignación de tareas del controlador

Los adversarios pueden modificar la asignación de tareas de un controlador para permitir la ejecución de sus propios programas. Esto puede permitir a un adversario manipular el flujo de ejecución y el comportamiento de un controlador.

Según la norma 61131-3, la asociación de una tarea con una Unidad de Organización de Programas (POU, por sus siglas en inglés) define una asociación de tarea. Un adversario puede modificar estas asociaciones o crear nuevas para manipular el flujo de ejecución de un controlador. La modificación de la asignación de tareas del controlador puede lograrse utilizando una Descarga de Programa además de otros tipos de modificaciones de programa, como edición en línea y añadido de programa.

Las tareas tienen propiedades, como intervalo, frecuencia y prioridad, para cumplir con los requisitos de ejecución del programa. Algunos fabricantes de controladores implementan tareas con propiedades implícitas y predefinidas, mientras que otros permiten que estas propiedades se formulen explícitamente. Un adversario puede asociar su programa con tareas que tengan una prioridad más alta o ejecuten los programas asociados con más frecuencia. Por ejemplo, para asegurar la ejecución cíclica de su programa en un controlador de Siemens, un adversario puede agregar su programa a la tarea, Bloque de Organización 1 (OB1).

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1006	PLC-Blaster	El código de PLC-Blaster se almacena en OB9999. El código original en el objetivo permanece intacto. El OB es detectado automáticamente por el PLC y ejecutado.
S0603	Stuxnet	Stuxnet infecta OB1 para que su secuencia de código malicioso se ejecute al inicio de un ciclo. También infecta OB35. OB35 actúa como un guardián y, bajo ciertas condiciones, puede detener la ejecución de OB1.
S1009	Triton	El argumento de Triton y el shellcode inject.bin se agregan a la tabla de programas en el Tricon para que sean ejecutados por el firmware una vez en cada ciclo.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Proporcionar la capacidad de verificar la integridad de la asignación de tareas del controlador. Aunque las técnicas como CRC y sumas de verificación se utilizan comúnmente, no son criptográficamente seguras y pueden ser vulnerables a colisiones. Preferiblemente, deberían utilizarse funciones hash criptográficas (por ejemplo, SHA2, SHA-3).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir la modificación de las tareas del controlador solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.
M0945	Firma de Código	Utilizar firmas de código para verificar la integridad y autenticidad de los programas instalados en activos de seguridad o control, incluida la asignación de tareas del controlador asociado.
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deberían admitir Políticas de Uso de Cuentas, Políticas de Contraseña y Gestión de Cuentas de Usuario.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicación de los activos para obtener información que indique que los parámetros de la tarea han cambiado.
DS0039	Activo	Software	El software de ingeniería y gestión de activos a menudo mantendrá una copia del programa esperado cargado en un controlador y también puede registrar cualquier cambio realizado en los programas y tareas del controlador. Los datos de estas plataformas se pueden utilizar para identificar la modificación de la asignación de tareas del controlador.

DS0040	Bases de Datos Operativas	Alarma de Dispositivo	Monitorear las alarmas del dispositivo que indiquen que los parámetros de la tarea del controlador han cambiado,
			aunque no todos los dispositivos producen tales alarmas. La Descarga de Programa puede ser utilizada para habilitar esta técnica. Monitorear las descargas de programas que pueden ser notables a través de alarmas operativas. Los sistemas de gestión de activos deben consultarse para comprender las versiones de programas esperadas.

API nativo

Los adversarios pueden interactuar directamente con la interfaz de programación de aplicaciones (API) nativa del sistema operativo para acceder a funciones del sistema. Las API nativas proporcionan un medio controlado para llamar a servicios del sistema operativo de bajo nivel dentro del núcleo, como aquellos que implican hardware/dispositivos, memoria y procesos. Estas API nativas son aprovechadas por el sistema operativo durante el arranque del sistema (cuando otros componentes del sistema aún no se han inicializado), así como para llevar a cabo tareas y solicitudes durante operaciones rutinarias.

La funcionalidad proporcionada por las API nativas a menudo también se expone a aplicaciones en modo de usuario a través de interfaces y bibliotecas. Por ejemplo, funciones como memcpy y operaciones directas en registros de memoria pueden utilizarse para modificar el espacio de memoria del usuario y del sistema.

Ejemplos de procedimiento

ID	Nombre	Descripción
S1006	PLC-Blaster	PLC-Blaster utiliza los bloques de funciones del sistema TCON y TDISCON para iniciar y destruir conexiones TCP a sistemas arbitrarios. Los buffers pueden ser enviados y recibidos en estas conexiones con los bloques de funciones del sistema TRCV y TSEND.
S0603	Stuxnet	Stuxnet llama a los bloques de funciones del sistema que son parte del sistema operativo que se ejecuta en el PLC. Se utilizan para ejecutar tareas del sistema, como leer el reloj del sistema (SFC1) y generar bloques de datos sobre la marcha.

S1009	Triton	La carga útil imain.bin de Triton toma comandos de las funciones TsHi.ExplReadRam(Ex), TsHi.ExplWriteRam(Ex) y TsHi.ExplExec para realizar operaciones en la memoria y
		registros del controlador utilizando llamadas al sistema escritas en shellcode de PowerPC.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Servidor Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0938	Prevención de Ejecución	Minimizar la exposición de llamadas de API que permitan la ejecución de código.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0009	Proceso	Ejecución de API del SO	Los dispositivos que proporcionan acceso de usuario al sistema operativo subyacente pueden permitir la instalación de software personalizado para monitorear la ejecución de API del SO. Monitorear las llamadas de API puede generar una cantidad significativa de datos y puede que no sea útil para la defensa a menos que se recolecten bajo circunstancias específicas,
			ya que el uso benigno de las funciones de API es común y puede ser difícil de distinguir del comportamiento malicioso. La correlación de otros eventos con el comportamiento que rodea las llamadas de funciones de API mediante el monitoreo de API proporcionará contexto adicional a un evento que puede ayudar a determinar si se debe a un comportamiento malicioso.

Scripting

Los adversarios pueden usar lenguajes de script para ejecutar código arbitrario en forma de un script preescrito o en forma de código suministrado por el usuario a un intérprete. Los lenguajes de script son lenguajes de programación que difieren de los lenguajes compilados en el sentido de que utilizan un intérprete en lugar de un compilador. Estos intérpretes leen y compilan parte del código fuente justo antes de que se ejecute, a diferencia de los compiladores, que compilan cada línea de código a un archivo ejecutable. El scripting permite a los desarrolladores de software ejecutar su código en cualquier sistema donde exista el intérprete. De esta manera, pueden distribuir un único paquete en lugar de precompilar ejecutables para muchos sistemas diferentes. Los lenguajes de script, como Python, tienen sus intérpretes incluidos de forma predeterminada en muchas distribuciones de Linux.

Además de ser una herramienta útil para desarrolladores y administradores, los intérpretes de lenguajes de script pueden ser abusados por el adversario para ejecutar código en el entorno objetivo. Debido a la naturaleza de los lenguajes de script, esto permite que el código se convierta en armas y sea desplegado fácilmente en un objetivo, y deja abierta la posibilidad de scripting sobre la marcha para realizar una tarea.

Ejemplos de procedimiento

ID	Nombre	Descripción
C0025	Ataque al suministro eléctrico de Ucrania de 2016	Durante el Ataque al suministro eléctrico de Ucrania de 2016, el equipo Sandworm utilizó VBS y scripts por lotes para el movimiento de archivos y como envoltorios para la ejecución de PowerShell.
G0064	APT33	APT33 utilizó scripts de PowerShell para establecer el comando y control e instalar archivos para la ejecución.
G0049	OilRig	OilRig ha incrustado una macro dentro de archivos adjuntos de spearphishing que se compone tanto de un script VBScript como de un script PowerShell.
S0496	REvil	REvil utiliza scripts de JavaScript, WScript y PowerShell para ejecutarse. El archivo adjunto de JavaScript malicioso tiene un script de PowerShell ofuscado que ejecuta el malware.
S1009	Triton	Triton se comunica con controladores Triconex utilizando un marco de componentes personalizado escrito completamente en Python. Los módulos que implementan el protocolo de comunicación TriStation y otros componentes de soporte se encuentran en un archivo separado: library.zip. El script principal que emplea esta funcionalidad se compila en un ejecutable independiente de Windows py2exe: trilog.exe, que incluye un entorno Python.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos

A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0012	Servidor Salto
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0948	Aislamiento y Protección de Aplicaciones	Considerar el uso de aislamiento y protección de aplicaciones para restringir interacciones específicas del sistema operativo, como el acceso a través de cuentas de usuario, servicios, llamadas al sistema, registro y acceso a la red. Esto puede ser aún más útil en casos donde se desconoce la fuente del script ejecutado.
M0942	Deshabilitar o Eliminar Funciones o Programas	Considerar la eliminación o deshabilitación de programas y funciones que podrían ser utilizados para ejecutar scripts maliciosos (por ejemplo, entornos de desarrollo de lenguajes de script, PowerShell, Visual Studio).
M0938	Prevención de Ejecución	La prevención de ejecución puede evitar que los scripts maliciosos accedan a recursos protegidos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear los argumentos de la línea de comandos para la ejecución de scripts y el comportamiento posterior. Las acciones pueden estar relacionadas con el Descubrimiento, Recopilación de información de red y del sistema, u otros comportamientos de compromiso posterior scriptables y podrían utilizarse como indicadores de detección que conducen al script fuente.

DS0011	Módulo	Carga de Módulos	Monitorear eventos asociados con la ejecución de scripts, como la carga de módulos asociados con lenguajes de scripting (por ejemplo, JScript.dll, vbscript.dll).
DS0009	Proceso	Creación de Procesos	Monitorear archivos de registro para la ejecución de procesos a través de actividades de línea de comandos y scripting. Esta información puede ser útil para obtener una visión adicional de las acciones de los adversarios a través de cómo utilizan procesos nativos o herramientas
			personalizadas. También monitorear la carga de módulos asociados con lenguajes específicos.
		Metadatos de Proceso	Monitorear datos contextuales sobre un proceso en ejecución, que pueden incluir información como variables de entorno, nombre de imagen, usuario/propietario u otra información que pueda revelar el abuso de características del sistema.
DS0012	Script	Ejecución de Scripts	Monitorear cualquier intento de habilitar scripts que se estén ejecutando en un sistema sería considerado sospechoso. Si los scripts no se utilizan comúnmente en un sistema, pero están habilitados, los scripts que se ejecutan fuera del ciclo de parcheo u otras funciones del administrador son sospechosos. Los scripts deben ser capturados del sistema de archivos cuando sea posible para determinar sus acciones e intenciones.

Ejecución de Usuario

Los adversarios pueden depender de la interacción del usuario de una organización objetivo para la ejecución de código malicioso. La interacción del usuario puede consistir en instalar aplicaciones, abrir adjuntos de correo electrónico o otorgar permisos elevados a documentos.

Los adversarios pueden incrustar código malicioso o código Visual Basic en archivos como documentos de Microsoft Word y Excel o instaladores de software. La ejecución de este código requiere que el usuario habilite la ejecución de scripts o el acceso de escritura dentro del documento. El código incrustado no siempre es perceptible para el usuario, especialmente en casos de software troyanizado.

Una campaña de spear phishing china que se desarrolló desde el 9 de diciembre de 2011 hasta el 29 de febrero de 2012 entregaba malware a través de adjuntos de spear phishing que requerían acción por parte del usuario para lograr la ejecución.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0093	Backdoor.Oldrea	La ejecución de Backdoor.Oldrea depende de que un usuario abra un instalador troyanizado adjunto a un correo electrónico.
S0606	Bad Rabbit	Bad Rabbit está disfrazado como un instalador de Adobe Flash. Cuando se abre el archivo, comienza a bloquear la computadora infectada.
S0496	REvil	REvil se ejecuta inicialmente cuando el usuario hace clic en un archivo JavaScript incluido en el archivo adjunto .zip de correos electrónicos de phishing.
S0603	Stuxnet	Stuxnet infecta DLL asociadas con el gestor Simatic de WinCC, que son responsables de abrir archivos de proyecto. Si un usuario abre un archivo de proyecto no infectado utilizando un gestor comprometido, el archivo se infectará con el código de Stuxnet. Si se abre un proyecto infectado con el gestor Simatic, el archivo de datos modificado activará una búsqueda del archivo xyz.dll. Si el archivo xyz.dll no se encuentra en ninguna de las ubicaciones especificadas, la DLL maliciosa se cargará y ejecutará por el gestor.

Activos Objetivo

ID	Activo
A0002	Interfaz Hombre-Máquina (HMI)
A0012	Host de Salto
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0949	Antivirus/Antimalware	Asegurar que la solución antivirus pueda detectar archivos maliciosos que permitan la ejecución por parte del usuario (por ejemplo, Macros de Microsoft Office, instaladores de programas).
M0945	Firma de Código	Prevenir el uso de ejecutables no firmados, como instaladores y scripts.
M0938	Prevención de Ejecución	El control de aplicaciones puede prevenir la ejecución de ejecutables que se hacen pasar por otros archivos.
M0931	Prevención de Intrusión en la Red	Si un usuario está visitando un enlace, los sistemas de prevención de intrusión en la red y los sistemas diseñados para escanear y eliminar descargas maliciosas pueden ser utilizados para bloquear la actividad.
M0921	Restricción de Contenido Web	Si un usuario está visitando un enlace, bloquear por defecto los archivos desconocidos o no utilizados en tránsito que no deberían ser descargados o por política desde sitios sospechosos como una mejor práctica para prevenir algunos vectores, como .scr, .exe, .pif, .cpl, etc. Algunos dispositivos de escaneo de descargas pueden abrir y analizar formatos comprimidos y encriptados, como zip y rar, que pueden ser utilizados para ocultar archivos maliciosos.
M0917	Entrenamiento de Usuarios	Usar el entrenamiento de usuarios como una forma de crear conciencia sobre técnicas de phishing comunes y spearphishing y cómo levantar sospechas sobre eventos potencialmente maliciosos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicaciones	Contenido del Registro de Aplicaciones	Monitorizar el registro de aplicaciones, mensajes y/u otros artefactos que puedan depender de acciones específicas por parte de un usuario para obtener ejecución.

DS0017	Comando	Ejecución de Comandos	Monitorizar los procesos recién ejecutados que dependen de la interacción del usuario, especialmente para aplicaciones que pueden incrustar capacidades programáticas (por ejemplo, productos de Microsoft Office con scripts, instaladores, archivos zip). Esto incluye aplicaciones de compresión, como las de archivos zip, que pueden ser utilizadas para
			desofuscar/decodificar archivos o información en cargas útiles.
DS0022	Archivo	Acceso a Archivos	El antivirus puede potencialmente detectar documentos y archivos maliciosos que son descargados y ejecutados en la computadora del usuario. La percepción de punto final o la percepción de red pueden potencialmente detectar eventos maliciosos una vez que el archivo es abierto (como un documento de Microsoft Word o PDF que se conecta a internet o que genera PowerShell).

DS0029	Tráfico de Red	Creación de Conexiones de Red	Monitorizar las conexiones de red basadas en web recién construidas que se envían a destinos maliciosos o sospechosos (por ejemplo, destinos atribuidos a campañas de phishing). Considerar la correlación con la monitorización de procesos y la línea de comandos para detectar ejecuciones de procesos anómalas y argumentos de línea de comandos (por ejemplo, monitorizar anomalías en el uso de archivos que normalmente no inician conexiones de red o conexiones inusuales iniciadas por regsvr32.exe, rundll.exe, SCF, HTA, MSI, DLLs o msiexec.exe).
		Contenido del Tráfico de Red	Monitorizar y analizar patrones de tráfico e inspección de paquetes asociados con conexiones de red basadas en web que se envían a destinos

			maliciosos o sospechosos (por ejemplo, destinos atribuidos a campañas de phishing). Considerar la correlación con la monitorización de procesos y la línea de comandos para detectar ejecuciones de procesos anómalas y argumentos de línea de comandos (por ejemplo, monitorizar anomalías en el uso de archivos que normalmente no inician conexiones de red o conexiones inusuales iniciadas por regsvr32.exe, rundll.exe, SCF, HTA, MSI, DLLs o msiexec.exe).
DS0009	Proceso	Creación de Procesos	Monitorizar los procesos recién ejecutados que dependen de la interacción del usuario, especialmente para aplicaciones que pueden incrustar capacidades programáticas (por ejemplo, productos de Microsoft Office con scripts, instaladores, archivos zip). Esto incluye aplicaciones de compresión, como las de archivos zip, que pueden ser utilizadas para desofuscar/decodificar archivos o información en cargas útiles.

PERSISTENCIA

El adversario está tratando de mantener su presencia en tu entorno ICS.

La persistencia consiste en técnicas que los adversarios utilizan para mantener el acceso a sistemas y dispositivos ICS a través de reinicios, cambios de credenciales y otras

interrupciones que podrían cortar su acceso. Las técnicas utilizadas para la persistencia incluyen cualquier acceso, acción o cambios de configuración que les permitan

asegurar su actividad continua y mantener su presencia en los sistemas. Esto puede incluir la sustitución o secuestro de código legítimo, firmware y otros archivos del proyecto, o la adición de código de inicio y la descarga de programas en dispositivos.

Credenciales codificadas en el código.

Los adversarios pueden causar daños y destrucción de propiedad a la infraestructura, equipos y el entorno circundante al atacar sistemas de control. Esta técnica puede resultar en el deterioro de dispositivos y equipos operativos, o representar daños tangenciales de otras técnicas utilizadas en un ataque. Dependiendo de la gravedad del daño físico y la interrupción causada a los procesos y sistemas de control, esta técnica puede resultar en Pérdida de Seguridad. Las operaciones que resultan en Pérdida de Control también pueden causar daños a la propiedad, que pueden estar directa o indirectamente motivados por un adversario que busca causar impacto en forma de Pérdida de Productividad e Ingresos.

La Oficina Federal de Seguridad de la Información (BSI) de Alemania informó sobre un ataque dirigido a un molino de acero en la sección de incidentes que afectan a los negocios de su Informe de Seguridad Informática de 2014. Estos ataques dirigidos afectaron las operaciones industriales y resultaron en fallos de componentes del sistema de control e incluso de instalaciones enteras. Como resultado de estos fallos, se produjo un impacto y daño masivo debido al apagado no controlado de un alto horno.

Un estudiante polaco utilizó un dispositivo de control remoto para interactuar con el sistema de tranvías de la ciudad de Lodz en Polonia. Utilizando este control remoto, el estudiante pudo capturar y reproducir señales legítimas de tranvía. Esto resultó en daños a los tranvías afectados, personas y la propiedad circundante. Según los informes, cuatro tranvías descarrilaron y tuvieron que hacer paradas de emergencia. Los comandos emitidos por el estudiante también pueden haber resultado en colisiones de tranvías, causando daños a los pasajeros y al entorno exterior.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede iniciar sesión en PLCs de Omron utilizando credenciales codificadas de manera fija, lo cual está documentado en CVE-2022-34151.
S0603	Stuxnet	Stuxnet utiliza una contraseña codificada de manera fija en el servidor de base de datos del software WinCC como uno de los mecanismos utilizados para propagarse a sistemas cercanos.

Activos Objetivo

ID	Activo
A0013	E/S de Campo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Asegurar que los controles integrados y los dispositivos de red estén protegidos mediante la gestión de acceso, ya que estos dispositivos a menudo tienen cuentas codificadas de manera fija desconocidas que podrían ser utilizadas para obtener acceso no autorizado.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0028	Sesión de Inicio de Sesión	Creación de Sesión de Inicio de Sesión	Monitorear las sesiones de inicio de sesión en busca de uso de credenciales codificadas de manera fija, cuando sea factible.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear el tráfico de red en busca de uso de credenciales codificadas de manera fija en protocolos que permitan la autenticación no cifrada.

Modificar Programa

Los adversarios pueden modificar o agregar un programa en un controlador para afectar cómo interactúa con el proceso físico, dispositivos periféricos y otros hosts en la red. La modificación de programas en el controlador puede llevarse a cabo utilizando una Descarga de Programa además de otros tipos de modificación de programa como la edición en línea y la adición de programa.

La modificación de programas abarca la adición y modificación de instrucciones y lógica contenida en Unidades de Organización de Programas (POU) y elementos de programación similares que se encuentran en los controladores. Esto puede incluir, por ejemplo, agregar nuevas funciones a un controlador, modificar la lógica en funciones existentes y realizar nuevas llamadas de una función a otra.

Algunos programas pueden permitir que un adversario interactúe directamente con la API nativa del controlador para aprovechar funciones u vulnerabilidades obscuros.

Ejemplos de procedimiento

ID	Nombre	Descripción
S1006	PLC-Blaster	PLC-Blaster se copia a diversas Unidades de Organización del Programa (POU, por sus siglas en inglés) en el dispositivo objetivo. Las POUs incluyen el Bloque de Datos, Función y Bloque de Función.
S0603	Stuxnet	Stuxnet infecta PLCs con diferentes códigos dependiendo de las características del sistema objetivo. Una secuencia de infección consiste en bloques de código y bloques de datos que serán descargados al PLC para alterar su comportamiento.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Proporciona la capacidad de verificar la integridad de la lógica de control o programas cargados en un controlador. Aunque técnicas como CRC y sumas de verificación son comúnmente utilizadas, no son criptográficamente fuertes y pueden ser vulnerables a colisiones. Preferiblemente, deberían utilizarse funciones hash criptográficas (por ejemplo, SHA-2, SHA-3).
M0800	Aplicación de Autorización	Todos los controladores de campo deberían restringir la modificación de programas solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.
M0945	Firma de Código	Utilizar firmas de código para verificar la integridad y autenticidad de los programas instalados en activos de seguridad o control.

M0804	Autenticación de Usuario Humano	Todos los controladores de campo deberían requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deberían admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Monitorear los logs de aplicación del dispositivo que indiquen que el programa ha cambiado, aunque no todos los dispositivos producen tales logs.
DS0039	Activo	Software	El software de ingeniería y gestión de activos a menudo mantendrá una copia del programa esperado cargado en un controlador y también puede registrar cualquier cambio realizado en los programas de controlador. Los datos de estas plataformas pueden ser utilizados para identificar programas de controlador modificados.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear los protocolos de gestión de dispositivos para funciones que modifican programas, como eventos de edición en línea y anexado de programas.
DS0040	Bases de Datos Operacionales	Alarma de Dispositivo	Monitorear las alarmas de dispositivo que indiquen que el programa ha cambiado, aunque no todos los dispositivos producen tales alarmas.

Firmware del Módulo

Los adversarios pueden instalar firmware malicioso o vulnerable en dispositivos de hardware modular. Los dispositivos de sistemas de control a menudo contienen dispositivos de hardware modulares. Estos dispositivos pueden tener su propio conjunto de firmware que es independiente del firmware del equipo principal del sistema de control.

Esta técnica es similar a la de Firmware del Sistema, pero se lleva a cabo en otros componentes del sistema que pueden no tener las mismas capacidades o nivel de verificación de integridad. Aunque resulta en una reimagenización del dispositivo, el firmware malicioso del dispositivo puede proporcionar acceso persistente a los dispositivos restantes.

Un punto de acceso fácil para un adversario es la tarjeta Ethernet, que puede tener su propia CPU, RAM y sistema operativo. El adversario puede atacar y probablemente explotar la computadora en una tarjeta Ethernet. La explotación de la computadora de la tarjeta Ethernet puede permitir al adversario llevar a cabo ataques adicionales, como los siguientes:

Ataque Diferido: El adversario puede preparar un ataque con anticipación y elegir cuándo lanzarlo, como en un momento particularmente dañino.

Ladrillo en la Tarjeta Ethernet: El firmware malicioso puede estar programado para provocar un fallo en la tarjeta Ethernet, lo que requiere un retorno a fábrica.

Ataque o Fallo Aleatorio: El adversario puede cargar firmware malicioso en múltiples dispositivos de campo. La ejecución de un ataque y el momento en que ocurre se genera mediante un generador de números pseudoaleatorios.

Gusano en Dispositivos de Campo: El adversario puede optar por identificar todos los dispositivos de campo del mismo modelo, con el objetivo final de realizar un compromiso a nivel de dispositivo.

Atacar Otras Tarjetas en el Dispositivo de Campo: Aunque no es el módulo más importante en un dispositivo de campo, la tarjeta Ethernet es más accesible para el adversario y el malware. El compromiso de la tarjeta Ethernet puede proporcionar una ruta más directa para comprometer otros módulos, como el módulo de CPU.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0801	Gestión de Acceso	Todos los cambios de dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere utilizar tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización fuertes.
M0947	Auditoría	Realizar verificaciones de integridad del firmware antes de cargarlo en un dispositivo. Utilice hashes criptográficos para verificar que el firmware no haya sido alterado comparándolo con un hash confiable del firmware. Esto podría ser desde fuentes de datos confiables (por ejemplo, el sitio del proveedor) o a través de un servicio de verificación de terceros.
M0946	Integridad de Arranque	Verifique la integridad del BIOS o EFI existente para determinar si es vulnerable a modificaciones. Utilice la tecnología Trusted Platform Module. Mueva la raíz de confianza del sistema al hardware para evitar la manipulación de la memoria flash SPI. Tecnologías como Intel Boot Guard pueden ayudar con esto.
M0945	Firma de Código	Los dispositivos deben verificar que el firmware haya sido firmado correctamente por el proveedor antes de permitir la instalación.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0808	Cifrado del Tráfico de Red	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0941	Cifrado de Información Sensible	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0937	Filtrado del Tráfico de Red	Filtre los protocolos y cargas útiles asociados con la activación o actualización del firmware.
M0804	Autenticación de Usuario Humano	Los dispositivos que permiten la gestión remota del firmware deben requerir autenticación antes de permitir cualquier cambio. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden

		usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Monitorear los logs de aplicación del dispositivo en busca de cambios de firmware, aunque no todos los dispositivos producirán tales logs.
DS0001	Firmware	Modificación de Firmware	Monitorear el firmware en busca de cambios inesperados. Se deben consultar sistemas de gestión de activos para comprender las versiones de firmware conocidas como válidas. Dump e inspeccione imágenes del BIOS en sistemas vulnerables y compárelas con imágenes conocidas como válidas. Analice las diferencias para determinar si se han realizado cambios maliciosos. Registre intentos de lectura/escritura en el BIOS y compárelos con el comportamiento de parcheo conocido. Del mismo modo, los módulos EFI pueden recopilarse y compararse con una lista conocida y limpia de

			binarios ejecutables EFI para detectar módulos potencialmente maliciosos. El marco CHIPSEC se puede utilizar para el análisis para determinar si se han realizado modificaciones en el firmware.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear los protocolos de gestión de ICS / protocolos de transferencia de archivos para funciones de protocolo relacionadas con cambios de firmware.
DS0040	Bases de Datos Operacionales	Alarma de Dispositivo	Monitorear cambios de firmware que pueden ser observables a través de alarmas operacionales de dispositivos.

Infección de Archivos de Proyecto

Los adversarios pueden intentar infectar archivos de proyecto con código malicioso. Estos archivos de proyecto pueden consistir en objetos, unidades de organización de programas, variables como etiquetas, documentación y otras configuraciones necesarias para que los programas PLC funcionen. Utilizando funciones incorporadas del software de ingeniería, los adversarios pueden ser capaces de descargar un programa infectado en un PLC en el entorno operativo, lo que permite técnicas adicionales de Ejecución y Persistencia.

Los adversarios pueden exportar su propio código en archivos de proyecto con condiciones para ejecutarse en intervalos específicos. Los programas maliciosos permiten a los adversarios controlar todos los aspectos del proceso habilitado por el PLC. Una vez que el archivo de proyecto se descarga en un PLC, el dispositivo de la estación de trabajo puede ser desconectado con el archivo de proyecto infectado aún en ejecución.

Procedimiento Ejemplos

ID	Nombre	Descripción

S0603	Stuxnet	Stuxnet se copia a proyectos de Step 7 de tal manera que se ejecuta automáticamente cuando se carga el proyecto de Step 7.

Activos Objetivo

ID	Activo
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Revisar la integridad de los archivos de proyecto para verificar que no hayan sido modificados por comportamientos adversarios. Verificar un hash criptográfico para el archivo con una versión conocida y confiable, o buscar otros indicadores de modificación (por ejemplo, marcas de tiempo).
M0945	Firma de Código	Permitir la firma de código de cualquier archivo de proyecto almacenado en reposo para evitar manipulaciones no autorizadas. Asegurarse de que las claves de firma no sean fácilmente accesibles en el mismo sistema.
M0941	Cifrado de Información Sensible	Cuando están en reposo, los archivos de proyecto deben estar cifrados para prevenir cambios no autorizados.
M0922	Restricción de Permisos de Archivos y Directorios	Asegurarse de que los permisos restrinjan el acceso a los archivos de proyecto solo a los grupos de usuarios y cuentas de ingenieros y técnicos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0022	Archivo	Modificación de Archivo	Monitorear cambios inesperados en los archivos de proyecto, aunque si la modificación maliciosa ocurre simultáneamente con cambios legítimos, será difícil aislar los cambios no deseados analizando solo las modificaciones en los sistemas de archivos.

Firmware del Sistema

El firmware del sistema en los activos modernos suele estar diseñado con una función de actualización. El firmware de dispositivos más antiguos puede estar instalado de fábrica y requerir equipo especial de reprogramación. Cuando está disponible, la función de actualización de firmware permite a los proveedores parchear errores y realizar actualizaciones de forma remota. Las actualizaciones de firmware de dispositivos suelen ser delegadas al usuario y pueden realizarse utilizando un paquete de actualización de software. También puede ser posible realizar esta tarea a través de la red.

Un adversario puede aprovechar la función de actualización de firmware en dispositivos accesibles para cargar firmware malicioso o desactualizado. La modificación maliciosa del firmware del dispositivo puede proporcionar a un adversario acceso de root a un dispositivo, dado que el firmware es una de las capas de abstracción de programación más bajas.

Procedimiento Ejemplos

ID	Nombre	Descripción
C0028	Ataque a la Energía Eléctrica de Ucrania de 2015	Durante el Ataque a la Energía Eléctrica de Ucrania de 2015, el Equipo Sandworm sobrescribió las pasarelas serie a Ethernet con firmware personalizado para deshabilitar, apagar y/o volver irreconocibles los sistemas.
S1009	Triton	Triton es capaz de leer, escribir y ejecutar código en la memoria del controlador de seguridad en una dirección arbitraria dentro de la región de firmware de los dispositivos. Esto permite que el malware realice cambios en el firmware en ejecución en la memoria y modifique cómo opera el dispositivo.

