



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Ciberconciencia Situacional

2024/2025

Francesco Lorenzoni
PCA25403GU

Trabajo Final 2

Caracterización de ataques a ICS con Mitre

Contents

1 Caracterización de ataques a ICS con Mitre	5
1.0.1 WWS and ICSs	5
1.0.2 Redes ICS	6
1.0.3 Ataques a ICS	6
1.1 Ataque 1: Maroochy Water Services, Australia, 2000	7
1.1.1 Descripción del incidente	7
1.1.2 Tácticas y técnicas según MITRE ATT&CK	7
1.1.3 Respuesta al incidente	8
1.1.3.1 Evaluación de la respuesta	8
1.2 Ataque 2: Kemuri Water Company (seudónimo), EE.UU., 2016	9
1.2.1 Descripción del incidente	9
1.2.2 Tácticas y técnicas según MITRE ATT&CK	9
1.2.2.1 Justificación de las tácticas y técnicas	9
1.2.3 Respuesta al incidente	9
1.2.3.1 Evaluación de la respuesta	10
1.3 Ataque 3: Empresa de agua europea, 2018	11
1.3.1 Descripción del incidente	11
1.3.2 Tácticas y técnicas según MITRE ATT&CK	11
1.3.2.1 Justificación de las tácticas y técnicas	11
1.3.3 Respuesta al incidente	12
1.3.3.1 Evaluación de la respuesta	12
1.4 Ataque 4: Riviera Beach Water Utility, U.S., 2019	13
1.4.1 Descripción del incidente	13
1.4.2 Tácticas y técnicas según MITRE ATT&CK	13
1.4.2.1 Justificación de las tácticas y técnicas	13
1.4.3 Respuesta al incidente	14
1.4.3.1 Evaluación de la respuesta	14
1.5 Ataque 5: Bowman Avenue Dam, EE.UU., 2013	15
1.5.1 Descripción del incidente	15
1.5.2 Tácticas y técnicas según MITRE ATT&CK	15
1.5.2.1 Justificación de las tácticas y técnicas	15
1.5.3 Respuesta al incidente	16
1.5.3.1 Evaluación de la respuesta	16

Chapter 1

Caracterización de ataques a ICS con Mitre

Introducción

La tarea nos pide de leer un artículo de revisión de 15 ataques a sistemas de control industrial (ICS) y elegir 5 de ellos para caracterizarlos con la matriz de [Mitre ATT&CK](#). La matriz de Mitre ATT&CK es una base de datos de tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes en el ciberespacio. Esta matriz se utiliza para comprender mejor las amenazas y mejorar la defensa cibernética.

Tarea a realizar

- ◊ Lee detenidamente el documento para reforzar los conceptos expuestos en clase sobre seguridad en ICS e infraestructuras críticas.
- ◊ Elige los 5 ataques que consideres más significativos o que pienses que están mejor descritos.
- ◊ Para cada uno de esos ataques, en base a la información del documento, y al contenido de la matriz de MITRE para ICS, indica que tácticas y técnicas utilizaron los atacantes. Explica porqué piensas que en cada caso utilizaron esas tácticas y técnicas. Indica también el tipo de respuesta descrito para cada ataque y si te parece adecuado, o bien propondrías otro tipo posible de respuesta.

1.0.1 WWS and ICSs

El artículo empieza con una introducción sobre el WWS (Water and Wastewater Sector), que es un sector crítico para la sociedad, ya que proporciona agua potable y trata las aguas residuales. Este es, según el *U.S. Department of Homeland Security*, uno de los sectores más targetados por los ciberataques. Su salvaguardia frente a las amenazas de ciberseguridad se considera una cuestión de prioridad nacional.

WWS son **sistemas de control industrial** (ICS) que se utilizan para supervisar y controlar las infraestructuras de agua y aguas residuales. Estos sistemas son esenciales para garantizar la calidad del agua, la eficiencia operativa y la seguridad pública.

La mayor parte de los ICS en el sector WWS son sistemas SCADA (*Supervisory Control and Data Acquisition*), que permiten la supervisión y control remoto de los procesos industriales. Estos sistemas se componen de sensores, controladores lógicos programables (PLC) y estaciones de trabajo que se comunican entre sí para supervisar y controlar los procesos.

Hay una MTU (*Master Terminal Unit*) que se encarga de la supervisión y control de los procesos, y una RTU (*Remote Terminal Unit*) que se encarga de la supervisión y control de los dispositivos remotos. La MTU se comunica con la RTU a través de una red de comunicación, que puede ser una red privada o una red pública. La HMI (*Human-Machine Interface*) es la interfaz que permite a los operadores interactuar con el sistema SCADA. La HMI se utiliza para supervisar y controlar los procesos, y para visualizar la información del sistema.

Durante muchos años, los sistemas SCADA y, en general, las redes OT en entornos industriales, *no* estaban conectadas a las redes informáticas corporativas ni a Internet. Sin embargo, a medida que la tecnología avanzaba, muchas organizaciones planearon consolidar las redes IT y OT superpuestas.

1.0.2 Redes ICS

La nueva generación de redes IT-OT convergentes en los sistemas de control industrial, también conocida como *Industrial Internet of Things* (IIoT), ya no está air-gapped.

