Identificador
[colCERT AD-0422-001]

Publicado 22/04/2022

Advertencia de Seguridad Digital

[TLP:WHITE]

Malware TRITON y Campaña de Intrusión HAVEX/Dragonfly del FSB que Afectan a Infraestructura Energéticas

Infraestructuras Críticas

Los ciberataques a Sistemas de Control Industrial - ICS que soporta infraestructuras críticas crecen continuamente, debido a su gran valor estratégico, al impacto económico y de pérdidas de vidas humanas que pueden generar en Colombia.

Los siguientes sectores son definidos por la Agencia de Seguridad se Infraestructura y Ciberseguridad (por sus siglas en inglés – CISA), como Infraestructura Crítica y Recursos Clave (por sus siglas en inglés - CIKR).

- Químico.
- Fabricación.
- Represas.
- Base industrial de defensa.
- Servicios de emergencia.
- Energía.
- Servicios financieros.
- Alimentos y agricultura.
- Instalaciones gubernamentales.
- Asistencia sanitaria y salud pública.
- TI.
- Reactores nucleares.
- Transporte.
- Acueducto y aguas residuales.
- Instalaciones comerciales.
- Comunicaciones.

La interdependencia y las cadenas de suministros de cada sector se ven afectadas cuando una infraestructura crítica se compromete, generando una afectación e impacto a mayor escala.

El siguiente es un contexto más amplio del malware TRITON enfocado a sistema SIS (Security Instrumented Systems) Triconex del fabricante Schneider Electric, éste se encarga de restablecer un proceso a un estado seguro cuando se violan condiciones predeterminadas.

Contexto Histórico

El malware es conocido como Tritón, Trisis o HatMan visto por primera vez en junio del 2017, atacando un sábado en la noche a una instalación petroquímica del oriente medio; los presuntos implicados en este ataque son el Instituto de Investigación Científica Central de Química y Mecánica de Rusia (TsNIIkhM), en días pasados, las autoridades estadounidenses señalaron a un ciudadano de origen ruso y a un empleado de TsNIIkhM, como los principales responsables del ataque.

Características del Entorno del Ataque

Para facilitar la puesta en marcha del ataque, era necesario que el switch de Triconex estuviese en "Program" para desplegar el malware Triton de tipo RAT (Figura No. 1).

Figura No. 1. *Triconex en estado "Program", estado que facilita la ejecución del malware.*

En la tabla 1, se describen los eventos, equipos afectados y actividades del troyano de acceso remoto una vez se vulnera el sistema.

Primer evento	Sábado en la noche de junio 2017
Equipos impactados	Un controlador ESD afectado, sistema DCS no detectan inseguridad.
Segundo evento	Viernes en la noche de agosto 2017
Equipos impactados	Múltiples controladores impactados alrededor de múltiples fases, el DCS aún no detecta inseguridad, se encuentran scripts en Python encargados de correr programas desconocidos que impactan la memoria de los controladores.
Debilidades que dieron lugar al ataque	Debilidades en la configuración en la región DMZ, conexión remota mediante RDP y probabilidad de exfiltración de credenciales del funcionario que se conecta con la red a través de este protocolo.
Artefactos	Ejecución de trilog.exe en el terminal de programación de TriStation y librería de comunicaciones: library.zip que cuenta con todos los módulos necesarios de compilación e infección.

Acciones del payload	• Lectura de programas. • Escritura de funciones. • Consultas del estado del controlador. • Mapea y escanea el sistema de control industrial. • Comunicación con los controladores Triconex.
Tipo de acceso	Físico y/o remoto

Tabla No 1. *Bitácora del ataque.*

La muestra analizada fue diseñada exclusivamente para al modelo y firmware especificado, el sistema operativo vulnerado fue Microsoft Windows; la muestra requiere [1]:

- Acceso a red SIS.
- Acceso a TMR Tricon modelo 3008 v10.3.

Posible Perfil Técnico del Atacante [2].