Activos Objetivo

ID	Activo
A0009	Pasarela de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios de dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere el uso de tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización fuertes.
M0947	Auditoría	Realice verificaciones de integridad del firmware antes de cargarlo en un dispositivo. Utilice hashes criptográficos para verificar que el firmware no haya sido manipulado comparándolo con un hash confiable del firmware. Esto podría ser desde fuentes de datos confiables (por ejemplo, el sitio del proveedor) o a través de un servicio de verificación de terceros.
M0946	Integridad de Arranque	Verifique la integridad del BIOS o EFI existente para determinar si es vulnerable a modificaciones. Utilice la tecnología del Módulo de Plataforma Confiable. Mueva la raíz de confianza del sistema al hardware para evitar la manipulación de la memoria flash SPI. Tecnologías como Intel Boot Guard pueden ayudar con esto.
M0945	Firma de Código	Los dispositivos deben verificar que el firmware haya sido correctamente firmado por el proveedor antes de permitir la instalación
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0808	Cifrado del Tráfico de Red	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0941	Cifrado de Información Sensible	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0937	Filtrado del Tráfico de Red	Filtre los protocolos y cargas útiles asociados con la activación o actualización del firmware.
M0804	Autenticación de Usuario Humano	Los dispositivos que permiten la gestión remota del firmware deben requerir autenticación antes de permitir cualquier cambio. Los mecanismos de autenticación

		también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden
		usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmente la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autentique conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.
M0951	Actualizar Software	Parchee el BIOS y EFI según sea necesario

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Monitorear los logs de aplicación del dispositivo en busca de cambios de firmware, aunque no todos los dispositivos producirán tales logs.

DS0001	Firmware	Modificación de Firmware	Monitorear el firmware en busca de cambios inesperados. Se deben consultar sistemas de gestión de activos para comprender las versiones de firmware conocidas como válidas. Dump e inspeccione imágenes del BIOS en sistemas vulnerables y compárelas con imágenes conocidas como válidas. Analice las diferencias para determinar si se han realizado cambios maliciosos. Registre intentos de lectura/escritura en el BIOS y compárelos con el comportamiento de parcheo conocido. Del mismo modo, los módulos EFI pueden recopilarse y compararse con una lista conocida y limpia de
			binarios ejecutables EFI para detectar módulos potencialmente maliciosos. El marco CHIPSEC se puede utilizar para el análisis para determinar si se han realizado modificaciones en el firmware.

Cuentas Válidas

Los adversarios pueden robar las credenciales de un usuario específico o de una cuenta de servicio utilizando técnicas de acceso a credenciales. En algunos casos, las credenciales predeterminadas para dispositivos de sistemas de control pueden estar disponibles públicamente. Las credenciales comprometidas pueden ser utilizadas para eludir los controles de acceso establecidos en varios recursos en los hosts y dentro de la red, e incluso pueden ser utilizadas para acceder de manera persistente a sistemas remotos. Las credenciales comprometidas y predeterminadas también pueden otorgar a un adversario un privilegio aumentado para sistemas y dispositivos específicos o acceso a áreas restringidas de la red. Los adversarios pueden optar por no utilizar malware o herramientas, junto con el acceso legítimo que proporcionan esas

credenciales, para hacer más difícil detectar su presencia o para controlar dispositivos y enviar comandos legítimos de manera no intencionada.

Los adversarios también pueden crear cuentas, a veces utilizando nombres de cuenta y contraseñas predefinidos, para proporcionar un medio de acceso de respaldo para la persistencia.

La superposición de credenciales y permisos en una red de sistemas es preocupante porque el adversario puede ser capaz de pivotar a través de cuentas y sistemas para alcanzar un alto nivel de acceso (es decir, administrador de dominio o de empresa) y posiblemente entre los entornos de tecnología de la información y tecnología operativa. Los adversarios pueden aprovechar las credenciales válidas de un sistema para obtener acceso a otro sistema.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque a la Energía Eléctrica de Ucrania de 2015	Durante el Ataque a la Energía Eléctrica de Ucrania de 2015, el Equipo Sandworm utilizó cuentas válidas para moverse lateralmente a través de conexiones VPN y sistemas de doble homologación. El Equipo Sandworm utilizó las credenciales de cuentas válidas para interactuar
		con aplicaciones de cliente y acceder a estaciones de trabajo de empleados que alojan aplicaciones de HMI
C0025	Ataque a la Energía Eléctrica de Ucrania de 2016	Durante el Ataque a la Energía Eléctrica de Ucrania de 2016, el Equipo Sandworm utilizó cuentas válidas para moverse lateralmente a través de conexiones VPN y sistemas de doble homologación.
G1000	ALLANITE	ALLANITE utilizó credenciales recopiladas a través de ataques de phishing y de sitios web maliciosos.
S0089	BlackEnergy	BlackEnergy utiliza credenciales de usuario y administrador válidas, además de crear nuevas cuentas de administrador para mantener presencia.
S1045	INCONTROLLER	INCONTROLLER puede realizar ataques de fuerza bruta contra la autenticación basada en contraseñas para PLCs Schneider a través del protocolo CODESYS (puerto UDP 1740). INCONTROLLER puede realizar adivinanzas de contraseñas mediante fuerza bruta para servidores OPC UA utilizando una lista predefinida de contraseñas.
G0049	OilRig	OilRig utilizó credenciales robadas para acceder a máquinas víctimas.

G0088	TEMP.Veles	TEMP.Veles utilizó credenciales válidas al moverse lateralmente a través de cajas de salto RDP hacia el entorno de ICS.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Pasarela de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Anfitrión de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autentica todo acceso a los controladores de campo antes de autorizar el acceso o modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizada pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en todo el sistema de control industrial (ICS).
M0936	Políticas de Uso de Cuenta	Configura características relacionadas con el uso de cuentas, como bloqueos de intentos de inicio de sesión, horarios específicos de inicio de sesión y requisitos de fortaleza de contraseñas, como ejemplos. Considera estas características en relación con los activos que pueden afectar la seguridad y disponibilidad.

M0915	Configuración de Directorio Activo	Considera la configuración y uso de un servicio de autenticación en toda la red, como Active Directory, LDAP o capacidades RADIUS que se pueden encontrar en dispositivos ICS.
M0913	Orientación para Desarrolladores de Aplicaciones	Asegúrate de que las aplicaciones y dispositivos no almacenen datos sensibles o credenciales de forma insegura (por ejemplo, credenciales en texto plano en el código, credenciales publicadas en repositorios o credenciales en almacenamiento en la nube pública).
M0947	Auditoría	Audita rutinariamente el código fuente, los archivos de configuración de la aplicación, los repositorios abiertos y el almacenamiento en la nube pública en busca de uso y almacenamiento inseguros de credenciales.
M0937	Filtrado del Tráfico de Red	Considera el uso de listas de permitidos de IP junto con la gestión de cuentas de usuario para asegurar que el acceso a los datos esté restringido no solo a usuarios válidos, sino solo desde rangos de IP esperados para mitigar el uso de credenciales robadas para acceder a datos.
M0932	Autenticación Multifactorial	La integración de la autenticación multifactorial (MFA) como parte de la política organizativa puede reducir considerablemente el riesgo de que un adversario obtenga acceso a credenciales válidas que puedan ser utilizadas para tácticas adicionales, como acceso inicial, movimiento lateral y recopilación de información. MFA también se puede utilizar para restringir el acceso a recursos y APIs en la nube.
M0927	Políticas de Contraseña	Las aplicaciones y dispositivos que utilizan nombres de usuario y contraseñas predeterminados deben cambiarse inmediatamente después de la instalación y antes de la implementación en un entorno de producción.
M0926	Gestión de Cuentas Privilegiadas	Audita regularmente las cuentas de dominio y locales y sus niveles de permisos para buscar situaciones que puedan permitir a un adversario obtener acceso a nivel de sistema con credenciales de cuenta privilegiada robadas. Estas auditorías también deben identificar si se han habilitado cuentas predeterminadas o si se han creado nuevas cuentas locales que no han sido autorizadas. Sigue las mejores prácticas para el diseño y administración de una red empresarial para limitar el uso de cuentas privilegiadas en los distintos niveles administrativos.

M0918	Gestión de Cuentas de Usuario	Asegúrate de que los usuarios y grupos de usuarios tengan permisos apropiados para sus roles a través de controles de Gestión de Identidad y Acceso (IAM). Implementa controles estrictos de IAM para prevenir el acceso a sistemas, excepto para las aplicaciones, usuarios y servicios que requieren acceso. Implementa cuentas de usuario para cada individuo para hacer cumplir y no repudiar acciones

ESCALADO DE PRIVILEGIOS

El adversario está intentando obtener permisos de nivel superior.

La Escalada de Privilegios consiste en técnicas que los adversarios utilizan para obtener permisos de nivel superior en un sistema o red. Los adversarios pueden entrar y explorar una red con acceso no privilegiado, pero requieren permisos elevados para llevar a cabo sus objetivos. Enfoques comunes incluyen aprovechar debilidades del sistema, configuraciones incorrectas y vulnerabilidades.

Explotación para Escalada de Privilegios

Los adversarios pueden aprovechar vulnerabilidades de software en un intento de elevar privilegios. La explotación de una vulnerabilidad de software ocurre cuando un adversario aprovecha un error de programación en un programa, servicio, o dentro del software del sistema operativo o el propio kernel para ejecutar código controlado por el adversario. Constructos de seguridad como niveles de permisos a menudo dificultarán el acceso a la información y el uso de ciertas técnicas, por lo que es probable que los adversarios necesiten realizar escalada de privilegios para incluir el uso de explotación de software para eludir esas restricciones.

Cuando inicialmente obtienen acceso a un sistema, un adversario puede estar operando dentro de un proceso de privilegios más bajos que les impedirá acceder a ciertos recursos en el sistema. Pueden existir vulnerabilidades, generalmente en componentes del sistema operativo y software que comúnmente se ejecutan con permisos más altos, que pueden ser explotadas para obtener niveles más altos de acceso en el sistema. Esto podría permitir a alguien pasar de permisos sin privilegios o de usuario a permisos de SYSTEM o root dependiendo del componente que sea vulnerable. Este puede ser un paso necesario para un adversario que compromete un sistema de punto final que ha sido configurado correctamente y limita otros métodos de escalada de privilegios.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER tiene la capacidad de explotar un controlador Asrock vulnerable (AsrDrv103.sys) utilizando CVE-2020-15368 para cargar su propio controlador no firmado en el sistema.
S1009	Triton	Triton aprovecha una vulnerabilidad previamente desconocida que afecta a las versiones de firmware Tricon MP3008 10.010.4, lo que permite que una llamada al sistema escrita de forma insegura sea explotada para lograr un primitivo de escritura de 2 bytes arbitrario, que luego se utiliza para obtener privilegios de supervisor.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Pasarela de Datos
A0006	Historiador de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Anfitrión de Salto
A0003	Controlador Lógico Programable (PLC)
A0014	Routers
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Intercepción

Los adversarios pueden engancharse en las funciones de interfaz de programación de aplicaciones (API) utilizadas por los procesos para redirigir llamadas para ejecución y medios de escalada de privilegios. Los procesos de Windows a menudo aprovechan estas funciones de API para realizar tareas que requieren recursos del sistema reutilizables. Las funciones de API de Windows suelen estar almacenadas en bibliotecas de vínculos dinámicos (DLL) como funciones exportadas.

Un tipo de enganche visto en sistemas de control industrial (ICS) implica redirigir llamadas a estas funciones a través de enganches en la tabla de direcciones de

importación (IAT). El enganche en la IAT utiliza modificaciones en la IAT de un proceso, donde se almacenan punteros a funciones de API importadas.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0603	Stuxnet	Stuxnet modifica las tablas de dirección de importación de las DLL para enganchar APIs específicas que se utilizan para abrir archivos de proyecto
S1009	Triton	El inyector de Triton, inject.bin, cambia el puntero de función del comando TriStation 'obtener datos de diagnóstico del procesador principal' a la dirección de imain.bin para que se ejecute antes del controlador norma

Activos Objetivos

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Enrutadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción

M0947	Auditoría	Realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc., para identificar posibles vulnerabilidades. Realizar controles de integridad periódicos del dispositivo para validar la corrección del firmware, software, programas y configuraciones. Los controles de integridad, que típicamente incluyen hashes criptográficos o firmas digitales, deben compararse con los obtenidos en estados válidos conocidos, especialmente después de eventos como reinicios del dispositivo, descargas de programas o reinicios de programas.
M0944	Restringir la Carga de Bibliotecas	Restringir el uso de bibliotecas no confiables o desconocidas, como DLLs remotas o desconocidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0009	Proceso	Ejecución de API del Sistema Operativo	Monitorear las llamadas a API que pueden ser utilizadas para instalar un procedimiento de enganche, como las funciones SetWindowsHookEx y SetWinEventHook. También considerar analizar las cadenas de enganches (que contienen punteros a procedimientos de enganche para cada tipo de enganche) utilizando herramientas o examinando programáticamente estructuras internas del kernel.
		Metadatos del Proceso	Verificar la integridad de los procesos en vivo comparando el código en memoria con el de los binarios estáticos

			correspondientes, específicamente verificando saltos y otras instrucciones que redirigen el flujo del código.

EVASIÓN

El adversario está tratando de evadir las defensas de seguridad.

La Evasión consiste en técnicas que los adversarios utilizan para evitar las defensas técnicas a lo largo de su campaña. Las técnicas utilizadas para la evasión incluyen la eliminación de indicadores de compromiso, el enmascaramiento de comunicaciones y la explotación de vulnerabilidades de software. Los adversarios también pueden aprovechar y abusar de dispositivos y procesos confiables para ocultar su actividad, posiblemente haciéndose pasar por dispositivos maestros o software nativo. Los métodos de evasión de defensa para este propósito suelen ser más pasivos en su naturaleza.

Cambiar Modo de Operación

Los adversarios pueden cambiar el modo de operación de un controlador para obtener acceso adicional a funciones de ingeniería como la Descarga de Programas. Los controladores programables suelen tener varios modos de operación que controlan el estado del programa de usuario y controlan el acceso a la API del controlador. Los modos de operación pueden ser seleccionados físicamente utilizando un interruptor de llave en la cara del controlador, pero también pueden ser seleccionados con llamadas a la API del controlador. Los modos de operación y los mecanismos por los cuales se seleccionan a menudo varían según el proveedor y la línea de productos. Algunos modos de operación comúnmente implementados se describen a continuación:

Programa: Este modo debe estar habilitado antes de que se puedan realizar cambios en el programa de un dispositivo. Esto permite la carga y descarga de programas entre el dispositivo y una estación de trabajo de ingeniería. A menudo, la lógica del PLC se detiene y todas las salidas pueden ser forzadas apagadas.

Ejecución (Run): La ejecución del programa del dispositivo ocurre en este modo. Las entradas y salidas (valores, puntos, etiquetas, elementos, etc.) se monitorean y utilizan de acuerdo con la lógica del programa. La Carga de Programa y la Descarga de Programa están deshabilitadas mientras se encuentra en este modo.

Remoto: Permite cambios remotos en el modo de operación de un PLC.

Parada: El PLC y el programa se detienen, mientras que en este modo, las salidas son forzadas apagadas.

Reinicio: Las condiciones en el PLC se restablecen a sus estados originales. Los reinicios cálidos pueden retener cierta memoria, mientras que los reinicios fríos restablecerán todos los E/S y registros de datos.

Modo de Prueba / Monitoreo: Similar al modo de ejecución, las E/S se procesan, aunque este modo permite el monitoreo, la configuración forzada, los reinicios y, más generalmente, la puesta a punto o depuración del sistema. A menudo, el modo de monitoreo puede ser utilizado como una prueba para la inicialización.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede establecer una conexión HTTP remota para cambiar el modo de operación de los PLCs de Omron.
S1006	PLC-Blaster	PLC-Blaster detiene la ejecución del programa de usuario en el objetivo para permitir la transferencia de su propio código. El gusano luego se copia a sí mismo en el objetivo y posteriormente reinicia el PLC objetivo.
S1009	Triton	Triton tiene la capacidad de detener o ejecutar un programa a través del protocolo TriStation. TsHi.py contiene instancias de las funciones de detención y ejecución siendo ejecutadas.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0801	Gestión de Acceso	Autenticar todo acceso a controladores de campo antes de autorizar el acceso o modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en todo el sistema de control industrial (ICS).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir los cambios de modo de operación solo a usuarios autenticados requeridos (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles. Además, también se pueden utilizar mecanismos físicos (por ejemplo, llaves) para limitar los cambios no autorizados en el modo de operación.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0804	Autenticación de Usuarios Humanos	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuentas, Políticas de Contraseñas y Gestión de Cuentas de Usuario
M0807	Listas de Permitidos de Red	Utilizar listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden utilizarse para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de ingeniería/conocidas.
M0930	Segmentación de Red	Segmentar la red y los sistemas operativos para restringir el acceso a funciones del sistema críticas a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicación del dispositivo que pueden contener información relacionada con cambios en el modo de operación, aunque no todos los dispositivos producen tales registros.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear los protocolos de gestión del ICS para funciones que cambien el modo de operación de un activo.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitorear las alarmas para obtener información sobre cuándo se cambia un modo de operación, aunque no todos los dispositivos producen tales registros.

Explotación para Evasión

Los adversarios pueden aprovechar una vulnerabilidad de software para aprovechar un error de programación en un programa, servicio, o dentro del software del sistema operativo o el propio kernel para evadir la detección. Las vulnerabilidades pueden existir en el software que se puede utilizar para deshabilitar o eludir características de seguridad.

Los adversarios pueden tener conocimiento previo a través del Descubrimiento Remoto de Información del Sistema sobre las características de seguridad implementadas en dispositivos de control. Es probable que estos dispositivos de seguridad sean el objetivo directo de explotación. Hay ejemplos de controles dirigidos por adversarios a comprobaciones de consistencia de RAM/ROM de firmware en dispositivos de control para habilitar la instalación de firmware de sistema malicioso.

Ejemplos de Procedimientos

ID	Nombre	Descripción

S1009	Triton	Triton desactiva una verificación de consistencia de RAM/ROM del firmware después de inyectar una carga útil (imain.bin) en la región de memoria del firmware. Los sistemas Triconex incluyen medios continuos de detección que incluyen sumas de comprobación para la integridad del firmware y del programa, integridad de la memoria y de las referencias de memoria, y configuración.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0014	Enrutadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0948	Aislamiento y Acondicionamiento de Aplicaciones	Dificultar que los adversarios avancen en sus operaciones mediante la explotación de vulnerabilidades no descubiertas o no parcheadas mediante el uso de acondicionamiento. Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto de algunos tipos de explotación. Sin embargo, aún pueden existir riesgos adicionales de exploits y debilidades en estos sistemas.

M0950	Protección contra Explotaciones	Las aplicaciones de seguridad que buscan comportamientos utilizados durante la explotación, como Windows Defender Exploit Guard (WDEG) y Enhanced Mitigation Experience Toolkit (EMET), pueden utilizarse para mitigar algunos
		comportamientos de explotación. La verificación de la integridad del flujo de control es otra forma de identificar y potencialmente detener una explotación de software. Muchas de estas protecciones dependen de la arquitectura y el binario de aplicación objetivo para la compatibilidad y es posible que no funcionen para todo el software o servicios objetivo.
M0919	Programa de Inteligencia de Amenazas	Desarrollar una capacidad robusta de inteligencia de amenazas cibernéticas para determinar qué tipos y niveles de amenaza pueden utilizar exploits de software y vulnerabilidades día cero contra una organización en particular.
M0951	Actualizar el Software	Actualizar el software regularmente mediante la gestión de parches para los puntos finales y servidores empresariales internos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Detectar la explotación de software puede ser difícil dependiendo de las herramientas disponibles. Las explotaciones de software no siempre tienen éxito o pueden hacer que el proceso explotado se vuelva inestable o se bloquee

Eliminación de Indicadores en el Host

Los adversarios pueden intentar eliminar indicadores de su presencia en un sistema en un esfuerzo por cubrir sus huellas. En casos donde un adversario sienta que la detección es inminente, pueden intentar sobrescribir, eliminar o encubrir los cambios que han realizado en el dispositivo.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0607	KillDisk	KillDisk elimina los registros de aplicaciones, seguridad, configuración y eventos del sistema de los sistemas Windows.
S1009	Triton	Triton restablecería el controlador al estado anterior sobre TriStation y, si esto fallaba, escribiría un programa ficticio en la memoria, probablemente en un intento de anti-forense.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0922	Restringir Permisos de Archivos y Directorios	Proteger los archivos almacenados localmente con permisos adecuados para limitar las oportunidades para que los adversarios eliminen indicadores de su actividad en el sistema.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos que pueden eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.

DS0022	Archivo	Eliminación de Archivos	Monitorear la presencia de un archivo que puede eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.
		Metadatos de Archivos	Monitorear datos contextuales de archivos que pueden mostrar signos de eliminación o alteración de artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.
		Modificación de Archivos	Monitorear cambios realizados en un archivo que pueden eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena
DS0009	Proceso	Ejecución de API del Sistema Operativo	Monitorear llamadas a API que pueden eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.

		Creación de Procesos	Monitorear procesos recién ejecutados que pueden eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.
DS0024	Registro de Windows	Eliminación de Claves del Registro de Windows	Monitorear claves del registro de Windows que pueden ser eliminadas o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena.
			Para obtener más contexto sobre los procedimientos de adversarios y antecedentes, consulte la Eliminación de Indicadores y sub-técnicas aplicables.
		Modificación de Claves del Registro de Windows	Monitorear cambios realizados en las claves o valores del Registro de Windows que pueden eliminar o alterar artefactos generados en un sistema host, incluidos registros o archivos capturados como malware en cuarentena. Para obtener más contexto sobre los procedimientos de adversarios y antecedentes, consulte la Eliminación de Indicadores y sub-técnicas aplicables.

Enmascaramiento

Los adversarios pueden utilizar el enmascaramiento para disfrazar una aplicación o ejecutable malicioso como otro archivo, para evitar la sospecha de operadores e ingenieros. Posibles disfraces de estos archivos de enmascaramiento pueden incluir programas comúnmente encontrados, ejecutables y archivos de configuración esperados del proveedor, y otras convenciones de nombres de aplicaciones y archivos

comunes. Al hacerse pasar por archivos y aplicaciones esperados y relevantes para el proveedor, los operadores e ingenieros pueden no notar la presencia del contenido malicioso subyacente y posiblemente terminar ejecutando esos archivos que se disfrazan como funciones legítimas.

Aplicaciones y otros archivos comúnmente encontrados en sistemas Windows o en estaciones de trabajo de ingeniería han sido suplantados antes. Esto puede ser tan simple como cambiar el nombre de un archivo para disfrazarlo efectivamente en el entorno de ICS.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0025	Ataque al Suministro Eléctrico de Ucrania de 2016	Durante el Ataque al Suministro Eléctrico de Ucrania de 2016, el equipo Sandworm transfirió archivos ejecutables como .txt y luego los renombró como .exe, probablemente para evitar la detección a través del seguimiento de extensiones.
S0605	EKANS	EKANS se disfraza como un ejecutable válido con el nombre de archivo update.exe. Muchos programas válidos utilizan el nombre de proceso update.exe para realizar actualizaciones de software en segundo plano.
S0496	REvil	REvil busca si el servicio autoup.exe de Ahnlab está en ejecución en el sistema objetivo e inyecta su carga útil en este proceso existente.
S0603	Stuxnet	Stuxnet renombra s7otbxdx.dll, una dll responsable de manejar comunicaciones con un PLC. Reemplaza este archivo dll con su propia versión que le permite interceptar cualquier llamada que se haga para acceder al PLC.
S1009	Triton	El inyector de Triton, inject.bin, se disfraza como un programa PowerPC compilado estándar para el Tricon. Triton se configuró para hacerse pasar por trilog.exe, que es el software Triconex para analizar los registros SIS.

Activos Objetivo

ID	Activo

A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0012	Host de Salto
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0945	Firma de Código	Requerir binarios firmados.
M0938	Prevención de Ejecución	Utilizar herramientas que restrinjan la ejecución del programa mediante el control de aplicaciones por
		atributos distintos al nombre de archivo para utilidades comunes del sistema y de la aplicación.
M0922	Restringir Permisos de Archivos y Directorios	Utilizar controles de acceso del sistema de archivos para proteger las carpetas del sistema y de la aplicación.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.

DS0022	Archivo	Metadatos de Archivos	Recopilar hashes de archivos. Monitorear nombres de archivos que no coincidan con su hash esperado. Realizar monitoreo de archivos. Los archivos con nombres conocidos pero en ubicaciones inusuales son sospechosos. Buscar indicaciones de caracteres comunes que puedan indicar un intento de engañar a los usuarios para que identifiquen incorrectamente el tipo de archivo, como un espacio como el último carácter de un nombre de archivo o los caracteres de anulación de derecha a izquierda "\u202E", "[U+202E]" y "%E2%80%AE".
		Modificación de Archivos	Monitorear los cambios realizados en archivos fuera de una actualización o parche que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.
DS0009	Proceso	Metadatos del Proceso	Monitorear nombres de archivos que no coincidan entre el nombre de archivo en el disco y el de los metadatos del binario. Este es un indicador probable de que un binario fue renombrado después de ser compilado.

DS0003	Tarea Programada	Creación de Tareas Programadas	Monitorear tareas programadas recién construidas que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.
		Modificación de Tareas Programadas	Monitorear cambios realizados en tareas programadas que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.
DS0019	Servicio	Creación de Servicios	Monitorear servicios/daemons recién construidos que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.
		Modificación de Servicios	Monitorear cambios realizados en servicios que puedan intentar manipular características de sus artefactos para que parezcan legítimos o benignos para los usuarios y/o herramientas de seguridad.

Rootkit

Los adversarios pueden desplegar rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Los rootkits son programas que ocultan la existencia de malware al interceptar y modificar las llamadas a las API del sistema operativo que suministran información del sistema. Los rootkits o la funcionalidad que permite los rootkits pueden residir en el nivel de usuario o en el núcleo del sistema operativo, o incluso más bajo.

Los rootkits de firmware que afectan al sistema operativo otorgan un control casi completo del sistema. Si bien los rootkits de firmware normalmente se desarrollan para la placa principal de procesamiento, también pueden desarrollarse para la E/S que está conectada a un activo. El compromiso de este firmware permite la modificación de todas las variables y funciones del proceso en las que se involucra el módulo. Esto puede provocar que se ignoren comandos y se alimenten falsas información al dispositivo principal. Al manipular los procesos del dispositivo, un adversario puede inhibir sus funciones de respuesta esperadas y posiblemente habilitar el Impacto.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0603	Stuxnet	Uno de los rootkits de Stuxnet está contenido completamente en el falso s7otbxdx.dll. Para continuar existiendo sin ser detectado en el PLC, debe tener en cuenta al menos las siguientes situaciones: solicitudes de lectura para sus propios bloques de código malicioso, solicitudes de lectura para bloques infectados (OB1, OB35, DP_RECV) y solicitudes de escritura que podrían sobrescribir el propio código de Stuxnet. Stuxnet contiene código para monitorear e interceptar estos tipos de solicitudes. El rootkit modifica estas solicitudes para que el código PLC de Stuxnet no sea descubierto o dañado.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Auditar la integridad del sistema PLC y la funcionalidad del código de la aplicación, como la manipulación de bloques de función estándar (por ejemplo, Bloques Organizacionales) que gestionan la ejecución de programas de lógica de aplicación.
M0945	Firma de Código	Las firmas digitales pueden ser utilizadas para asegurar que las DLLs de la aplicación sean auténticas antes de su ejecución.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0001	Firmware	Modificación de Firmware	Monitorear los cambios realizados en el firmware para detectar modificaciones inesperadas en la configuración y/o datos que puedan ser utilizados por rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Se deben consultar los
			sistemas de gestión de activos para comprender las versiones y configuraciones de firmware conocidas y válidas.

Mensaje de Reporte Falsificado

Los adversarios pueden falsificar mensajes de reporte en entornos de sistemas de control para evasión y para impedir el control del proceso. En los sistemas de control, los mensajes de reporte contienen datos de telemetría (por ejemplo, valores de E/S) relacionados con el estado actual del equipo y el proceso industrial. Los mensajes de reporte son importantes para monitorear la operación normal de un sistema o identificar eventos importantes como desviaciones de los valores esperados.

Si un adversario tiene la capacidad de Falsificar Mensajes de Reporte, pueden impactar el sistema de control de muchas maneras. El adversario puede falsificar mensajes de reporte que indiquen que el proceso está funcionando normalmente, como una forma de evasión. El adversario también podría falsificar mensajes de reporte para hacer que los defensores y operadores piensen que están ocurriendo otros errores para distraerlos de la fuente real de un problema.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0020	Violación de Maroochy Water	En la Violación de Maroochy Water, el adversario utilizó un sistema de radio bidireccional analógico dedicado para enviar datos falsos e instrucciones a estaciones de bombeo y al ordenador central.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. Si no es así, utilice dispositivos de inserción en línea o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de admitir esto (por ejemplo, controladores heredados, RTUs).
M0937	Filtrar Tráfico de Red	Realice la lista blanca en línea de los comandos de protocolos de automatización para evitar que los dispositivos envíen mensajes de comando o de informe no autorizados. Las técnicas de lista de permitidos/lista de denegados deben diseñarse con suficiente precisión para evitar el bloqueo no deseado de mensajes de informe válidos.
M0807	Listas Blancas de Red	Utilice listas blancas basadas en el host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas blancas pueden ser utilizadas para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de
		gestión/ingeniería conocidas.

M0930	Segmentación de Red	Segmente los activos operativos y sus dispositivos de gestión según su función dentro del proceso. Permita un aislamiento más estricto para la información de control y operacional más crítica dentro del entorno de control.
M0813	Autenticación de Procesos de Software y Dispositivos	Los dispositivos deben autenticar todos los mensajes entre activos maestros y de estación externa.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Los mensajes de informes falsificados pueden ser detectados revisando el contenido de los protocolos de automatización, ya sea mediante la detección basada en valores esperados o comparando con otras fuentes de datos de proceso fuera de banda. Los mensajes falsificados pueden no coincidir exactamente con los mensajes legítimos, lo que puede llevar a un tráfico malformado, aunque el tráfico puede estar malformado por muchas razones benignas. Monitorear mensajes de informes para cambios en cómo están construidos. Varias técnicas permiten falsificar un mensaje de informe. Considere

			monitorear la actividad de Maestro Falso y Adversarioen-Medio.
		Flujo de Tráfico de Red	Varias técnicas permiten falsificar un mensaje de informe. Considere monitorear la actividad de Maestro Falso y Adversarioen-Medio que pueden preceder a esta técnica.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitorear los registros de activos para alarmas u otra información que el adversario no pueda suprimir directamente. Las alarmas relevantes incluyen las de pérdida de comunicaciones debido a la actividad de Adversario-enMedio.
DS0024	Registro de Windows	Modificación de Claves del Registro de Windows	Varias técnicas permiten falsificar un mensaje de informe. Monitoree el envenenamiento LLMNR/NBT-NS a través de nuevos servicios/daemons que pueden ser utilizados para habilitar esta técnica. Para obtener más contexto sobre los procedimientos de adversarios y antecedentes, consulte Envenenamiento LLMNR/NBT-NS y Relevación de SMB.

DESCUBRIMIENTO

El adversario está localizando información para evaluar e identificar sus objetivos en tu entorno.

El Descubrimiento consiste en técnicas que los adversarios utilizan para examinar tu entorno ICS y obtener conocimiento sobre la red interna, los dispositivos del sistema de control y cómo interactúan sus procesos. Estas técnicas ayudan a los adversarios a

observar el entorno y determinar los próximos pasos para la selección de objetivos y el Movimiento Lateral. También les permiten explorar lo que pueden controlar y obtener información sobre las interacciones entre varios procesos del sistema de control. Las técnicas de descubrimiento son often una acción de progresión en el entorno que permite al adversario orientarse antes de decidir cómo actuar. Los adversarios pueden utilizar técnicas de Descubrimiento que resulten en Recolección, para ayudar a determinar cómo los recursos disponibles benefician su objetivo actual. Una combinación de comunicaciones y funciones de dispositivos nativos, así como herramientas personalizadas, se utilizan a menudo para este objetivo de recopilación de información post-compromiso.