Una red ICS está dividida por niveles y zonas:

- ◊ **Enterprise zone** - that includes assets for business logistics and enterprise systems, representing Level 4 and 5, respectively. This zone is also known as IT network.
- ◊ **Demilitarized zone (DMZ)** - that separates IT and OT networks, thus preventing direct access to OT devices from the IT network. All corporate-accessible services (e.g., web, 120 email) reside in this zone
- ◊ **Manufacturing and Control zone** - The former refers to the entire OT domain, including Levels 0, 1, 2, and 3; the latter refers to Levels 0, 1, and 2, so it is equivalent to the traditional ICS architecture shown in Fig. 1.1. Level 3 provides site-level operation and asset management. Plant historian, production scheduling and reporting, patch and file services reside at Level 3

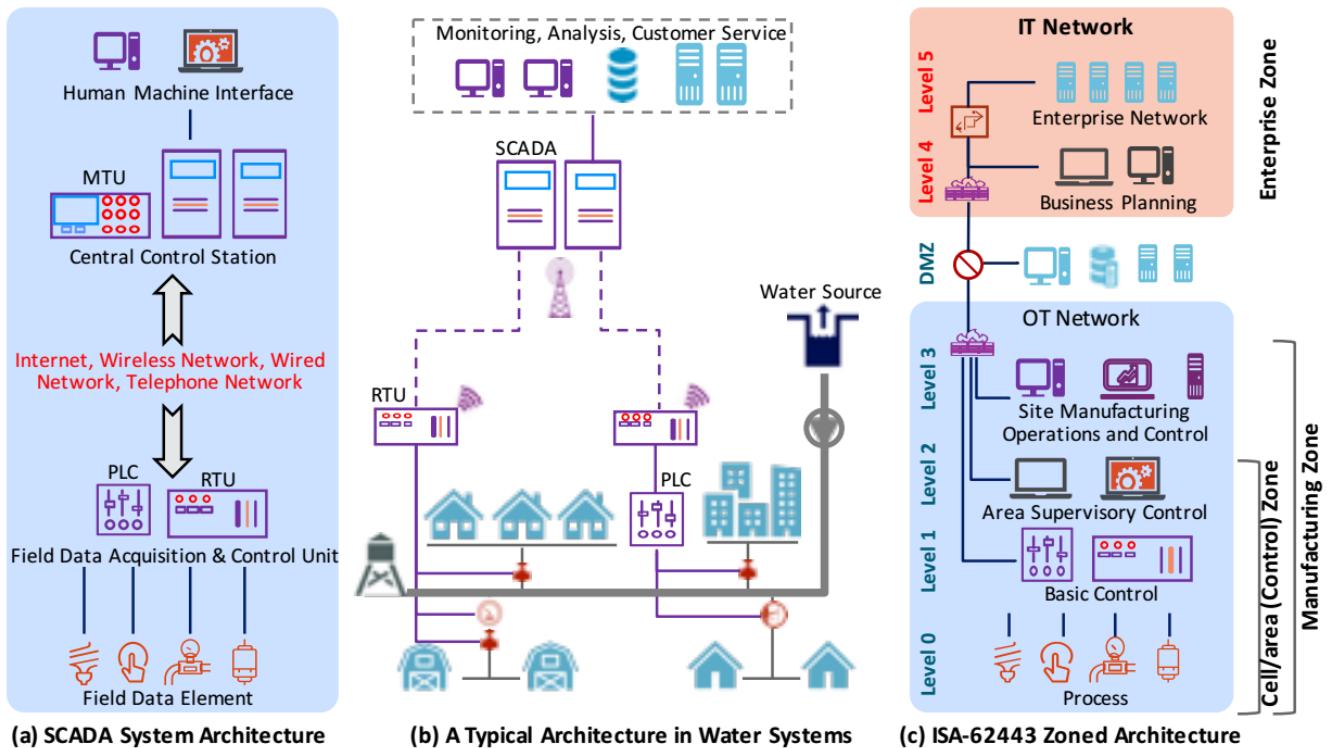


Figure 1.1: (a)Traditional ICS systems; (b) Water system architectures; (c) Converged IT/OT systems.

1.0.3 Ataques a ICS

Los ataques a sistemas de control industrial (ICS) son cada vez más frecuentes y sofisticados. En este trabajo, analizaremos cinco ataques significativos a sistemas de agua y aguas residuales (WWS), utilizando la matriz de MITRE ATT&CK para ICS. Esta matriz nos permite categorizar las tácticas, técnicas y procedimientos utilizados por los atacantes en entornos ICS.

Vamos a analizar las tácticas y técnicas utilizadas en cada ataque, así como la respuesta a los incidentes y su efectividad.

1.1 Ataque 1: Maroochy Water Services, Australia, 2000

1.1.1 Descripción del incidente

En el año 2000, un **ex empleado** atacó el sistema SCADA de Maroochy Shire en Queensland, Australia. El atacante era un antiguo supervisor de sitio para Hunter Watertech Pty Ltd (HWT), un contratista externo que había instalado RTUs en 142 estaciones de bombeo. Después de renunciar en diciembre de 1999, realizó múltiples intrusiones al sistema SCADA entre enero y abril del 2000, causando malfuncionamientos como pérdida de comunicaciones, falsas alarmas y alteración de configuraciones. El resultado fue la liberación de aproximadamente un millón de litros de aguas residuales sin tratar al medio ambiente.