- Conocimiento en controladores programables como SIS.
- Conocimiento en Ladder Logic Programming (61131).
- Conocimiento en configuración y vulnerabilidades en el ICS TriStation (1131).
- Ciberdelincuentes patrocinados al parecer por Rusia y Corea del Norte.
- Conocimientos de sistemas SCADA.
- Comprometen o causan daño físico al sistema de seguridad de modo que se pueda deshabilitar ya que allí se encuentran los controladores de presión y temperatura entre otros, esto con el fin de lanzar el ataque en segunda etapa
- Instalación de un backdoor en los controladores de seguridad.
- Macro .dotm que se intenta conectar con el servidor SMB controlado por los ciberdelincuentes con el fin de robar credenciales y comprometer zona IT, vulnerar la red OT, aprovechándose de viejos sistemas operativos Windows sin actualizar. Se aprovecharon credenciales débiles para instalar el malware en los equipos SCADA y de allí migrar al controlador de seguridad (PLC), el RAT era insertado en la zona de la memoria del controlador del firmware sin interrupción normal de la operación, monitorizaron también permisos R/W para controlar la memoria.

En la figura No. 2 se observan las fases de reconocimiento, entrega, instalación y ejecución del troyano triton:

Fase 1: Se compromete la estación de trabajo donde se encuentra el aplicativo TriStation, dicha estación posee la distribución Microsoft Windows, se instala allí el archivo *trilog.exe* con una librería que despliega los archivos de infección *inject.bin* (código de función maliciosa) e *imain.exe* (control lógico malicioso y backdoor), cabe aclarar que trilog.exe primero realiza una inspección del estado del controlador y ese reconocimiento lo puede realizar a través de TriStation, este software realiza la configuración de los controladores a través del puerto UDP 1502.

Fase 2: Módulos *inject.bin* e *imain.bin* se ejecutan si en la inspección se conoce que los controladores están en modo operativo, el protocolo TriStation ejecutado por su programa legítimo TriStation no requiere medidas de autenticación y cifrado.

Fase 3: En un intento de pasar desapercibido, el malware se nombra como la aplicación legítima Triconex Trilog en la suite de TriStation, el cual analiza logs de las estaciones Triconex, de esta forma puede ejecutarse por el sistema sin ninguna evidencia que sea un archivo malicioso; el malware se sitúa en la sección de firmware de la memoria de los controladores.

Fase final: los controladores Triconex cuentan con un switch físico, cuando se encuentra en modo "Program" se puede ejecutar el malware sin ningún problema, no sucede igual con la instancia "Run" ya que esta solo admite permisos de lectura. El atacante controla los dispositivos de tal forma que identifiquen una supuesta anormalidad y entren en estado "safe mode", con esta característica se logra detener completamente el proceso de por ejemplo una planta eléctrica.