Enumeración de Conexiones de Red

Los adversarios pueden realizar la enumeración de conexiones de red para descubrir información sobre los patrones de comunicación de los dispositivos. Si un adversario puede inspeccionar el estado de una conexión de red con herramientas como Netstat, en conjunto con Firmware del Sistema, entonces pueden determinar el rol de ciertos dispositivos en la red. El adversario también puede usar el Sniffing de Red para observar el tráfico de red en busca de detalles sobre la fuente, destino, protocolo y contenido.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0605	EKANS	EKANS realiza una búsqueda DNS de un nombre de dominio interno asociado con su red objetivo para identificar si fue desplegado en el sistema previsto.
S0604	Industroyer	Industroyer contiene un módulo IEC 61850 que enumera todos los adaptadores de red conectados para determinar sus máscaras de subred TCP/IP.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)

A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0816	Mitigación Limitada o No Efectiva	La enumeración de conexiones de red probablemente se obtiene utilizando herramientas de sistema comunes (por ejemplo, netstat, ipconfig).

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos que pueden buscar detalles sobre la configuración y ajustes de red, como direcciones IP y/o MAC, de sistemas a los que acceden o a través del descubrimiento de información de sistemas remotos. También monitorear comandos ejecutados y argumentos que pueden intentar obtener un listado de conexiones de red hacia o desde el sistema comprometido al que están accediendo actualmente o desde sistemas remotos consultando información a través de la red.

DS0009	Proceso	Ejecución de API del SO	Monitorear llamadas a API (como GetAdaptersInfo() y GetIpNetTable()) que pueden recopilar detalles sobre la configuración y ajustes de red, como direcciones IP y/o MAC. También monitorear llamadas a API que pueden intentar obtener un listado
			de conexiones de red hacia o desde el sistema comprometido al que están accediendo actualmente o desde sistemas remotos consultando información a través de la red.
		Creación de Procesos	Monitorear procesos ejecutados (como ipconfig/ifconfig y arp) con argumentos que pueden buscar detalles sobre la configuración y ajustes de red, como direcciones IP y/o MAC. También monitorear procesos ejecutados que pueden intentar obtener un listado de conexiones de red hacia o desde el sistema comprometido al que están accediendo actualmente o desde sistemas remotos consultando información a través de la red.

DS0012	Script	Ejecución de Script	Monitorear cualquier intento de habilitar scripts en un sistema se consideraría sospechoso. Si los scripts no se usan comúnmente en un sistema, pero están habilitados, los scripts que se ejecutan fuera del ciclo de parches u otras funciones de administrador son sospechosos. Los scripts deben ser capturados del sistema de archivos cuando sea posible para determinar sus acciones e intenciones.

Intercepción de red

La intercepción de red es la práctica de utilizar una interfaz de red en un sistema informático para monitorear o capturar información, independientemente de si es el destino especificado para la información. Un adversario puede intentar espiar el tráfico para obtener información sobre el objetivo. Esta información puede variar en nivel de importancia. La información relativamente no importante son las comunicaciones generales hacia y desde las máquinas. La información relativamente importante sería la información de inicio de sesión. Las credenciales de usuario pueden enviarse a través de un protocolo no cifrado, como Telnet, que puede ser capturado y obtenido a través del análisis de paquetes de red. Además, el envenenamiento de ARP y el Servicio de Nombres de Dominio (DNS) pueden usarse para capturar credenciales de sitios web, proxies y sistemas internos al redirigir el tráfico a un adversario.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede desplegar Tcpdump para espiar el tráfico de red y recolectar archivos PCAP.

S0603	Stuxnet	DP_RECV es el nombre de un bloque de función estándar utilizado por coprocesadores de red. Se utiliza para recibir tramas de red en el Profibus, un bus de red industrial estándar utilizado para la E/S distribuida. El bloque original se copia en FC1869 y luego se reemplaza por un bloque malicioso. Cada vez que se utiliza la función para recibir un paquete, el bloque malicioso de Stuxnet toma el control: llamará al DP_RECV original en FC1869 y luego realizará un postprocesamiento en los datos del paquete. El bloque DP_RECV reemplazado (más tarde referido como el monitor DP_RECV) está destinado a monitorear los datos enviados por los convertidores de frecuencia a la CPU 315-2 a través de los módulos de comunicación Profibus CP 342-5.
S1010	VPNFilter	El sniffer de paquetes de VPNFilter busca autenticación básica y monitorea el tráfico de ICS, y es específico para el TP-LINK R600-VPN. El malware utiliza un socket en bruto para buscar conexiones a una dirección IP predefinida, solo observando los paquetes TCP que tienen 150 bytes o más. Los paquetes que no están en el puerto 502 son escaneados en busca de BasicAuth, y esa información se registra. Esto puede haber permitido la recolección de
		credenciales de comunicaciones entre dispositivos que acceden a un HMI habilitado para Modbus.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0808	Encriptación del Tráfico de Red	Asegurar que el tráfico cableado y/o inalámbrico esté encriptado cuando sea posible. Usar las mejores prácticas para protocolos de autenticación, como Kerberos, y garantizar que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
M0932	Autenticación Multifactorial	Utilizar autenticación multifactorial siempre que sea posible.
M0930	Segmentación de Redes	Segmentar redes y sistemas adecuadamente para reducir el acceso a comunicaciones críticas de sistemas y servicios.
M0926	Gestión de Cuentas Privilegiadas	Restringir el acceso de root o administrador en cuentas de usuario para limitar la capacidad de capturar tráfico promiscuo en una red a través de herramientas comunes de captura de paquetes.
M0814	Configuración de Red Estática	Las entradas ARP definidas estáticamente pueden prevenir la manipulación y el espionaje del tráfico de red conmutada, ya que algunas técnicas de AiTM dependen del envío de mensajes ARP falsificados para manipular las tablas ARP dinámicas de los hosts de red.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos para acciones que ayuden a espiar el tráfico de red para capturar información sobre un entorno.
DS0009	Proceso	Creación de Procesos	Monitorear procesos recién ejecutados que puedan ayudar a espiar el tráfico de red para capturar información sobre un entorno.

Descubrimiento remoto de sistemas.

Los adversarios pueden intentar obtener un listado de otros sistemas por dirección IP, nombre de host u otro identificador lógico en una red que pueda ser utilizado para

técnicas posteriores de Movimiento Lateral o Descubrimiento. La funcionalidad podría existir dentro de herramientas de adversarios para habilitar esto, pero también podrían utilizarse utilidades disponibles en el sistema operativo o software del proveedor.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm descubrió de forma remota activos operacionales una vez en la red OT.
S0093	Backdoor.Oldrea	El complemento de malware ICS Backdoor.Oldrea se basa en la red de Windows (WNet) para descubrir todos los servidores, incluidos los servidores OPC, que son accesibles desde la máquina comprometida a través de la red.
S1045	INCONTROLLER	INCONTROLLER puede realizar un escaneo de multidifusión UDP del puerto UDP 27127 para identificar PLCs Schneider que utilizan ese puerto para el protocolo NetManage. INCONTROLLER puede utilizar el protocolo FINS (Factory Interface Network Service) para escanear y obtener la dirección MAC asociada con dispositivos Omron.
		INCONTROLLER tiene la capacidad de realizar escaneos para el puerto TCP 4840 para identificar dispositivos que ejecutan servidores OPC UA.
S0604	Industroyer	El componente de carga útil IEC 61850 de Industroyer tiene la capacidad de descubrir dispositivos relevantes en la subred de la red del host infectado intentando conectarse al puerto 102. Industroyer contiene un módulo OPC DA que enumera todos los servidores OPC utilizando el método ICatInformation::EnumClassesOfCategories con el identificador de categoría CATID_OPCDAServer20 y IOPCServer::GetStatus para identificar los que están en ejecución.
S1006	PLC-Blaster	PLC-Blaster escanea la red para encontrar otros dispositivos PLC Siemens S7 para infectar. Localiza estos dispositivos comprobando si hay un servicio escuchando en el puerto TCP 102.
S1009	Triton	Triton utiliza un script de Python que es capaz de detectar controladores Triconex en la red enviando un paquete de difusión UDP específico sobre el puerto 1502.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0814	Configuración de Red Estática	Los entornos ICS típicamente tienen más dispositivos definidos estáticamente, por lo tanto, minimice el uso tanto de protocolos de descubrimiento de TI (por ejemplo, DHCP,
		LLDP) como de funciones de descubrimiento en protocolos de automatización.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0022	Archivo	Acceso a Archivos	Monitorear archivos (como /etc/hosts) que están siendo accedidos y que pueden intentar obtener una lista de otros sistemas por dirección IP, nombre de host u otro identificador lógico en una red que pueda ser utilizada para el Movimiento Lateral desde el sistema actual.

DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear anomalías relacionadas con funciones de descubrimiento de ICS, incluidos dispositivos que previamente no han utilizado estas funciones o para funciones que se envían a muchos subsistemas. Tenga en cuenta que algunos protocolos ICS usan funcionalidades de difusión o multidifusión, lo que puede producir falsos positivos.
		Flujo de Tráfico de Red	Monitorear nuevas conexiones de protocolos ICS a activos existentes o para escaneo de dispositivos (es decir, un host conectándose a muchos dispositivos) sobre protocolos ICS y empresariales (por ejemplo, ICMP, DCOM, WinRM). Para obtener más contexto sobre los procedimientos y antecedentes empresariales del adversario, consulta el
			descubrimiento remoto del sistema.
DS0009	Proceso	Creación de Procesos	Monitorea los procesos recién ejecutados que pueden ser utilizados para descubrir sistemas remotos, como ping.exe y tracert.exe, especialmente cuando se ejecutan rápidamente en sucesión. Considera monitorear nuevos procesos que participan en actividades de escaneo o se conectan a múltiples sistemas correlacionando

			datos de creación de procesos de red.

Descubrimiento remoto de información del sistema.

Un adversario puede intentar obtener información detallada sobre sistemas remotos y sus periféricos, como marca/modelo, función y configuración. Los adversarios pueden utilizar información del Descubrimiento remoto de información del sistema para ayudar en la selección y configuración de comportamientos posteriores. Por ejemplo, el rol operacional y la información del modelo del sistema pueden dictar si es un objetivo relevante para los objetivos operacionales del adversario. Además, la configuración del sistema puede ser utilizada para delimitar el uso de técnicas posteriores.

Las solicitudes de información del sistema suelen implementarse utilizando protocolos de automatización y gestión, y a menudo son solicitadas automáticamente por el software del proveedor durante la operación normal. Esta información puede ser utilizada para adaptar acciones de gestión, como la descarga de programas y firmware del sistema o del módulo. Un adversario puede aprovechar esta misma información emitiendo llamadas directamente a la API del sistema.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0093	Backdoor.Oldrea	El payload Backdoor.Oldrea recopila información del servidor que incluye CLSID, nombre del servidor, ID de programa, versión de OPC, información del proveedor, estado de ejecución, cantidad de grupos y ancho de banda del servidor. Esta información ayuda a indicar el papel que tiene el servidor en el proceso de control.
S1045	INCONTROLLER	INCONTROLLER incluye una biblioteca que crea conexiones Modbus con un dispositivo para solicitar su ID de dispositivo.

S0604	Industroyer	El componente IEC 61850 de Industroyer envía la solicitud MMSgetNameList específica del dominio para determinar qué nodos lógicos soporta el dispositivo. Luego, busca los nodos lógicos para el valor CSW, que indica que el dispositivo realiza una función de control de interruptores o de circuito. El módulo OPC DA de Industroyer también utiliza IOPCBrowseServerAddressSpace para buscar elementos con las siguientes cadenas: ctlSelOn, ctlOperOn, ctlSelOff, ctlOperOff, Pos y stVal. El módulo IEC 60870-5-104 de Industroyer incluye un modo de rango para descubrir Direcciones de Objetos de Información (IOAs) enumerando cada una.
S1072	Industroyer2	Industroyer2 tiene la capacidad de sondear un dispositivo objetivo sobre su estado de conexión, estado de transferencia de datos, Dirección Común (CA), Direcciones de Objetos de Información (IOAs) y valores de estado de IO a través de múltiples niveles de prioridad.
S0603	Stuxnet	Stuxnet enumera y analiza los Bloques de Datos del Sistema (SDB) utilizando las llamadas API s7blk_findfirst y s7blk_findnext en s7otbxdx.dll. Stuxnet debe encontrar un SDB con el DWORD en el desplazamiento 50h igual a 0100CB2Ch. Esto especifica que el sistema utiliza el módulo procesador de comunicaciones Profibus CP 3425. Además, se buscan y cuentan valores específicos: 7050h y 9500h. 7050h está asignado al número de parte KFC750V3 que parece ser un convertidor de frecuencia (también conocido como variador de frecuencia) fabricado por Fararo Paya en Teherán, Irán. 9500h está asignado a convertidores de frecuencia Vacon NX fabricados por Vacon con sede en Finlandia. Stuxnet estaba dirigido específicamente a las CPU 6ES7315-2 (Serie 300) con características especiales de bloque de datos del sistema para la secuencia A o B y 6ES7-3152 para la secuencia C. El tipo de PLC también se puede verificar utilizando la API s7ag_read_szl.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones

A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0814	Configuración de Red Estática	Los entornos de ICS típicamente tienen dispositivos más estáticamente definidos, por lo tanto, minimice el uso de protocolos de descubrimiento de TI (por ejemplo, DHCP, LLDP) y funciones de descubrimiento en protocolos de automatización. Ejemplos de protocolos de automatización con capacidades de descubrimiento incluyen Descubrimiento de Dispositivos OPC UA, BACnet y Ethernet/IP.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0022	Archivo	Acceso a Archivo	Monitoree los archivos (como /etc/hosts) que se están accediendo y que pueden intentar obtener una lista de otros sistemas por dirección IP, nombre de host u otro identificador lógico en una red que pueda usarse para Movimiento Lateral desde el sistema actual.

DS0029	Trafico de Red	Contenido del Trafico de Red	Monitoree anomalías relacionadas con funciones de descubrimiento de ICS, incluidos dispositivos que no hayan utilizado previamente estas funciones o funciones que se envíen a muchas estaciones exteriores. Tenga en cuenta que algunos protocolos de ICS utilizan funcionalidades de difusión o multidifusión, lo que puede producir falsos positivos. También monitoree hosts que enumeren recursos conectados a la red utilizando protocolos empresariales no ICS.
		Flujo de Trafico de Red	Monitoree nuevas conexiones de protocolos de ICS a activos existentes o para el escaneo de dispositivos (es decir, un host que se conecta a muchos dispositivos) sobre protocolos de ICS y empresariales (por ejemplo, ICMP, DCOM, WinRM).
DS0009	Proceso	Creación de Procesos	Monitoree procesos recién ejecutados que pueden usarse para descubrir sistemas remotos, como ping.exe y tracert.exe, especialmente cuando se ejecutan en rápida sucesión. Considere monitorear nuevos procesos que participen en actividades de escaneo o que se conecten a

			múltiples sistemas correlacionando datos de
			red de creación de procesos.

Espionaje inalámbrico

El espionaje inalámbrico consiste en la captura de comunicaciones de radiofrecuencia (RF) utilizadas para el control remoto y la transmisión de información en entornos distribuidos. Las frecuencias de comunicación RF varían entre 3 kHz y 300 GHz, aunque comúnmente se encuentran entre 300 MHz y 6 GHz. La longitud de onda y la frecuencia de la señal afectan cómo se propaga la señal a través del aire libre, obstáculos (como paredes y árboles) y el tipo de radio necesario para capturarlas. Estas características suelen estandarizarse en el protocolo y el hardware, y pueden afectar cómo se captura la señal. Algunos ejemplos de protocolos inalámbricos que pueden encontrarse en entornos ciberfísicos son: WirelessHART, Zigbee, WIA-FA y el Espectro de Seguridad Pública de 700 MHz.

Los adversarios pueden capturar comunicaciones RF utilizando hardware especializado, como radio definida por software (SDR), radio portátil o una computadora con un demodulador de radio sintonizado a la frecuencia de comunicación. La información transmitida a través de un medio inalámbrico puede ser capturada en tránsito, ya sea que el dispositivo de espionaje sea el destino previsto o no. Esta técnica puede ser particularmente útil para un adversario cuando las comunicaciones no están cifradas.

En el incidente de la sirena de Dallas en 2017, se sospecha que los adversarios capturaron probablemente emisiones de mensajes de comando inalámbricos en una frecuencia de 700 MHz durante una prueba regular del sistema. Estos mensajes fueron posteriormente reproducidos para activar los sistemas de alarma.

Activos Objetivo

ID	Activo
A0013	E/S de Campo

A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0808	Cifrar el Tráfico de Red	Utilice técnicas y protocolos criptográficos sólidos para evitar el espionaje en las comunicaciones de red.
M0806	Minimizar la Propagación de Señales Inalámbricas	Reduzca el alcance de las comunicaciones de RF a su rango de funcionamiento previsto cuando sea posible. Los métodos de reducción de propagación pueden incluir (i) reducir la potencia de transmisión en las señales
		inalámbricas, (ii) ajustar la ganancia de la antena para evitar extensiones más allá de los límites organizacionales y (iii) emplear técnicas de blindaje de RF para bloquear la propagación excesiva de la señal.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0029	Trafico de Red	Flujo de Trafico de Red	El espionaje de red puramente pasivo no puede detectarse de manera efectiva. En casos donde el adversario interactúa con la red inalámbrica (por ejemplo, uniéndose a una red Wi-Fi), la detección puede ser posible. Monitoree flujos de tráfico de red nuevos o irregulares que puedan indicar dispositivos o sesiones potencialmente no deseados en redes inalámbricas. En redes WiFi, monitoree cambios como puntos de acceso falsos o baja intensidad de señal, lo que indica que un dispositivo está más lejos del punto de acceso de lo esperado y cambios en la señal de la capa física. El contenido del tráfico de red proporcionará un contexto importante, como direcciones de hardware (por ejemplo, MAC), cuentas de usuario y tipos de mensajes enviados.

MOVIMIENTO LATERAL

El adversario está intentando moverse a través de tu entorno ICS.

El Movimiento Lateral consiste en técnicas que los adversarios utilizan para entrar y controlar sistemas remotos en una red. Estas técnicas abusan de credenciales predeterminadas, cuentas conocidas y servicios vulnerables, y también pueden aprovechar dispositivos de doble homologación y sistemas que residen tanto en las redes de IT como en las de OT. El adversario utiliza estas técnicas para pivotar hacia su próximo punto en el entorno, posicionándose donde quieren estar o creen que deberían estar. Para cumplir su objetivo principal, a menudo requieren Descubrir la red

y Recopilar información para desarrollar conciencia sobre dispositivos y procesos ICS únicos, con el fin de encontrar su objetivo y posteriormente obtener acceso a él. Alcanzar este objetivo a menudo implica pivotar a través de múltiples sistemas, dispositivos y cuentas. Los adversarios pueden instalar sus propias herramientas remotas para lograr el Movimiento Lateral o aprovechar herramientas predeterminadas, programas y credenciales legítimas nativas de la red, que pueden ser más sigilosas.

Credenciales predeterminadas.

Los adversarios pueden aprovechar las credenciales predeterminadas establecidas por el fabricante o proveedor en dispositivos de sistemas de control. Estas credenciales predeterminadas pueden tener permisos administrativos y pueden ser necesarias para la configuración inicial del dispositivo. Es una práctica recomendada cambiar las contraseñas de estas cuentas lo antes posible, pero algunos fabricantes pueden tener dispositivos que tengan contraseñas o nombres de usuario que no se pueden cambiar.

Las credenciales predeterminadas suelen estar documentadas en un manual de instrucciones que se incluye con el dispositivo, se publica en línea a través de medios oficiales o se publica en línea a través de medios no oficiales. Los adversarios pueden aprovechar las credenciales predeterminadas que no han sido modificadas o deshabilitadas correctamente.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Ruteadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Asegúrese de que los controles integrados y los dispositivos de red estén protegidos mediante la gestión de acceso, ya que estos dispositivos suelen tener cuentas predeterminadas desconocidas que podrían usarse para obtener acceso no autorizado.
M0927	Políticas de Contraseñas	Revise los documentos de los proveedores y las alertas de seguridad en busca de credenciales predeterminadas potencialmente desconocidas o pasadas por alto dentro de los dispositivos existentes.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0028	Sesión de Inicio	Sesión de Inicio de Sesión	Monitoree las sesiones de inicio de sesión para detectar el uso de credenciales predeterminadas.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitoree el tráfico de red en busca del uso de credenciales
			predeterminadas en protocolos que permiten la autenticación no cifrada.

Explotación de servicios remotos.

La explotación de servicios remotos ocurre cuando los adversarios aprovechan una vulnerabilidad de software para aprovechar un error de programación en un programa, servicio o dentro del propio software del sistema operativo o kernel para habilitar el abuso de servicios remotos. Un objetivo común para la explotación posterior al compromiso de servicios remotos es obtener acceso inicial y movimiento lateral dentro del entorno de ICS para permitir el acceso a sistemas específicos.

Los propietarios y operadores de activos de ICS se han visto afectados por ransomware (o malware disruptivo que se hace pasar por ransomware) que migra de la TI empresarial a entornos de ICS: WannaCry, NotPetya y BadRabbit. En cada uno de estos casos, el malware autorreproducible (gusano) infectó inicialmente redes de TI, pero a través de la explotación (especialmente la vulnerabilidad MS17-010 que apunta a SMBv1) se propagó a redes industriales, produciendo impactos significativos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0606	Bad Rabbit	Bad Rabbit inicialmente infectó redes de TI, pero mediante un exploit (particularmente la vulnerabilidad MS17-010 que apunta a SMBv1) se propagó a redes industriales.
S0368	NotPetya	NotPetya inicialmente infectó redes de TI, pero mediante un exploit (particularmente la vulnerabilidad MS17-010 que apunta a SMBv1) se propagó a redes industriales.
S0603	Stuxnet	Stuxnet ejecuta comandos SQL maliciosos en el servidor de base de datos WinCC para propagarse a sistemas remotos. Los comandos SQL maliciosos incluyen xp_cmdshell, sp_dumpdbilog y sp_addextendedproc.
S0366	WannaCry	WannaCry inicialmente infectó redes de TI, pero mediante un exploit (particularmente la vulnerabilidad MS17-010 que apunta a SMBv1) se propagó a redes industriales.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Ruteadores
A0010	Controlador de Seguridad

A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0948	Aislamiento y Contención de Aplicaciones	Dificulte el avance de los adversarios en su operación mediante la explotación de vulnerabilidades no descubiertas o no parcheadas mediante el uso de contención de aplicaciones. Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto de algunos tipos de explotación. Sin embargo, aún pueden existir riesgos de exploits adicionales y debilidades en estos sistemas.
M0942	Deshabilitar o Eliminar Funciones o Programas	Asegúrese de que los puertos y servicios innecesarios estén cerrados para prevenir el riesgo de descubrimiento y posible explotación.
M0950	Protección contra Exploits	Las aplicaciones de seguridad que buscan comportamientos utilizados durante la explotación, como Windows Defender Exploit Guard (WDEG) y la Enhanced Mitigation Experience Toolkit (EMET), pueden usarse para mitigar algunos comportamientos de explotación. La verificación de la integridad del flujo de control es otra forma de identificar y posiblemente detener un exploit de software. Muchas de estas protecciones dependen de la arquitectura y el binario de la aplicación objetivo para su compatibilidad y pueden no funcionar para todo el software o servicios objetivo.
M0930	Segmentación de Redes	Segmentar redes y sistemas de manera apropiada para reducir el acceso a comunicaciones de sistemas y servicios críticos.
M0926	Gestión de Cuentas Privilegiadas	Minimice los permisos y el acceso para las cuentas de servicio para limitar el impacto de la explotación.
M0919	Programa de Inteligencia de Amenazas	Desarrolle una capacidad de inteligencia de amenazas cibernéticas robusta para determinar qué tipos y niveles de amenazas pueden utilizar exploits de software y 0days contra una organización en particular.
M0951	Actualizar Software	Actualice regularmente el software mediante la gestión de parches para puntos finales y servidores internos de la empresa.

M0916	Escaneo de Vulnerabilidades	Escanee regularmente la red interna en busca de servicios disponibles para identificar servicios nuevos y potencialmente vulnerables.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Detectar la explotación de software puede ser difícil según las herramientas disponibles. Los exploits de software no siempre tienen éxito o pueden hacer que el proceso explotado se vuelva inestable o se bloquee, lo que puede registrarse en el log de la aplicación.
DS0029	Trafico de Red	Contenido del Trafico de Red	Utilice la inspección profunda de paquetes para buscar artefactos de tráfico de exploits comunes, como payloads conocidos.

Credenciales codificadas en el código.

Las credenciales codificadas en el código se refieren a aquellas que están integradas en el software o firmware y que pueden ser aprovechadas por adversarios para obtener una sesión de usuario interactiva no autorizada en un activo. Ejemplos de credenciales que pueden estar codificadas en un activo incluyen:

- Nombres de usuario/contraseñas
- Claves criptográficas/Certificados
- Tokens de API

A diferencia de las Credenciales Predeterminadas, estas credenciales están integradas en el sistema de una manera que o bien no pueden ser cambiadas por el propietario del activo, o puede ser poco factible cambiarlas debido al impacto que causaría en la operación del sistema de control. Estas credenciales pueden ser reutilizadas en líneas de productos completas o modelos de dispositivos y a menudo no son publicadas ni conocidas por el propietario y operadores del activo.

Los adversarios pueden utilizar estas credenciales codificadas en el código para moverse a través del entorno del sistema de control o proporcionar acceso confiable para que sus herramientas interactúen con los activos industriales.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede iniciar sesión en los PLCs de Omron utilizando credenciales codificadas en el software, lo cual está documentado en CVE-2022-34151.
S0603	Stuxnet	Stuxnet utiliza una contraseña codificada en el servidor de base de datos del software WinCC como uno de los mecanismos utilizados para propagarse a sistemas cercanos.

Activos Objetivo

ID	Activo
A0013	E/S de Campo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Asegúrese de que los controles integrados y los dispositivos de red estén protegidos mediante la gestión de acceso, ya que estos dispositivos a menudo tienen cuentas codificadas desconocidas que podrían usarse para obtener acceso no autorizado.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0028	Sesión de Inicio	Sesión de Inicio de Sesión	Monitorear las sesiones de inicio de sesión en busca del uso de credenciales codificadas cuando sea posible.

DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear el tráfico de red en busca del uso de credenciales codificadas en protocolos que permitan la autenticación no cifrada.

Transferencia Lateral de Herramientas.

Los adversarios pueden transferir herramientas u otros archivos de un sistema a otro para preparar herramientas adversarias u otros archivos a lo largo de una operación. La copia de archivos también puede realizarse lateralmente entre sistemas víctimas internos para respaldar el Movimiento Lateral con Ejecución remota utilizando protocolos de intercambio de archivos inherentes, como el intercambio de archivos sobre SMB en carpetas compartidas en red conectadas.

En entornos de sistemas de control, el malware puede utilizar SMB y otros protocolos de intercambio de archivos para moverse lateralmente a través de redes industriales.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania en 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm movió sus herramientas lateralmente dentro de la red ICS.
C0025	Ataque al Suministro Eléctrico de Ucrania en 2016	Durante el Ataque al Suministro Eléctrico de Ucrania en 2016, el Equipo Sandworm utilizó un script VBS para facilitar la transferencia lateral de herramientas. El script VBS se utilizó para copiar cargas útiles específicas de ICS con el siguiente comando: cscript C:\Backinfo\ufn.vbs C:\Backinfo\101.dll C:\Delta\101.dll.
S0606	Bad Rabbit	Bad Rabbit puede moverse lateralmente a través de redes industriales mediante el servicio SMB
S1045	INCONTROLLER	INCONTROLLER puede utilizar una sesión Telnet para cargar un implante de malware en los PLCs de Omron.
S0368	NotPetya	NotPetya puede moverse lateralmente a través de redes industriales mediante el servicio SMB.

S0603	Stuxnet	Stuxnet envía una declaración SQL que crea una tabla e inserta un valor binario en la tabla. El valor binario es una representación de cadena hexadecimal del archivo ejecutable principal de Stuxnet DLL (formado usando el recurso 210) y un bloque de datos de configuración actualizado.
S0366	WannaCry	WannaCry puede moverse lateralmente a través de redes industriales mediante el servicio SMB.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0013	E/S de Campo
A0012	Host de Salto
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0931	Prevención de Intrusiones en la Red	Los sistemas de detección y prevención de intrusiones en red que utilizan firmas de red para identificar el tráfico de malware específico del adversario o transferencia de datos inusual sobre herramientas y protocolos conocidos como FTP pueden utilizarse para mitigar la actividad a nivel de red.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0017	Comando	Ejecución de Comando	Monitorear los comandos ejecutados y los argumentos para el uso anormal de utilidades y argumentos de línea de comandos que pueden ser utilizados en apoyo de la transferencia remota de archivos.
DS0022	Archivo	Creación de Archivo	Monitorear la creación de archivos en conjunto con otras técnicas (por ejemplo, transferencias de archivos utilizando Servicios Remotos).
		Metadatos de Archivo	Monitorear hashes de archivos similares o características (por ejemplo, nombre de archivo) que se crean en múltiples hosts.
DS0033	Compartir de Red	Acceso a Compartir de Red	Monitorear el acceso inesperado a compartir de red, como archivos transferidos entre compartidos dentro de una red utilizando protocolos como el Bloque de Mensajes del Servidor (SMB).
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear procesos inusuales con conexiones de red internas que crean
			archivos en el sistema que pueden ser sospechosos.
		Flujo de Trafico de Red	Monitorear el tráfico de red que proviene de hosts desconocidos / inesperados. Los metadatos del tráfico de red local (como la dirección MAC de origen) así como el uso de protocolos de gestión de red como DHCP pueden ser útiles para identificar hardware.

DS0009	Proceso	Creación de Proceso	Monitorear procesos recién construidos que ayuden en la transferencia lateral de herramientas, como programas de transferencia de archivos.

Descarga de programas.

Los adversarios pueden llevar a cabo una descarga de programa para transferir un programa de usuario a un controlador.

Las variaciones de la descarga de programa, como la edición en línea y la adición de programa, permiten que un controlador continúe funcionando durante el proceso de transferencia y reconfiguración sin interrupción en el control del proceso. Sin embargo, antes de comenzar una descarga completa del programa (es decir, descargar todo), es posible que un controlador necesite pasar a un estado de parada. Esto puede tener consecuencias negativas en el proceso físico, especialmente si el controlador no puede cumplir con una acción sensible al tiempo. Los adversarios pueden optar por evitar una descarga completa en favor de una edición en línea o una adición de programa para evitar interrumpir el proceso físico. Un adversario puede necesitar utilizar la técnica Detectar Modo de Operación o Cambiar Modo de Operación para asegurarse de que el controlador esté en el modo adecuado para aceptar una descarga de programa.