“The main hazard involved in this incident was the unauthorized access to the SCADA system, which enabled the malevolent actor to release raw sewage into the surrounding environment. There were no cybersecurity procedures, policies, or defenses present, and the service contract was deficient or inadequate to handle the contractor’s responsibilities.” —

1.1.2 Tácticas y técnicas según MITRE ATT&CK

Según la matriz MITRE ATT&CK para ICS, el ataque utilizó las siguientes tácticas y técnicas:

- ◊ **Persistence/Initial Access** - El atacante utilizó la técnica de *Valid Accounts* (T0859), ya que mantuvo acceso a sus credenciales después de dejar la empresa.
T0859 aparece en la sección *Persistence* de la matriz MITRE ATT&CK para ICS, pero claro que las credenciales se pueden utilizar también para el acceso inicial al sistema.
La falta de procedimientos para revocar accesos de empleados facilitó su intrusión y persistencia en el sistema durante meses.
- ◊ **Execution** - Empleó la técnica de *Execution through API* (T0871), utilizando su conocimiento para enviar comandos legítimos con intenciones maliciosas.
Siendo un ex supervisor, tenía un conocimiento profundo del sistema y su funcionamiento. Esto le permitió emitir comandos de ingeniería que parecían legítimos pero causaban daños significativos.
- ◊ **Impact** - Utilizó la técnica de *Modify Parameter* (T0836), alterando la configuración de las estaciones de bombeo para causar el vertido de aguas residuales.
También utilizó la técnica de *Loss of Safety* (T0880), desactivando exitosamente las alarmas de cuatro bombas.
La manipulación de parámetros de control fue una táctica efectiva dada la ausencia de monitoreo de comportamientos anómalos en el sistema.

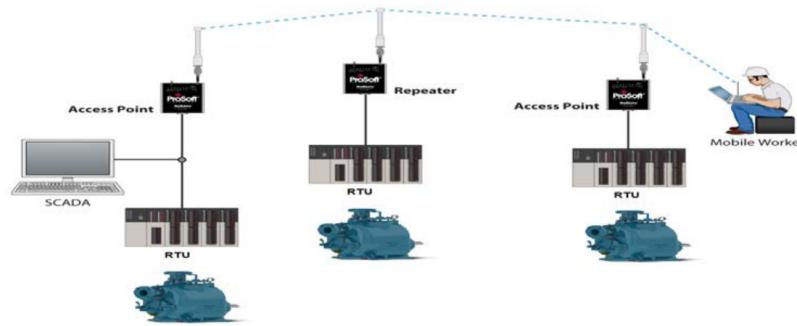


Figure 1.2: Cómo funcionarían el SCADA de Maroochy y la RTU (Unidad Terminal Remota)

1.1.3 Respuesta al incidente

La respuesta consistió en una investigación que culminó con la captura del sospechoso en abril de 2000. Se le encontró en posesión de equipos de control industrial, como un ordenador COMPACT 500, un radio bidireccional, un portátil, un transformador y cables. Posteriormente fue sentenciado a dos años de prisión y ordenado a pagar 13,111 dólares australianos por los daños causados. La limpieza del vertido requirió días y recursos sustanciales.

1.1.3.1 Evaluación de la respuesta

La respuesta fue reactiva y no preventiva. Como se sugiere en el artículo, la respuesta parece inadecuada por varias razones:

- ◊ No existían procedimientos de ciberseguridad que pudieran prevenir el ataque.
- ◊ No había un sistema para revocar accesos cuando un empleado dejaba la empresa.
- ◊ Tardaron mucho tiempo en identificar que las fallas eran causadas por intervención humana.

Una respuesta más adecuada habría incluido la implementación de controles de seguridad básicos según el protocolo NIST SP 800-53, como la terminación inmediata de accesos de empleados, autenticación multifactor, segregación de redes y monitoreo continuo de actividades sospechosas en el sistema SCADA.

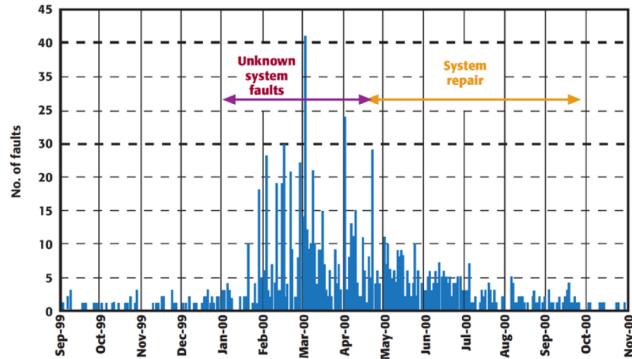


Figure 1.3: Número de fallas en el sistema SCADA de Maroochy Shire, antes y después del incidente

Parece interesante ver que el número de fallas tomó bastante tiempo después del último ataque el 23 de abril para volver a valores normales.

Bloquear el **acceso inicial** a los atacantes es fundamental. Constituye la primera línea de defensa contra ataques a ICS y a sistemas informáticos en general. Tras obtener acceso, los atacantes pueden escanear la red, detectar vulnerabilidades, moverse lateralmente y comprometer sistemas críticos.

La falta de ciberconciencia situacional, es decir, la falta de conocimiento sobre lo que está sucediendo en el sistema, no ha permitido de detectar sin demora el ataque.

Además de la falta de ciberconciencia situacional, parece evidente que faltaba la definición clara de políticas de **Access Control**, que es fundamental y que tiene que funcionar como guía para la implementación y configuración de las herramientas de seguridad.

Un firewall, sin una política de acceso bien definida, no es más que un filtro que pero no puede resolver ningún problema concreto de seguridad.