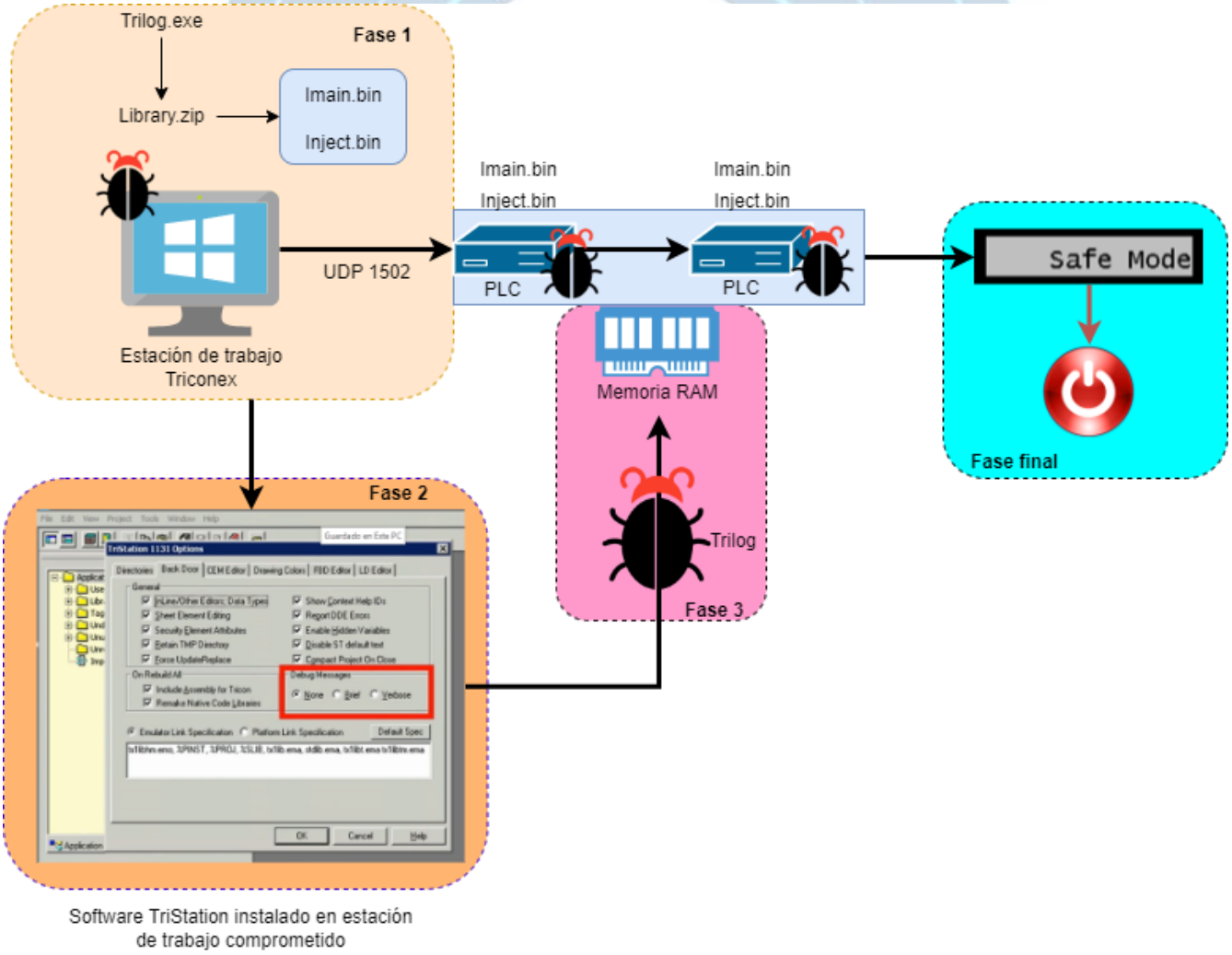

Figura No 2. *Instalación y ejecución del payload.*

Al parecer el primer comprometimiento fue en la red de tecnología operativa (OT), al comprometer la estación de trabajo de OT se pueden ver la infraestructura completa de la topología de red y descubrir otros objetivos de mayor envergadura.

Tácticas, Técnicas y Procedimientos - TTP de Campaña Triton

En la figura No. 3 se observan las TTP ejercidas durante esta campaña de ataque hacia las entidades energéticas.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Impact
T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1078: Valid Accounts	T1552: Unsecured Credentials	T1018: Remote System Discovery	T1021: Remote Services	T1071: Application Layer Protocol	T1485: Data Destruction
	T1106: Native API	T1078: Valid Accounts	T1078: Valid Accounts			T1082: System Information Discovery			T1565: Data Manipulation
									T1495: Firmware Corruption
									T1498: Network Denial of Service
									T1489: Service Stop
									T1529: System Shutdown/Reboot

Figura No. 3. *TTP campaña Triton [3].*

En la figura No 4, se visualiza el proceso de ingeniería inversa para tratar de comprender el encabezado de la muestra y así desvelar los procesos ejecutados, en donde se visualiza un código de operación que según su valor permite leer (17), escribir (41) o ejecutar (f9) en memoria de los controladores.

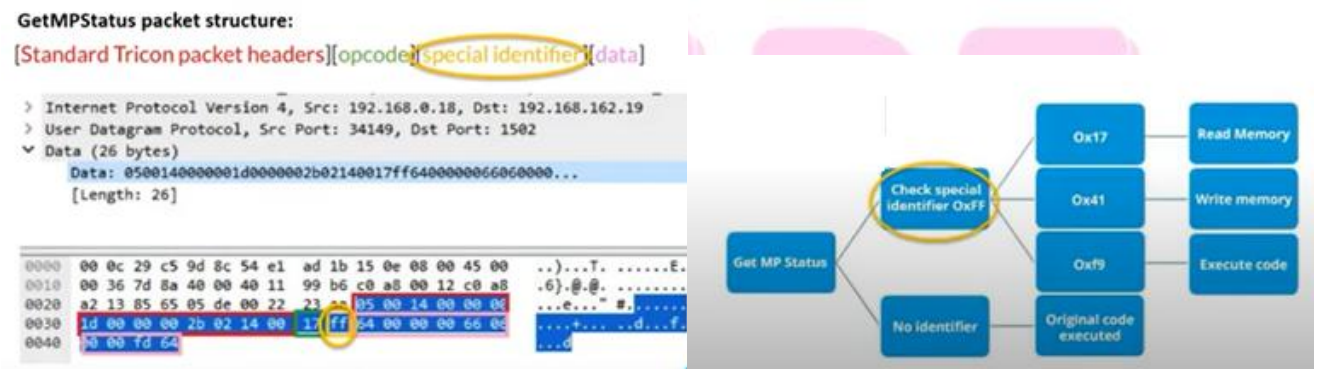

Figura No 4*. Encabezado de paquete de muestra Triton.*

Consecuencias

- Paradas de proceso no autorizadas.