La granularidad del control para transferir un programa de usuario en su totalidad o partes está dictada por el protocolo de gestión (por ejemplo, S7CommPlus, TriStation) y la API subyacente del controlador. Por lo tanto, la descarga de programa es un término de alto nivel para el conjunto de llamadas de API específicas del proveedor utilizadas para configurar el espacio de memoria del programa de usuario de un controlador.

Modificar la asignación de tareas del controlador y modificar el programa representan los cambios de configuración que se transfieren a un controlador mediante una descarga de programa.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede utilizar el protocolo CODESYS para descargar programas en PLCs de Schneider. INCONTROLLER puede modificar la lógica del programa en PLCs de Omron utilizando las funciones de descarga de programa o transferencia de respaldo disponibles a través del servidor HTTP.
S1006	PLC-Blaster	PLC-Blaster utiliza la API de comunicación y gestión de PLC para cargar Unidades de Organización de Programas ejecutables.

S0603	Stuxnet	La secuencia de infección de Stuxnet consiste en bloques de código y bloques de datos que se descargarán en el PLC para alterar su comportamiento.
S1009	Triton	Triton aprovechó el protocolo TriStation para descargar programas en el Sistema Instrumentado de Seguridad Triconex.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autenticar todo acceso a controladores de campo antes de autorizar el acceso o modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en todo el ICS.
M0947	Auditoría	Proporcionar la capacidad de verificar la integridad de los programas descargados en un controlador. Aunque las técnicas como CRC y checksums se utilizan comúnmente, no son criptográficamente seguras y pueden ser
		vulnerables a colisiones. Preferiblemente, se deben usar funciones hash criptográficas (por ejemplo, SHA-2, SHA-3).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir la descarga de programas, incluidas las ediciones en línea y los anexos de programas, solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.
M0945	Firma de Código	Utilizar firmas de código para verificar la integridad y autenticidad de los programas descargados en el dispositivo.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.

M0937	Filtrado del Tráfico de Red	Filtrar los protocolos y cargas asociadas con la actividad de descarga de programas para evitar configuraciones no autorizadas del dispositivo.
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas Blancas de Red	Utilizar listas blancas basadas en hosts para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas blancas pueden usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones del sistema crítico a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar las conexiones de software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Monitorizar los registros de configuración de dispositivos que pueden contener alertas que indiquen si se ha producido una descarga de programas.
			Los dispositivos pueden mantener registros de aplicaciones que indiquen si se ha producido una descarga completa del programa, una edición en línea o una función de anexo de programa.
DS0039	Inventario de Activos	Activos	Consultar sistemas de gestión de activos para comprender las versiones de programas esperadas.

DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear las funciones de protocolo relacionadas con la descarga o modificación de programas. Las descargas de programas pueden ser observables en protocolos de automatización ICS y protocolos de gestión remota.

Servicios Remotos

Los adversarios pueden aprovechar servicios remotos para moverse entre activos y segmentos de red. Estos servicios suelen utilizarse para permitir que los operadores interactúen con sistemas de forma remota dentro de la red, algunos ejemplos son RDP, SMB, SSH y otros mecanismos similares.

Los servicios remotos podrían ser utilizados para admitir acceso remoto, transmisión de datos, autenticación, resolución de nombres y otras funciones remotas. Además, los servicios remotos pueden ser necesarios para permitir que los operadores y administradores configuren sistemas dentro de la red desde sus estaciones de trabajo de ingeniería o gestión. Un adversario puede usar esta técnica para acceder a dispositivos que pueden estar conectados a múltiples segmentos de red, y pueden ser utilizados para la descarga de programas o para ejecutar ataques en dispositivos de control directamente a través de Cuentas Válidas.

Servicios remotos específicos (RDP y VNC) pueden ser un precursor para habilitar la ejecución de la interfaz de usuario gráfica en dispositivos como HMIs o software de estaciones de trabajo de ingeniería.

Según datos de incidentes, CISA y el FBI evaluaron que actores patrocinados por el estado chino también comprometieron diversos canales de acceso remoto autorizados, incluidos sistemas diseñados para transferir datos y/o permitir el acceso entre redes corporativas y de ICS.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania en 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm utilizó un software de servicio de asistencia técnica para mover el ratón en dispositivos de control ICS y liberar maliciosamente interruptores eléctricos.

C0025	Ataque al Suministro Eléctrico de Ucrania en 2016	Durante el Ataque al Suministro Eléctrico de Ucrania en 2016, el Equipo Sandworm utilizó el acceso a MS-SQL en una máquina pivote, permitiendo la ejecución de código en toda la red ICS.
S1045	INCONTROLLER	INCONTROLLER puede utilizar el protocolo CODESYS para conectarse de forma remota a PLCs Schneider y realizar funciones de mantenimiento en el dispositivo. INCONTROLLER puede utilizar Telnet para cargar cargas útiles y ejecutar comandos en PLCs Omron. El malware también puede utilizar scripts CGI basados en HTTP (por ejemplo, cpu.fcgi, ecat.fcgi) para obtener acceso administrativo al dispositivo.
S0496	REvil	REvil utiliza el protocolo SMB para cifrar archivos ubicados en comparticiones de archivos conectadas de forma remota.
S0603	Stuxnet	Stuxnet ejecuta comandos SQL maliciosos en el servidor de base de datos WinCC para propagarse a sistemas remotos. Los comandos SQL maliciosos incluyen xp_cmdshell, sp_dumpdbilog y sp_addextendedproc.
G0088	TEMP.Veles	TEMP.Veles utilizó cajas de salto de protocolo de escritorio remoto (RDP) para ingresar al entorno ICS.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0012	Servidor Salto
A0011	Servidor de Red Privada Virtual (VPN)

Mitigaciones

ID	Mitigación	Descripción

M0801	Gestión de Acceso	Las tecnologías de Gestión de Acceso pueden ayudar a hacer cumplir la autenticación en servicios remotos críticos, ejemplos incluyen, pero no se limitan a, servicios de gestión de dispositivos (por ejemplo, telnet, SSH), servidores de acceso a datos (por ejemplo, HTTP, historiadores), y sesiones de HMI (por ejemplo, RDP, VNC).
M0800	Aplicación de Autorización	Proporcionar privilegios correspondientes a la restricción de una sesión de GUI para operaciones del sistema de control (ejemplos incluyen modos de solo lectura vs. lectura-escritura HMI). Asegurar que los usuarios locales, como operadores e ingenieros, tengan prioridad sobre las sesiones remotas y tengan la autoridad para recuperar el control sobre una sesión remota si es necesario. Evitar que las sesiones de acceso remoto (por ejemplo, RDP, VNC) tomen el control de las sesiones locales, especialmente aquellas utilizadas para el control de ICS, especialmente HMIs.
M0937	Filtrado de Tráfico de Red	Filtrar mensajes de protocolo de capa de aplicación para servicios remotos para bloquear cualquier actividad no autorizada.
M0804	Autenticación de Usuario Humano	Todos los servicios remotos deben requerir una autenticación fuerte antes de proporcionar acceso de usuario.
M0807	Listas de Permisos de Red	Las listas de permisos de red se pueden implementar a través de archivos basados en host o archivos de host del sistema para especificar qué conexiones externas (por ejemplo, dirección IP, dirección MAC, puerto, protocolo) pueden realizarse desde un dispositivo.
M0930	Segmentación de Red	Segmentar y controlar el movimiento de software entre los entornos empresariales y OT mediante DMZ unidireccionales. El acceso web debe estar restringido desde el entorno OT. Las estaciones de trabajo de ingeniería, incluidos los activos cibernéticos transitorios (TCAs), deben tener una conectividad mínima con las redes externas, incluidas Internet y correo electrónico, limitando aún más el alcance en el que estos dispositivos están conectados a múltiples redes.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos para servicios específicamente diseñados para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. El adversario puede realizar estas acciones utilizando Cuentas Válidas.
DS0028	Sesión de Inicio Sesión	Creación de Sesión de Inicio	Monitorear cuentas de usuario conectadas a sistemas a los que normalmente no tendrían acceso o patrones de acceso anormales, como múltiples sistemas en un período relativamente corto de tiempo. Correlacionar el uso de actividad de inicio de sesión relacionada con servicios remotos con comportamientos inusuales u otras actividades maliciosas o sospechosas. Es probable que los adversarios necesiten conocer un entorno y las relaciones entre sistemas a través de técnicas de Descubrimiento antes de intentar el Movimiento Lateral.
DS0011	Módulo	Carga de Módulos	Monitorear eventos asociados con la ejecución de scripts, como la carga de módulos asociados con lenguajes de scripting, como RDP, Telnet, SSH y VNC.
DS0033	Red Compartida	Acceso a Compartición de Red	Monitorear interacciones con comparticiones de red, como lecturas o

			transferencias de archivos, utilizando servicios remotos como Server Message Block (SMB).
DS0029	Tráfico de Red	Creación de Conexión de Red	Monitorear conexiones de red recién construidas en un servicio específicamente diseñado para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. Monitorear conexiones de red que involucren protocolos de administración remota comunes, como los puertos tcp:3283 y tcp:5900, así como los puertos tcp:3389 y tcp:22 para inicio de sesión remoto. El adversario puede usar Cuentas Válidas para habilitar inicios de sesión remotos.
		Flujo de Tráfico de Red	Monitorear datos de red para flujos de datos no comunes (por ejemplo, hora del día, dirección de origen/destino inusual) que puedan estar relacionados con el abuso de Cuentas Válidas para iniciar sesión en un servicio específicamente diseñado para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC.
DS0009	Proceso	Creación de Procesos	Monitorear procesos recién ejecutados relacionados con servicios específicamente diseñados para aceptar conexiones remotas, como RDP, Telnet, SSH y VNC. El adversario puede usar Cuentas Válidas para iniciar

			sesión y puede realizar acciones adicionales que
			generen procesos adicionales como el usuario.

Cuentas Válidas

Los adversarios pueden robar las credenciales de un usuario específico o de una cuenta de servicio utilizando técnicas de acceso a credenciales. En algunos casos, las credenciales predeterminadas para dispositivos de sistemas de control pueden estar públicamente disponibles. Las credenciales comprometidas pueden utilizarse para eludir los controles de acceso establecidos en varios recursos en los hosts y dentro de la red, e incluso pueden usarse para acceder de manera persistente a sistemas remotos. Las credenciales comprometidas y predeterminadas también pueden otorgar a un adversario un mayor privilegio en sistemas y dispositivos específicos o acceso a áreas restringidas de la red. Los adversarios pueden optar por no utilizar malware o herramientas, junto con el acceso legítimo que proporcionan esas credenciales, para dificultar la detección de su presencia o para controlar dispositivos y enviar comandos legítimos de manera no intencionada.

Los adversarios también pueden crear cuentas, a veces utilizando nombres de cuenta y contraseñas predefinidos, para proporcionar un medio de acceso de respaldo para la persistencia.

La superposición de credenciales y permisos en una red de sistemas es preocupante porque el adversario puede pivotar a través de cuentas y sistemas para alcanzar un alto nivel de acceso (es decir, administrador de dominio o de la empresa) y posiblemente entre los entornos de tecnología empresarial y operativa. Los adversarios pueden aprovechar las credenciales válidas de un sistema para acceder a otro sistema.

Ejemplos de Procedimientos

ID	Nombre	Descripción

C0028	Ataque al Suministro Eléctrico de Ucrania en 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm utilizó cuentas válidas para moverse lateralmente a través de conexiones VPN y sistemas de doble conexión. El Equipo Sandworm utilizó las credenciales de cuentas válidas para interactuar con aplicaciones de cliente y acceder a estaciones de trabajo de empleados que alojaban aplicaciones de HMI.
C0025	Ataque al Suministro Eléctrico de Ucrania en 2016	Durante el Ataque al Suministro Eléctrico de Ucrania en 2016, el Equipo Sandworm utilizó cuentas válidas para moverse lateralmente a
		través de conexiones VPN y sistemas de doble conexión.
G1000	ALLANITE	ALLANITE utilizó credenciales obtenidas a través de ataques de phishing y de agujeros de agua.
S0089	BlackEnergy	BlackEnergy utiliza credenciales de usuario y administrador válidas, además de crear nuevas cuentas de administrador para mantener presencia.
S1045	INCONTROLLER	INCONTROLLER puede realizar autenticación basada en contraseñas mediante fuerza bruta en PLCs Schneider a través del protocolo CODESYS (puerto UDP 1740). INCONTROLLER puede realizar adivinación de contraseñas mediante fuerza bruta en servidores OPC UA utilizando una lista predefinida de contraseñas.
G0049	OilRig	OilRig utilizó credenciales robadas para obtener acceso a máquinas víctimas.
G0088	TEMP.Veles	TEMP.Veles utilizó credenciales válidas al moverse lateralmente a través de cajas de salto RDP hacia el entorno ICS.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos

A0013	E/S de Campo
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Servidor Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autenticar todo acceso a controladores de campo antes de autorizar el acceso o la modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizada pueden ayudar a gestionar el gran número de cuentas de controlador de campo necesarias en todo el ICS.
M0936	Políticas de Uso de Cuentas	Configurar características relacionadas con el uso de cuentas como bloqueos de intentos de inicio de sesión, horarios de inicio de sesión específicos y requisitos de fuerza de contraseña, como ejemplos. Considerar estas características en relación con activos que pueden afectar la seguridad y la disponibilidad.
M0915	Configuración de Directorio Activo	Considerar la configuración y el uso de un servicio de autenticación en toda la red, como Active Directory, LDAP o capacidades RADIUS que se pueden encontrar en dispositivos ICS.
M0913	Guía para Desarrolladores de Aplicaciones	Asegurar que las aplicaciones y dispositivos no almacenen datos o credenciales sensibles de manera insegura (por ejemplo, credenciales en texto plano en el código, credenciales publicadas en repositorios o credenciales en almacenamiento en la nube público).
M0947	Auditoría	Auditar rutinariamente el código fuente, los archivos de configuración de aplicaciones, los repositorios abiertos y el almacenamiento en la nube pública en busca de uso y almacenamiento inseguros de credenciales.

M0937	Filtrado de Tráfico de Red	Considerar el uso de listas de permitidos de IP junto con la gestión de cuentas de usuario para asegurar que el acceso a los datos esté restringido no solo a usuarios válidos, sino también desde rangos de IP esperados para mitigar el uso de credenciales robadas para acceder a datos.
M0932	Autenticación Multifactorial	Integrar la autenticación multifactorial (MFA) como parte de la política organizacional puede reducir en gran medida el riesgo de que un adversario obtenga acceso a credenciales válidas que puedan ser utilizadas para tácticas adicionales como acceso inicial, movimiento lateral y recolección de información. MFA también se puede utilizar para restringir el acceso a recursos y APIs en la nube.
M0927	Políticas de Contraseñas	Las aplicaciones y dispositivos que utilizan nombres de usuario y contraseñas predeterminados deben cambiarse inmediatamente después de la instalación, y antes de su implementación en un entorno de producción.
M0926	Gestión de Cuentas Privilegiadas	Auditar cuentas de dominio y locales y sus niveles de permisos rutinariamente para buscar situaciones que podrían permitir a un adversario obtener acceso de sistema con credenciales de cuenta privilegiadas robadas. Estas auditorías también deben identificar si se han habilitado cuentas predeterminadas o si se han creado nuevas cuentas locales que no han sido autorizadas.
M0918	Gestión de Cuentas de Usuario	Asegurar que los usuarios y grupos de usuarios tengan permisos adecuados para sus roles a través de controles de Identidad y Acceso (IAM). Implementar controles de IAM estrictos para prevenir el acceso a sistemas excepto para las aplicaciones, usuarios y servicios que requieren acceso. Implementar cuentas de usuario para cada individuo para hacer cumplir y no repudiar acciones.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0028	Sesión de Inicio de Sesión	Creación de Sesión de Inicio de Sesión	Monitorear comportamientos de inicio de sesión que pueden abusar de credenciales de cuentas existentes como un medio para obtener Movimiento Lateral o Persistencia. Correlacionar otros sistemas de seguridad con información de inicio de sesión (por ejemplo, un usuario tiene una sesión de inicio de sesión activa pero no ha ingresado al edificio o no tiene acceso VPN).
		Metadatos de Sesión de Inicio de Sesión	Monitorear comportamientos sospechosos de cuenta en sistemas que comparten cuentas, ya sea de usuario, administrador o de servicio. Ejemplos: una cuenta inició sesión en múltiples sistemas simultáneamente; múltiples cuentas iniciaron sesión en la misma máquina simultáneamente; cuentas iniciaron sesión en
			momentos inusuales o fuera del horario laboral. La actividad puede ser desde sesiones de inicio de sesión interactivas o propiedad de procesos de cuentas que se utilizan para ejecutar binarios en un sistema remoto como una cuenta específica.

DS0002	Cuenta de Usuario	Autenticación de Cuenta de Usuario	Monitorear un intento de autenticación por parte de un usuario que pueda obtener y abusar de credenciales de cuentas existentes como un medio para obtener Acceso Inicial, Persistencia, Escalada de Privilegios o Evasión de Defensas.

RECOLECCIÓN

El adversario está intentando recopilar datos de interés y conocimiento del dominio sobre tu entorno ICS para informar su objetivo.

La Recolección consiste en técnicas que los adversarios utilizan para obtener conocimiento del dominio y obtener retroalimentación contextual en un entorno ICS. Esta táctica se realiza a menudo como parte del Descubrimiento, para recopilar datos sobre sistemas de control y objetivos de interés que pueden ser utilizados para cumplir el objetivo del adversario. Ejemplos de estas técnicas incluyen observar estados de operación, capturar capturas de pantalla, identificar roles de dispositivos únicos y recopilar esquemas de sistemas y diagramas. La recopilación de estos datos puede desempeñar un papel clave en la planificación, ejecución e incluso revisión de un ataque dirigido a un sistema ICS. Los métodos de recopilación dependen de las categorías de datos que se están buscando, que pueden incluir configuraciones y funcionalidades específicas de protocolos, dispositivos y procesos. La información recopilada puede estar relacionada con una combinación de datos del sistema, supervisión, dispositivos y redes, que conceptualmente se encuentran en niveles alto, medio y bajo de operaciones planificadas. Por ejemplo, repositorios de información sobre datos de la planta a un nivel alto o programas específicos de dispositivos a un nivel bajo. Los planos de planta sensibles, los manuales de dispositivos de proveedores y otras referencias también pueden estar en riesgo y expuestos en Internet o de otra manera accesibles públicamente.

Adversary-in-the-Middle

Los adversarios con acceso privilegiado a la red pueden intentar modificar el tráfico de red en tiempo real utilizando ataques de adversario en el medio (AiTM, por sus siglas en inglés). Este tipo de ataque permite al adversario interceptar el tráfico hacia y/o desde un dispositivo particular en la red. Si se establece un ataque AiTM, entonces el adversario tiene la capacidad de bloquear, registrar, modificar o inyectar tráfico en el flujo de comunicación. Hay varias formas de llevar a cabo este ataque, pero algunas de las más comunes son el envenenamiento del Protocolo de Resolución de Direcciones (ARP) y el uso de un proxy.

Un ataque AiTM puede permitir que un adversario realice los siguientes ataques:

Bloquear Mensaje de Reporte, Falsificar Mensaje de Reporte, Modificar Parámetro, Mensaje de Comando No Autorizado.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1010	VPNFilter	El módulo ssler de VPNFilter configura las iptables del dispositivo para redirigir todo el tráfico destinado al puerto 80 a su servicio local que escucha en el puerto 8888. Cualquier solicitud web saliente en el puerto 80 ahora es interceptada por ssler y puede ser inspeccionada por el módulo ps y manipulada antes de ser enviada al servicio HTTP legítimo.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Servidor Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Routers
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Limitar el acceso a la infraestructura de red y los recursos que pueden ser utilizados para remodelar el tráfico o de otro modo producir condiciones de Intercepción y Modificación de Tráfico (AiTM, por sus siglas en inglés).

M0802	Autenticidad de la Comunicación	La autenticidad de la comunicación asegurará que cualquier mensaje manipulado a través de AiTM pueda ser detectado, pero no puede prevenir el espionaje de estos. Además, proporcionar autenticidad de comunicación en diversos protocolos de descubrimiento, como DNS, puede utilizarse para prevenir varios procedimientos de AiTM.
M0942	Inhabilitar o Eliminar Característica o Programa	Desactivar protocolos de red heredados innecesarios que puedan ser utilizados para AiTM si corresponde.
M0931	Prevención de Intrusiones en la Red	Los sistemas de detección y prevención de intrusos en la red que pueden identificar patrones de tráfico indicativos de actividad de AiTM pueden ser utilizados para mitigar la actividad a nivel de red.
M0930	Segmentación de Red	La segmentación de red puede utilizarse para aislar componentes de infraestructura que no requieren un amplio acceso a la red. Esto puede mitigar, o al menos aliviar, el alcance de la actividad de AiTM.
M0810	Canal de Comunicaciones Fuera de Banda	Utilizar la comunicación fuera de banda para validar la integridad de los datos del canal primario.
M0813	Autenticación de Procesos de Software y Dispositivos	Para protegerse contra AiTM, los mecanismos de autenticación no deben enviar credenciales a través de la red en texto plano y también deben implementar mecanismos para prevenir ataques de reproducción (como nonces o sellos de tiempo). Las técnicas de autenticación basadas en desafío-respuesta que no envían directamente credenciales a través de la red proporcionan una mejor protección contra AiTM.
M0814	Configuración de Red Estática	Las entradas ARP definidas estáticamente pueden evitar la manipulación y el espionaje del tráfico de red conmutado, ya que algunas técnicas de AiTM dependen del envío de mensajes ARP falsificados para manipular las tablas ARP dinámicas de los hosts de red.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Registro de Aplicaciones	Contenido del Registro de Aplicaciones	Monitorear los registros de aplicaciones en busca de cambios en la configuración y otros eventos asociados con protocolos de red y otros servicios comúnmente abusados para AiTM.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear el tráfico de red en busca de anomalías asociadas con el comportamiento conocido de AiTM. Para actividades de Recolección donde los datos transmitidos no son manipulados, las anomalías pueden estar presentes en protocolos de gestión de red (por ejemplo, ARP, DHCP).
		Flujo de Tráfico de Red	Monitorear el tráfico de red que se origina desde hosts desconocidos / inesperados. Los metadatos del tráfico de red local (como la dirección MAC de origen) así como el uso de protocolos de gestión de red como DHCP pueden ser útiles para identificar hardware. Para obtener más contexto sobre los procedimientos y antecedentes del adversario, consulte Intercepción y Modificación de Tráfico (AiTM) y sub-técnicas aplicables.
DS0009	Proceso	Creación de Procesos	Las implementaciones basadas en host de esta técnica pueden utilizar llamadas al sistema basadas en red o comandos de utilidad de red (por ejemplo, iptables) para interceptar el tráfico localmente. Monitorear eventos relevantes de creación de procesos.
DS0019	Servicio	Creación de Servicios	Monitorear la creación de servicios/demonios recién construidos a través de los registros de eventos de Windows para los ID de eventos 4697 y 7045.
DS0024	Registro de Windows	Modificación de Clave del Registro de Windows	Monitorear HKLM\Software\Policies\Microsoft\Windows NT\DNSClient en busca de cambios en el valor DWORD "EnableMulticast". Un valor de "0" indica que LLMNR está deshabilitado.

Colección Automatizada

Los adversarios pueden automatizar la recolección de información del entorno industrial utilizando herramientas o scripts. Esta recolección automatizada puede aprovechar los protocolos de control nativos y las herramientas disponibles en el entorno de sistemas de control. Por ejemplo, el protocolo OPC puede ser utilizado para enumerar y recopilar información. El acceso a un sistema o interfaz con estos protocolos nativos puede permitir la recolección y enumeración de otros servidores y dispositivos conectados que estén comunicándose.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0093	Backdoor.Oldrea	Utilizando OPC, un componente de Backdoor.Oldrea recopila cualquier detalle sobre los dispositivos conectados y los envía de vuelta al C2 para que los atacantes los analicen.
S0604	Industroyer	Industroyer recopila automáticamente datos de objetos de protocolo para conocer los dispositivos de control en el entorno.
S1072	Industroyer2	Industroyer2 aprovecha una lista codificada de direcciones IP de estaciones remotas para iniciar comunicaciones de manera iterativa y recopilar información en múltiples niveles de prioridad IEC-104.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0006	Historiador de Datos
A0003	Controlador Lógico Programable (PLC)

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos en Red	Utilizar listas de permitidos en red para restringir conexiones no necesarias a dispositivos de red (por ejemplo, servidores de comunicaciones, convertidores serie a Ethernet) y servicios, especialmente en casos en los que los dispositivos tienen límites en el número de sesiones simultáneas que admiten.

M0930	Segmentación de Red	Evitar que sistemas no autorizados accedan a servidores de control o dispositivos de campo que contengan información industrial, especialmente servicios utilizados para protocolos de automatización comunes (por ejemplo, DNP3, OPC).

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos para acciones que podrían tomarse para recopilar datos internos.
DS0022	Archivo	Acceso a Archivos	Monitorear la visualización de archivos inesperados (por ejemplo, .pdf, .docx, .jpg) para la recopilación de datos internos.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitorear la recopilación de información sobre activos que pueda indicar desviaciones de las herramientas operativas estándar. Ejemplos incluyen funciones de protocolos de automatización industrial inesperadas, nuevas sesiones de comunicación de alto volumen o recopilación amplia en muchos hosts dentro de la red.

DS0012	Script	Ejecución de Scripts	Monitorear cualquier intento de habilitar scripts en un sistema se consideraría sospechoso. Si los scripts no se utilizan comúnmente en un sistema, pero están habilitados, los scripts que se ejecutan fuera del ciclo de parches u otras funciones administrativas son sospechosos. Los scripts
			deben capturarse del sistema de archivos cuando sea posible, para determinar sus acciones e intenciones.

Datos de Repositorios de Información

Los adversarios pueden dirigirse y recopilar datos de repositorios de información. Esto puede incluir datos sensibles como especificaciones, esquemas o diagramas de disposiciones de sistemas de control, dispositivos y procesos. Ejemplos de repositorios de información incluyen bases de datos de referencia en el entorno de procesos, así como bases de datos en la red corporativa que pueden contener información sobre el ICS.

La información recopilada de estos sistemas puede proporcionar al adversario una mejor comprensión del entorno operativo, proveedores utilizados, procesos o procedimientos del ICS.

En una campaña entre 2011 y 2013 contra organizaciones ONG, actores patrocinados por el estado chino buscaron en repositorios de documentos información específica como manuales de sistema, sitios de unidades terminales remotas (RTU), listas de personal, documentos que incluían la cadena SCAD*, credenciales de usuario e información de acceso remoto por marcación telefónica.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0038	Duqu	Duqu descarga módulos adicionales para la recopilación de datos en repositorios de información, incluido el módulo Infostealer 2 que puede acceder a datos de Windows Shares.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0006	Historiador de Datos

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Considerar revisiones periódicas de cuentas y privilegios para repositorios críticos y sensibles.
M0941	Encriptar Información Sensible	La información sensible para el funcionamiento y la arquitectura del entorno del proceso puede ser encriptada para garantizar la confidencialidad y restringir el acceso solo a aquellos que necesitan conocerla.
M0926	Gestión de Cuentas Privilegiadas	Minimizar permisos y acceso para cuentas de servicio para limitar la información que puede ser expuesta o recopilada por usuarios o software maliciosos.
M0922	Restringir Permisos de Archivos y Directorios	Proteger archivos con permisos adecuados para limitar las oportunidades para que los adversarios interactúen y recopilen información de bases de datos.
M0918	Gestión de Cuentas de Usuario	Asegurar que los usuarios y grupos de usuarios tengan permisos apropiados para sus roles a través de controles de Gestión de Identidad y Acceso (IAM) para prevenir el mal uso.
M0917	Capacitación de Usuarios	Desarrollar y publicar políticas que definan la información aceptable para ser almacenada en repositorios.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear el registro de aplicaciones de terceros, mensajería y/u otros artefactos que puedan aprovechar los repositorios de información para extraer información valiosa.

DS0028	Sesión de Inicio de Sesión	Creación de Sesión de Inicio de Sesión	Monitorear el comportamiento de inicio de sesión recién creado dentro de Microsoft SharePoint que puede configurarse para informar el acceso a ciertas páginas y documentos.
DS0033	Compartir de Red	Acceso a Compartir de Red	En el caso de detectar la recopilación de unidades de red compartidas, monitorear accesos
			inesperados y anormales a los recursos compartidos de red.

Datos del Sistema Local

Los adversarios pueden dirigirse y recopilar datos de fuentes del sistema local, como sistemas de archivos, archivos de configuración o bases de datos locales. Esto puede incluir datos sensibles como especificaciones, esquemas o diagramas de disposiciones de sistemas de control, dispositivos y procesos.

Los adversarios pueden hacer esto utilizando técnicas de Interfaz de Línea de Comandos o de Scripting para interactuar con el sistema de archivos y recopilar información. También pueden utilizar la Recolección Automatizada en el sistema local.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1000	ACAD/Medre.A	ACAD/Medre.A recopila información relacionada con la aplicación AutoCAD. El gusano recolecta archivos de AutoCAD (*.dwg) con dibujos de sistemas infectados.
S0038	Duqu	Duqu descarga módulos adicionales para la recopilación de datos de sistemas locales. Los módulos se llaman: infostealer 1, infostealer 2 y reconocimiento.
S0143	Flame	Flame tiene módulos integrados para recopilar información de computadoras comprometidas.

Mitigaciones

ID	Mitigación	Descripción

M0803	Prevención de Pérdida de Datos	La prevención de pérdida de datos puede restringir el acceso a datos sensibles y detectar datos sensibles que no están encriptados.
M0941	Encriptar Información Sensible	La información sensible para el funcionamiento y la arquitectura del entorno del proceso puede ser encriptada para garantizar la confidencialidad y restringir el acceso solo a aquellos que necesitan conocerla.
M0922	Restringir Permisos de Archivos y Directorios	Proteger archivos almacenados localmente con permisos adecuados para limitar oportunidades para que adversarios interactúen y recopilen información del sistema local.
M0917	Capacitación de Usuarios	Desarrollar y publicar políticas que definan la información aceptable a ser almacenada en sistemas locales.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos que pueden buscar y recopilar fuentes del sistema local, como sistemas de archivos o bases de datos locales, para encontrar archivos de interés y datos sensibles.
DS0022	Archivo	Acceso a Archivos	Monitorear accesos inesperados/anormales a archivos que pueden ser recopilación maliciosa de datos locales, como archivos de usuario (por ejemplo, .pdf, .docx, .jpg, .dwg) o bases de datos locales.

DS0009	Proceso	Ejecución de API del SO	Monitorear llamadas a API que pueden buscar fuentes del sistema local, como sistemas de archivos o bases de datos locales, para encontrar archivos de interés y datos sensibles.
		Creación de Procesos	Monitorear procesos recién ejecutados que pueden buscar fuentes del sistema local, como sistemas de archivos o bases de datos locales, para encontrar archivos de interés y datos sensibles.
DS0012	Script	Ejecución de Scripts	Monitorear cualquier intento sospechoso de habilitar scripts en un sistema. Si los scripts no se utilizan comúnmente en un
			sistema, pero están habilitados, los scripts que se ejecutan fuera del ciclo de parcheo u otras funciones de administrador son sospechosos. Los scripts deben ser capturados del sistema de archivos cuando sea posible para determinar sus acciones e intenciones.