1.2 Ataque 2: Kemuri Water Company (seudónimo), EE.UU., 2016

1.2.1 Descripción del incidente

En 2016, una empresa de servicios de agua en EE.UU. (bajo el seudónimo Kemuri Water Company) contrató a Verizon Security Solutions para realizar una evaluación de ciberseguridad de sus sistemas. La evaluación reveló vulnerabilidades de alto riesgo, incluyendo el uso de sistemas obsoletos como un ordenador **AS400** que servía para funciones críticas de IT y OT, con conexiones directas a múltiples redes. El análisis forense descubrió que hacktivistas patrocinados por un estado habían explotado la aplicación de pago en internet para acceder al sistema AS400, resultando en la exfiltración de 2.5 millones de registros únicos y manipulación de productos químicos y tasas de flujo.



Figure 1.4: AS400 IBM

1.2.2 Tácticas y técnicas según MITRE ATT&CK

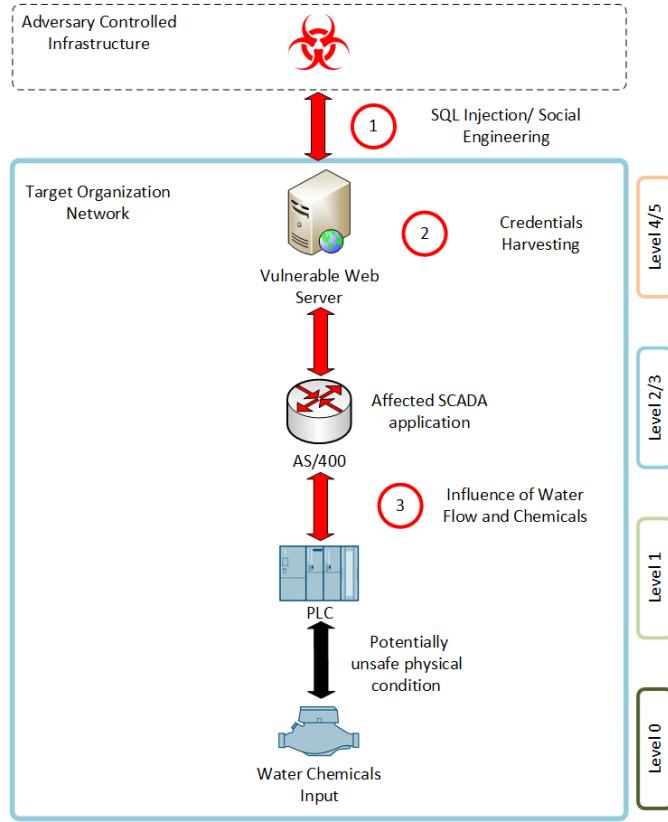


Figure 1.3: Kemuri attack diagram

Según la matriz MITRE, este ataque empleó:

- ◊ **Initial Access - Exploit Public-Facing Application** (T0819), aprovechando vulnerabilidades en la aplicación de pago por internet. Esto permitió a los atacantes obtener acceso inicial al sistema IT, que estaba conectado directamente al sistema OT (AS400).
- ◊ **Collection - Automated Collection** (T0802), obteniendo información sobre el sistema de control industrial.
- ◊ **Impact - Modify Parameter** (T0836), alterando productos químicos y tasas de flujo.

1.2.2.1 Justificación de las tácticas y técnicas

Los atacantes eligieron estas tácticas porque:

- ◊ La aplicación de pago por internet presentaba una puerta de entrada fácil al no estar adecuadamente protegida.
- ◊ La conexión directa entre el sistema IT (aplicación de pago) y OT (AS400) representaba una ruta de confianza que eliminaba la necesidad de superar barreras adicionales de seguridad.
- ◊ El sistema AS400 obsoleto carecía de parches de seguridad y controles modernos, facilitando la recolección de datos y manipulación de parámetros.
- ◊ La autenticación de factor único simplificó el acceso no autorizado a sistemas críticos.

1.2.3 Respuesta al incidente

La respuesta incluyó la terminación inmediata del acceso hacia y desde el sistema de gestión de cuentas web y el bloqueo de la conectividad saliente del sistema AS400. Se recomendó reemplazar los sistemas antiguos con versiones más modernas.

Lo que parece extraño es que algunos empleados sabían de las vulnerabilidades del sistema, y por lo tanto existe una duda sobre si la investigación requerida fue en realidad proactiva o reactiva.

1.2.3.1 Evaluación de la respuesta

La respuesta parece adecuada porque reveló apropiadamente las vulnerabilidades y llevó a la identificación del vector de ataque. Sin embargo, parece ser principalmente reactiva y carece de la implementación de medidas preventivas fuertes inmediatas.

Algunas ideas de mejora serían:

- ◊ Implementación de arquitectura de **segmentación de red** con zonas desmilitarizadas (DMZ) entre IT y OT.
- ◊ **Autenticación multifactor** para todos los sistemas críticos.
- ◊ **Monitoreo continuo** de tráfico de red entre zonas IT y OT.
- ◊ **Evaluaciones periódicas** de vulnerabilidades y **pruebas de penetración**.

Si hubiera habido un **control periódico** y mayor monitoreo, las vulnerabilidades habrían sido identificadas antes, y —esperablemente— el ataque habría sido prevenido.

Además, el hecho de que algunos empleados conocían vulnerabilidades denota negligencia y/o falta de comunicación entre equipos.

La **falta de comunicación** y un monitoring deficiente evidentemente contribuyeron a una “*Ciberconciencia situacional*” parcial, es decir, que no se sabía lo que estaba pasando en el sistema. Hemos visto en clase que, herramientas de **Visualización** o una **COP** (*Common Operational Picture*) pueden ayudar a mejorar la comunicación entre los equipos y a obtener una vista general más completa. En cualquier caso, es importante recalcar nuevamente que un sistema de filtrado o de autenticación para hacer segura una aplicación de cara al público por sí solos no son suficientes, es necesario definir reglas de acceso y autorización claras y eficaces, para que tales herramientas puedan efectivamente proteger el sistema.