- Programación arbitraria de dispositivos SIS, de manera que se arriesguen vidas humanas y elementos físicos.
- Afectación a la continuidad de negocio de la operación.
- Imposibilidad de detener y asegurar un proceso que se sale del control.

Servicio Federal de Seguridad de Rusia – FSB - Campaña HAVEX/Dragonfly del FSB

Los miembros del grupo operativo "Unidad Militar 71330" – "Centro 16" y " Energetic Bear" – Crouching Yeti" del Servicio Federal de Seguridad de Rusia – FSB, realizaron una campaña de instrucción al sector energético mundial, en dos fases.

La Primera Fase denominada "Dragonfly" o "Havex", consistió en un ataque a la cadena de suministros, comprometiendo la infraestructura tecnológica de los proveedores y desarrolladoras de software para productos ICS/SCADA, comprometiendo a 17.000 dispositivos y controladores ICS/SCADA utilizados por compañías eléctricas y de energía ubicadas principalmente en Estados Unidos, permitiendo a este grupo copiar credenciales de inicio de sesión, recopilar datos de usuarios, instalar puerta traseras para acceder y controlar los dispositivos y controladores.

La Segunda Fase denominada "Dragonfly 2.0", donde este grupo realizo ataques específicos a entidades del sector energéticos y en ingenieros que trabajaban con sistemas OCS/SCADA, realizando ataques de tipo
Watering hole' o ataques de abrevadero, donde perfilaban, estudiaban e infectaban su equipo con malware con el propósito de tomar el control del equipo y poder así espiar y robar información de la compañía.
Spear Phishing realizado a ingenieros perfilando las víctimas a través de fuentes abiertas, redes sociales, con el propósito de crear paginas falsas con contenido relacionado con ICS/SCADA generando confianza para la extracción de información.

Esta segunda fase afecto a más de 3.300 usuarios de 500 empresas de Estados Unidos e internacionales, comprometiendo las redes e infraestructura tecnológica.

Indicadores de Compromiso

Pese a que los siguientes indicadores de compromiso IoC pueden ser obsoletos, se describen con el propósito de que las administradores las utilicen como guía, para realizar una inspección sobre el sistema y establecer la existencia de estos en su plataforma. (Ver tabla No. 2)

Filename	Hash
trilog.exe	MD5: 6c39c3f4a08d3d78f2eb973a94bd7718

	SHA-256: e8542c07b2af63ee7e72ce5d97d91036c5da56e2b091aa2afe737b224305d230
imain.bin	MD5: 437f135ba179959a580412e564d3107f SHA-256: 08c34c6ac9186b61d9f29a77ef5e618067e0bc9fe85cab1ad25dc6049c376949
inject.bin	MD5: 0544d425c7555dc4e9d76b571f31f500 SHA-256: fc4b0076eac7aa7815302b0c3158076e3569086c4c6aa2f71cd258238440d14
library.zip	MD5: 0face841f7b2953e7c29c064d6886523 SHA-256: bef59b9a3e00a14956e0cd4a1f3e7524448cbe5d3cc1295d95a15b83a3579c59
TS_cnames.pyc	MD5: e98f4f3505f05bf90e17554fbc97bba9 SHA-256:2c1d3d0a9c6f76726994b88589219cb8d9c39dd9924bc8d2d02bf41d955fe326
TsBase.pyc	MD5: 288166952f934146be172f6353e9a1f5 SHA-256: 1a2ab4df156ccd685f795baee7df49f8e701f271d3e5676b507112e30ce03c42
TsHi.pyc	MD5: 27c69aa39024d21ea109cc9c9d944a04 SHA-256: 758598370c3b84c6fbb452e3d7119f700f970ed566171e879d3cb41102154272
TsLow.pyc	MD5: f6b3a73c8c87506acda430671360ce15 SHA-256: 5c776a33568f4c16fee7140c249c0d2b1e0798a96c7a01bfd2d5684e58c9bb32
sh.pyc	MD5: 8b675db417cc8b23f4c43f3de5c83438 SHA-256: c96ed56bf7ee85a4398cc43a98b4db86d3da311c619f17c8540ae424ca6546e1