Detectar Modo de Operación

Los adversarios pueden recopilar información sobre el modo de operación actual de un PLC o controlador. Los modos de operación dictan qué funciones de cambio o mantenimiento pueden ser manipuladas y son controladas frecuentemente por un interruptor de llave en el PLC (por ejemplo, ejecutar, prog [programa], y remoto). El conocimiento de estos estados puede ser valioso para un adversario para determinar si pueden reprogramar el PLC. Los modos de operación y los mecanismos mediante los cuales se seleccionan a menudo varían según el proveedor y la línea de productos. A continuación, se describen algunos modos de operación comúnmente implementados:

Programa: Este modo debe estar habilitado antes de que se puedan realizar cambios en el programa de los dispositivos. Esto permite la carga y descarga de programas entre el

dispositivo y una estación de trabajo de ingeniería. A menudo, la lógica del PLC se detiene y todas las salidas pueden ser forzadas a apagarse.

Ejecución: La ejecución del programa del dispositivo ocurre en este modo. La entrada y salida (valores, puntos, etiquetas, elementos, etc.) son monitoreados y utilizados de acuerdo con la lógica del programa. La carga y descarga de programas están desactivadas mientras se encuentra en este modo.

Remoto: Permite cambios remotos al modo de operación de un PLC.

Detener: El PLC y el programa se detienen, mientras que en este modo, las salidas son forzadas a apagarse.

Restablecer: Las condiciones en el PLC se restablecen a sus estados originales. Los reinicios cálidos pueden retener algo de memoria mientras que los reinicios fríos restablecerán todos los registros de E/S y de datos.

Modo de prueba / monitoreo: Similar al modo de ejecución, las E/S son procesadas, aunque este modo permite la monitorización, la configuración forzada, los reinicios y, más generalmente, la configuración o depuración del sistema. A menudo, el modo de monitoreo puede ser utilizado como un ensayo para la inicialización.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1009	Triton	Triton contiene un archivo llamado TS_cnames.py que contiene definiciones predeterminadas para el estado del programa (TS_progstate). El estado del programa se hace referencia en TsHi.py. Triton contiene un archivo llamado TS_cnames.py que contiene definiciones predeterminadas para el estado de la tecla (TS_keystate). El estado de la tecla se hace referencia en TsHi.py.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0801	Gestión de Acceso	Autenticar todo acceso a controladores de campo antes de autorizar el acceso o modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en los Sistemas de Control Industrial (ICS).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir la modificación de programas solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. Si no es así, utilice dispositivos bump-inthe-wire o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de admitir esto (por ejemplo, controladores heredados, RTU).
M0937	Filtrado de Tráfico de Red	Realice la inclusión en línea de comandos de protocolos de automatización para evitar que los dispositivos envíen comandos no autorizados o mensajes de informes. Las técnicas de lista de permitidos/denegados deben estar diseñadas con suficiente precisión para evitar el bloqueo no deseado de mensajes válidos.
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación
		también deben admitir Políticas de Uso de Cuentas, Políticas de Contraseñas y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidos basadas en hosts para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden usar para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Dispositivos y Procesos de Software	Autenticar las conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear los protocolos de red de automatización de ICS para funciones relacionadas con la lectura del modo de operación de un activo. En algunos casos, puede haber múltiples formas de detectar el modo de operación de un dispositivo, una de las cuales se utiliza típicamente en el entorno operativo. Monitorear el modo de operación que se verifica de formas inesperadas.

Imagen de E/S

Los adversarios pueden buscar capturar los valores del proceso relacionados con las entradas y salidas de un PLC. Durante el ciclo de escaneo, un PLC lee el estado de todas las entradas y las almacena en una tabla de imagen. La tabla de imagen es la ubicación de almacenamiento interno del PLC donde se almacenan los valores de entradas/salidas para un escaneo mientras ejecuta el programa de usuario. Después de que el PLC ha resuelto todo el programa lógico, actualiza la tabla de imagen de salida. El contenido de esta tabla de imagen de salida se escribe en los puntos de salida correspondientes en los módulos de E/S.

Las tablas de imagen de entrada y salida descritas anteriormente conforman la Imagen de E/S en un PLC. Esta imagen es utilizada por el programa de usuario en lugar de interactuar directamente con la E/S física.

Los adversarios pueden recopilar el estado de la Imagen de E/S de un PLC utilizando una API nativa de los dispositivos para acceder directamente a las regiones de memoria. La recopilación del estado de la E/S del PLC podría ser utilizada para reemplazar valores o informar sobre futuras etapas de un ataque.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0603	Stuxnet	Stuxnet copia el área de entrada de una imagen de E/S en bloques de datos con un intervalo de un segundo entre copias, formando una grabación de 21 segundos del área de entrada. El área de entrada contiene información que se envía al PLC desde un periférico. Por ejemplo, el estado actual de una válvula o la temperatura de un dispositivo.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0816	Mitigación Limitada o No Efectiva	Esta técnica puede no ser mitigada efectivamente, considere controles para activos y procesos que conduzcan al uso de esta técnica.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0039	Activo	Software	La recopilación de información de la imagen de E/S requiere analizar el programa de aplicación que se ejecuta en el PLC para lecturas específicas de bloques de datos. Detectar esto requiere obtener y analizar el programa de aplicación de un PLC, ya sea directamente desde el dispositivo o desde plataformas de gestión de activos.

Monitorear el Estado del Proceso

Los adversarios pueden recopilar información sobre el estado físico del proceso. Esta información puede ser utilizada para obtener más detalles sobre el propio proceso o como un disparador para acciones maliciosas. Las fuentes de información sobre el estado del proceso pueden variar, como etiquetas OPC, datos de historiador, información específica de bloques de PLC o tráfico de red.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	Los módulos de protocolo OPC e IEC 61850 de Industroyer incluyen la capacidad de enviar solicitudes stVal para leer el estado de variables operativas.
S1072	Industroyer2	Industroyer2 utiliza un comando de Interrogación General para monitorear las Direcciones de Objeto de Información (IOAs) del dispositivo y sus valores de estado de IO.
S0603	Stuxnet	Stuxnet examina los campos registrados por el
		monitor DP_RECV para determinar si el sistema objetivo se encuentra en un estado particular de operación.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)

A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0816	Mitigación Limitada o No Efectiva	Este tipo de técnica de ataque no puede ser fácilmente mitigada con controles preventivos ya que se basa en el abuso de características del sistema.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicaciones en busca de intentos de acceso a bases de datos operativas (por ejemplo, historiadores) u otras fuentes de datos operativos dentro del entorno del ICS. Estos dispositivos deben ser monitoreados para la recopilación del adversario utilizando técnicas relevantes para las tecnologías subyacentes
			(por ejemplo, Windows, Linux).

DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear los protocolos de red de automatización del ICS para funciones relacionadas con la lectura de un estado de proceso operativo (por ejemplo, códigos de función "Leer" en protocolos como DNP3 o Modbus). En algunos casos, puede haber múltiples formas de monitorear el estado de un proceso operativo, una de las cuales se usa típicamente en el entorno operativo. Monitorear el modo de operación que se verifica de formas inesperadas.

Identificación de Puntos y Etiquetas

Los adversarios pueden recopilar valores de puntos y etiquetas para obtener una comprensión más completa del entorno del proceso. Los puntos pueden ser valores como entradas, ubicaciones de memoria, salidas u otras variables específicas del proceso. Las etiquetas son los identificadores dados a los puntos para la conveniencia del operador.

Recopilar tales etiquetas proporciona un contexto valioso para los puntos ambientales y permite a un adversario mapear entradas, salidas y otros valores a sus procesos de control. Comprender los puntos que se están recopilando puede informar a un adversario sobre qué procesos y valores mantener seguimiento a lo largo de una operación.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0093	Backdoor.Oldrea	La carga útil de Backdoor.Oldrea tiene la capacidad de enumerar etiquetas OPC, además de información más genérica del servidor OPC. Los datos del servidor y los nombres de las etiquetas pueden proporcionar
		información sobre los nombres y la función de los dispositivos de control.

S1045	INCONTROLLER	INCONTROLLER puede leer de forma remota la estructura OCP UA de los dispositivos.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autentique todo acceso a los controladores de campo antes de autorizar el acceso o la modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controlador de campo necesarias en todo el entorno ICS.
M0800	Ejecución de Autorización	Los sistemas y dispositivos deben restringir el acceso a cualquier dato con posibles preocupaciones de confidencialidad, incluida la información de puntos y etiquetas.
M0802	Autenticidad de Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. Si no es así, utilice dispositivos de inserción en la línea o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de admitir esto (por ejemplo, controladores heredados, RTU).
M0937	Filtrado del Tráfico de Red	Realice una lista de permitidos en línea de comandos de protocolos de automatización para evitar que los dispositivos envíen mensajes de comando o informes no autorizados. Las técnicas de lista permitida/lista denegada deben diseñarse con suficiente precisión para evitar el bloqueo no intencionado de mensajes válidos.

M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidos basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden utilizar para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión según su función dentro del proceso. Permitir un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0813	Autenticación de Procesos de Software y Dispositivos	Los dispositivos deben autenticar todos los mensajes entre los activos maestros y de estación remota.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitoree los registros de aplicaciones de los activos que pueden proporcionar información sobre solicitudes de puntos o etiquetas. Busque anomalías relacionadas con la lectura de datos de punto o etiqueta, como nuevos activos que usan estas funciones, cambios en el volumen o el tiempo, o información inusual que se consulta. Muchos dispositivos proporcionan múltiples formas de lograr el mismo resultado (por ejemplo, funciones con/sin confirmación o funciones

			que operan en un solo punto vs. varios puntos).
			Monitoree los cambios en las funciones utilizadas.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitoree los protocolos de automatización del ICS en busca de anomalías relacionadas con la lectura de datos de punto o etiqueta, como nuevos activos que usan estas funciones, cambios en el volumen o el tiempo, o información inusual que se consulta. Muchos protocolos proporcionan múltiples formas de lograr el mismo resultado (por ejemplo, funciones con/sin confirmación o funciones que operan en un solo punto vs. varios puntos). Monitoree los cambios en las funciones utilizadas.

Carga de Programa

Los adversarios pueden intentar cargar un programa desde un PLC para recopilar información sobre un proceso industrial. La carga de un programa puede permitirles adquirir y estudiar la lógica subyacente. Los métodos de carga de programa incluyen software del proveedor, que permite al usuario cargar y leer un programa que se ejecuta en un PLC. Este software puede ser utilizado para cargar el programa objetivo en una estación de trabajo, un jump box o un dispositivo de interfaz.

Procedimiento Ejemplos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede utilizar el protocolo CODESYS para cargar programas desde PLCs de Schneider. INCONTROLLER puede obtener la lógica de programa existente de los PLCs de Omron utilizando las funciones de carga de programa o de respaldo disponibles a través del servidor HTTP.
S1009	Tritón	Tritón llama a SafeAppendProgramMod para transferir sus cargas útiles al Tricon. Parte de esta llamada incluye realizar una carga de programa.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Manejo de Acceso	Autenticar todo acceso a controladores de campo antes de autorizar el acceso o la modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar el gran número de cuentas de controladores de campo necesarias en todo el ICS.
M0800	Aplicación de Autorización	Todos los controladores de campo deberían restringir las cargas de programa solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.

M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deberían autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0937	Filtrar Tráfico de Red	Filtrar los protocolos y cargas útiles asociadas con la actividad de carga de programas para evitar el acceso no autorizado a las configuraciones del dispositivo.
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deberían requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deberían soportar Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilizar listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden usarse para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predefinidos.
M0813	Autenticación de Proceso de Software y Dispositivo	Autenticar conexiones de software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Log de Aplicación	Contenido del Log de Aplicación	Monitorear las alarmas del dispositivo producidas cuando ocurren cargas de programas, aunque no todos los dispositivos producirán tales alarmas.

DS0029	Tráfico de Red	Contenido del Tráfico de Red	Las cargas de programas pueden ser observables en los protocolos de gestión de ICS o protocolos de transferencia de archivos. Observar cuando ocurran funciones de protocolo relacionadas con cargas de programas. En casos donde el protocolo de ICS no se entienda bien, una opción es examinar el tráfico de red para los archivos de programa mismos utilizando herramientas basadas en firmas.
		Flujo de Tráfico de Red	Monitorear los patrones de comunicación del dispositivo para identificar transferencias de datos a granel irregulares entre el activo de ICS incrustado y otros nodos dentro de la red. Notar que estos indicadores dependen del perfil de operaciones normales y las capacidades de los protocolos de automatización industrial involucrados (por ejemplo, cargas de programas parciales).

Captura de Pantalla

Los adversarios pueden intentar realizar capturas de pantalla de dispositivos en el entorno del sistema de control. Las capturas de pantalla pueden tomarse de estaciones de trabajo, interfaces hombre-máquina (HMIs) u otros dispositivos que muestren datos relevantes del entorno, como procesos, dispositivos, informes, alarmas o datos relacionados. Estas pantallas de dispositivos pueden revelar información sobre el proceso de ICS, diseño, control y esquemas relacionados. En particular, un HMI puede proporcionar mucha información importante sobre el proceso industrial. El análisis de las capturas de pantalla puede proporcionar al adversario una comprensión de las operaciones previstas y las interacciones entre dispositivos críticos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede utilizar el protocolo CODESYS para cargar programas desde PLCs Schneider. INCONTROLLER puede obtener la lógica de programas existente de PLCs Omron utilizando las funciones de carga de programas o copia de seguridad disponibles a través del servidor HTTP.
S1009	Triton	Triton llama a SafeAppendProgramMod para transferir sus cargas útiles al Tricon. Parte de esta llamada incluye realizar una carga de programa.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Autenticar todo el acceso a los controladores de campo antes de autorizar el acceso o la modificación del estado, lógica o programas de un dispositivo. Las técnicas de autenticación centralizadas pueden ayudar a gestionar la gran cantidad de cuentas de controladores de campo necesarias en los sistemas de control industrial (ICS).
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir las cargas de programas solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante
		la implementación de un mecanismo de acceso basado en roles.
M0802	Autenticidad de Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0937	Filtrar Tráfico de Red	Filtrar los protocolos y cargas asociadas con la actividad de carga de programas para evitar el acceso no autorizado a las configuraciones del dispositivo.

M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilizar listas de permitidos basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden utilizar para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red y los sistemas operativos para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Proceso de Software y Dispositivo	Autenticar conexiones de software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear las alarmas de dispositivos producidas cuando ocurren cargas de programas, aunque no todos los dispositivos producirán tales alarmas.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Las cargas de programas pueden ser observables en protocolos de gestión de ICS o protocolos de transferencia de archivos. Notar cuándo ocurren funciones de protocolo relacionadas con cargas de programas. En casos donde los protocolos de ICS no

			son bien comprendidos, una opción es examinar el tráfico de red para los archivos de programas mismos utilizando herramientas basadas en firmas.
		Flujo de Tráfico de Red	Monitorear los patrones de comunicación del dispositivo para identificar transferencias irregulares masivas de datos entre el activo de ICS incrustado y otros nodos dentro de la red. Notar que estos indicadores dependen del perfil de operaciones normales y las capacidades de los protocolos de automatización industrial involucrados (por ejemplo, cargas de programas parciales).

Espionaje inalámbrico

El espionaje inalámbrico consiste en la captura de comunicaciones de radiofrecuencia (RF) utilizadas para el control remoto y la transmisión de información en entornos distribuidos. Las frecuencias de comunicación RF varían entre 3 kHz y 300 GHz, aunque comúnmente se encuentran entre 300 MHz y 6 GHz. La longitud de onda y la frecuencia de la señal afectan cómo se propaga la señal a través del aire libre, obstáculos (como paredes y árboles) y el tipo de radio necesario para capturarlas. Estas características suelen estandarizarse en el protocolo y el hardware, y pueden afectar cómo se captura la señal. Algunos ejemplos de protocolos inalámbricos que pueden encontrarse en entornos ciberfísicos son: WirelessHART, Zigbee, WIA-FA y el Espectro de Seguridad Pública de 700 MHz.

Los adversarios pueden capturar comunicaciones RF utilizando hardware especializado, como radio definida por software (SDR), radio portátil o una computadora con un demodulador de radio sintonizado a la frecuencia de comunicación. La información transmitida a través de un medio inalámbrico puede ser capturada en tránsito, ya sea que el dispositivo de espionaje sea el destino previsto o no. Esta técnica puede ser particularmente útil para un adversario cuando las comunicaciones no están cifradas.

En el incidente de la sirena de Dallas en 2017, se sospecha que los adversarios capturaron probablemente emisiones de mensajes de comando inalámbricos en una

frecuencia de 700 MHz durante una prueba regular del sistema. Estos mensajes fueron posteriormente reproducidos para activar los sistemas de alarma.

Activos Objetivo

ID	Activo
A0013	E/S de Campo
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0808	Cifrar el Tráfico de Red	Utilice técnicas y protocolos criptográficos sólidos para evitar el espionaje en las comunicaciones de red.
M0806	Minimizar la Propagación de Señales Inalámbricas	Reduzca el alcance de las comunicaciones de RF a su rango de funcionamiento previsto cuando sea posible. Los métodos de reducción de propagación pueden incluir (i) reducir la potencia de transmisión en las señales inalámbricas, (ii) ajustar la ganancia de la antena para evitar extensiones más allá de los límites organizacionales y (iii) emplear técnicas de blindaje de RF para bloquear la propagación excesiva de la señal.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Trafico de Red	Flujo de Trafico de Red	El espionaje de red puramente pasivo no puede detectarse de manera efectiva. En casos donde el adversario interactúa con la red inalámbrica (por ejemplo, uniéndose a una red Wi-Fi), la detección puede ser posible. Monitoree flujos de tráfico de red nuevos o irregulares que puedan indicar dispositivos o sesiones potencialmente no deseados en redes inalámbricas. En redes WiFi,

			monitoree cambios como puntos de acceso falsos o
			baja intensidad de señal, lo que indica que un dispositivo está más lejos del punto de acceso de lo esperado y cambios en la señal de la capa física. El contenido del tráfico de red proporcionará un contexto importante, como direcciones de hardware (por ejemplo, MAC), cuentas de usuario y tipos de mensajes enviados.

COMANDO Y CONTROL

El adversario está intentando comunicarse y controlar sistemas comprometidos, controladores y plataformas con acceso a tu entorno ICS.

El Comando y Control consiste en técnicas que los adversarios utilizan para comunicarse y enviar comandos a sistemas comprometidos, dispositivos, controladores y plataformas con aplicaciones especializadas utilizadas en entornos ICS. Ejemplos de estos dispositivos de comunicación especializados incluyen interfaces hombre-máquina (HMIs), historiadores de datos, servidores SCADA y estaciones de trabajo de ingeniería (EWS). Los adversarios a menudo buscan utilizar recursos comúnmente disponibles y simular el tráfico de red esperado para evitar detección y sospecha. Por ejemplo, puertos y protocolos comúnmente utilizados en entornos ICS, e incluso recursos de TI esperados, dependiendo de la red objetivo. El Comando y Control puede establecerse

con diversos grados de sigilo, a menudo dependiendo de la estructura y defensas de la red de la víctima.

Puerto Comúnmente Utilizado

Los adversarios pueden comunicarse a través de un puerto comúnmente utilizado para evadir los firewalls o sistemas de detección de red y mezclarse con la actividad normal de la red, evitando una inspección más detallada. Pueden utilizar el protocolo asociado con el puerto, o un protocolo completamente diferente. Pueden utilizar puertos comúnmente abiertos, como los ejemplos proporcionados a continuación:

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP/UDP:53 (DNS)
- TCP:1024-4999 (OPC en XP/Win2k3)
- TCP:49152-65535 (OPC en Vista y versiones posteriores)
- TCP:23 (TELNET)
- UDP:161 (SNMP)
- TCP:502 (MODBUS)
- TCP:102 (S7comm/ISO-TSAP)
- TCP:20000 (DNP3)
- TCP:44818 (Ethernet/IP)

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque de Energía Eléctrica de Ucrania 2015	Durante el Ataque de Energía Eléctrica de Ucrania en 2015, el Equipo Sandworm utilizó el puerto 443 para comunicarse con sus servidores C2.
S0603	Stuxnet	Stuxnet intenta contactar con servidores de comando y control en el puerto 80 para enviar información básica sobre la computadora que ha comprometido.
S1009	Triton	Triton utiliza el puerto UDP predeterminado de TriStation, 1502, para comunicarse con dispositivos.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones

A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Enrutadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0942	Deshabilitar o Eliminar Característica o Programa	Asegurar que los puertos y servicios innecesarios estén cerrados para prevenir el riesgo de detección y posible explotación.
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben soportar Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.

M0931	Prevención de Intrusión en la Red	Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red para identificar el tráfico para malware específico del adversario pueden ser utilizados para mitigar la actividad a nivel de red. Las firmas suelen ser para indicadores únicos dentro de protocolos y pueden basarse en el protocolo específico utilizado por un adversario o herramienta en particular y probablemente serán diferentes en varias familias y versiones de malware. Los adversarios probablemente cambiarán las firmas de C2 de la herramienta con el tiempo o construirán protocolos de tal manera que eviten la detección por herramientas defensivas comunes. Configurar firewalls internos y externos para bloquear el tráfico utilizando puertos comunes que se asocian a protocolos de red que pueden ser innecesarios para ese segmento de red en particular.
M0930	Segmentación de Red	

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear las discrepancias entre protocolos y sus puertos esperados (por ejemplo, tráfico no HTTP en tcp:80). Analizar el contenido de paquetes para detectar comunicaciones
			que no siguen el comportamiento de protocolo esperado para el puerto que se está utilizando.

		Flujo de Tráfico de Red	Analizar los datos de red para flujos de datos no comunes (por ejemplo, nuevos protocolos en uso entre hosts, puertos inesperados en uso). Los procesos que utilizan la red y que normalmente no tienen comunicación en red o que nunca se han visto antes son sospechosos.

Proxy de Conexión

Los adversarios pueden utilizar un proxy de conexión para dirigir el tráfico de red entre sistemas o actuar como intermediario para las comunicaciones de red.

La definición de un proxy también puede ampliarse para abarcar relaciones de confianza entre redes en conexiones punto a punto, en mallas o en conexiones de confianza entre redes que consisten en hosts o sistemas que se comunican regularmente entre sí.

La red puede estar dentro de una sola organización o abarcar múltiples organizaciones con relaciones de confianza. Los adversarios podrían utilizar estos tipos de relaciones para gestionar las comunicaciones de comando y control, para reducir el número de conexiones de red salientes simultáneas, para proporcionar resistencia frente a la pérdida de conexión, o para aprovechar las rutas de comunicaciones de confianza existentes entre las víctimas y evitar sospechas.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania de 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm estableció un proxy interno antes de la instalación de puertas traseras dentro de la red.

S1045	INCONTROLLER	El módulo PLCProxy de INCONTROLLER puede agregar una ruta IP a la puerta de enlace CODESYS que se ejecuta en PLC Schneider para permitirle enrutar mensajes a través del PLC a otros dispositivos en esa red. Esto permite que el malware eluda las reglas del firewall que le impiden comunicarse directamente con dispositivos en la misma red que el PLC.
S0604	Industroyer	Industroyer intenta conectarse con un proxy interno codificado en el puerto TCP 3128 [proxy Squid predeterminado]. Si se establece, la puerta trasera intenta alcanzar un servidor C2 externo a través del proxy interno.
G0034	Equipo Sandworm	El Equipo Sandworm establece un proxy interno antes de la instalación de puertas traseras dentro de la red.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Routers
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción

M0937	Filtrado del Tráfico de Red	El tráfico hacia redes de anonimato conocidas y la infraestructura de C2 pueden bloquearse mediante el uso de listas de permitidos y bloqueo de red. Se debe tener en cuenta que este tipo de bloqueo puede ser eludido por otras técnicas como el Domain Fronting.
M0807	Listas de Permitidos de Red	Las listas de permitidos de red se pueden implementar a través de archivos basados en host o archivos de sistema para especificar qué conexiones externas (por ejemplo, dirección IP, dirección MAC, puerto, protocolo) pueden realizarse desde un dispositivo. Las técnicas de lista de permitidos que operan en la capa de aplicación (por ejemplo, DNP3, Modbus, HTTP) se abordan en la mitigación de Filtrado del Tráfico de Red.
M0931	Prevención de Intrusiones en la Red	Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red para identificar el tráfico de malware específico del adversario pueden utilizarse para mitigar la actividad a nivel de red. Las firmas suelen ser para indicadores únicos dentro de los protocolos y pueden estar basadas en el protocolo C2 específico utilizado por un adversario o herramienta en particular y probablemente serán diferentes en varias familias y versiones de malware. Es probable que los adversarios cambien las firmas de C2 de la herramienta con el tiempo o construyan protocolos de manera tal que eviten la detección por parte de herramientas defensivas comunes.
M0920	Inspección de SSL/TLS	Si es posible inspeccionar el tráfico HTTPS, las capturas pueden analizarse en busca de conexiones que parezcan ser domain fronting.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitoree y analice patrones de tráfico e inspección de paquetes asociados con protocolo(s) que no siguen los estándares de protocolo esperados y flujos de tráfico (por ejemplo, paquetes excesivos que no pertenecen a flujos establecidos, patrones de tráfico gratuitos o

			anómalos, sintaxis o estructura anómala). Considere la correlación con el monitoreo de procesos y la línea de comandos para detectar la ejecución de procesos y argumentos de línea de comandos anómalos asociados con patrones de tráfico (por ejemplo, monitoree anomalías en el uso de archivos que normalmente no inician conexiones para protocolo(s) respectivos).
		Flujo de Tráfico de Red	Monitoree los protocolos de proxy conocidos (por ejemplo, SOCKS, Tor, protocolos peer-to-peer) y el uso de herramientas (por ejemplo, Squid, software peer-to-peer) en la red que no forman parte de las operaciones normales. También monitoree los datos de la red para flujos de datos inusuales. Los procesos que utilizan la red y que normalmente no tienen comunicación en red o que nunca se han visto antes son sospechosos.

Protocolo Estándar de Capa de Aplicación

Los adversarios pueden establecer capacidades de comando y control sobre protocolos de capa de aplicación comúnmente utilizados, como HTTP(S), OPC, RDP, Telnet, DNP3 y Modbus. Estos protocolos pueden ser utilizados para disfrazar las acciones del adversario como tráfico de red benigno. Los protocolos estándar pueden ser vistos en su puerto asociado o, en algunos casos, sobre un puerto no estándar. Los adversarios pueden utilizar estos protocolos para comunicarse hacia afuera de la red para el comando y control, o en algunos casos hacia otros dispositivos infectados dentro de la red.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0089	BlackEnergy	BlackEnergy utiliza solicitudes HTTP POST para contactar a servidores externos de comando y control.
S1045	INCONTROLLER	INCONTROLLER puede enviar comandos de forma remota a un agente malicioso cargado en PLCs Omron a través de HTTP o HTTPS.
G0049	OilRig	OilRig se comunicaba con su comando y control utilizando solicitudes HTTP.
S0496	REvil	REvil envía mensajes HTTPS POST con URL generadas aleatoriamente para comunicarse con un servidor remoto.
S0603	Stuxnet	Stuxnet utiliza un hilo para monitorear un bloque de datos DB890 de la secuencia A o B. Este hilo se ejecuta constantemente y sondea este bloque (cada 5 minutos). En un PLC infectado, si se encuentra el bloque DB890 y contiene un valor de magia especial (utilizado por Stuxnet para identificar su propio bloque DB890), los datos de este bloque pueden leerse y escribirse. Este hilo probablemente se utiliza para optimizar la forma en que funcionan las secuencias A y B, y modificar su comportamiento cuando se abre el editor Step7.
S1009	Triton	Triton puede comunicarse con el implante utilizando el comando 'get main processor diagnostic data' de TriStation y busca un paquete específicamente diseñado del cual extrae un valor de comando y sus argumentos.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos de Red	Las listas de permitidos de red se pueden implementar a través de archivos basados en host o archivos de sistema para especificar qué conexiones externas (por ejemplo, dirección IP, dirección MAC, puerto, protocolo) pueden realizarse desde un dispositivo. Las técnicas de lista de permitidos que operan en la capa de aplicación (por ejemplo, DNP3, Modbus, HTTP) se abordan en la mitigación de Filtrado del Tráfico de Red.
M0931	Prevención de Intrusiones en la Red	Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red para identificar el tráfico de malware específico del adversario pueden utilizarse para mitigar la actividad a nivel de red.
M0930	Segmentación de Red	Asegúrese de la segmentación adecuada de la red entre los recursos corporativos de nivel superior y el entorno de proceso de control.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitoree y analice patrones de tráfico e inspección de paquetes asociados con protocolo(s), aprovechando la inspección de SSL/TLS para el tráfico cifrado, que no siguen los estándares de protocolo esperados y flujos de tráfico (por ejemplo, paquetes excesivos que no pertenecen a flujos establecidos, patrones de tráfico gratuitos o anómalos, sintaxis o estructura anómala). Considere la correlación con el monitoreo de procesos y la línea de comandos para detectar la ejecución de procesos y argumentos de línea de comandos anómalos asociados con patrones de tráfico (por ejemplo, monitoree
			anomalías en el uso de archivos que normalmente no inician conexiones para protocolo(s) respectivos).

		Flujo de Tráfico de Red	Monitoree y analice flujos de tráfico que no siguen los estándares de protocolo esperados y flujos de tráfico (por ejemplo, paquetes excesivos que no pertenecen a flujos establecidos, o patrones de tráfico gratuitos o anómalos). Considere la correlación con el monitoreo de procesos y la línea de comandos para detectar la ejecución de procesos y argumentos de línea de comandos anómalos asociados con patrones de tráfico (por ejemplo, monitoree anomalías en el uso de archivos que normalmente no inician conexiones para protocolo(s) respectivos).

FUNCIÓN DE INHIBICIÓN DE RESPUESTA

El adversario está intentando evitar que las funciones de seguridad, protección, aseguramiento de la calidad y de intervención del operador respondan a una falla, peligro o estado inseguro.

La Inhibición de la Función de Respuesta consiste en técnicas que los adversarios utilizan para obstaculizar las salvaguardias establecidas para procesos y productos. Esto puede implicar la inhibición de funciones de seguridad, protección, aseguramiento de la calidad o intervención del operador para interrumpir las salvaguardias que tienen como objetivo prevenir la pérdida de vidas, la destrucción de equipos y la interrupción de la producción. Estas técnicas tienen como objetivo disuadir activamente y prevenir las alarmas y respuestas esperadas que surgen debido a los estados en el entorno ICS. Los adversarios pueden modificar o actualizar la lógica del sistema, o incluso impedir las respuestas con un ataque de denegación de servicio. Esto puede resultar en la prevención, destrucción, manipulación o modificación de programas, lógica, dispositivos y comunicaciones. Dado que las funciones de prevención generalmente están inactivas, las funciones de informe y procesamiento pueden parecer normales, pero pueden haber sido alteradas para evitar respuestas de falla en escenarios peligrosos. A diferencia de la Evasión, las técnicas de Inhibición de la Función de Respuesta pueden ser más intrusivas, como evitar activamente las respuestas a un

escenario peligroso conocido. Los adversarios pueden usar estas técnicas para llevar a cabo o proporcionar cobertura para técnicas de Impacto.

Activar el Modo de Actualización de Firmware

Los adversarios pueden activar el modo de actualización de firmware en dispositivos para evitar que las funciones de respuesta esperadas se activen en caso de una emergencia o mal funcionamiento del proceso. Por ejemplo, dispositivos como relés de protección pueden tener un modo de operación diseñado para la instalación de firmware. Este modo puede detener la monitorización del proceso y funciones relacionadas para permitir la carga de nuevo firmware. Un dispositivo dejado en modo de actualización puede ser puesto en un estado de espera inactivo si no se le proporciona firmware. Al entrar y salir de este modo en un dispositivo, el adversario puede negar sus funcionalidades habituales.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	El módulo de denegación de servicio (DoS) de SIPROTEC de Industroyer coloca al dispositivo víctima en modo de actualización de firmware. Este es un caso de uso legítimo en circunstancias normales, pero en este caso es utilizado por el adversario para evitar que el SIPROTEC realice sus funciones protectoras diseñadas. Como resultado, las salvaguardias normales quedan desactivadas, dejando un enlace desprotegido en la transmisión eléctrica.

Activos Objetivo

ID	Activo
A0009	Puerta de Datos
A0013	E/S de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios en dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere el uso de tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización sólidas.
M0800	Aplicación de Autorización	Restringir los cambios de configuraciones y las capacidades de actualización de firmware solo a individuos autorizados.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0937	Filtrar Tráfico de Red	Filtrar los protocolos y las cargas útiles asociadas con la actividad de activación o actualización de firmware.
M0804	Autenticación de Usuario Humano	Los dispositivos que permiten la gestión remota de firmware deben requerir autenticación antes de permitir cualquier cambio. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuentas, Políticas de Contraseñas y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden utilizarse para asegurar que los dispositivos solo se conecten con estaciones maestras o estaciones de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones del sistema críticas a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear el registro de activos que puede proporcionar información

			de que un activo ha sido colocado en Modo de
			Actualización de Firmware. Algunos activos pueden registrar actualizaciones de firmware por sí mismos sin registrar que el dispositivo ha sido colocado en modo de actualización.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitorear los protocolos de red de automatización de ICS para obtener información de que un activo ha sido colocado en Modo de Actualización de Firmware.
DS0040	Bases de Datos Operativas	Alarma de Dispositivo	Monitorear las alarmas de dispositivos que indican que los dispositivos han sido colocados en Modo de Actualización de Firmware, aunque no todos los dispositivos producen tales alarmas.

Supresión de Alarmas

Los adversarios pueden dirigirse a las alarmas de funciones de protección para evitar que notifiquen a los operadores sobre condiciones críticas. Los mensajes de alarma pueden ser parte de un sistema de informes general y ser de particular interés para los adversarios. La interrupción del sistema de alarmas no implica necesariamente la interrupción del sistema de informes en su totalidad.

Una presentación de Secura sobre el objetivo de los adversarios al intentar suprimir alarmas señala un objetivo de doble propósito: evitar que se emitan alarmas salientes y evitar que se responda a las alarmas entrantes. El método de supresión puede depender en gran medida del tipo de alarma en cuestión:

Una alarma generada por un mensaje de protocolo.

Una alarma señalada con E/S.

Un bit de alarma establecido en una bandera (y leído).

En entornos de ICS, el adversario puede tener que suprimir o enfrentarse a múltiples alarmas y/o propagación de alarmas para lograr un objetivo específico de evadir la detección o evitar que ocurran las respuestas previstas. Los métodos de supresión pueden implicar manipular o alterar las pantallas y registros de dispositivos, modificar el código en memoria a valores fijos, o incluso manipular el código de instrucciones a nivel de ensamblador.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario suprimió la notificación de alarmas al ordenador central.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos de Red	Utilice listas de permitidos de red para restringir las conexiones innecesarias a dispositivos de red (por ejemplo, servidores de comunicación, convertidores serie a Ethernet) y servicios, especialmente en casos en los que los dispositivos tienen límites en el número de sesiones simultáneas que admiten.

M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión en función de su papel funcional dentro del proceso. Permitir un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0810	Canal de Comunicaciones Fuera de Banda	Proporcione un método alternativo para que las alarmas sean reportadas en caso de una falla de comunicación.
M0814	Configuración de Red Estática	Las conexiones no autorizadas pueden ser prevenidas definiendo estáticamente los hosts y puertos utilizados para las conexiones de protocolos de automatización.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0029	Trafico de Red	Flujo de Tráfico de Red	Monitorear la pérdida de tráfico de red que podría indicar que las alarmas están siendo suprimidas. Una pérdida de comunicaciones esperadas asociadas con los protocolos de red utilizados para comunicar eventos de alarma o datos de proceso podría indicar que se está utilizando esta técnica.
DS0040	Bases de Datos Operativas	Alarma de Dispositivo	Monitorear la pérdida de alarmas de dispositivos esperadas que podrían indicar que las alarmas están siendo suprimidas. Como se señala en la descripción de la técnica, puede haber múltiples fuentes de alarmas en un entorno de ICS. Las discrepancias entre las alarmas pueden indicar que el adversario está suprimiendo algunas pero no todas las alarmas en el entorno.

		Historial de Procesos/Datos en Vivo	Monitorear la pérdida de datos de proceso operativos que podrían indicar que las alarmas están siendo suprimidas.
		Alarma de Proceso/Evento	Monitorear la pérdida de alarmas de proceso operativas esperadas que podrían indicar que las alarmas están siendo suprimidas. Como se señala
			en la descripción de la técnica, puede haber múltiples fuentes de alarmas en un entorno de ICS. Las discrepancias entre las alarmas pueden indicar que el adversario está suprimiendo algunas pero no todas las alarmas en el entorno.

Bloqueo de Mensajes de Comando

Los adversarios pueden bloquear un mensaje de comando para evitar que llegue a su destino previsto y así prevenir la ejecución del comando. En redes OT, los mensajes de comando se envían para proporcionar instrucciones a los dispositivos del sistema de control. Un mensaje de comando bloqueado puede inhibir las funciones de respuesta para corregir una interrupción o condición insegura.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm bloqueó los mensajes de comando utilizando firmware malicioso para dejar inoperables los convertidores serie a Ethernet.
S0604	Industroyer	En Industroyer, el primer puerto COM del archivo de configuración se utiliza para la comunicación real y los otros dos puertos COM simplemente se abren para evitar que otros procesos accedan a ellos. Por lo tanto, el componente de carga útil IEC 101 es capaz de tomar el control y mantener el control del dispositivo RTU.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0013	Entradas/Salidas de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos de Red	Utilice listas de permitidos de red para restringir las conexiones innecesarias a dispositivos de red (por ejemplo, servidores de comunicación, convertidores serie a Ethernet) y servicios, especialmente en casos en los que los dispositivos tienen límites en el número de sesiones simultáneas que admiten.
M0810	Canal de Comunicaciones Fuera de Banda	Proporcione un método alternativo para enviar mensajes de comandos críticos a estaciones remotas, esto podría incluir el uso de comunicación de radio/celular para enviar mensajes a un técnico de campo que realiza físicamente la función de control.
M0814	Configuración de Red Estática	Las conexiones no autorizadas pueden ser prevenidas definiendo estáticamente los hosts y puertos utilizados para las conexiones de protocolos de automatización.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicaciones en busca de cambios en la configuración y otros eventos asociados con los protocolos de red que puedan ser utilizados para bloquear comunicaciones.

DS0029	Trafico de Red	Flujo de Tráfico de Red	Monitorear la pérdida de comunicaciones de red, lo que puede indicar que se está utilizando esta técnica.
DS0040	Bases de Datos Operativas	Historial de Procesos/Datos en Vivo	Monitorear la falta de datos de procesos operativos que pueden ayudar a identificar una pérdida de comunicaciones. Esto no detectará directamente la ejecución de la técnica, sino que puede proporcionar evidencia adicional de que la técnica ha sido utilizada y
			puede complementar otras detecciones.
		Alarma de Proceso/Evento	Monitorear las alarmas de activos que pueden ayudar a identificar una pérdida de comunicaciones. Considere correlacionar las alarmas con otras fuentes de datos que indiquen que el tráfico ha sido bloqueado, como el tráfico de red. En casos donde existan métodos alternativos de comunicación con estaciones remotas, las alarmas aún pueden ser visibles incluso si se bloquean los mensajes de comando.
DS0009	Proceso	Terminación de Proceso	Monitorear la terminación de procesos o servicios asociados con protocolos de automatización de ICS y software de aplicación que podrían ayudar a detectar comunicaciones bloqueadas.

Bloqueo de Mensaje de Informe

Los adversarios pueden bloquear o evitar que un mensaje de informe llegue a su destino previsto. En sistemas de control, los mensajes de informe contienen datos de telemetría (por ejemplo, valores de E/S) relacionados con el estado actual del equipo y el proceso industrial. Al bloquear estos mensajes de informe, un adversario puede potencialmente ocultar sus acciones a un operador.

El bloqueo de mensajes de informe en sistemas de control que gestionan procesos físicos puede contribuir al impacto en el sistema, causando la inhibición de una función de respuesta. Un sistema de control puede no ser capaz de responder de manera adecuada o oportuna a un evento, como una falla peligrosa, si su correspondiente mensaje de informe es bloqueado.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm bloqueó mensajes de informes utilizando firmware malicioso para dejar inoperables los convertidores serie a Ethernet.
S0604	Industroyer	Industroyer utiliza el primer puerto COM del archivo de configuración para la comunicación y los otros dos puertos COM se abren para evitar que otros procesos accedan a ellos. Esto puede bloquear procesos u operadores para recibir mensajes de informes de un dispositivo.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos de Red	Utilice listas de permitidos de red para restringir conexiones innecesarias a dispositivos de red (por ejemplo, servidores de comunicación, convertidores serie a Ethernet) y servicios, especialmente en casos donde los dispositivos tienen límites en el número de sesiones simultáneas que admiten.
M0810	Canal de Comunicaciones Fuera de Banda	Proporcione un método alternativo para enviar mensajes de informes críticos a operadores, esto podría incluir el uso de comunicación de radio/celular para obtener mensajes de técnicos de campo que pueden obtener localmente datos de telemetría y estado.
M0814	Configuración de Red Estática	Las conexiones no autorizadas pueden ser prevenidas definiendo estáticamente los hosts y puertos usados para las conexiones de protocolos de automatización.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitoree los registros de aplicaciones para cambios en la configuración y otros eventos asociados con protocolos de red que pueden ser usados para bloquear comunicaciones.
DS0029	Trafico de Red	Flujo de Tráfico de Red	Monitoree la pérdida de comunicaciones de red, lo que puede indicar que esta técnica está siendo utilizada.

DS0040	Bases de Datos Operativas	Historial de Procesos/Datos en Vivo	Monitoree la falta de datos de proceso operativo que puede ayudar a identificar una pérdida de comunicaciones. Esto no detectará directamente la ejecución de la técnica, pero puede proporcionar evidencia adicional de que la técnica ha sido utilizada y puede complementar otras detecciones.
		Alarma de Proceso/Evento	Monitoree las alarmas de activos que pueden ayudar a identificar una pérdida de comunicaciones. Considere correlacionar alarmas con otras fuentes de datos que indiquen que el tráfico ha sido bloqueado, como el tráfico de red. En casos donde existan métodos alternativos de comunicación con estaciones remotas, las alarmas aún pueden ser visibles incluso si los
			mensajes de informes están bloqueados.
DS0009	Proceso	Terminación de Proceso	Monitoree la terminación de procesos o servicios asociados con protocolos de automatización ICS y software de aplicación que podrían ayudar a detectar comunicaciones bloqueadas.

Bloqueo de Puerto Serial COM

Los adversarios pueden bloquear el acceso al puerto serial COM para evitar que las instrucciones o configuraciones lleguen a los dispositivos objetivo. Los puertos de comunicación serial (COM) permiten la comunicación con dispositivos del sistema de

control. Los dispositivos pueden recibir mensajes de comando y configuración a través de dichos puertos serial COM. Los dispositivos también utilizan el puerto serial COM para enviar mensajes de comando e informes. Bloquear el puerto serial COM del dispositivo también puede bloquear los mensajes de comando y los mensajes de informe.

A menudo, un convertidor de serie a Ethernet está conectado a un puerto serial COM para facilitar la comunicación entre dispositivos serie y Ethernet. Un enfoque para bloquear un puerto serial COM sería crear y mantener abierta una sesión TCP con el lado Ethernet del convertidor. Un convertidor de serie a Ethernet puede tener algunos puertos abiertos para facilitar múltiples comunicaciones. Por ejemplo, si hay tres puertos serial COM disponibles: 1, 2 y 3, el convertidor podría estar escuchando en los puertos correspondientes 20001, 20002 y 20003. Si se abre y mantiene abierta una conexión TCP/IP con uno de estos puertos, entonces el puerto no estará disponible para ser utilizado por otra parte. Una forma en que el adversario podría lograr esto sería iniciar una sesión TCP con el convertidor de serie a Ethernet en 10.0.0.1 a través de Telnet en el puerto serial 1 con el siguiente comando: telnet 10.0.0.1 20001.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm sobrescribió el firmware del convertidor serie a Ethernet, dejando
		los dispositivos inoperativos. Esto significaba que la comunicación con los dispositivos serie aguas abajo no era posible o era más difícil.

S0604	Industroyer	En Industroyer, el primer puerto COM del archivo de configuración se utiliza para la comunicación real y los otros dos puertos COM simplemente se abren para evitar que otros procesos accedan a ellos. Por lo tanto, el componente de carga útil IEC 101 es capaz de tomar el control y mantener el control del dispositivo RTU.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0807	Listas de Permitidos de Red	Implementar listas de permitidos de red para minimizar el acceso a puertos de comunicación serie solo a hosts autorizados, como servidores de comunicación y RTUs.
M0930	Segmentación de Red	Restringir que dispositivos no autorizados accedan a puertos de comunicación serie.
M0810	Canal de Comunicaciones Fuera de Banda	Asegurar que los dispositivos tengan un método alternativo para comunicarse en caso de que un puerto COM válido no esté disponible.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicaciones en busca de cambios en la configuración y otros eventos asociados con protocolos de red que pueden ser utilizados para bloquear comunicaciones.
DS0029	Trafico de Red	Flujo de Tráfico de Red	Monitorear la pérdida de comunicaciones de red, lo que puede indicar que esta técnica está siendo utilizada.
DS0040	Bases de Datos Operativas	Historial de Procesos/Datos en Vivo	Monitorear la falta de datos de procesos operativos que pueden ayudar a identificar una pérdida de comunicaciones. Esto no detectará directamente la ejecución de la técnica, pero puede proporcionar evidencia adicional de que la técnica ha sido utilizada y puede complementar otras detecciones.
		Alarma de Proceso/Evento	Monitorear las alarmas de los activos que pueden ayudar a identificar una pérdida de comunicaciones. Considere correlacionar alarmas con otras fuentes de datos que indiquen que el tráfico ha sido bloqueado, como el tráfico de red. En casos donde existan métodos alternativos de comunicación con estaciones remotas, las alarmas aún pueden ser

			visibles incluso si los mensajes a través de puertos serie COM están bloqueados.
DS0009	Proceso	Terminación de Proceso	Monitorear la terminación de procesos o servicios asociados con protocolos de automatización ICS y software de aplicación que podrían ayudar a detectar comunicaciones bloqueadas.

Destrucción de Datos

Los adversarios pueden llevar a cabo la destrucción de datos durante el transcurso de una operación. El adversario puede dejar o crear malware, herramientas u otros archivos no nativos en un sistema objetivo para lograr esto, potencialmente dejando rastros de actividades maliciosas. Tales archivos no nativos y otros datos pueden ser eliminados durante el transcurso de una intrusión para mantener un perfil bajo o como parte estándar del proceso de limpieza posterior a la intrusión.

La destrucción de datos también puede utilizarse para hacer que las interfaces de los operadores sean incapaces de responder y para interrumpir las funciones de respuesta que se esperan. Un adversario también puede destruir las copias de seguridad de datos que son vitales para la recuperación después de un incidente.

Los comandos estándar de eliminación de archivos están disponibles en la mayoría de los sistemas operativos e interfaces de dispositivos para realizar la limpieza, pero los adversarios también pueden usar otras herramientas. Dos ejemplos son SDelete de Windows Sysinternals y Active@ Killdisk.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1045	INCONTROLLER	INCONTROLLER puede borrar la memoria de los PLCs de Omron y restablecer la configuración a través del servicio HTTP remoto.
S0604	Industroyer	Industroyer cuenta con un borrador destructivo que sobrescribe todos los archivos de configuración de ICS en los discos duros y todas las unidades de red mapeadas, dirigidos específicamente a los archivos de configuración de ABB PCM600.

S0607	KillDisk	KillDisk es capaz de eliminar archivos del sistema para hacer que el sistema no pueda arrancar y se dirige a 35 tipos diferentes de archivos para su eliminación.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Enrutadores
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0953	Copia de Seguridad de Datos	Utilizar servidores de almacenamiento central para operaciones críticas siempre que sea posible (por ejemplo, historiadores) y mantener copias de seguridad remotas. Para estaciones remotas, utilizar almacenamiento redundante local para grabadores de eventos. Contar con plataformas de sistemas de control de respaldo, preferiblemente como reservas calientes, para responder inmediatamente a eventos de destrucción de datos.
M0926	Gestión de Cuentas Privilegiadas	Minimizar los permisos y el acceso para las cuentas de servicio para limitar la información que podría verse afectada por usuarios o software maliciosos.

M0922	Restringir Permisos de Archivos y Directorios	Proteger los archivos almacenados localmente con permisos adecuados para limitar las oportunidades para que los adversarios afecten el almacenamiento de datos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear comandos ejecutados y argumentos para binarios que podrían estar involucrados en actividades de destrucción de datos, como SDelete.
DS0022	Archivo	Eliminación de Archivos	Monitorear la eliminación inesperada de archivos.
		Modificación de Archivos	Monitorear los cambios realizados en una gran cantidad de archivos para modificaciones inesperadas tanto en directorios de usuario como en directorios utilizados para almacenar programas y componentes del sistema operativo.
DS0009	Proceso	Creación de Procesos	Monitorear la ejecución de procesos recién creados de binarios que podrían estar involucrados en actividades de destrucción de datos, como SDelete.

Denegación de Servicio

Los adversarios pueden llevar a cabo ataques de Denegación de Servicio (DoS) para interrumpir la funcionalidad esperada del dispositivo. Ejemplos de ataques de DoS incluyen abrumar al dispositivo objetivo con un alto volumen de solicitudes en un corto período de tiempo y enviar al dispositivo objetivo una solicitud que no sabe cómo manejar. Al interrumpir el estado del dispositivo, este puede quedar temporalmente sin respuesta, posiblemente hasta que se reinicie. Cuando se coloca en este estado, los dispositivos pueden ser incapaces de enviar y recibir solicitudes, y es posible que no

realicen las funciones de respuesta esperadas en reacción a otros eventos en el entorno.

Algunos dispositivos de ICS son particularmente sensibles a los eventos de DoS y pueden volverse no responsivos incluso ante una simple exploración de ping. Los adversarios también pueden intentar ejecutar una Denegación de Servicio Permanente (PDoS) contra ciertos dispositivos, como en el caso del malware BrickerBot.

Los adversarios pueden explotar una vulnerabilidad de software para causar una denegación de servicio aprovechando un error de programación en un programa, servicio o dentro del software del sistema operativo o del kernel mismo para ejecutar código controlado por el adversario. Pueden existir vulnerabilidades en el software que puedan ser utilizadas para causar una condición de denegación de servicio.

Los adversarios pueden tener conocimiento previo sobre protocolos industriales o dispositivos de control utilizados en el entorno a través del Descubrimiento de Información del Sistema Remoto. Hay ejemplos de adversarios causando un Reinicio/Apagado del Dispositivo de forma remota al explotar una vulnerabilidad que induce el consumo no controlado de recursos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque a la Red Eléctrica de Ucrania 2015	Durante el Ataque a la Red Eléctrica de Ucrania en 2015, los operadores de las líneas telefónicas de la compañía eléctrica fueron afectados con un ataque de denegación de servicio para que no pudieran atender las llamadas de los clientes sobre cortes de energía. También se les denegó el servicio a los operadores para sus dispositivos aguas abajo cuando los convertidores serie a Ethernet tuvieron su firmware sobrescrito, lo que dejó inutilizables los dispositivos.
S0093	Backdoor.Oldrea	La carga útil de Backdoor.Oldrea ha causado que múltiples plataformas OPC comunes se bloqueen intermitentemente. Esto podría causar un efecto de denegación de servicio en aplicaciones que dependen de comunicaciones OPC.
S0604	Industroyer	El módulo de denegación de servicio (DoS) de SIPROTEC de Industroyer explota la vulnerabilidad CVE-2015-5374 para dejar un dispositivo Siemens SIPROTEC sin respuesta. Una vez que esta vulnerabilidad se explota con éxito, el dispositivo objetivo deja de responder a cualquier comando hasta que se reinicia manualmente. Una vez que se ejecuta la herramienta, envía paquetes específicamente diseñados al puerto 50,000 de las direcciones IP objetivo utilizando UDP. El paquete UDP contiene la siguiente

		carga útil de 18 bytes: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E.
S1006	PLC-Blaster	La ejecución en el PLC puede detenerse violando el límite de tiempo del ciclo. PLC-Blaster implementa un bucle sin fin que desencadena una condición de error dentro del PLC con el impacto de una denegación de servicio (DoS).

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0815	Relojes de Control	Los reinicios del sistema y del proceso deben realizarse cuando ocurre una condición de tiempo de espera.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear el registro de aplicaciones, mensajes y/u otros artefactos que puedan resultar de ataques de denegación de servicio (DoS) que degradan o bloquean la disponibilidad de servicios para los usuarios. Además de las detecciones a nivel de red, el registro e instrumentación de los puntos finales pueden ser útiles para la detección.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear y analizar patrones de tráfico e inspección de paquetes asociados con protocolos que no siguen los
			estándares esperados y flujos de tráfico (por ejemplo, paquetes no relacionados con flujos establecidos, patrones de tráfico gratuitos o anómalos, sintaxis o estructura anómalas). Considerar la correlación con el monitoreo de procesos y la línea de comandos para detectar ejecuciones de procesos anómalas y argumentos de línea de comandos asociados a patrones de tráfico (por ejemplo, monitorear anomalías en el uso de archivos que normalmente no inician conexiones para los protocolos respectivos).

		Flujo de Tráfico de Red	Monitorear datos de red para flujos de datos no comunes. Los procesos que utilizan la red y que normalmente no tienen comunicación en red o nunca han sido vistos antes son sospechosos.
DS0040	Bases de Datos Operacionales	Historial de Procesos/Datos en Vivo	Monitorear datos operativos en busca de indicadores de pérdida temporal de datos que pueden indicar una denegación de servicio. Esto no detectará directamente la ejecución de la técnica, pero en su lugar puede proporcionar evidencia adicional de que la técnica ha sido utilizada y puede complementar otras detecciones.

Reinicio/Apagado del Dispositivo

Los adversarios pueden reiniciar o apagar forzosamente un dispositivo en un entorno de ICS para interrumpir y potencialmente afectar negativamente los procesos físicos. Los métodos de reinicio y apagado de dispositivos existen en algunos dispositivos como funcionalidades integradas y estándar. Estas funcionalidades pueden ejecutarse utilizando interfaces web interactivas del dispositivo, interfaces de línea de comandos (CLI) y comandos de protocolo de red.

El reinicio o apagado inesperado de dispositivos de control puede evitar que las funciones de respuesta esperadas ocurran durante estados críticos.

Un reinicio del dispositivo también puede ser un indicio de modificaciones maliciosas del dispositivo, ya que muchas actualizaciones requieren un apagado para surtir efecto.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque a la Red Eléctrica de Ucrania 2015	Durante el Ataque a la Red Eléctrica de Ucrania en 2015, el Equipo Sandworm programó las fuentes de alimentación ininterrumpible (UPS) para apagar los servidores de datos y teléfono a través de la interfaz de gestión de las UPS.

S0604	Industroyer	El módulo de denegación de servicio (DoS) SIPROTEC de Industroyer aprovecha la vulnerabilidad CVE-2015-5374 para dejar un dispositivo Siemens SIPROTEC sin respuesta. Aunque la vulnerabilidad no causa directamente el reinicio o apagado del dispositivo, el dispositivo debe reiniciarse manualmente antes de que pueda reanudar las operaciones.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	Entrada/Salida de Campo
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host Puente
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0014	Routers
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios de dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considerar el uso de tecnologías de gestión de acceso para aplicar autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización sólidas.
M0800	Aplicación de Autorización	Todos los controladores de campo deben restringir la modificación de programas solo a ciertos usuarios (por ejemplo, ingenieros, técnicos de campo), preferiblemente mediante la implementación de un mecanismo de acceso basado en roles.

M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. De lo contrario, utilizar dispositivos bumpin-the-wire o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de admitir esto (por ejemplo, controladores heredados, RTU).
M0942	Deshabilitar o Eliminar Funcionalidad o Programa	Asegurarse de que los comandos remotos que habilitan el apagado del dispositivo estén deshabilitados si no son necesarios. Ejemplos incluyen el código de función 0x0D de DNP3 o funciones de gestión de dispositivos innecesarias.
M0937	Filtrar el Tráfico de Red	Las listas de denegación de aplicaciones pueden utilizarse para bloquear funciones de protocolo de automatización utilizadas para iniciar el apagado o reinicio del dispositivo, como el código de función 0x0D de DNP3 o vulnerabilidades que pueden utilizarse para desencadenar apagados del dispositivo (por ejemplo, CVE-2014-9195, CVE-2015-5374).
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir políticas de uso de cuentas, políticas de contraseñas y gestión de cuentas de usuario.
M0807	Listas de Permitidos de Red	Utilizar listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden usarse para asegurarse de que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red y los sistemas operativos para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones desde software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Los reinicios y apagados de dispositivos pueden ser observables en los registros de aplicaciones del dispositivo. Monitorear reinicios o apagados inesperados del dispositivo.
DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear protocolos de automatización de ICS para funciones que reinician o apagan un dispositivo. Los comandos para reiniciar o apagar dispositivos también pueden ser observables en protocolos de gestión de TI tradicionales.
		Flujo de Trafico de Red	Monitorear la pérdida de comunicaciones de red, lo que puede indicar que un dispositivo ha sido apagado o reiniciado. Esto no detectará directamente la ejecución de la técnica, pero en su lugar puede proporcionar evidencia adicional de que la técnica ha sido utilizada y puede complementar otras detecciones.
DS0040	Bases de Datos Operacionales	Alarma del Dispositivo	Los dispositivos pueden producir alarmas sobre reinicios o apagados. Monitorear reinicios o apagados inesperados del dispositivo.

Manipular la Imagen de E/S

Manipular la imagen de E/S de los PLCs mediante diversos métodos para evitar que funcionen según lo esperado. Los métodos de manipulación de la imagen de E/S pueden incluir la anulación de la tabla de E/S mediante la manipulación directa de la memoria o el uso de la función de anulación utilizada para probar los programas de los PLC. Durante el ciclo de escaneo, un PLC lee el estado de todas las entradas y las

almacena en una tabla de imagen. Esta tabla de imagen es la ubicación de almacenamiento interno del PLC donde se almacenan los valores de las entradas/salidas durante un escaneo mientras ejecuta el programa del usuario. Una vez que el PLC ha resuelto todo el programa lógico, actualiza la tabla de imagen de salida. El contenido de esta tabla de imagen de salida se escribe en los puntos de salida correspondientes en los módulos de E/S.

Una de las características únicas de los PLCs es su capacidad para anular el estado de una entrada discreta física o para anular la lógica que controla una bobina de salida física y forzar la salida a un estado deseado.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1006	PLC-Blaster	PLC-Blaster puede manipular cualquier salida del PLC. Usando el POU POKE, se puede modificar cualquier valor dentro de la imagen del proceso.
S0603	Stuxnet	Cuando se escribe en la salida periférica, la secuencia C intercepta la salida y se asegura de que no se escriba en la salida de la imagen del proceso. La salida son las instrucciones que el PLC envía a un dispositivo para cambiar su comportamiento operativo. Al interceptar la salida periférica, Stuxnet evita que un operador note comandos no autorizados enviados al periférico.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0816	Mitigación Limitada o No Efectiva	Esta técnica puede no mitigarse efectivamente, considerar controles para activos y procesos que conduzcan al uso de esta técnica.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0039	Activo	Software	Una imagen de E/S manipulada requiere analizar el programa de aplicación que se ejecuta en el PLC para escrituras específicas en el bloque de datos. Detectar esto requiere obtener y analizar el programa de aplicación de un PLC, ya sea directamente desde el dispositivo o desde plataformas de gestión de activos.

Modificar la configuración de alarmas

Los adversarios pueden modificar la configuración de alarmas para evitar alertas que podrían informar a los operadores de su presencia o para evitar respuestas a situaciones peligrosas e inadvertidas. Los mensajes de informe son una parte estándar de la adquisición de datos en los sistemas de control. Estos mensajes se utilizan para transmitir información del estado del sistema y confirmar que se han realizado acciones específicas. Proporcionan información vital para la gestión de un proceso físico y mantienen a los operadores, ingenieros y administradores al tanto del estado de los dispositivos del sistema y los procesos físicos.

Si un adversario logra cambiar la configuración de los informes, ciertos eventos podrían impedirse de ser reportados. Este tipo de modificación también puede evitar que los operadores o dispositivos realicen acciones para mantener el sistema en un estado seguro. Si los mensajes de informe críticos no pueden desencadenar estas acciones, podría ocurrir un impacto.

En entornos de sistemas de control industrial (ICS), el adversario puede tener que utilizar la supresión de alarmas o lidiar con múltiples alarmas y/o propagación de alarmas para lograr un objetivo específico de evadir la detección o prevenir que ocurran respuestas previstas. Los métodos de supresión a menudo dependen de la modificación de la configuración de alarmas, como modificar el código en memoria a valores fijos o manipular el código de instrucciones a nivel de ensamblador.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0020	Violación del Agua de Maroochy	En la violación del agua de Maroochy, el adversario desactivó las alarmas en cuatro estaciones de bombeo, impidiendo las notificaciones al ordenador central.

Activos Objetivo

ID	Activo
A0009	Puerta de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios de dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere utilizar tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización sólidas.
M0800	Aplicación de Autorización	Solo el personal autorizado debería poder cambiar los ajustes de las alarmas
M0804	Autenticación de Usuario Humano	Todos los controladores de campo deben requerir que los usuarios se autentiquen para todas las sesiones de gestión remotas o locales. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas de Permitidos de Red	Utilice listas de permitidas basadas en hosts para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos pueden usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Divida la red y los sistemas operativos para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autenticar conexiones de software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

M0918	Gestión de Cuentas de Usuario	Limite los privilegios de las cuentas de usuario y grupos para que solo los administradores o ingenieros designados puedan interactuar con la gestión de alarmas y los umbrales de configuración de alarmas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitoree los registros de aplicaciones de activos de ICS que indiquen cambios en la configuración de alarmas, aunque no todos los activos producirán tales registros.
DS0039	Activo	Inventario de Activos	Consulte los sistemas de gestión de activos para comprender los ajustes de alarma esperados.
DS0029	Trafico de Red	Contenido del Tráfico de Red	Monitoree los cambios en la configuración de alarmas observables en los protocolos de red de automatización o gestión.
DS0040	Bases de Datos Operacionales	Historial de Procesos/Datos en Vivo	Los datos sobre el proceso industrial pueden indicar que está funcionando fuera de los límites esperados y podrían ayudar a indicar que se ha cambiado un ajuste de alarma. Esto no detectará directamente la ejecución de la técnica, sino que proporcionará evidencia adicional de que se ha utilizado la técnica y puede complementar otras detecciones.

Rootkit

Los adversarios pueden desplegar rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Los rootkits son programas que ocultan la existencia de malware al interceptar y

modificar las llamadas a la API del sistema operativo que suministran información del sistema. Los rootkits o la funcionalidad que permite rootkits pueden residir a nivel de usuario o de kernel en el sistema operativo, o más bajo.

Los rootkits de firmware que afectan al sistema operativo otorgan un control casi completo del sistema. Si bien los rootkits de firmware suelen desarrollarse para la placa principal de procesamiento, también pueden desarrollarse para la E/S que está conectada a un activo. El compromiso de este firmware permite la modificación de todas las variables y funciones de proceso en las que se involucra el módulo. Esto puede resultar en la ignorancia de comandos y en la alimentación de información falsa al dispositivo principal. Al manipular los procesos del dispositivo, un adversario puede inhibir las funciones de respuesta esperadas y posiblemente habilitar el impacto.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0603	Stuxnet	Uno de los rootkits de Stuxnet está contenido completamente en el falso s7otbxdx.dll. Para continuar existiendo sin ser detectado en el PLC, debe tener en cuenta al menos las siguientes situaciones: solicitudes de lectura para sus propios bloques de código malicioso, solicitudes de lectura para bloques infectados (OB1, OB35, DP_RECV) y solicitudes de escritura que podrían sobrescribir el propio código de Stuxnet. Stuxnet contiene código para monitorear e interceptar estos tipos de solicitudes. El rootkit modifica estas solicitudes para que no se descubra ni se dañe el código del PLC de Stuxnet.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0013	E/S de Campo
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0947	Auditoría	Audite la integridad del sistema PLC y del código de aplicación, como la manipulación de bloques de función estándar (por ejemplo, Bloques Organizacionales) que gestionan la ejecución de programas de lógica de aplicación.
M0945	Firma de Código	Las firmas digitales pueden ser utilizadas para asegurar que los archivos DLL de la aplicación sean auténticos antes de la ejecución.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0001	Firmware	Modificación de Firmware	Monitoree los cambios realizados en el firmware para modificaciones inesperadas en la configuración y/o datos que puedan ser utilizados por rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Se deben consultar los sistemas de gestión de activos para comprender las versiones de firmware y configuraciones conocidas como válidas.

Detención del servicio

Los adversarios pueden detener o deshabilitar servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos. Detener servicios críticos puede inhibir o detener la respuesta a un incidente o ayudar en los objetivos generales del adversario de causar daño al entorno. Los servicios pueden no permitir la modificación de sus almacenes de datos mientras están en funcionamiento. Los adversarios pueden detener servicios para llevar a cabo la Destrucción de Datos

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0605	EKANS	Antes de cifrar el proceso, EKANS primero detiene el proceso si su nombre coincide con uno de los procesos definidos en la lista de terminación. EKANS también utiliza comandos netsh para implementar reglas de firewall que bloquean cualquier comunicación remota con el dispositivo.
S0604	Industroyer	Industroyer tiene la capacidad de detener un servicio por sí mismo, o de iniciar sesión como un usuario y detener un servicio como ese usuario.
S1072	Industroyer2	Industroyer2 tiene la capacidad de terminar procesos especificados (es decir, PServiceControl.exe y PService_PDD.exe) y cambiar el nombre de cada proceso para evitar el reinicio. Estos se definen a través de una configuración codificada.
S0607	KillDisk	KillDisk busca y termina dos procesos no estándar, uno de los cuales es una aplicación ICS.
S0496	REvil	REvil busca todos los procesos enumerados en el campo prc dentro de su archivo de configuración y luego termina cada proceso.

Activos Objetivo

ID	Activo
A0008	Servidor de Aplicaciones
A0007	Servidor de Control
A0009	Puerta de Datos
A0006	Historiador de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0012	Host de Salto
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)
A0001	Estación de Trabajo

Mitigaciones

ID	Mitigación	Descripción
M0930	Segmentación de Red	Segmentar la red y los sistemas operativos para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0922	Restricción de Permisos de Archivos y Directorios	Asegurar los permisos adecuados de archivos y procesos para evitar que los adversarios desactiven o interfieran con servicios críticos.
M0924	Restricción de Permisos de Registro	Asegurar los permisos adecuados del registro para evitar que los adversarios desactiven o interfieran con servicios críticos.
M0918	Gestión de Cuentas de Usuario	Limitar los privilegios de las cuentas de usuario y grupos para que solo los administradores autorizados puedan cambiar los estados y configuraciones del servicio.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0017	Comando	Ejecución de Comandos	Monitorear los comandos ejecutados y los argumentos que puedan detener o desactivar servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos.
DS0022	Archivo	Modificación de Archivos	Monitorear los cambios realizados en archivos que pueden detener o desactivar servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos.
DS0009	Proceso	Ejecución de API del SO	Las herramientas de acceso remoto con funciones incorporadas pueden interactuar directamente con la API de Windows para realizar estas funciones fuera de los utilitarios típicos del sistema.
		Creación de Procesos	Monitorear los procesos recién ejecutados que puedan detener o desactivar servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos.
		Terminación de Procesos	Monitorear los procesos y los argumentos de la línea de comandos para ver si los procesos críticos se terminan o dejan de ejecutarse.
DS0019	Servicio	Metadatos del Servicio	Las alteraciones en la ruta binaria del servicio o el tipo de inicio del servicio cambiado a deshabilitado pueden ser sospechosas.

DS0024	Registro de Windows	Modificación de Clave del Registro de Windows	Monitorear los cambios realizados en las claves y/o valores del registro de Windows que pueden detener o desactivar servicios en un sistema para que esos servicios no estén disponibles para los usuarios legítimos.

Firmware del sistema

El firmware del sistema en activos modernos a menudo está diseñado con una función de actualización. El firmware de dispositivos más antiguos puede estar instalado en fábrica y requerir equipo especial de reprogramación. Cuando está disponible, la función de actualización del firmware permite a los proveedores parchear errores y realizar actualizaciones de forma remota. Las actualizaciones de firmware del dispositivo suelen ser responsabilidad del usuario y pueden realizarse mediante un paquete de actualización de software. También puede ser posible realizar esta tarea a través de la red.

Un adversario puede aprovechar la función de actualización de firmware en dispositivos accesibles para cargar firmware malicioso o desactualizado. La modificación maliciosa del firmware del dispositivo puede proporcionar a un adversario acceso root a un dispositivo, dado que el firmware es una de las capas de abstracción de programación más bajas.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Sistema Eléctrico de Ucrania 2015	Durante el Ataque al Sistema Eléctrico de Ucrania en 2015, el Equipo Sandworm sobrescribió las pasarelas serie a Ethernet con firmware personalizado para deshabilitar, apagar y/o volver irrecuperables los sistemas.
S1009	Triton	Triton es capaz de leer, escribir y ejecutar código en la memoria del controlador de seguridad en una dirección arbitraria dentro de la región de firmware del dispositivo. Esto permite que el malware realice cambios en el firmware en ejecución en la memoria y modifique cómo opera el dispositivo.

Activos Objetivo

ID	Activo
A0009	Puerta de Datos
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad
A0011	Servidor de Red Privada Virtual (VPN)

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios en dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere el uso de tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización sólidas.
M0947	Auditoría	Realice controles de integridad del firmware antes de cargarlo en un dispositivo. Utilice hashes criptográficos para verificar que el firmware no haya sido modificado comparándolo con un hash confiable del firmware. Esto podría provenir de fuentes de datos confiables (por ejemplo, sitio del proveedor) o a través de un servicio de verificación de terceros.
M0946	Integridad del Arranque	Verifique la integridad del BIOS o EFI existente para determinar si es vulnerable a modificaciones. Utilice la tecnología del Módulo de Plataforma Confiable. Mueva la raíz de confianza del sistema al hardware para evitar la manipulación de la memoria flash SPI. Tecnologías como Intel Boot Guard pueden ayudar con esto.
M0945	Firma de Código	Los dispositivos deben verificar que el firmware haya sido firmado correctamente por el proveedor antes de permitir la instalación.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.

M0808	Cifrado de Tráfico de Red	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0941	Cifrado de Información Sensible	Se debe considerar el cifrado del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0937	Filtrado de Tráfico de Red	Filtre los protocolos y cargas útiles asociados con la activación o actualización del firmware.
M0804	Autenticación de Usuario Humano	Los dispositivos que permiten la gestión remota del firmware deben requerir autenticación antes de permitir cualquier cambio. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuentas, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas Blancas de Red	Utilice listas blancas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas blancas pueden usarse para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmente la red y los sistemas operativos para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autentique conexiones de software y dispositivos para evitar que los sistemas no autorizados accedan a funciones de gestión protegidas.
M0951	Actualizar el Software	Parchee el BIOS y EFI según sea necesario.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitoree los registros de aplicaciones del dispositivo en busca de cambios de firmware, aunque no todos los dispositivos producirán tales registros.

DS0001	Firmware	Modificación de Firmware	Monitoree el firmware en busca de cambios inesperados. Se debe consultar a los sistemas de gestión de activos para comprender las versiones de firmware conocidas como válidas.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitoree los protocolos de gestión de ICS /
			protocolos de transferencia de archivos en busca de funciones de protocolo relacionadas con cambios de firmware.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitoree los cambios de firmware que pueden ser observables a través de alarmas operativas de dispositivos.

PROCESO DE CONTROL IMPAR

El adversario está intentando manipular, desactivar o dañar los procesos de control físico.

La Alteración del Control de Procesos consiste en técnicas que los adversarios utilizan para interrumpir la lógica de control y causar efectos perjudiciales en los procesos que se están controlando en el entorno objetivo. Los objetivos de interés pueden incluir procedimientos activos o parámetros que manipulan el entorno físico. Estas técnicas también pueden incluir la prevención o manipulación de elementos de informe y lógica de control. Si un adversario ha modificado la funcionalidad del proceso, también puede ocultar los resultados, que a menudo se revelan por sí mismos en su impacto en el resultado de un producto o del entorno. El control físico directo que ejercen estas técnicas también puede amenazar la seguridad de los operadores y usuarios aguas abajo, lo que puede provocar mecanismos de respuesta. Los adversarios pueden seguir con técnicas de Inhibición de la Función de Respuesta o usarlas en conjunto para ayudar con el abuso exitoso de los procesos de control para causar Impacto.

Fuerza bruta de entrada/salida

Los adversarios pueden cambiar repetitiva o sucesivamente los valores de los puntos de E/S para realizar una acción. La Fuerza Bruta de E/S puede lograrse cambiando

repetidamente un rango de valores de puntos de E/S o un valor de punto único para manipular una función de proceso. El objetivo del adversario y la información que tengan sobre el entorno objetivo influirán en cuál de las opciones eligen. En el caso de la fuerza bruta de un rango de valores de puntos, el adversario puede lograr un impacto sin apuntar a un punto específico. En el caso en que se apunte a un solo punto, el adversario puede generar inestabilidad en la función de proceso asociada con ese punto en particular.Los adversarios pueden usar la Fuerza Bruta de E/S para causar fallas en varios procesos industriales. Estas fallas podrían ser el resultado del desgaste del equipo o el daño al equipo aguas abajo.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	El módulo IEC 104 de Industroyer tiene 3 modos disponibles para realizar su ataque. Estos modos son rango, desplazamiento y secuencia. El modo de rango opera en 2 etapas. La primera etapa del modo de rango recopila Direcciones de Objetos de Información (IOA) y envía paquetes de selección y ejecución para cambiar el estado. La segunda etapa del modo de rango tiene un bucle infinito donde cambiará el estado de todas las IOAs previamente descubiertas. El modo de desplazamiento es similar al modo de rango, pero en lugar de permanecer dentro del mismo rango, agregará un valor de desplazamiento a los valores de rango predeterminados.
S1072	Industroyer2	Industroyer2 puede iterar a través de las IOAs de un dispositivo para modificar el valor ENCENDIDO/APAGADO de un estado IO dado.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0002	Interfaz Persona-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0937	Filtrar Tráfico de Red	Las listas de permitidos/denegados pueden ser utilizadas para bloquear el acceso cuando se detectan conexiones I/O excesivas desde un sistema o dispositivo durante un período de tiempo especificado.
M0807	Listas de Permitidos de Red	Utilizar listas de permitidos de red para restringir conexiones innecesarias a dispositivos
		de red (por ejemplo, servidores de comunicación, convertidores serie a Ethernet) y servicios, especialmente en casos en los que los dispositivos tienen límites en el número de sesiones simultáneas que admiten.
M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión según su rol funcional dentro del proceso. Habilitar un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0813	Autenticación de Proceso de Software y Dispositivo	Los dispositivos deben autenticar todos los mensajes entre activos maestros y estaciones externas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0015	Log de Aplicación	Contenido del Log de Aplicación	Algunos registros de aplicación de activos pueden proporcionar información sobre puntos de E/S relacionados con comandos de escritura. Monitorear comandos de escritura para un número excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear el tráfico de red para funciones de ICS relacionadas con comandos de escritura para un número
			excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces.
DS0040	Bases de Datos Operativas	Historial de Procesos/Datos en Vivo	Monitorear datos operativos de proceso para comandos de escritura para un número excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces. Esto no detectará directamente la ejecución de la técnica, pero en cambio puede proporcionar evidencia adicional de que se ha utilizado la técnica y puede complementar otras detecciones.

Modificar parámetro

Los adversarios pueden modificar parámetros utilizados para instruir dispositivos de sistemas de control industrial. Estos dispositivos operan a través de programas que dictan cómo y cuándo realizar acciones basadas en dichos parámetros. Tales parámetros pueden determinar el alcance en el que se realiza una acción y pueden especificar opciones adicionales. Por ejemplo, un programa en un dispositivo de sistema de control que dicta procesos de motores puede tomar un parámetro que define el número total de segundos para ejecutar ese motor.

Un adversario puede potencialmente modificar estos parámetros para producir un resultado fuera de lo que los operadores pretendían. Al modificar parámetros críticos del sistema y del proceso, el adversario puede causar impacto en el equipo y/o en los procesos de control. Los parámetros modificados pueden convertirse en valores peligrosos, fuera de límites o inesperados en comparación con las operaciones típicas. Por ejemplo, especificar que un proceso se ejecute durante más o menos tiempo del necesario, o dictar un valor inusualmente alto, bajo o inválido como parámetro.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	El módulo IEC 104 de Industroyer tiene 3 modos disponibles para realizar su ataque. Estos modos son rango, desplazamiento y secuencia. El modo rango opera en 2 etapas. La primera etapa del modo rango recopila las Direcciones de Objetos de Información (IOA, por sus siglas en inglés) y envía paquetes de selección y ejecución para cambiar el estado. La segunda etapa del modo rango tiene un bucle infinito donde cambiará el estado de todas las IOAs previamente descubiertas. El modo desplazamiento es similar al modo rango, pero en lugar de quedarse dentro del mismo rango, agregará un valor de desplazamiento a los valores de rango predeterminados.
S1072	Industroyer2	Industroyer2 puede iterar a través de las IOAs de un dispositivo para modificar el valor de ENCENDIDO/APAGADO de un estado de entrada/salida dado.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0002	Interfaz Humano-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0937	Filtrar Tráfico de Red	Se pueden utilizar listas de permitir/denegar para bloquear el acceso cuando se detectan conexiones de E/S excesivas desde un sistema o dispositivo durante un período de tiempo especificado.
M0807	Listas Blancas de Red	Utilice listas blancas de red para restringir conexiones innecesarias a dispositivos de red (por ejemplo, servidores de comunicaciones, convertidores de serie a Ethernet) y servicios, especialmente en casos en que los dispositivos tengan límites en el número de sesiones simultáneas que admiten.
M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión según su rol funcional dentro del proceso. Habilitar
		un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0813	Autenticación de Procesos de Software y Dispositivos	Los dispositivos deben autenticar todos los mensajes entre activos maestros y de estación externa.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Algunos registros de aplicaciones de activos pueden proporcionar información sobre puntos de E/S relacionados con comandos de escritura. Monitorear los comandos de escritura para un número excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces.

DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear el tráfico de red para funciones de ICS relacionadas con comandos de escritura para un número excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces.
DS0040	Bases de Datos Operativas	Historial de Procesos/Datos en Vivo	Monitorear los datos operativos del proceso para comandos de escritura para un número excesivo de puntos de E/S o manipulación de un valor único un número excesivo de veces. Esto no detectará directamente la ejecución de la técnica, pero en cambio, puede proporcionar evidencia adicional de que la técnica ha sido utilizada y puede complementar otras detecciones.

Firmware del módulo

Los adversarios pueden instalar firmware malicioso o vulnerable en dispositivos de hardware modulares. Los dispositivos de sistemas de control a menudo contienen dispositivos de hardware modulares. Estos dispositivos pueden tener su propio conjunto de firmware que es independiente del firmware del equipo principal del sistema de control.

Esta técnica es similar a la del Firmware del Sistema, pero se lleva a cabo en otros componentes del sistema que pueden no tener las mismas capacidades o niveles de verificación de integridad. Aunque resulta en una reimagen del dispositivo, el firmware malicioso puede proporcionar acceso persistente a los dispositivos restantes.

Un punto de acceso fácil para un adversario es la tarjeta Ethernet, que puede tener su propia CPU, RAM y sistema operativo. El adversario puede atacar y probablemente explotar el equipo informático de una tarjeta Ethernet. La explotación del equipo informático de la tarjeta Ethernet puede permitir al adversario llevar a cabo ataques adicionales, como los siguientes:

Ataque Retardado: El adversario puede preparar un ataque con antelación y elegir cuándo lanzarlo, como en un momento especialmente dañino.

Convertir en "ladrillo" la Tarjeta Ethernet: El firmware malicioso puede estar programado para dejar inutilizable la tarjeta Ethernet, lo que requeriría un retorno a la fábrica para su reparación.

Ataque o Falla Aleatoria: El adversario puede cargar firmware malicioso en varios dispositivos de campo. La ejecución de un ataque y el momento en que ocurre se generan mediante un generador de números pseudoaleatorios.

Gusano de Dispositivo de Campo: El adversario puede optar por identificar todos los dispositivos de campo del mismo modelo, con el objetivo final de realizar un compromiso en toda la red de dispositivos.

Ataque a Otras Tarjetas en el Dispositivo de Campo: Aunque no es el módulo más importante en un dispositivo de campo, la tarjeta Ethernet es la más accesible para el adversario y el malware. El compromiso de la tarjeta Ethernet puede proporcionar una ruta más directa para comprometer otros módulos, como el módulo de CPU.

Activos Objetivo

ID	Activo
A0003	Controlador Lógico Programable (PLC)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0801	Gestión de Acceso	Todos los cambios en dispositivos o sistemas, incluidas todas las funciones administrativas, deben requerir autenticación. Considere el uso de tecnologías de gestión de acceso para hacer cumplir la autorización en todos los intentos de acceso a la interfaz de gestión, especialmente cuando el dispositivo no proporciona inherentemente funciones de autenticación y autorización sólidas.
M0947	Auditoría	Realice controles de integridad del firmware antes de cargarlo en un dispositivo. Utilice hashes criptográficos para verificar que el firmware no haya sido manipulado comparándolo con un hash confiable del firmware. Esto podría provenir de fuentes de datos confiables (por ejemplo, el sitio del proveedor) o a través de un servicio de verificación de terceros.
M0946	Integridad de Arranque	Verifique la integridad del BIOS o EFI existente para determinar si es vulnerable a modificaciones. Utilice la tecnología del Módulo de Plataforma Confiable. Mueva la raíz de confianza del sistema al hardware para evitar manipulaciones en la memoria flash SPI. Tecnologías como Intel Boot Guard pueden ayudar con esto.

M0945	Firma de Código	Los dispositivos deben verificar que el firmware haya sido firmado correctamente por el proveedor antes de permitir la instalación.
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para la gestión de dispositivos deben autenticar todos los mensajes de red para evitar cambios no autorizados en el sistema.
M0808	Encriptar el Tráfico de Red	Se debe considerar la encriptación del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0941	Encriptar Información Sensible	Se debe considerar la encriptación del firmware para evitar que los adversarios identifiquen posibles vulnerabilidades dentro del firmware.
M0937	Filtrar Tráfico de Red	Filtre los protocolos y cargas útiles asociados con la activación o actualización del firmware.
M0804	Autenticación de Usuario Humano	Los dispositivos que permiten la gestión remota del firmware deben requerir autenticación antes de permitir cualquier cambio. Los mecanismos de autenticación también deben admitir Políticas de Uso de Cuenta, Políticas de Contraseña y Gestión de Cuentas de Usuario.
M0807	Listas Blancas de Red	Utilice listas blancas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas blancas pueden usarse para garantizar que los dispositivos solo puedan conectarse
		con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar la red operativa y los sistemas para restringir el acceso a funciones críticas del sistema a sistemas de gestión predeterminados.
M0813	Autenticación de Procesos de Software y Dispositivos	Autentique las conexiones de software y dispositivos para evitar que sistemas no autorizados accedan a funciones de gestión protegidas.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear los registros de aplicación del dispositivo para cambios en el firmware, aunque no todos los dispositivos producirán tales registros.

DS0001	Firmware	Modificación de Firmware	Monitorear el firmware en busca de cambios inesperados. Se debe consultar a los sistemas de gestión de activos para comprender las versiones de firmware conocidas como válidas. Volcar e inspeccionar imágenes de BIOS en sistemas vulnerables y compararlas con imágenes conocidas como válidas. Analizar las diferencias para determinar si se han realizado cambios maliciosos. Del mismo modo, se pueden recopilar módulos EFI y compararlos con una lista conocida como limpia de binarios ejecutables EFI para detectar módulos potencialmente maliciosos. El framework CHIPSEC se puede usar para analizar si se han realizado
			modificaciones en el firmware.
DS0029	Tráfico de Red	Contenido del Tráfico de Red	Monitorear los protocolos de gestión de ICS/protocolos de transferencia de archivos para funciones de protocolo relacionadas con cambios en el firmware.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitorear cambios en el firmware que puedan ser observables a través de alarmas operativas de los dispositivos.

Falsificar mensaje de informe

Los adversarios pueden falsificar mensajes de informes en entornos de sistemas de control para evadir la detección y obstaculizar el control del proceso. En los sistemas de

control, los mensajes de informes contienen datos de telemetría (por ejemplo, valores de E/S) relacionados con el estado actual del equipo y el proceso industrial. Los mensajes de informes son importantes para monitorear la operación normal de un sistema o identificar eventos importantes, como desviaciones de los valores esperados.

Si un adversario tiene la capacidad de Falsificar Mensajes de Informes, puede impactar el sistema de control de muchas maneras. El adversario puede Falsificar Mensajes de Informes que indiquen que el proceso está funcionando normalmente, como una forma de evasión. El adversario también podría Falsificar Mensajes de Informes para hacer que los defensores y operadores piensen que están ocurriendo otros errores con el fin de distraerlos de la fuente real de un problema.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario utilizó un sistema de radio bidireccional analógico dedicado para enviar datos e instrucciones falsas a estaciones de bombeo y la computadora central.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0009	Puerta de Datos
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción

M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. Si no es así, utilice dispositivos bump-in-the-wire o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no sean capaces de admitir esto (por ejemplo, controladores heredados, RTUs).
M0937	Filtrar Tráfico de Red	Realice listas de permitidos en línea de comandos de protocolos de automatización para evitar que los dispositivos envíen mensajes de comando o informes no autorizados. Las técnicas de lista de permitidos/de negados deben diseñarse con suficiente precisión para evitar el bloqueo no intencionado de mensajes de informes válidos.
M0807	Listas Blancas de Red	Utilice listas blancas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas blancas pueden usarse para garantizar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión según su rol funcional dentro del proceso. Permitiendo un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0813	Autenticación de Procesos de Software y Dispositivos	Los dispositivos deben autenticar todos los mensajes entre activos maestros y externos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta

DS0029	Tráfico de Red	Contenido del Tráfico de Red	Los mensajes de informes falsificados pueden detectarse revisando el contenido de los protocolos de automatización, ya sea mediante la detección basada en valores esperados o comparando con otras fuentes de datos de proceso fuera de banda. Los mensajes falsificados pueden no coincidir precisamente con los mensajes legítimos, lo que puede llevar a un tráfico mal formado, aunque el tráfico puede estar mal formado por muchas razones benignas. Monitorear los mensajes de informes en busca de cambios en cómo están construidos. Varias técnicas permiten falsificar un mensaje de informe. Considere monitorear la actividad de Rogue Master y Adversario en el Medio.
		Flujo de Tráfico de Red	Varias técnicas permiten falsificar un mensaje de informe. Considere monitorear la actividad de Rogue Master y Adversario en el Medio, que pueden preceder a esta técnica.
DS0040	Bases de Datos Operativas	Alarma del Dispositivo	Monitoree los registros de activos en busca de alarmas u otra información que el adversario no pueda suprimir directamente. Las alarmas relevantes incluyen aquellas de una pérdida de comunicaciones debido a la
			actividad de Adversario en el Medio.

DS0024	Registro de Windows	Modificación de Clave de Registro de Windows	Varias técnicas permiten falsificar un mensaje de informe. Monitorear el envenenamiento LLMNR/NBT-NS mediante nuevos servicios/demonios que pueden usarse para habilitar esta técnica. Para obtener más contexto sobre los procedimientos y antecedentes del adversario, consulte Envenenamiento LLMNR/NBT-NS y Relevación de SMB.

Mensaje de comando no autorizado

Los adversarios pueden enviar mensajes de comando no autorizados para instruir a los activos del sistema de control para que realicen acciones fuera de su funcionalidad prevista, o sin las condiciones lógicas necesarias para activar su función esperada. Los mensajes de comando se utilizan en redes de sistemas de control industrial para dar instrucciones directas a los dispositivos de sistemas de control. Si un adversario puede enviar un mensaje de comando no autorizado a un sistema de control, entonces puede instruir al dispositivo de sistemas de control para que realice una acción fuera de los límites normales de las acciones del dispositivo. Un adversario podría potencialmente ordenar a un dispositivo de sistemas de control que realice una acción que cause un Impacto.

En el incidente de las sirenas de Dallas, los adversarios pudieron enviar mensajes de comando para activar sistemas de alarmas de tornado en toda la ciudad sin que hubiera un tornado inminente u otro desastre.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm emitió comandos no autorizados a las subestaciones después de tomar el control de las estaciones de trabajo del operador y acceder a una aplicación de sistema de gestión de distribución (DMS).

S1045	INCONTROLLER	INCONTROLLER puede enviar comandos Modbus personalizados para escribir valores de registro en PLCs Schneider. INCONTROLLER puede enviar valores de etiquetas de escritura en servidores OPC UA.
S0604	Industroyer	Utilizando sus cargas de protocolo, Industroyer envía comandos no autorizados a RTUs para cambiar el estado del equipo.
S1072	Industroyer2	Industroyer2 es capaz de enviar mensajes de comando desde el dispositivo comprometido a estaciones remotas objetivo para abrir canales de datos, recuperar la ubicación y los valores de las Direcciones de Objetos de Información (IOAs) y modificar los valores del estado de IO a través de operaciones de Seleccionar antes de Operar IO, Seleccionar/Ejecutar e Invertir Estado Predeterminado.
C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario utilizó un sistema de radio bidireccional analógico dedicado para enviar datos e instrucciones falsas a estaciones de bombeo y la computadora central.

Activos Objetivo

ID	Activo
A0007	Servidor de Control
A0002	Interfaz Hombre-Máquina (HMI)
A0005	Dispositivo Electrónico Inteligente (IED)
A0003	Controlador Lógico Programable (PLC)
A0004	Unidad Terminal Remota (RTU)
A0010	Controlador de Seguridad

Mitigaciones

ID	Mitigación	Descripción
M0802	Autenticidad de Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. De lo contrario, utilice dispositivos bump-in-the-wire o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de admitir esto (por ejemplo, controladores heredados, RTUs).

M0937	Filtrar Tráfico de Red	Realice listas de permitidos en línea de comandos de protocolos de automatización para evitar que los dispositivos envíen comandos no autorizados o mensajes de informe. Las técnicas de listado de permitidos/denegados deben diseñarse con suficiente precisión para evitar el bloqueo no intencionado de mensajes válidos.
M0807	Listas de Permitidos en Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden usar para asegurar que los dispositivos solo puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0930	Segmentación de Red	Segmentar los activos operativos y sus dispositivos de gestión según su rol funcional dentro del proceso. Habilitar un aislamiento más estricto para la información de control y operativa más crítica dentro del entorno de control.
M0813	Autenticación de Proceso de Software y Dispositivo	Los dispositivos deben autenticar todos los mensajes entre activos maestros y de salida.
M0818	Validar Entradas del Programa	Los dispositivos y programas que reciben mensajes de comando de sistemas remotos (por ejemplo, servidores de control) deben verificar esos comandos antes de tomar cualquier acción sobre ellos.

Detección

ID	Fuente de Datos	Componente de Datos	Detecta
DS0015	Registro de Aplicación	Contenido del Registro de Aplicación	Monitorear comandos anómalos o inesperados que puedan provocar cambios en la operación del proceso (por ejemplo, escritura discreta, configuración de lógica y dispositivo, cambios de modo) observables a través de registros de aplicaciones de activos.

DS0029	Trafico de Red	Contenido del Trafico de Red	Monitorear funciones de comando de protocolos ICS inesperadas hacia controladores desde dispositivos maestros existentes (incluidos nuevos procesos) o desde nuevos dispositivos. El último es como detección para Maestro Falso pero requiere una visión a nivel de función ICS para determinar si un dispositivo no

			autorizado está emitiendo comandos (por ejemplo, un historiador). El monitoreo de valores inesperados o problemáticos por debajo del nivel de función proporcionará mejores conocimientos sobre actividades potencialmente maliciosas, pero a costa de falsos positivos adicionales según el proceso operativo subyacente.
		Flujo de Trafico de Red	Monitorear conexiones nuevas o inesperadas a controladores, lo que podría indicar que se envía un Mensaje de Comando No Autorizado a través de un Maestro Falso.

DS0040	Bases de Datos Operativas	Datos de Historial de Procesos/Datos en Vivo	Monitorear datos de historial de procesos industriales en busca de eventos que correspondan con funciones de mensajes de comando, como modificación de punto de ajuste o cambios en el estado del sistema para dispositivos clave. Esto no detectará directamente la ejecución de la técnica, pero en cambio puede proporcionar evidencia adicional de que se ha utilizado la técnica y puede complementar otras detecciones.
		Alarma de Proceso/Evento	Monitorear comandos anómalos o inesperados que puedan provocar cambios en la operación del proceso (por ejemplo, escritura discreta, configuración de lógica y dispositivo, cambios de
			modo) observables a través de registros de aplicaciones de activos.

IMPACTO

El adversario está intentando manipular, interrumpir o destruir tus sistemas ICS, datos y su entorno circundante.

El Impacto consiste en técnicas que los adversarios utilizan para interrumpir, comprometer, destruir y manipular la integridad y disponibilidad de las operaciones, procesos, dispositivos y datos del sistema de control. Estas técnicas abarcan la influencia y los efectos resultantes de los esfuerzos adversarios para atacar el entorno ICS o que impactan tangencialmente en él. Las técnicas de Impacto pueden provocar una interrupción más instantánea en los procesos de control y en el operador, o pueden resultar en daños o pérdidas a largo plazo en el entorno ICS y las operaciones relacionadas. El adversario puede aprovechar las técnicas de Alteración del Control de Procesos, que a menudo se manifiestan en impactos más evidentes en las operaciones,

o técnicas de Inhibición de la Función de Respuesta para obstaculizar salvaguardias y alarmas con el fin de llevar a cabo y proporcionar cobertura para el Impacto. En algunos escenarios, los procesos del sistema de control pueden parecer funcionar como se esperaba, pero pueden haber sido alterados para beneficiar el objetivo del adversario a lo largo de un período más prolongado. Estas técnicas pueden ser utilizadas por los adversarios para cumplir su objetivo final o para proporcionar cobertura para una violación de confidencialidad.

La Pérdida de Productividad y de Ingresos, el Robo de Información Operativa y el Daño a la Propiedad están destinados a abarcar algunos de los objetivos más específicos de los adversarios en ataques dirigidos y no dirigidos. Estas técnicas en sí mismas no son necesariamente detectables, pero el comportamiento adversario asociado puede ser potencialmente mitigado y/o detectado.

Daño a la propiedad

Los adversarios pueden causar daños y destrucción de propiedad a la infraestructura, equipos y el entorno circundante al atacar sistemas de control. Esta técnica puede provocar el colapso de equipos y equipos operativos, o representar daños colaterales de otras técnicas utilizadas en un ataque. Dependiendo de la gravedad del daño físico y la interrupción causada a los procesos y sistemas de control, esta técnica puede resultar en Pérdida de Seguridad. Las operaciones que resultan en Pérdida de Control también pueden causar daños a la propiedad, que pueden ser directa o indirectamente motivados por un adversario que busca causar impacto en forma de Pérdida de Productividad y de Ingresos.

La Oficina Federal de Seguridad de la Información de Alemania (BSI) informó sobre un ataque dirigido a una acería en la sección de incidentes que afectan a los negocios de su Informe de Seguridad de TI de 2014. Estos ataques dirigidos afectaron las operaciones industriales y resultaron en el colapso de componentes del sistema de control e incluso de instalaciones enteras. Como resultado de estos colapsos, se produjo un impacto masivo y daños debido al apagado no controlado de un alto horno.

Un estudiante polaco utilizó un dispositivo controlador remoto para interactuar con el sistema de tranvías de la ciudad de Lodz en Polonia. Utilizando este control remoto, el estudiante pudo capturar y reproducir señales de tranvía legítimas. Esto resultó en daños a los tranvías afectados, personas y la propiedad circundante. Según informes, cuatro tranvías descarrilaron y se vieron obligados a realizar paradas de emergencia. Los comandos emitidos por el estudiante también pueden haber resultado en colisiones de tranvías, causando daños a los pasajeros y al entorno exterior.

Ejemplos de Procedimientos

ID	Nombre	Descripción

C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario obtuvo acceso remoto a la computadora de control y alteró datos de manera que cualquier función que debía ocurrir en las estaciones de bombeo afectadas no ocurrió o ocurrió de manera diferente. Esto condujo en última instancia a que 800,000 litros de aguas residuales crudas se derramaran en la comunidad. Las aguas residuales crudas afectaron parques locales, ríos e incluso un hotel local. Esto resultó en daños a la vida marina y produjo un hedor nauseabundo en los ríos afectados de la comunidad.

Mitigaciones

ID	Mitigación	Descripción
M0805	Capas de Protección Mecánica	Los dispositivos de protección deben tener componentes digitales mínimos para evitar la exposición a técnicas adversariales relacionadas. Ejemplos incluyen bloqueos, discos de ruptura, válvulas de liberación, etc.
M0807	Listas de Permitidos en Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden usar para asegurar que los dispositivos solo
		puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0812	Sistemas Instrumentados de Seguridad	Asegúrese de que todos los SIS estén segmentados de las redes operativas para evitar que sean objeto de comportamientos adversarios adicionales.

Negación de control

Los adversarios pueden causar una negación de control para evitar temporalmente que los operadores e ingenieros interactúen con los controles del proceso. Un adversario puede intentar negar el acceso al control del proceso para causar una pérdida temporal de comunicación con el dispositivo de control o para evitar que el operador ajuste los controles del proceso. Durante el período de pérdida de control, el proceso afectado puede seguir operando, pero no necesariamente en un estado deseado.

En el incidente de las sirenas de Dallas en 2017, los operadores no pudieron desactivar las alarmas falsas desde la sede de la Oficina de Gestión de Emergencias.

Ejemplos de Procedimientos

ID	Nombre	Descripción

C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario obtuvo acceso remoto a la computadora de control y alteró datos de manera que cualquier función que debía ocurrir en las estaciones de bombeo afectadas no ocurrió o ocurrió de manera diferente. Esto condujo en última instancia a que 800,000 litros de aguas residuales crudas se derramaran en la comunidad. Las aguas residuales crudas afectaron parques locales, ríos e incluso un hotel local. Esto resultó en daños a la vida marina y produjo un hedor nauseabundo en los ríos afectados de la comunidad.

Mitigaciones

ID	Mitigación	Descripción
M0805	Capas de Protección Mecánica	Los dispositivos de protección deben tener componentes digitales mínimos para evitar la exposición a técnicas adversariales relacionadas. Ejemplos incluyen bloqueos, discos de ruptura, válvulas de liberación, etc.
M0807	Listas de Permitidos en Red	Utilice listas de permitidas basadas en host para evitar que los dispositivos acepten conexiones de sistemas no autorizados. Por ejemplo, las listas de permitidos se pueden usar para asegurar que los dispositivos solo
		puedan conectarse con estaciones maestras o estaciones de trabajo de gestión/ingeniería conocidas.
M0812	Sistemas Instrumentados de Seguridad	Asegúrese de que todos los SIS estén segmentados de las redes operativas para evitar que sean objeto de comportamientos adversarios adicionales.

Negación de Vista

Los adversarios pueden causar una negación de vista en un intento de interrumpir y prevenir la supervisión por parte de los operadores sobre el estado de un entorno de sistemas de control industrial (ICS, por sus siglas en inglés). Esto puede manifestarse como una falla temporal de comunicación entre un dispositivo y su fuente de control, donde la interfaz se recupera y vuelve a estar disponible una vez que cesa la interferencia.

Un adversario puede intentar negar la visibilidad del operador al evitar que reciban mensajes de estado e informes. Negar esta vista puede bloquear temporalmente y evitar que los operadores noten un cambio de estado o un comportamiento anómalo. Los datos y procesos del entorno pueden seguir siendo operativos, pero funcionando de manera no deseada o adversa.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	Industroyer es capaz de bloquear temporalmente canales COM serie causando una denegación de vista.
C0020	Violación del Agua de Maroochy	En la Violación del Agua de Maroochy, el adversario temporalmente excluyó a un investigador de la red, impidiéndole ver el estado del sistema.

Mitigaciones

ID	Mitigación	Descripción
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de sistemas de usuario final y servidores críticos. Asegurarse de que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para prevenir compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluida la gestión de imágenes de copia de seguridad de referencia y configuraciones para sistemas clave para permitir una recuperación y respuesta rápida
		ante actividades adversarias que afecten el control, la visualización o la disponibilidad.
M0810	Canal de Comunicaciones Fuera de Banda	Proporcionar a los operadores una comunicación redundante fuera de banda para respaldar el monitoreo y control de los procesos operativos, especialmente al recuperarse de una interrupción de red. La comunicación fuera de banda debe utilizar sistemas y tecnologías diversas para minimizar los modos de falla comunes y las vulnerabilidades dentro de la infraestructura de comunicaciones. Por ejemplo, las redes inalámbricas (por ejemplo, 3G, 4G) se pueden utilizar para proporcionar entrega diversa y redundante de datos.
M0811	Redundancia de Servicio	Los sistemas de reserva en ubicaciones diversas pueden garantizar operaciones continuas si los sistemas principales están comprometidos o no están disponibles. En la capa de red, se pueden utilizar protocolos como el Protocolo de Redundancia Paralela para utilizar simultáneamente comunicaciones redundantes y diversas sobre una red local.

Pérdida de Disponibilidad

Los adversarios pueden intentar interrumpir componentes o sistemas esenciales para evitar que los propietarios y operadores entreguen productos o servicios.

Los adversarios pueden aprovecharse del malware para eliminar o cifrar datos críticos en interfaces hombre-máquina (HMI), estaciones de trabajo o bases de datos.

En el incidente de ransomware del Oleoducto Colonial en 2021, las operaciones del oleoducto fueron temporalmente detenidas el 7 de mayo y no se reiniciaron completamente hasta el 12 de mayo.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, el Equipo Sandworm abrió los interruptores en los sitios infectados, cortando la energía eléctrica para miles de negocios y hogares durante alrededor de 6 horas.
S0608	Conficker	Una infección de Conficker en una planta de energía nuclear obligó a la instalación a cerrar temporalmente.

Mitigaciones

ID	Mitigación	Descripción
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de sistemas de usuario final y servidores críticos. Asegurarse de que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para prevenir compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluida la gestión de imágenes de copia de seguridad de referencia y configuraciones para sistemas clave para permitir una recuperación y respuesta rápida ante actividades adversarias que afecten el control, la visualización o la disponibilidad.

M0810	Canal de Comunicaciones Fuera de Banda	Proporcionar a los operadores una comunicación redundante fuera de banda para respaldar el monitoreo y control de los procesos operativos, especialmente al recuperarse de una interrupción de red. La comunicación fuera de banda debe utilizar sistemas y tecnologías diversas para minimizar los modos de falla comunes y las vulnerabilidades dentro de la infraestructura de comunicaciones. Por ejemplo, las redes inalámbricas (por ejemplo, 3G, 4G) se pueden utilizar para proporcionar entrega diversa y redundante de datos.
M0811	Redundancia de Servicio	Los sistemas de reserva en ubicaciones diversas pueden garantizar operaciones continuas si los sistemas principales están comprometidos o no están disponibles. En la capa de red, se pueden utilizar protocolos como el Protocolo de Redundancia Paralela para utilizar simultáneamente comunicaciones redundantes y diversas sobre una red local.

Pérdida de Control

Los adversarios pueden buscar lograr una pérdida de control sostenida o una condición de "runaway" en la que los operadores no puedan emitir ningún comando incluso si la interferencia maliciosa ha disminuido.

La Oficina Federal de Seguridad de la Información de Alemania (BSI) informó sobre un ataque dirigido a una acería en su Informe de Seguridad de TI de 2014. Estos ataques dirigidos afectaron las operaciones industriales y resultaron en el colapso de componentes del sistema de control e incluso de instalaciones enteras. Como resultado de estos colapsos, se produjo un impacto masivo en daños y condiciones inseguras debido al apagado no controlado de un alto horno.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, los operadores fueron excluidos de sus equipos ya sea mediante la denegación de uso periférico o la degradación del equipo. Por lo tanto, los operadores no pudieron recuperarse del incidente a través de sus medios tradicionales. Gran parte de la energía fue restaurada manualmente.
S0604	Industroyer	El componente de borrado de datos de Industroyer elimina la ruta de la imagen del registro en todo el sistema y sobrescribe todos los archivos, dejando el sistema inservible.

S0372	LockerGoga	Algunos de los sistemas de producción de Norsk Hydro se vieron afectados por una infección de LockerGoga. Esto resultó en una pérdida de control que obligó a la empresa a cambiar a operaciones manuales.

Mitigaciones

ID	Mitigación	Descripción
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de sistemas de usuario final y servidores críticos. Asegurarse de que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para prevenir compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluida la gestión de imágenes de copia de seguridad de referencia y configuraciones para sistemas clave para permitir una recuperación y respuesta rápida ante actividades adversarias que afecten el control, la visualización o la disponibilidad.
M0810	Canal de Comunicaciones Fuera de Banda	Proporcionar a los operadores una comunicación redundante fuera de banda para respaldar el monitoreo y control de los procesos operativos, especialmente al recuperarse de una interrupción de red. La comunicación fuera de banda debe utilizar sistemas y tecnologías diversas para minimizar los modos de falla comunes y las vulnerabilidades dentro de la infraestructura de comunicaciones. Por ejemplo, las redes inalámbricas (por ejemplo, 3G, 4G) se pueden utilizar para proporcionar entrega diversa y redundante de datos.
M0811	Redundancia de Servicio	Los sistemas de reserva en ubicaciones diversas pueden garantizar operaciones continuas si los sistemas principales están comprometidos o no están disponibles. En la capa de red, se pueden utilizar protocolos como el Protocolo de Redundancia Paralela para utilizar
		simultáneamente comunicaciones redundantes y diversas sobre una red local.

Pérdida de Productividad y de Ingresos

Los adversarios pueden causar pérdida de productividad y de ingresos mediante la interrupción e incluso el daño a la disponibilidad y la integridad de las operaciones del sistema de control, dispositivos y procesos relacionados. Esta técnica puede manifestarse como un efecto directo de un ataque dirigido al sistema de control

industrial (ICS) o, de manera tangencial, debido a un ataque dirigido a tecnologías de la información (IT) en entornos no segregados.

En los casos en que estas operaciones o servicios se detienen, la pérdida de productividad puede eventualmente presentar un impacto para los usuarios finales o consumidores de productos y servicios. La cadena de suministro interrumpida puede resultar en escasez de suministros y aumentos de precios, entre otras consecuencias.

Un ataque de ransomware a una empresa de bebidas australiana resultó en el cierre de algunas plantas de fabricación, incluidas paradas precautorias para proteger los sistemas clave. La empresa anunció la posibilidad de escasez temporal de sus productos después del ataque.

En el incidente de ransomware del Oleoducto Colonial en 2021, el oleoducto no pudo transportar aproximadamente 2.5 millones de barriles de combustible por día a la costa este.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania en 2015, se abrieron interruptores de energía lo que causó que las empresas operadoras no pudieran suministrar energía, dejando a miles de negocios y hogares sin electricidad durante alrededor de 6 horas.
S0606	Bad Rabbit	Según informes de medios, varias organizaciones de transporte en Ucrania han sufrido infecciones por Bad Rabbit, lo que ha provocado que algunas computadoras queden encriptadas.
S0608	Conficker	Una infección de Conficker en una planta de energía nuclear obligó a la instalación a cerrar y pasar por procedimientos de seguridad involucrados en tales eventos, con su personal escaneando sistemas informáticos y pasando por todos los controles y procedimientos habituales antes de poner la planta nuevamente en producción.
S0605	EKANS	La infección por EKANS resultó en una pérdida temporal de producción dentro de una planta de fabricación de Honda.
S0372	LockerGoga	Mientras Norsk Hydro intentaba recuperarse de una infección de LockerGoga, la mayoría de sus 160 ubicaciones de fabricación pasaron a operaciones manuales (no impulsadas por TI). Las operaciones manuales pueden resultar en una pérdida de productividad.

S0368	NotPetya	NotPetya interrumpió las instalaciones de fabricación que suministraban vacunas, lo que resultó en la detención de la producción y la imposibilidad de satisfacer la demanda de vacunas específicas.
S0496	REvil	El malware REvil obtuvo acceso a la red de una organización y encriptó archivos sensibles utilizados por equipos de OT.
S0446	Ryuk	Un servidor de planificación de recursos empresariales (ERP) de fabricación se perdió debido al ataque de Ryuk. El proceso de fabricación tuvo que depender de papel y pedidos existentes para mantener abierta la planta.

Mitigaciones

ID	Mitigación	Descripción
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de sistemas de usuario final y servidores críticos. Asegurarse de que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para prevenir compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluida la gestión de imágenes de copia de seguridad de referencia y configuraciones para sistemas clave para permitir una recuperación y respuesta rápida ante actividades adversarias que afecten el control, la visualización o la disponibilidad.

Pérdida de Protección

Los adversarios pueden comprometer las funciones de sistemas de protección diseñadas para prevenir los efectos de fallas y condiciones anormales. Esto puede resultar en daños al equipo, interrupciones prolongadas en los procesos y peligros para el personal.

Muchas fallas y condiciones anormales en el control de procesos ocurren demasiado rápido para que un operador humano reaccione. La velocidad es crucial para corregir estas condiciones y limitar impactos graves como la Pérdida de Control y el Daño a la Propiedad.

Los adversarios pueden dirigirse y desactivar funciones de sistemas de protección como un requisito previo para la ejecución de ataques posteriores o para permitir que futuras fallas y condiciones anormales pasen desapercibidas. La detección de una Pérdida de Protección por parte de los operadores puede resultar en el apagado de un proceso debido a políticas estrictas con respecto a los sistemas de protección. Esto puede causar una Pérdida de Productividad e Ingresos y puede cumplir con los objetivos técnicos de los adversarios que buscan causar interrupciones en el proceso.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	Industroyer contenía un módulo que aprovechaba una vulnerabilidad en los relés de protección Siemens SIPROTEC (CVE-2015-5374) para crear una Denegación de Servicio contra relés de protección automatizados.

Mitigaciones

Este tipo de técnica de ataque no puede mitigarse fácilmente con controles preventivos, ya que se basa en el abuso de características del sistema.

Pérdida de Seguridad

Los adversarios pueden comprometer las funciones de los sistemas de seguridad diseñados para mantener la operación segura de un proceso cuando ocurren condiciones inaceptables o peligrosas. Los sistemas de seguridad a menudo están compuestos por los mismos elementos que los sistemas de control, pero tienen el único propósito de garantizar que el proceso falle de manera segura de acuerdo con un plan predeterminado.

Muchas condiciones inseguras en el control de procesos ocurren demasiado rápido para que un operador humano reaccione. La velocidad es crucial para corregir estas condiciones y limitar impactos graves como la Pérdida de Control y el Daño a la Propiedad.

Los adversarios pueden dirigirse y desactivar las funciones de los sistemas de seguridad como un requisito previo para la ejecución de ataques posteriores o para permitir que futuras condiciones inseguras pasen desapercibidas. La detección de una Pérdida de Seguridad por parte de los operadores puede resultar en el apagado de un proceso debido a políticas estrictas con respecto a los sistemas de seguridad. Esto puede causar una Pérdida de Productividad e Ingresos y puede cumplir con los objetivos técnicos de los adversarios que buscan causar interrupciones en el proceso.

Ejemplos de procedimiento

ID	Name	Description
S1009	Triton	Triton tiene la capacidad de reprogramar la lógica del Sistema Instrumentado de Seguridad (SIS) para permitir que persistan condiciones inseguras o reprogramar el SIS para permitir un estado inseguro mientras utiliza el Sistema de Control Distribuido (DCS) para crear un estado inseguro o un peligro.

Mitigaciones

ID	Mitigación	Descripción
M0805	Capas de Protección Mecánica	Los dispositivos de protección deben tener componentes digitales mínimos para evitar la exposición a técnicas adversarias relacionadas. Ejemplos incluyen bloqueos, discos de ruptura, válvulas de liberación, etc.
M0812	Sistemas Instrumentados de Seguridad	Asegúrese de que todos los SIS estén segmentados de las redes operativas para evitar que sean objeto de comportamientos adversarios adicionales.

Pérdida de Vista

Los adversarios pueden causar una pérdida de vista sostenida o permanente en la que el equipo de sistemas de control industrial (ICS) requerirá intervención local y manual por parte de los operadores; por ejemplo, un reinicio o operación manual. Al causar una pérdida sostenida de informes o visibilidad, el adversario puede ocultar efectivamente el estado actual de las operaciones. Esta pérdida de vista puede ocurrir sin afectar los procesos físicos en sí mismos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	El componente de borrado de datos de Industroyer elimina la ruta de imagen del registro en todo el sistema y sobrescribe todos los archivos, dejando el sistema inutilizable.
S0607	KillDisk	KillDisk borra el registro maestro de arranque (MBR) y los registros del sistema, dejando el sistema inutilizable.
S0372	LockerGoga	Algunos de los sistemas de producción de Norsk Hydro fueron afectados por una infección de LockerGoga. Esto resultó en una pérdida de visión que obligó a la empresa a cambiar a operaciones manuales.

Mitigaciones

ID	Mitigación	Descripción

M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de los sistemas de usuario final y servidores críticos. Asegurar que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para evitar compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluyendo la gestión de imágenes de copia de seguridad de copia dorada y configuraciones para sistemas clave para permitir una recuperación rápida y respuesta ante actividades adversas que afecten al control, visión o disponibilidad.
M0810	Canal de Comunicación Fuera de Banda	Proporcionar a los operadores comunicación redundante, fuera de banda para apoyar la monitorización y control de los procesos operativos, especialmente al recuperarse de una interrupción de red. La comunicación fuera de banda debe utilizar sistemas y tecnologías diversas para minimizar los modos de fallo comunes y las vulnerabilidades dentro de la infraestructura de comunicaciones. Por ejemplo, las redes inalámbricas (por ejemplo, 3G, 4G) pueden utilizarse para proporcionar entrega diversa y redundante de datos.
M0811	Redundancia del Servicio	Los sistemas de reserva activa en ubicaciones diversas pueden garantizar operaciones continuas si los sistemas primarios están comprometidos o no están disponibles. En la capa de red, protocolos como el Protocolo de Redundancia Paralela pueden utilizarse para utilizar simultáneamente comunicación redundante y diversa sobre una red local.

Manipulación de Control

Los adversarios pueden manipular el control de procesos físicos dentro del entorno industrial. Los métodos de manipulación del control pueden incluir cambios en los valores de punto de ajuste, etiquetas u otros parámetros. Los adversarios pueden manipular dispositivos de sistemas de control o posiblemente aprovechar los suyos propios, para comunicarse y ordenar procesos de control físico. La duración de la manipulación puede ser temporal o más prolongada, dependiendo de la detección por parte del operador.

Los métodos de manipulación del control incluyen:

- Hombre en el medio
- Mensaje de comando falso
- Cambio de puntos de ajuste

Un estudiante polaco utilizó un dispositivo de control remoto para interactuar con el sistema de tranvías de la ciudad de Lodz en Polonia. Usando este control remoto, el estudiante pudo capturar y reproducir señales legítimas de tranvía. Como

consecuencia, cuatro tranvías descarrilaron y doce personas resultaron heridas debido a las paradas de emergencia resultantes. Los comandos de control de la vía emitidos también podrían haber resultado en colisiones de tranvías, representando un riesgo adicional para los pasajeros y las áreas cercanas a los puntos de impacto.

Ejemplos de Procedimientos

ID	Nombre	Descripción
C0028	Ataque al Suministro Eléctrico de Ucrania 2015	Durante el Ataque al Suministro Eléctrico de Ucrania de 2015, el Equipo Sandworm abrió interruptores en vivo mediante comandos remotos al HMI, causando apagones.
S0604	Industroyer	Industroyer cambia los interruptores al estado abierto utilizando mensajes de comando no autorizados.
S0603	Stuxnet	Stuxnet puede reprogramar un PLC y cambiar parámetros críticos de tal manera que los comandos legítimos puedan ser anulados o interceptados. Además, Stuxnet puede aplicar secuencias o parámetros de comando inapropiados para causar daños a la propiedad.

Mitigaciones

ID	Mitigación	Descripción
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. De lo contrario, utilizar dispositivos de paso o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de soportar esto (por ejemplo, controladores heredados, RTUs).
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de los sistemas de usuario final y servidores críticos. Asegurar que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red corporativa para evitar compromisos. Mantener y ejercitar planes de respuesta a incidentes, incluyendo la gestión de imágenes de copia de seguridad de copia dorada y configuraciones para sistemas clave para permitir una recuperación rápida y respuesta ante actividades adversas que afecten al control, visión o disponibilidad.

M0810	Canal de Comunicación Fuera de Banda	Utilizar comunicación fuera de banda para validar la integridad de los datos del canal primario.

Manipulación de la Vista

Los adversarios pueden intentar manipular la información reportada a los operadores o controladores. Esta manipulación puede ser a corto plazo o sostenida. Durante este tiempo, el proceso mismo podría estar en un estado muy diferente al que se reporta.

Los operadores pueden ser engañados para hacer algo que sea perjudicial para el sistema en una situación de pérdida de visión. Con una vista manipulada de los sistemas, los operadores pueden emitir secuencias de control inapropiadas que introducen fallas o fallos catastróficos en el sistema. Los sistemas de análisis empresarial también pueden recibir datos inexactos que conducen a decisiones de gestión deficientes.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S0604	Industroyer	El módulo OPC de Industroyer puede forzar valores y enviará un estado 0x01 que, para los sistemas objetivo, equivale a un Valor Principal Fuera de Límites, desviando a los operadores de comprender el estado del relé de protección.
S0603	Stuxnet	Stuxnet manipula la vista de los operadores reproduciendo la entrada del proceso y manipulando la imagen de E/S para evadir la detección e inhibir las funciones de protección.

Mitigaciones

ID	Mitigación	Descripción
M0802	Autenticidad de la Comunicación	Los protocolos utilizados para funciones de control deben proporcionar autenticidad a través de funciones MAC o firmas digitales. De lo contrario, utilizar dispositivos de paso o VPN para hacer cumplir la autenticidad de la comunicación entre dispositivos que no son capaces de soportar esto (por ejemplo, controladores heredados, RTUs).
M0953	Copia de Seguridad de Datos	Realizar y almacenar copias de seguridad de datos de los sistemas de usuario final y servidores críticos. Asegurar que los sistemas de copia de seguridad y almacenamiento estén fortificados y se mantengan separados de la red

		corporativa para evitar compromisos. Mantener y ejercitar planes de respuesta a incidentes , incluyendo la gestión de imágenes de copia de seguridad de copia dorada y configuraciones para sistemas clave para permitir una recuperación rápida y respuesta ante actividades adversas que afecten al control, visión o disponibilidad.
M0810	Canal de Comunicación Fuera de Banda	Utilizar comunicación fuera de banda para validar la integridad de los datos del canal primario.

Robo de Información Operativa

Los adversarios pueden robar información operativa en un entorno de producción como resultado directo de su misión para obtener beneficio personal o para informar operaciones futuras. Esta información puede incluir documentos de diseño, horarios, datos rotacionales u artefactos similares que proporcionen información sobre las operaciones. En el incidente de la presa Bowman, los adversarios exploraron los sistemas en busca de datos operativos.

Ejemplos de Procedimientos

ID	Nombre	Descripción
S1000	ACAD/Medre.A	ACAD/Medre.A puede recopilar archivos de AutoCad con dibujos. Estos dibujos pueden contener información operativa.
S0038	Duqu	El propósito de Duqu es recopilar datos de inteligencia y activos de entidades como infraestructuras industriales y fabricantes de sistemas, entre otros no pertenecientes al sector industrial, para poder realizar más fácilmente un ataque futuro contra otro tercero.
S0143	Flame	Flame puede recopilar datos de diseño de AutoCAD y diagramas de Visio, así como otros documentos que pueden contener información operativa.
S0496	REvil	REvil envía datos exfiltrados del sistema de las víctimas utilizando mensajes POST HTTPS enviados al sistema de comando y control (C2).

Mitigaciones

ID	Mitigación	Descripción
M0803	Prevención de Pérdida de Datos	Aplicar DLP para proteger la confidencialidad de la información relacionada con procesos operativos, ubicaciones de instalaciones, configuraciones de dispositivos, programas o bases de datos que pueden contener información que pueda utilizarse para inferir secretos comerciales, recetas y otra propiedad intelectual (PI) organizacional.
M0941	Encriptar Información Sensible	Encriptar cualquier dato operativo con requisitos estrictos de confidencialidad, incluidos secretos comerciales de la organización, recetas y otra propiedad intelectual (PI).
M0809	Confidencialidad de la Información Operativa	Las mitigaciones de ejemplo podrían incluir minimizar su distribución/almacenamiento u ofuscar la información (por ejemplo, términos de cobertura de instalaciones, nombres en clave). En muchos casos, esta información puede ser necesaria para respaldar funciones críticas de ingeniería, mantenimiento u operativas, por lo tanto, puede que no sea factible implementarla.
M0922	Restringir Permisos de Archivos y Directorios	Proteger los archivos almacenados localmente con permisos adecuados para limitar las oportunidades para que los adversarios interactúen y recopilen información de las bases de datos.

Exploits disponibles

CJ2M-CPU31(Firmware)

Nombre	Vector de ataque	Tipo	Metasploit
CVE-2023-38744	Red	DoS	No
CVE-2023-27396	Red	Interceptar comunicaciones/Ejecutar comandos arbitrarios/Recuperar información del sistema	No
CVE-2023-45790	Red	Interceptar mensajes/Omitir la autenticación/Modificar valores	No

(No he encontrado más antiguos)

CJ2M(Hardware)

Nombre	Vector de ataque	Tipo	Metasploit
CVE-2015-1015	Local	Vulnerabilidad de contraseñas reversibles	No
CVE-2015-0987	Red	Transmisión insegura de contraseñas	No

CX-Programmer

Nombre	Vector de ataque	Tipo	Metasploit
CVE-2023-38748	Local	Corrupcion de memoria/Filtracion de informacion	No
CVE-2023-38747	Local	Desbordamiento/Corrupcion de memoria/Filtracion de informacion	No
CVE-2023-38746	Local	Filtracion de informacion	No
CVE-2023-22317	Local	Corrupcion de memoria/Filtracion de informacion	No
CVE-2023-22314	Local	Corrupcion de memoria/Filtracion de informacion	No
CVE-2023-22277	Local	Corrupcion de memoria/Filtracion de informacion	No

CVE-2022-43667	Local	Desbordamiento/Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-43509	Local	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-43508	Local	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-25325	Local/Red	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-25234	Local/Red	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-25230	Local/Red	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-21219	Local/Red	Filtracion de informacion	No
CVE-2022-21124	Local/Red	Corrupcion de memoria/Filtracion de informacion	No
CVE-2022-3398	Local/Red	Corrupcion de memoria/Ejecutar codigo	No
CVE-2022-3397	Local/Red	Corrupcion de memoria/Ejecutar codigo	No
CVE-2022-3396	Local/Red	Corrupcion de memoria/Ejecutar codigo	No
CVE-2022-2979	Local/Local	Corrupcion de memoria	No
CVE-2019-6556	Local/Red	Ejecutar codigo	No
CVE-2018-18993	Local/Red	Desbordamiento/Corrupcion de memoria/Ejecutar codigo	No
CVE-2018-18989	Local/Red	Ejecutar codigo	No
CVE-2018-8834	Local/Local	Desbordamiento/Corrupcion de memoria	No
CVE-2018-7514	Local/Local	Desbordamiento/Corrupcion de memoria	No

(Los que son de doble vector es que se puede utilizar de una manera o de otra)

BIBLIOGRAFIA

https://attack.mitre.org/tactics/ics/
https://www.cvedetails.com/vulnerability-list/vendor_id-527/Omron.html