1.3 Ataque 3: Empresa de agua europea, 2018

1.3.1 Descripción del incidente

En enero de 2018, una empresa europea de servicios de agua con un sistema de análisis OT basado en la nube contrató a Radiflow para monitorear su red. El 21 de enero, se detectó tráfico de red sospechoso en la red SCADA, con nuevos enlaces a direcciones IP externas que generaban un cambio importante en la topología de la red. La investigación reveló que las direcciones pertenecían a un “*MinerCircle Monero Pool*”, lo que llevó a la detección de malware de criptominería en la red OT. Aproximadamente el 40% del tráfico estaba relacionado con operaciones de minería, causando un aumento del 60% en el consumo total de ancho de banda. Este incidente se considera el primer caso conocido de “cryptojacking” contra un sistema ICS.

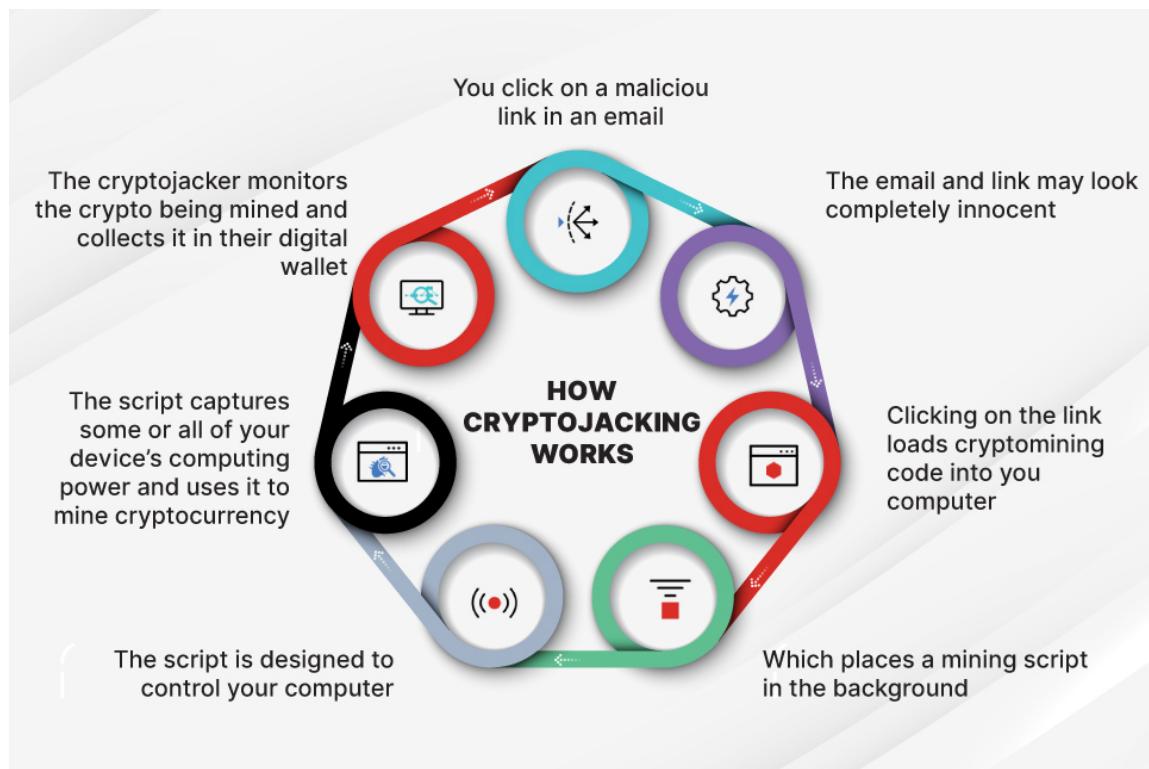


Figure 1.4: Cryptojacking esquema

1.3.2 Tácticas y técnicas según MITRE ATT&CK

Las tácticas y técnicas utilizadas incluyen:

- ◊ **Initial Access** - Aunque no se especifica en el documento, probablemente utilizaron *Exploit Public-Facing Application* (T0819). De lo contrario, un empleado podría haber sido el culpable, o bien víctima de phishing (*Spearphishing Attachment* T0865).
- ◊ **Execution - Scripting** (T0853), ejecutando scripts maliciosos para la minería de criptomonedas.
- ◊ **Impact - Resource Hijacking¹** (/Loss of Availability T0826), utilizando recursos computacionales del sistema para minar criptomonedas.

No hay exactamente la intención de causar daño directo a los activos, sino de aprovechar sus recursos para beneficio económico del atacante. Sin embargo, el resultado es un mayor consumo de recursos y uso de ancho de banda, lo que puede llevar a degradación del rendimiento y potencial denegación de servicio para operaciones legítimas.

1.3.2.1 Justificación de las tácticas y técnicas

Los atacantes eligieron estas tácticas por:

- ◊ El malware de criptominería es relativamente fácil de implementar y puede pasar desapercibido durante períodos prolongados si no se monitorea adecuadamente el rendimiento del sistema.
- ◊ A diferencia de ataques que buscan interrumpir servicios o robar datos, el cryptojacking busca mantenerse operativo el mayor tiempo posible para maximizar ganancias.

¹Esta es la técnica T1496, mencionada en la categoría *Enterprise*, no *ICS*; sin embargo si puede considerar relacionada a la T0826

- ◊ Los sistemas ICS suelen tener capacidad computacional constante y conexión permanente a internet, lo que los convierte en objetivos atractivos para la minería de criptomonedas.

1.3.3 Respuesta al incidente

La empresa de seguridad informó a la empresa de agua sobre el malware de criptominería y los servidores infectados. La recuperación incluyó la actualización del software antivirus en algunos servidores y el refuerzo de la seguridad del firewall. El software antivirus actualizado tuvo éxito en detectar el malware CoinMiner.

1.3.3.1 Evaluación de la respuesta

La respuesta fue adecuada pero “bastante” reactiva.

No pidieron la evaluación de seguridad tras la detección de un problema, y esto es positivo, ya que demuestra que la empresa tenía en cuenta la seguridad de su infraestructura, pero actividades como el básico monitoreo de tráfico de red deberían haber estado implementadas previamente.

La reacción se puede considerar reactiva, ya que se actualizó tras la detección del malware, y no antes.

La detección temprana del tráfico sospechoso permitió mitigar el impacto. La actualización de antivirus y refuerzo de firewalls fueron medidas apropiadas, que deberían ayudar a prevenir incidentes similares en el futuro.

Para fortalecer un ICS contra ataques similares, propondría adicionalmente:

- ◊ Implementación de sistemas de **monitoreo** de rendimiento para detectar anomalías en el uso de recursos. Para ICSs, el tráfico y uso de recursos son a menudo predecibles, por lo que un valor anómalo en el uso de CPU o ancho de banda puede indicar actividad maliciosa, y se puede fácilmente detectar.
- ◊ **Segmentación de red** más estricta entre sistemas OT y conexiones externas. Esto se puede combinar con auditorías regulares de tráfico de red para identificar comunicaciones sospechosas, que de alguna manera se desvían de los patrones previstos.
- ◊ Implementación de **listas blancas de aplicaciones** para prevenir la ejecución de software no autorizado. Para una empresa de distribución de agua esto no debería ser demasiado difícil de implementar y mantener actualizado.

Hay técnicas de active/passive *fingerprinting* para establecer un perfil de tráfico normal, que pueden ayudar a detectar anomalías en el tráfico de red.

Sin embargo, un uso continuo de técnicas de active fingerprinting pueden causar problemas de rendimiento y disponibilidad, que en un ICS pueden ser críticos. Por esta razón, puede ser mejor utilizar técnicas pasivas, o herramientas de *traffic analysis* que solo analizan un traffic dump, así que no afectan el tráfico de red en tiempo real. Tras la análisis pasiva, se puede establecer un perfil de tráfico normal, y configurar herramientas de monitoreo para alertar sobre desviaciones significativas de este perfil.

1.4 Ataque 4: Riviera Beach Water Utility, U.S., 2019

1.4.1 Descripción del incidente

El 29 de mayo de 2019, Riviera Beach, una pequeña ciudad de 35.000 habitantes ubicada al norte de West Palm Beach (Florida), fue víctima de un devastador ataque de **ransomware** que comenzó cuando un empleado del departamento de policía abrió un correo electrónico infectado. El malware se propagó rápidamente, paralizando los sistemas informáticos del departamento de policía, el ayuntamiento y otras oficinas gubernamentales locales, enviando todas las operaciones fuera de línea y cifrando sus datos.

El ataque también se extendió a la utilidad de agua, comprometiendo los sistemas informáticos que controlaban las estaciones de bombeo y las pruebas de calidad del agua, así como sus operaciones de pago. Aunque los sistemas se vieron comprometidos, las autoridades aseguraron que la calidad del agua nunca estuvo en peligro, aunque las pruebas de calidad tuvieron que realizarse manualmente durante el incidente.

“Although paying a ransom looks like the easiest way to solve the problem, FBI and security experts suggest never to pay ransom as it only encourages future criminal activity. Preventing cyber-attacks from happening is always the best practice.” —

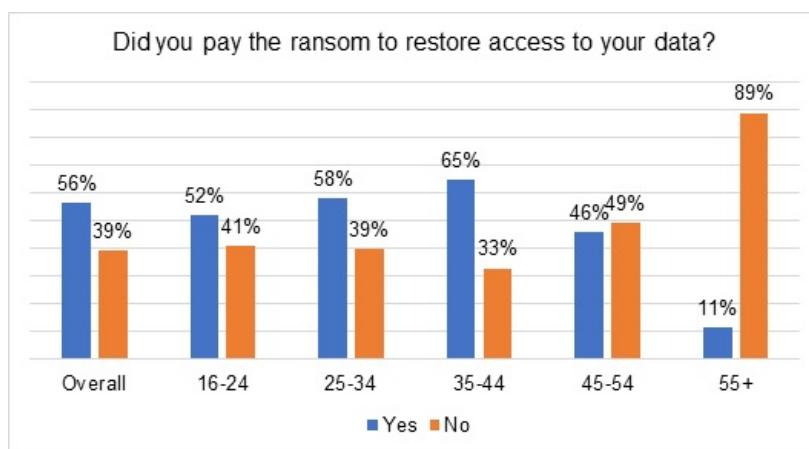


Figure 1.5: Segun una encuesta de Kaspersky, más del 50% de las victimas pagan el ransom, especialmente los usuarios más jóvenes

1.4.2 Tácticas y técnicas según MITRE ATT&CK

Según la matriz MITRE ATT&CK para ICS, este ataque utilizó las siguientes tácticas y técnicas:

- ◊ **Initial Access** - *Spearphishing Attachment* (T0865), ya que el ataque comenzó cuando un empleado abrió un correo electrónico infectado.
 - ◊ **Execution** - *User Execution* (T0863), aprovechando el error humano para ejecutar código malicioso contenido en el correo electrónico.
 - ◊ **Impact** - *Data Encrypted for Impact* (T1486 of Enterprise Matrix), el ransomware cifró datos críticos para exigir un rescate y paralizó las operaciones normales de la utilidad.
- Esto se puede relacionar con las técnicas de *Loss of Control/Productivity and Revenue/Safety/Availability* (T0827, T0828, T0880 T0826).

1.4.2.1 Justificación de las tácticas y técnicas

Los atacantes eligieron estas tácticas por varias razones:

- ◊ El **phishing** sigue siendo uno de los vectores de ataque más efectivos debido a su simplicidad y alta tasa de éxito, especialmente en organizaciones con personal no capacitado en seguridad cibernética.
- ◊ Las pequeñas municipalidades y servicios públicos suelen tener **sistemas obsoletos** y con parches de seguridad desactualizados, lo que las convierte en objetivos atractivos para ataques de ransomware.
- ◊ El cifrado de datos críticos para operaciones diarias crea una urgencia inmediata que aumenta la probabilidad de que la víctima pague el rescate.
- ◊ Los sistemas de control industrial conectados a redes administrativas permiten que un ataque que comienza en sistemas IT se propague a componentes OT críticos.
- ◊ Pueblos pequeños a menudo no tienen **fondos** suficiente para invertir en ciberseguridad, lo que los hace más vulnerables a ataques de ransomware. El hardware y software obsoleto, como el sistema de control de la utilidad

de agua, a menudo carece de las actualizaciones de seguridad necesarias para resistir ataques modernos.

1.4.3 Respuesta al incidente

Pocos días después del ataque, el ayuntamiento votó unánimemente autorizar a su aseguradora a pagar 65 bitcoins, aproximadamente \$600,000, a los atacantes, más \$25,000 adicionales como deducible del seguro. A pesar del pago, los datos seguían siendo inaccesibles al 20 de junio de 2019, y no había garantía de recuperación completa.

Durante la recuperación, el departamento de IT logró restaurar parcialmente el sitio web de la ciudad y los servicios de correo electrónico. Las estaciones de bombeo de agua y los sistemas de prueba de calidad del agua se restablecieron solo parcialmente, requiriendo operaciones manuales para garantizar la continuidad del servicio.

Además del rescate, la ciudad autorizó gastar más de \$900,000 en nueva infraestructura informática, una inversión que estaba planificada para el año siguiente. Según un concejal, gran parte del hardware existente era antiguo y obsoleto, lo que lo hacía vulnerable a ciberataques.

1.4.3.1 Evaluación de la respuesta

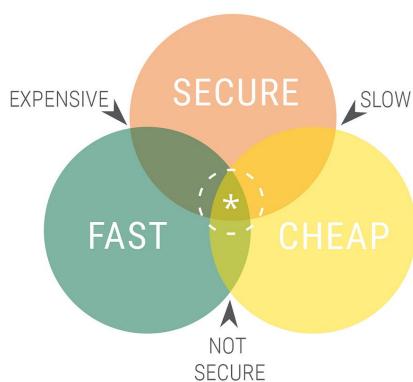
La respuesta al incidente presenta aspectos cuestionables:

- ◊ Aunque es comprensible la decisión de pagar el rescate dado el impacto en servicios esenciales, esta acción, en general, incentiva futuros ataques.
- ◊ La inversión reactiva en nueva infraestructura demuestra que la ciudad reconoció la necesidad de modernización, pero lo hizo demasiado tarde, después de sufrir el ataque y pagar el rescate.
- ◊ La falta de actualizaciones y parches oportunos refleja una gestión de seguridad deficiente, especialmente considerando que estos sistemas controlaban infraestructura crítica.

Una respuesta más adecuada habría incluido:

- ◊ Implementación continua y proactiva de un programa de actualización y aplicación de **parches de seguridad**.
- ◊ **Formación regular** en concienciación sobre ciberseguridad para todos los empleados, especialmente sobre la identificación de correos electrónicos de phishing.
- ◊ **Segmentación** efectiva entre redes IT y OT para evitar que un compromiso en sistemas administrativos afecte a los sistemas de control industrial. Este caso es un ejemplo claro de cómo la falta de segmentación y controles adecuados ha llevado al compromiso no solo de la utilidad de agua, sino de múltiples oficinas gubernamentales, paralizando muchas operaciones de la ciudad.
- ◊ Desarrollo de un plan de continuidad de operaciones que permita la **restauración rápida desde copias** de seguridad sin necesidad de pagar rescates.

Este caso ilustra claramente cómo la falta de inversión en seguridad cibernética básica puede resultar en costos mucho mayores tras un incidente, incluyendo no solo el rescate y las nuevas adquisiciones, sino también daños reputacionales y pérdida de confianza pública.



Sin embargo, ilustra también cómo la seguridad sea un coste no indiferente, especialmente para pequeñas municipalidades que no tienen muchos recursos, y inversiones en ciberseguridad pueden ser vistas como un gasto innecesario.

Claro que, típicamente el coste de un ataque exitoso es mucho mayor que el coste de una inversión en ciberseguridad, pero esto no es evidente para todos los responsables de la toma de decisiones, y para el público en general.

Cómo un seguro de salud, o del coche, la ciberseguridad es una inversión que no se ve hasta que se necesita, y por lo tanto a menudo es minimizada o ignorada.

Dado que ser robusto contra ciberataques puede ser difícil y costoso, debería haber al menos mecanismos de resistencia, que tienden a ser más baratos y fáciles de implementar, y que pueden ayudar a recuperarse —casi— fácilmente de un ataque sin pagar un rescate.

1.5 Ataque 5: Bowman Avenue Dam, EE.UU., 2013

1.5.1 Descripción del incidente

En el año 2013, entre el 28 de agosto y el 18 de septiembre, hackers obtuvieron “acceso remoto no autorizado” al sistema SCADA de la presa Bowman Avenue en Rye, New York. Esta presa utiliza una compuerta controlada remotamente desde 2013 para controlar el flujo de agua según los niveles y temperaturas del arroyo Blind Brook. Los atacantes lograron recopilar información sobre niveles de agua, temperatura y estado de la compuerta, aunque esta estaba desconectada manualmente para mantenimiento durante la intrusión.

El ataque se realizó mediante “*Google dorking*”, una técnica que utiliza el motor de búsqueda Google para localizar vulnerabilidades en aplicaciones web. Los atacantes utilizaron comandos de búsqueda avanzada para identificar sistemas de control industrial expuestos en Internet, específicamente la aplicación web de monitoreo y control de la presa que carecía de medidas de seguridad básicas como firewall o autenticación.

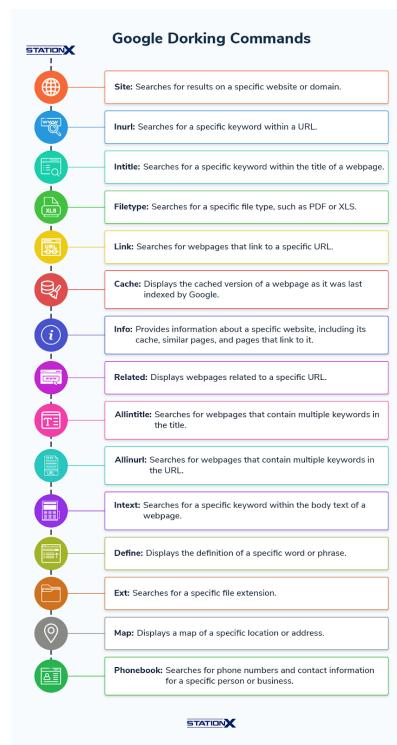


Figure 1.6: Google advanced search commands

1.5.2 Tácticas y técnicas según MITRE ATT&CK

Las tácticas y técnicas utilizadas incluyen:

- ◊ **Reconnaissance** - *Network Sniffing* (T0842) y *Spoof Reporting Message* (T0856), utilizando Google dorking para identificar vulnerabilidades en la aplicación web de control de la presa.
- ◊ **Initial Access** - *Exploit Public-Facing Application* (T0819), accediendo a la aplicación web de control sin protección adecuada.
- ◊ **Collection** - *Automated Collection* (T0802), recopilando datos sobre niveles de agua, temperatura y estado de la compuerta.

1.5.2.1 Justificación de las tácticas y técnicas

Los atacantes eligieron estas tácticas porque:

- ◊ El sistema de control estaba directamente accesible desde Internet sin firewall ni controles de autenticación, haciendo del reconocimiento una táctica efectiva.
- ◊ *Google dorking* es una técnica de bajo esfuerzo que permite identificar sistemas vulnerables sin alertar a los objetivos.
- ◊ La aplicación web para monitoreo y control no implementaba medidas de seguridad básicas, facilitando el acceso no autorizado.
- ◊ La recopilación de datos sobre el sistema proporcionaba información valiosa para posibles ataques futuros más destructivos. De hecho, se considera como el primer paso de la “Cyber Kill Chain” (CKC), que es un modelo que describe las etapas de un ciberataque, siendo las etapas posteriores el ataque real al sistema.



Figure 1.6: Bowman Avenue Dam

1.5.3 Respuesta al incidente

Después del ataque, se instalaron un nuevo software y una nueva compuerta. Por dirección del Gobernador Cuomo, el Estado de Nueva York tomó múltiples medidas para mejorar sus capacidades de ciberseguridad en varios sectores. Las investigaciones realizadas por el DHS y el Departamento de Justicia resultaron en la acusación de varios hackers patrocinados por un estado. El ataque causó más de 30,000\$ en costos de remediación.

1.5.3.1 Evaluación de la respuesta

La respuesta fue bastante adecuada. La instalación de nuevo software y hardware con mejores características de seguridad es una medida importante para prevenir ataques básicos.

Además, es positivo que el ataque haya llevado al gobierno a tomar medidas para mejorar las capacidades de ciberseguridad a nivel estatal.

Algunas mejoras podrían ser:

- ◊ Establecimiento de una arquitectura de acceso remoto seguro con múltiples capas de **autenticación**, posiblemente incluyendo información biométrica.
- ◊ Mejor **segmentación de red** para aislar sistemas críticos de control industrial de redes públicas y aplicaciones web.
La compuerta de la presa estaba manualmente desconectada para mantenimiento durante la intrusión, por lo que los hackers no pudieron manipularla, pero esto fue simplemente suerte.
- ◊ Monitoreo continuo de búsquedas en Internet que puedan revelar información sensible sobre infraestructuras críticas, o vulnerabilidades en las aplicaciones utilizadas da dichas infraestructuras.