Tabla No 2. *Indicadores de compromiso.*

Recomendaciones:

- Tomar medidas inmediatas para fortalecer la infraestructura tecnológica de TI/OT
- Validar y reforzar los acuerdos de niveles de servicios relacionados con la ciberseguridad, en la implementación de Planes de Recuperación ante Desastres y Continuidad.
- Realice segmentaciones de red, asilando la red de seguridad, establezca una red física independiente para los sistemas SIS.
- Mantenga actualizados con las últimas versiones sus soluciones antivirus.
- Proteja físicamente las instalaciones de los controladores, equipos y red de seguridad.

- Revise los accesos autorizados de servicios SSH o VNC, en lo posible evite acceso remoto a los sistemas de seguridad.
- Tenga un entorno claro y definido de la red OT, así como sus vulnerabilidades y brechas de seguridad no deberían ser ajenas a los administradores de red IT.
- Establezca líneas de comunicación entre OT y SOC.
- Integre la tecnología de seguridad con la automatización, esto no requiere hardware adicional, reduce cableado y hay una respuesta ante incidentes más rápida debido a esta integración.
- Implemente firewall de Nueva Generación (NGFW).
- Implemente IDS/IPS a nivel de red en NGFW.
- Para el Workstation SIS, aplique los siguientes controles:
    - Control de acceso a usuarios autorizados y permisos específicos.
    - Lista blanca de aplicación.
    - Control de dispositivos USB.
- Registro de logs y revisión de estos cada vez que se opere sobre la región SIS.
- Verifique la posición correcta del controlador, la posición menos vulnerable es “run”; nunca en “program” ya que este último facilita la inserción y ejecución del malware. Sitúe los controladores en cabinas que no estén a la visibilidad de otros.
- Escanee minuciosamente dispositivos como CD, USB, DVD, entre otros, antes de insertar en la estación que ejecute la aplicación Tristation o la aplicación encargada de logs.
- PC y portátiles deben escanearse antes de ser conectadas a la red de seguridad o a cualquier controlador.
- Configure las estaciones de operador de modo que salte una alarma cuando se active el interruptor de tricon en modo “Program”.
- Use la última versión de Triconex Tricon CX y cumpla con la norma IEC 62443 estándar de ciberseguridad.
- Sistemas como estaciones de trabajo, red y controladores de seguridad deben estar separados del resto de la red en una sola red VLAN siguiendo la norma IEC-62443.
- En caso de tener conexión peer to peer usando switches, asegúrese que estos posean la configuración indicada por la norma IEC-62443 – norma para la ciberseguridad industrial.
- Si ha conectado estación de trabajo que ejecuta TriStation a otra red, realícelo siempre a través de un firewall, seguidamente use medidas de saneamiento.
- Mantenga copias de seguridad actualizadas y salvaguardadas cuidadosamente en lugares físicos con los debidos controles de acceso.
- Configure una contraseña para acceder al controlador, además de credenciales para entrar al aplicativo TriStation, la contraseña por defecto debe cambiarla.
- Trate de usar solo un solo proveedor de equipos y soluciones para decrementar el riesgo.
- Use un Gateway unidireccional para aplicaciones que necesiten recibir datos de sistema SIS.
- Cualquier información que afecte a la infraestructura critica, reportarla, con el propósito de replicarla a los demás sectores para conocimiento y toma de acciones de mitigación.

Referencias

[1] CISA, “Schneider Electric Triconex Tricon (Update B)” [Online]
https://www.cisa.gov/uscert/ics/advisories/ICSA-18-107-02

[2] CISA, “APT Cyber Tools Targeting ICS/SCADA Devices” [Online]
https://www.cisa.gov/uscert/ncas/alerts/aa22-103a?_sp=2e04f970-1f45-418b-a34b-d4465286eceb.1650287922501

[3] MITRE ATT&CK®

Nota Administrativa

Este producto está marcado como TLP:WHITE. Sujeto a las reglas estándar de derechos de autor, la información de este producto se puede compartir sin restricciones.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con ColCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT