



Universitat
Oberta
de Catalunya



Universitat Autònoma
de Barcelona



UNIVERSITAT
ROVIRA I VIRGILI



Universitat de les
Illes Balears

FASE, Framework de Ataque para Sector Eléctrico

Nombre Estudiante: Aarón Flecha Menéndez

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre Profesor Colaborador: Omar Benjumea Gómez

Nombre Profesor Responsable: Jordi Serra Ruiz

Centro: Universitat Oberta de Catalunya (UOC)

Fecha entrega: 04/06/19

Agradecimientos

A mi familia, amigos, tutor y gente que ha confiado en mí. Especial mención a:

Mildrey Carbonell Castro

Francisco Luis de Andres Perez

Rubén Ramón Sobrino

Y a la empresa Estabanell Energia

“Lo esencial es invisible para los ojos”



Esta obra está sujeta a una licencia de Reconocimiento-Compartir Igual [3.0 España de Creative Commons](#)

FICHA DEL TRABAJO FINAL

Título del trabajo:	FASE, Framework de Ataque para Sector Eléctrico
Nombre del autor:	Aarón Flecha Menéndez
Nombre del consultor:	Omar Benjumea Gómez
Fecha de entrega (mm/aaaa):	06/2019
Área del Trabajo Final:	Seguridad en sistemas operativos
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Resumen del Trabajo (máximo 250 palabras):	

Abstract (in English, 250 words or less):

Palabras clave (entre 4 y 8):

Cybersecurity, Electric Sector, Hacking, Industrial Control Systems, Red Team

Índice

1	Introducción	1
1.1	Contexto y justificación del Trabajo	2
1.2	Objetivos del Trabajo.....	3
1.3	Enfoque y método seguido	3
1.4	Planificación del Trabajo.....	4
1.5	Breve sumario de productos obtenidos	6
1.6	Breve descripción de los otros capítulos de la memoria.....	6
2	Sector eléctrico, distribución – Introducción del sector eléctrico	8
2.1	Dispositivos y Sistemas	9
2.1.1	Gateway	9
2.1.2	HMI – Human Machine Interface.....	10
2.1.3	RTU – Remote Terminal Unit	10
2.1.4	IED – Intelligent Electronic Device	10
2.1.5	SCADA – Supervision Control And Data Acquisition.....	10
2.1.6	Switch industrial	10
2.1.7	UCS.....	10
2.1.8	Cortafuegos industrial	11
2.2	Comunicaciones	11
2.2.1	IEC 60870-5-104.....	11
2.2.2	DNP3 – Distributed Network Protocol v3.....	12
2.2.3	Protocolos del estándar 61850.....	12
2.3	Normativa y estándares	14
2.3.1	ISO 27001	14
2.3.2	ISO 27002	15
2.3.3	ISO 27019.....	16
2.3.4	IEC 62351	17
2.3.5	IEC 62443	17
2.3.6	NERC CIP	19
2.4	Amenazas en el sector eléctrico	19
2.4.1	Actores y vectores de ataque en entornos industriales	19
2.4.2	BlackEnergy 3	21
2.4.3	CrashOverride/Industroyer	22
2.4.4	DragonFly 2.0.....	23
2.4.5	GreyEnergy	23
3	Taxonomías de ataque, Cyber Kill Chain y CAT.....	25
3.1	Cyber Kill Chain (CKC)	25
3.2	CAT – Cyber Attack Taxonomy	31
3.3	Cyber Kill Chain vs. CAT	35
4	Framework de Ataque para el Sector Eléctrico.....	39
4.1	Uso del framework, ¿Y ahora qué?	40
4.2	CAT en los entornos industriales, <i>caffeine</i>	40
4.3	Escenario de ataque y modelado con CAT para sector eléctrico (<i>caffeine</i>) 44	
4.4	Desde el punto de vista defensivo.....	48
4.5	Modelado de un ataque, GREYENERGY.....	49

4.5.1	Matriz MITRE	49
4.5.2	Taxonomía CAT	54
5	Conclusiones	55
5.1	Lecciones aprendidas.....	55
5.2	Reflexión crítica	55
5.3	Futuras líneas de trabajo	55
6	Glosario	56
6.1	Acrónimos.....	56
6.2	Términos.....	56
7	Bibliografía.....	57
8	Anexo I – Diagramas de planificación	59
9	Anexo II – Ciberataque a Venezuela, revisión técnica.....	62

Lista de figuras

Ilustración 1: Datos extraídos del INCIBE-CERT	2
Ilustración 2: Explicación de la red eléctrica y concretamente la parte de distribución, fuente: Red Eléctrica Española (REE)	9
Ilustración 3: Ejemplo, red de subestación de distribución	11
Ilustración 4: Cabecera y sección de datos del protocolo IEC-104	12
Ilustración 5: Modelo de capas del estándar 61850, fuente: INCIBE-CERT	13
Ilustración 6: Disector del protocolo GOOSE (wireshark) explicando cada campo definido en el protocolo	14
Ilustración 7: Cuadro con el modelo "Plan-Do-Check-Act"	15
Ilustración 8: Enfoques de seguridad para protocolos de comunicación en el sector energía.	17
Ilustración 9: Documentos de los que se compone la IEC 62443	18
Ilustración 10: Evolución de BlackEnergy a lo largo del tiempo hasta el ataque en Ucrania	21
Ilustración 11: Funcionamiento de CrashOverride	23
Ilustración 12: Proceso de infección de GreyEnergy	24
Ilustración 13: Taxonomía Cyber-Kill Chain Extendida	27
Ilustración 14: Diferentes modelos desarrollados a partir de la taxonomía CKC o derivados de la misma, fuente: The unified kill chain	27
Ilustración 15: Parte de la matriz MITRE (Enterprise) donde se pueden observar las técnicas y tácticas de los adversarios	28
Ilustración 16: Matriz que cubre las primeras fases de un ataque	29
Ilustración 17: Matriz relacionada con acceso a los dispositivos	29
Ilustración 18: Matriz relacionada con los efectos originados por un ataque en la red (dispositivos)	29
Ilustración 19: Adaptación del modelo CKC a los sistemas de control, fuente: SANS	30
Ilustración 20: Modelado de CrashOverride con la matriz de MITRE	31
Ilustración 21: Fases de CAT, fuente: S21sec	32
Ilustración 22: Fases de la taxonomía CAT	34
Ilustración 23: Planteamiento de la metodología CAT siguiendo el modelo DML, fuente: Modelado de escenarios de ataque con metodología CAT, Hack&Beers Alicante vol.5	35
Ilustración 24: Mapeo de BlackEnergy con el modelado Cyber Kill Chain para sistemas de control industrial, fuente: Analysis of the Cyber Attack on the Ukrainian Power Grid	37
Ilustración 25: Estrategia, tácticas, técnicas y procedimientos de CAT, fuente: Modelado de escenarios de ataque con metodología CAT, Hack&Beers Alicante vol.5	38
Ilustración 26: Situación que tendría la red del escenario propuesto	44
Ilustración 27: Ataque realizado utilizando comandos IEC-104 suplantando una RTU en sus comunicaciones hacia el SCADA	48
Ilustración 28: Ejemplo de implementar reglas Snort para la detección de anomalías con el envío de paquetes del protocolo IEC104. Uso de herramienta Snorby para mostrar las alertas	49

Ilustración 29: Técnicas utilizadas por el backdoor FELIXROOT (Mini GreyEnergy), fuente: MITRE	52
Ilustración 30: Técnicas utilizadas por el backdoor GreyEnergy escrito en C y compilado en Visual Studio, fuente: MITRE	53
Ilustración 31: Búsqueda de dispositivos conectados a Internet desde ZoomEye ubicados en Venezuela	63
Ilustración 32: Uso de shodan para detectar posibles dispositivos con DNP3 en Venezuela	63
Ilustración 33: Búsqueda de dispositivos conectados a Internet con shodan que utilicen el protocolo Modbus/TCP (502/TCP)	64
Ilustración 34: Ejemplo de dispositivo desplegado por ABB en la hidroeléctrica de Simón Bolívar	65
Ilustración 35: Captura del vídeo donde se muestra cómo programar el dispositivo ABB DCS AC 800M, fuente: YouTube	65

1 Introducción

Dentro del mundo industrial, la disponibilidad es el pilar más importante por delante de la confidencialidad y la integridad. Este hecho, sumado a otros factores como la falsa sensación de seguridad por el aislamiento de los sistemas industriales a Internet, hacían que los ejercicios de ciberseguridad en producción o simplemente en estos entornos, fuesen impensables y prácticamente inalcanzables.

Con el paso del tiempo se fueron detectando diferentes piezas de malware empezando por Stuxnet¹ y siguiendo por otras como una de las últimas piezas detectadas bajo el nombre de GreyEnergy². Estas amenazas avanzadas permitieron la entrada de diferentes tecnologías a la industria que posibilitarían la mejora de la seguridad tanto de las redes industriales como de los propios dispositivos que se comunican dentro de ellas. Al inicio, sólo las opciones más pasivas empezaron a implantarse dada la complejidad inicial de las redes industriales. Entre estas opciones, se pueden encontrar el despliegue de sondas para la recopilación de información o la instalación de agentes que se ejecutasesen en los propios dispositivos industriales sin consumir muchos recursos.

Dado que las amenazas, al igual que la tecnología que se implanta de forma defensiva está en constante evolución, nos encontramos ante un nuevo reto en el mundo industrial, otro escalón que subir para evitar futuros ciberataques.

Tras las lecciones aprendidas con anteriores piezas de malware, algunos sectores como el financiero³ han optado por los ejercicios de Red Team como respuesta en forma de entrenamiento ante posibles ataques avanzados. Este tipo de ejercicios se basan en la explotación de diferentes vulnerabilidades en entornos de producción para:

- Detectar debilidades dentro de los elementos que se encuentran en una red.
- Llegar a conocer realmente la magnitud de los ataques.
- Mejora de los procedimientos y tareas a ejecutar frente a un ataque real.

Dicho esto, parece que otros sectores industriales están empezando a tomar cartas en el asunto y a plantearse de forma seria el uso de ejercicios Red Team para analizar sus sistemas. Entre estos sectores encontramos el sector Energía en el que se centrará a partir de ahora todo el proyecto.

El sector Energía, es uno de los sectores industriales donde los investigadores reportan más vulnerabilidades. Este hecho se debe a que es la piedra angular de los sectores a nivel industrial y posee, tanto presupuestos destinados a ciberseguridad como profesionales que focalizan sus trabajos e investigaciones en dicho sector.

¹ https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

² <https://www.nozominetworks.com/downloads/US/Nozomi-Networks-GreyEnergy-Dissecting-the-Malware.pdf>

³ https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

1.1 Contexto y justificación del Trabajo

Basándonos en el documento Unified CyberKill Chain⁴ donde se analizan en profundidad las diferentes taxonomías y modelados de ataque, podemos afirmar y justificar la necesidad de una nueva taxonomía que cubra ciertas carencias existentes en las ya planteadas y además posea un enfoque de ciberseguridad industrial. El gran objetivo que persigue este proyecto es crear un framework de ataque para entornos industriales que usen equipos red team en el sector eléctrico. Concretamente para subestaciones de distribución en producción. Es importante recalcar en producción por el hecho de que sectores como el financiero, ya están empezando a realizar ejercicios de este estilo sobre sus entornos en producción. Ejemplo de ello puede verse en el framework TIBER-EU⁵, TIBER-NL⁶ o el CBEST⁷ de Reino Unido. En este aspecto, también será importante recalcar los pros y contras que se encontrarán los equipos de red team a la hora de auditar entornos en producción, cómo poder solventar posibles problemas, arquitecturas tipo, uso de normativas para basar la argumentación de algunas pruebas (NIST framework, IEC 27019, IEC 62443, etc.) y otras características que se puedan tener en cuenta a la hora de poder argumentar pruebas con una base tanto en la normativa, como a nivel técnico.

En este proyecto será importante acotar el alcance ya que el sector energía, en concreto el subsector eléctrico (distribución) es uno de los subsectores que más está invirtiendo en materia de ciberseguridad. Según últimos datos del INCIBE-CERT, el sector energía es uno de los sectores donde los investigadores descubren más vulnerabilidades.

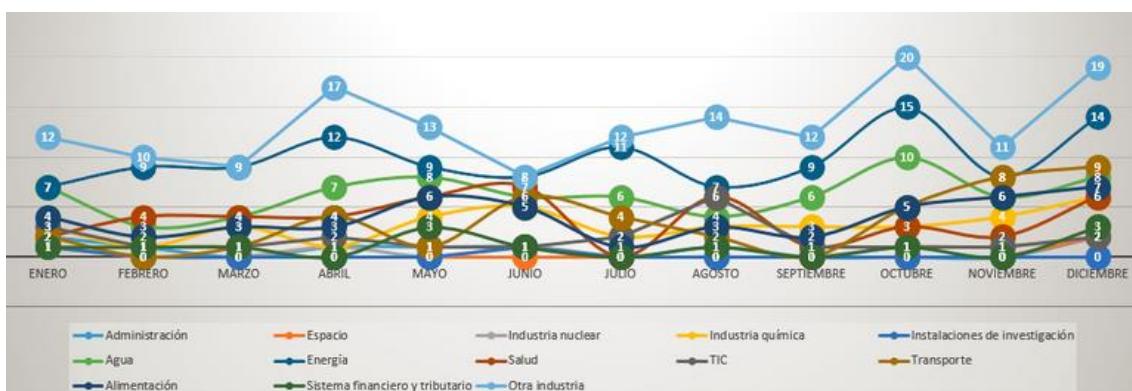


Ilustración 1: Datos extraídos del INCIBE-CERT

Para entender de mejor forma el framework a desarrollar, se analizarán ataques que han afectado al sector eléctrico como BlackEnergy 3 o uno de los últimos, GreyEnergy. El objetivo de estos análisis será identificar pasos ejecutados por los atacantes que permitan modelar el ataque completo y sirvan tanto para equipos de respuesta a incidentes como para equipos de red team a la hora de poder ejecutar pruebas controladas. En resumen, usar casos de ataques conocidos y bien documentados, con el objetivo reproducirlos en un entorno

⁴ <https://www.csacademy.nl/images/scripts/2018/Paul-Pols---The-Unified-Kill-Chain.pdf>

⁵ https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

⁶ https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf

⁷ <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide>

industrial real y comprobar si las medidas defensivas que se tienen podrían haber evitado los ataques reales⁸.

1.2 Objetivos del Trabajo

Entre los diferentes objetivos que tiene este trabajo, han de destacarse los siguientes:

- Creación de un Framework de ataque para el sector eléctrico teniendo en cuenta la problemática de la disponibilidad y el caso concreto de las distribuidoras eléctricas.
- Potenciar la taxonomía Cyber Attack Taxonomy (CAT) en sistemas de control industrial. Dicha taxonomía de ataque se está desarrollando en formato open source de tal forma que cualquier persona pueda contribuir y utilizarla en base a sus necesidades. Para conseguir este objetivo se desarrollará un ejemplo utilizando la taxonomía CAT y el framework de ataque para el sector eléctrico. En dicho ejemplo se analizará una pieza de malware reciente que ha afectado al sector energía.

La consecución de este objetivo se verá reflejada con el desarrollo del propio proyecto que contendrá bastante información para aplicar la taxonomía CAT, y, concretamente, el framework orientado a entornos industriales.

Partes de este proyecto serán añadidos a la cuenta de github oficial de la taxonomía CAT.

- Comparación de la taxonomía de ataque planteada por Lockheed Martin (Cyber Kill Chain) y el modelado de ataque propuesto por MITRE frente a la taxonomía Cyber Attack Taxonomy (CAT). Este objetivo quiere mostrar algunas de las deficiencias que poseen taxonomías de ataque y modelados como el propuesto por Mitre en casos como los “*insiders*” u otras situaciones que pueden darse en las empresas. Gracias a la muestra de estas deficiencias y a los ejemplos que se desarrollarán, se pretende dar una visión tanto de la taxonomía CAT como de su aplicación a los entornos industriales (framework creado).
- Proporcionar una serie de pasos clave a ejecutar por equipos de Red Team en un entorno de producción. Estos pasos se centrarán en la parte de distribución eléctrica que poseen las subestaciones.

1.3 Enfoque y método seguido

Para el desarrollo del framework *caffeine* desarrollado en apartados más adelante dentro de este mismo documento, se optó por el uso de la metodología CAT. El framework se enmarcará dentro de esta metodología y permitirá a equipos de red team disponer de tácticas, técnicas y herramientas específicas

⁸ <https://www.youtube.com/watch?v=pL9q2IOZ1Fw&feature=youtu.be>

para la ejecución de pruebas en entornos de distribución eléctrica que se encuentren en producción. Dado que CAT no pretende ser un sustituto del modelado de ataque que plantea MITRE o PwnWiki, sino que se alimenta de las tácticas, técnicas, herramientas y otros recursos que poseen. Esta elección permitirá realizar tanto modelarlos como plantear diferentes ejercicios de red team de una forma más clara y eficiente tanto a nivel técnico como visual.

En resumen, dado que el framework *caffeine* se enmarcará dentro de CAT, dentro de este framework se encontrarán técnicas, tácticas y herramientas tanto específicas para el sector eléctrico (distribución) como heredadas del propio CAT, de MITRE o de PwnWiki entre otros.

1.4 Planificación del Trabajo

Dado este proyecto ha sido planteado por el alumno, la primera tarea realizada fue la recopilación de documentación y envío de argumentaciones al responsable del área de seguridad en sistemas operativos. Tras un intercambio de correos y explicación del proyecto, se pasó a la planificación del mismo. Las diferentes entregas planteadas con el contenido que se incluiría en cada una son las siguientes:

- **PEC 1**
 - Planificación del trabajo e introducción del proyecto
 - Alcance y objetivos del trabajo a desarrollar
 - Argumentación del proyecto
 - Metodología utilizada
 - Contenido del proyecto
 - Organización de la documentación. En este punto se valoró el uso de gestores documentales como nuxeo, alfresco o el propio google drive.
- **PEC 2**
 - **Introducción** – Breve descripción del estado actual de la ciberseguridad en los entornos industriales y concretamente en el sector eléctrico (distribución).
 - **Contexto y justificación del Trabajo** - Punto de partida del trabajo (¿Cuál es la necesidad a cubrir? ¿Por qué es un tema relevante? ¿Cómo se resuelve el problema de momento?) y aportación realizada (¿Qué resultado se quiere obtener?)
 - **Objetivos del Trabajo** - Listado de los objetivos del trabajo
 - **Enfoque y método seguido** - Indicar cuáles son las posibles estrategias para llevar a cabo el trabajo e indicar cuál es la estrategia elegida (desarrollar un producto nuevo, adaptar un producto existente, ...).

Valorar porque esta es la estrategia más apropiada para conseguir los objetivos.

- **Planificación del Trabajo** - Descripción de los recursos necesarios para realizar el trabajo, las tareas a realizar y una planificación temporal de cada tarea utilizando un diagrama de Gantt o similar. Esta planificación tendría que marcar cuáles son los hitos parciales de cada una de las PEC.
- **Breve sumario de productos obtenidos** - No hay que entrar en detalle: la descripción detallada se hará en el resto de capítulos.
- **Breve descripción de los otros capítulos de la memoria** - Explicación de los contenidos de cada capítulo y su relación con el trabajo en global.
- **Sector eléctrico, distribución** – Introducción del sector eléctrico
 - **Dispositivos** – Diferentes dispositivos que pueden encontrarse en una red de una subestación y su comunicación con el centro de control.
 - **Comunicaciones** – Arquitecturas que suele tener una subestación eléctrica de distribución, protocolos utilizados (IEC104, DNP3, 61850, etc.).
 - **Normativa** – Comentar diferentes normativas a tener en cuenta y que servirán a la hora de desarrollar el framework de ataque. En este punto, sobre todo se abordarán los estándares ISO/IEC 27019, IEC 62351, IEEE 1686-2013, NERC CIP y 62443.
 - **Ataques** – Comentar los ataques de malware más famosos y recientes al sector eléctrico (BlackEnergy, GreyEnergy, etc.).
- **PEC 3**
 - **ICS Cyber Kill Chain y las taxonomías de ataque** – Introducción a la taxonomía de ataque Cyber Kill Chain desarrollada por Lockheed Martin (CKC) y concretamente al adecuado para entornos industriales. Tras comentar dicha taxonomía, se hará una descripción con algo de profundidad de la taxonomía CAT y del modelado que posee Mitre con sus matrices que incorporan TTPs.

- **Framework del NIST y otros frameworks a nivel industrial** – Comentar las últimas actualizaciones del framework que posee el NIST y otros posibles frameworks.
- **PEC 4**
 - **Framework de Ataque para el Sector Eléctrico** – Desarrollo de la idea principal.
 - **Espacios temporales de actuación**
 - **Explicación del entorno creado para las pruebas**
 - **Aplicación de CAT a las pruebas**
 - **Pruebas ejecutadas, resultados y recomendaciones**
 - **Herramientas**
 - ...
- **Entrega final**
 - **Incorporación de todas las correcciones y mejoras detectadas tanto por el tutor como por el propio alumno.**
 - **Añadir los siguientes apartados:**
 - **Conclusiones finales** – Exposición de las conclusiones extraídas tras el trabajo realizado y las posibilidades de mejora que posee el proyecto.
 - **Glosario** – Muestra de los diferentes términos utilizados en el documento.
 - **Bibliografía** – Descripción del material utilizado.
 - **Anexos** – El uso de anexos dependerá directamente del desarrollo que posea el trabajo.

Se han elaborado diferentes diagramas y tablas que recogen toda la planificación de forma más visual. Todo este material puede consultarse en el Anexo I – Diagramas de planificación.

1.5 Breve sumario de productos obtenidos

El desarrollo del framework *caffeine* ha proporcionado diferentes aportaciones en el proyecto que posee CAT en github con nuevas tácticas y técnicas específicas para el sector industrial y concretamente para el sector eléctrico (distribución). Dichas tácticas y técnicas se irán publicando en base a la revisión que vaya haciendo la comunidad. Además, será el punto de partida para otros profesionales del sector que deseen tanto modelar un ataque como plantear nuevos escenarios de ataque para equipos de red team.

1.6 Breve descripción de los otros capítulos de la memoria

Los contenidos de cada apartado y la importancia de cada uno en este proyecto se describen a continuación:

- **Introducción** – Breve descripción del estado actual de la ciberseguridad en los entornos industriales y concretamente en el sector eléctrico (distribución). Estado del arte de la ciberseguridad industrial y algunos datos de interés de forma genérica.
- **Sector eléctrico, distribución** – Introducción del sector eléctrico. Este capítulo permite poner al lector en situación y focalizar los términos de los que se va a hablar. Se describirán dispositivos, comunicaciones, normativas, estándares y ataques que afectan directamente al sector eléctrico.
- **Taxonomías de ataque, Cyber Kill Chain y CAT** – En este capítulo se describirá tanto la taxonomía de ataque propuesta por Lockheed Martin (Cyber Kill Chain) como la taxonomía en la que se basará el desarrollo del framework para el sector eléctrico CAT (Cyber Attack Taxonomy).
- **Framework de Ataque para el Sector Eléctrico** – Desarrollo de la idea principal del proyecto, el framework. Se incluirán ejemplos de nuevas tácticas y técnicas específicas del sector eléctrico y un modelado del incidente GreyEnergy.
- **Conclusiones finales** – Exposición de las conclusiones extraídas tras el trabajo realizado y las posibilidades de mejora que posee el proyecto.
- **Anexos** – El trabajo posee 2 anexos. El primero en el que se muestra de forma gráfica y en tablas una planificación más en profundidad del trabajo realizado y en el segundo anexo, una visión técnica de los ataques sufridos por Venezuela en su sector eléctrico.

2 Sector eléctrico, distribución – Introducción del sector eléctrico

El sector eléctrico es un sector que sustenta otros muchos y permite, entre otras muchas acciones, proporcionar energía a poblaciones. En caso de verse comprometido el suministro energético en una población, podrían generarse diferentes revueltas dada la importancia que tiene la electricidad en las vidas de las personas actualmente. Uno de los casos más recientes, donde se trata esta problemática puede verse en el Anexo II – Ciberataque a Venezuela, revisión técnica.

Dentro de una red eléctrica encontramos diferentes fases o etapas a las que debe estar sujeta la electricidad antes de llegar a nuestros hogares. En este proyecto nos centraremos en la fase de distribución, pero sin dejar indiferentes las demás fases que serán enumeradas y brevemente comentadas para tener una mejor visión de cómo es una red eléctrica.

1. **Generación.** El origen de la energía eléctrica deriva de diferentes elementos primarios como puedan ser el agua, viento, sol, etc. Todos ellos, y gracias a un tratamiento adecuado de los mismos proporcionado por plantas generadoras (centrales hidroeléctricas, eólicas, solares, etc.) originan la electricidad.

En muchas ocasiones, las plantas generadoras no cumplen las regulaciones adecuadas y pueden dañar el medio ambiente por lo que es importante, además de generar energía eléctrica, hacerlo de manera sostenible y eficiente.

2. **Transporte.** La energía generada en la fase inicial ha de ser transformada previamente por las denominadas estaciones transformadoras. La misión de estas estaciones no es otra que elevar o reducir la tensión de salida de las centrales generadoras a un valor de tensión adecuado (en España entre 220 y 400 kV) para obtener una mayor eficiencia en el transporte eléctrico y evitar pérdidas energéticas causadas por el Efecto Joule⁹.

Para cumplir con el objetivo que tiene la fase de transporte, suelen utilizarse elementos como postes eléctricos y cables de alta tensión que transportan la electricidad a lo largo de grandes extensiones kilométricas.

En España, Red Eléctrica de España (REE) es la compañía encargada de gestionar la red de transporte, desde que entrara en vigor la Ley 17/2007¹⁰, que le otorgó la condición de transportista único de la electricidad.

3. **Distribución.** Una vez transportada, la electricidad ha de ser repartida y distribuida a las diferentes zonas pobladas o que necesiten energía por alguna necesidad concreta. Para alcanzar este objetivo, encontramos las

⁹ https://es.wikipedia.org/wiki/Efecto_Joule

¹⁰ <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-13024>

estaciones transformadoras reductoras que permiten realizar un tratamiento de la electricidad previo para que los valores pasen de alta a media tensión y de media a baja tensión antes de llegar a los clientes finales, es decir, los centros poblados o ubicaciones concretas.

La red de reparto parte de las subestaciones de transformadoras reductoras, y mediante anillos que rodean los grandes centros de consumo llegan hasta las estaciones transformadoras de distribución. Las tensiones habituales son 25, 30, 45, 66, 110 o 132 kV. La segunda etapa la constituye la red de distribución en media tensión, que es una red de topología radial que une las subestaciones transformadoras de distribución con los centros de transformación. Las tensiones empleadas son 3, 6, 10, 11, 15, 20, 25 o 30 kV.

Esta será la fase en la que centraremos la investigación para poder reducir el alcance y mostrar un mayor detalle técnico.

4. **Comercialización.** Esta es la fase final de la electricidad en la que las empresas venden mediante un régimen de competencia, al menos en España, la electricidad a los consumidores finales. Estas empresas que venden la electricidad, previamente han tenido que comprarla a las compañías generadoras.

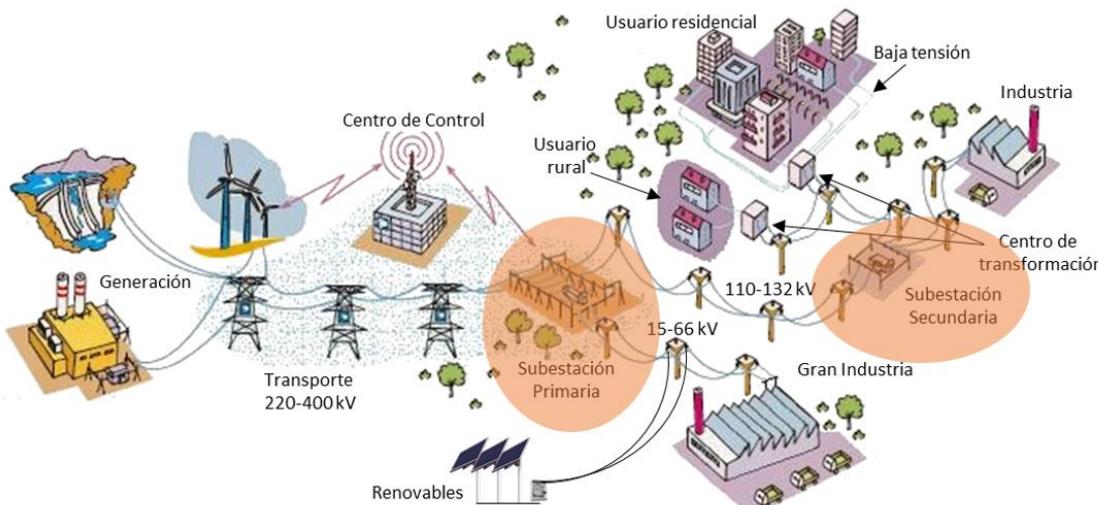


Ilustración 2: Explicación de la red eléctrica y concretamente la parte de distribución, fuente: Red Eléctrica Española (REE)

2.1 Dispositivos y Sistemas

Dentro de una subestación de distribución eléctrica pueden encontrarse diferentes dispositivos de ámbito industrial entre los que destacan:

2.1.1 Gateway

La puerta de enlace permite traducir los protocolos utilizados en las comunicaciones internas de la subestación a protocolos utilizados entre centro de control y la propia subestación (IEC 104). En este caso, puede tratarse de un

dispositivo totalmente independiente o de una función que posea otro dispositivo dentro de la subestación.

Algunos de las traducciones más extendidas a nivel industrial en el sector eléctrico son:

- Modbus TCP a IEC 104. (Subestaciones de distribución clásicas que han sufrido una digitalización de los procesos)
- IEC 61850 a IEC 104. (Subestaciones de distribución más modernas)

2.1.2 HMI – Human Machine Interface

Muestran información del estado de los procesos para que los operadores coordinen y controlen las acciones a realizar. En ocasiones permiten realizar acciones para ajustar el proceso o modificar variables del mismo.

2.1.3 RTU – Remote Terminal Unit

Es un dispositivo que permite obtener señales de los procesos y enviar información a un sitio remoto para su posterior procesamiento. Se encuentra principalmente en subestaciones sin un sistema eléctrico de automatización y posee tantos cables como señales se intercambian con el centro de control.

2.1.4 IED – Intelligent Electronic Device

Dispositivos que permiten la extracción de información. Comúnmente esta información suelen ser valores de voltaje e intensidad entre otros que permiten controlar la operativa de la subestación eléctrica.

2.1.5 SCADA – Supervision Control And Data Acquisition

Este tipo de sistemas, realizan acciones de supervisión, control y gestión de información en tiempo real dentro de la subestación eléctrica. Además, permiten una centralización de señales generadas por uno o varios procesos industriales (control de alertas) y poseen la capacidad de comunicarse con multitud de dispositivos ubicados en redes de control (PLC, RTU, HMI, etc.).

2.1.6 Switch industrial

Elemento de red que permite la comunicación entre dispositivos. Los switches industriales, además de estar rúgerizados por las condiciones bajo las que trabajan, también poseen las capacidades de los switches que se ven comúnmente en entornos más corporativos. Además, una de las funcionalidades más utilizadas además de la creación de VLAN (802.1Q), es la de capacidades PRP para redundancia de tráfico de red.

2.1.7 UCS

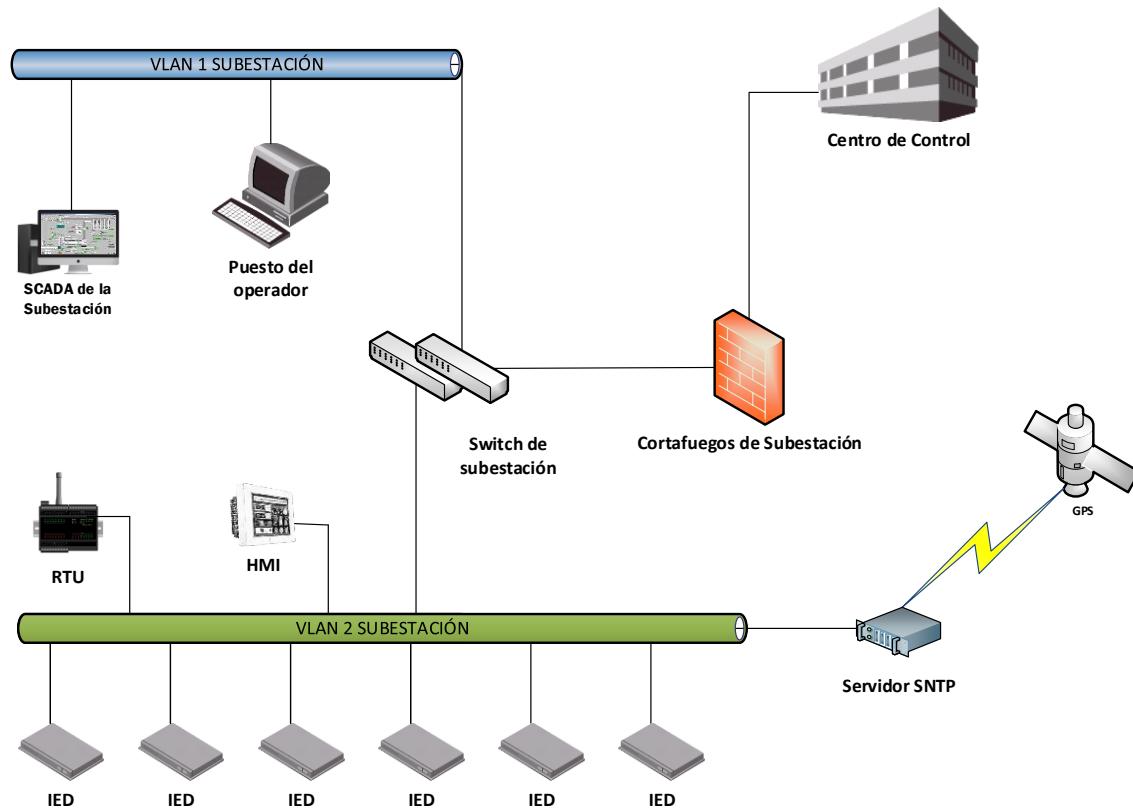
La unidad central de subestación permite centralizar las órdenes y señales provenientes de todas las unidades de control locales de cada una de las posiciones que constituyen la subestación.

2.1.8 Cortafuegos industrial

Dispositivo de seguridad que permite la gestión de las comunicaciones con funcionalidades como DPI (Deep Packet Inspection) y DPBI (Deep Packet Behavior Inspection) entre otras interesantes enfocadas al mundo industrial. Estas funcionalidades permiten realizar una inspección en profundidad de los protocolos utilizados dentro de las subestaciones y en las comunicaciones con el centro de control, comúnmente implementadas bajo el protocolo IEC-104.

2.2 Comunicaciones

Para que los dispositivos interactúen entre ellos han de existir una serie de comunicaciones que permitan enviar información de relevancia en la parte de control y supervisión. Para ello se describen a continuación los protocolos más destacados que pueden encontrarse en el sector eléctrico y concretamente en una subestación.



2.2.1 IEC 60870-5-104

Este protocolo es utilizado para comunicaciones entre subestación y centro de control. Se considera una extensión del protocolo IEC 101 que trabaja en comunicaciones serie. Por ello, IEC 104 implementa cambios en los servicios a diferentes niveles de la capa OSI (transporte, enlace y física), de este modo consigue la implementación TCP/IP.

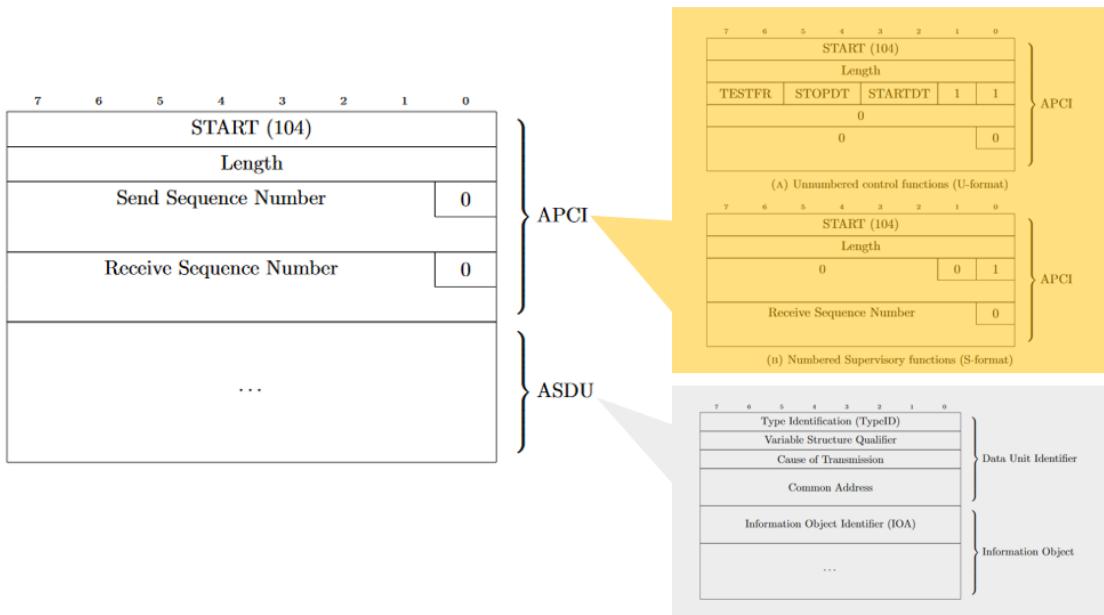


Ilustración 4: Cabecera y sección de datos del protocolo IEC-104

2.2.2 DNP3 – Distributed Network Protocol v3¹¹

Protocolo de comunicaciones desarrollado en 1993 y bastante extendido a nivel estadounidense y canadiense. DNP3 es un protocolo industrial destinado a comunicaciones entre equipos inteligentes (IED) y estaciones controladoras. Su presencia en Europa es escasa por la presencia de alternativas como IEC-60870-5-101 o IEC-60870-5-104.

DNP3 es un protocolo de tres capas o niveles según el modelo OSI: nivel de enlace (Data Link Layer), Nivel de Aplicación (Application Layer), y un tercer nivel de Transporte (Transport Layer) que realmente no cumple con todas las especificaciones del modelo OSI, y por lo cual se suele denominar pseudo-nivel de Transporte. Por este motivo suele referirse a él como un protocolo de dos capas o niveles.

La estructuración en capas o niveles, sigue el siguiente esquema:

- **Los mensajes a nivel de aplicación son denominados Fragmentos.** El tamaño máximo de un fragmento está establecido en 1024 bytes.
- **Los mensajes a nivel de transporte son denominados Segmentos.**
- **Los mensajes a nivel de enlace son denominados Tramas.** El tamaño máximo de una trama DNP3 es de 292 bytes.

2.2.3 Protocolos del estándar 61850¹²

El estándar IEC 61850 es el primero de los estándares considerados como una solución global ante la problemática existente entre protocolos propietarios y dispositivos de diferentes fabricantes incapaces de comunicarse entre sí. Este estándar define aspectos como interoperabilidad, protección, monitorización, control y automatización de los diferentes dispositivos de forma individual y entre

¹¹ <https://es.wikipedia.org/wiki/DNP3>

¹² <https://www.incibe-cert.es/blog/estandar-iec-61850-todos-uno-y-uno-todos>

ellos. Uno de los objetivos más importantes en su definición fue la interoperabilidad, pero otro aspecto muy importante fue la reducción de costes. Por ejemplo, funciona bajo una red LAN, lo que hace reducir el cableado y por tanto el coste.

El estándar está dividido en numerosas partes, en las cuales se tratan temas como las comunicaciones, el modelo de datos o los test de cumplimiento, pero ninguna de ellas habla sobre los aspectos técnicos de ciberseguridad. En realidad, la seguridad correspondiente a IEC 61850 se delega en otro estándar, en concreto, el IEC 62351.

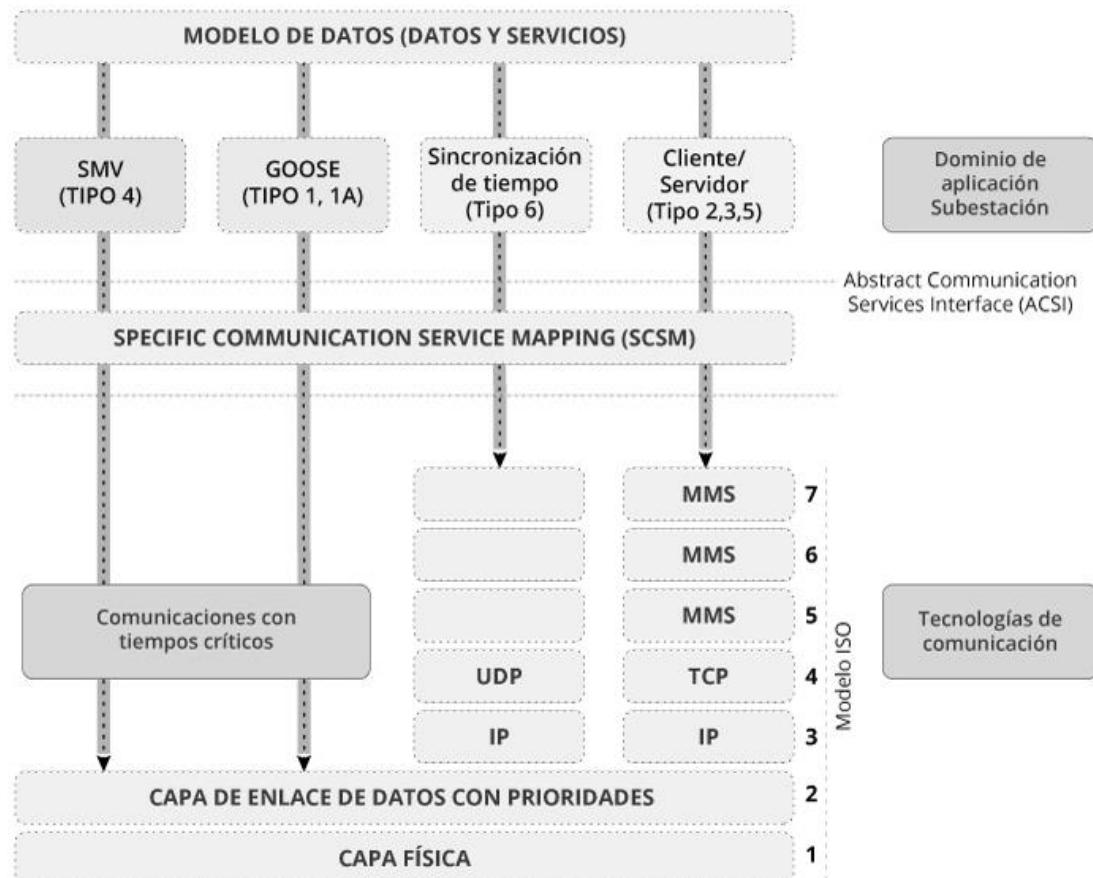


Ilustración 5: Modelo de capas del estándar 61850, fuente: INCIBE-CERT

- **Sampled Measured Values** es utilizado para proporcionar una comunicación rápida de valores de medición, protección y control. Funciona a través de Ethernet (Capa 2 OSI) y los mensajes son encapsulados como multicast, siguiendo una estructura emisor – suscriptor, donde el emisor envía los datos a todos los equipos de la red y cada equipo se suscribe a los datos para acceder a los mismos.
- **GOOSE** es utilizado para la transmisión en tiempo real de eventos críticos y funciona, al igual que Sampled Measured Values, a través de mensajes multicast de Ethernet (Capa 2 OSI). El modelo de funcionamiento de GOOSE también sigue la estructura emisor – suscriptor.

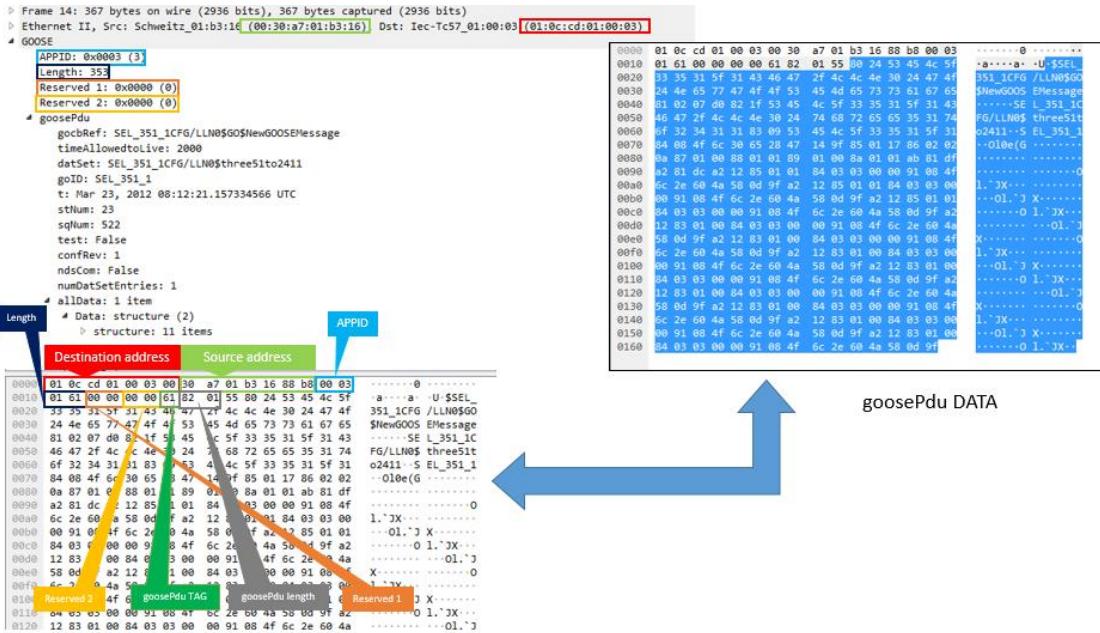


Ilustración 6: Disector del protocolo GOOSE (wireshark) explicando cada campo definido en el protocolo

- Para la sincronización de tiempo de los dispositivos se utiliza el protocolo **SNTP**. Como su propio nombre indica, es una versión simplificada del protocolo NTP, utilizado en equipos que no necesitan la funcionalidad completa del protocolo. Para la transmisión de los mensajes SNTP se utiliza el protocolo UDP (Capa 4 OSI).
- Por último, el protocolo **MMS** es la base de las comunicaciones de datos de aplicación en el estándar IEC 61850. El protocolo envía sus mensajes a través de conexiones TCP (Capa 4 OSI) y es utilizado para las comunicaciones cliente/servidor. Así, es utilizado para el intercambio de datos de la aplicación, así como parámetros de configuración de los dispositivos o datos de monitorización.

2.3 Normativa y estándares

Tanto en el sector eléctrico como en otros sectores, existen diferentes normativas que guardan relación con la ciberseguridad. En este punto se destacan las normativas y estándares más conocidos y que poseen una gran madurez en su aplicación al sector eléctrico.

2.3.1 ISO 27001

La norma ISO 27001 cubre diferentes tipos de organizaciones ya sean empresas, organizaciones sin ánimo de lucro o gubernamentales, pequeñas o grandes empresas, etc. Por ello no es una norma específica sólo para el sector Energía, pero de ella se pueden sacar diferentes ideas a la hora de desarrollar algunos de los controles que aparecerán reflejados en este documento.

Este estándar fue confeccionado para mostrar un modelo a la hora de implantar un Sistema de Gestión de Seguridad de la Información (SGSI) en las empresas siguiendo el modelo “Plan-Do-Check-Act” (PDCA).

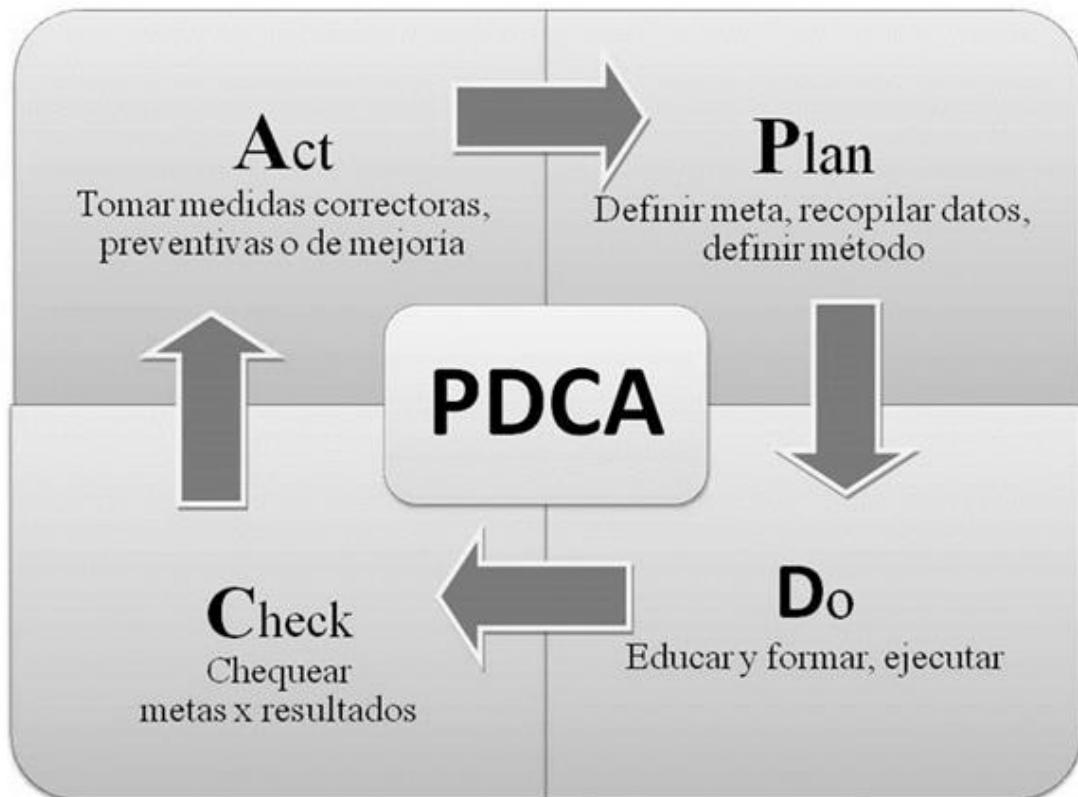


Ilustración 7: Cuadro con el modelo "Plan-Do-Check-Act"

El objetivo que persigue la creación de un SGSI es velar por las tres características elementales a la hora de proteger la información dentro de las organizaciones:

- **Confidencialidad.** La información sólo debe ser vista por aquellos que tienen permiso para ello, no debe poder ser accedida por alguien sin el permiso correspondiente.
- **Integridad.** La información podrá ser modificada solo por aquellos con derecho a cambiarla.
- **Disponibilidad.** La información deberá estar disponible en el momento en que los usuarios autorizados requieren acceder a ella.

2.3.2 ISO 27002

La ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar que proporciona recomendaciones para aplicar una serie de buenas prácticas en la gestión de seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).

En su nueva versión de 2013, la ISO 27002 se presenta con 14 dominios, 35 objetivos de control y 114 controles.

Entre las novedades a resaltar que aparecen en esta nueva versión comparándola con la versión de 2005 basada en 11 dominios, 39 objetivos de control y 133 controles, se puede encontrar el cambio de sección de todo lo relacionado con dispositivos móviles y teletrabajo asociado en la versión 2005 al Control de Accesos y con la nueva versión asociado a la sección 6 “Organización de la Seguridad de la Información”. Dentro de la propia sección de Control de Accesos se engloba lo relacionado con accesos al sistema operativo, a las aplicaciones y a la información. Aparecen nuevos dominios como el de Criptografía (sección 10), dentro del cual encontramos todos los controles criptográficos sugeridos para una organización. Y ya para finalizar, otro cambio a tener en cuenta es que los casos a la hora de plantearse una recuperación de desastres están dentro de la sección 17.

Además, cabe resaltar que existen versiones específicas de la norma ISO/IEC 27002, enfocadas en diferentes tipos de empresas: sector de la salud (ISO 27799:2016), sector de la energía (ISO 27019 descrita en el siguiente punto), servicios en la nube (ISO/IEC 27017:2015), entre otros.

2.3.3 ISO 27019

La norma IEC 27019 proviene de una base de sistemas de información (IEC 27002) y provee principios y controles específicos para los sistemas de control eléctricos. El objetivo de ISO/IEC TR 27019:2013 es extender las series ISO/IEC 27000 al dominio de los procesos de automatización y control en el sector eléctrico y, de esta forma, dar soporte a la industria eléctrica en la implementación de un sistema de gestión de la seguridad de la información.

El estándar cubre el proceso de controlar y monitorizar la generación, transmisión, almacenamiento y distribución de energía, en combinación con el control de procesos de soporte. Incluye controles para las siguientes aplicaciones y componentes:

- Centro de control: sistema TI y sistema de monitorización, así como el sistema de automatización.
- Componentes de automatización y controladores digitales tales como PLC, incluyendo actuadores y sensores.
- El resto de sistemas TI utilizados en el control del proceso del dominio.
- Conjunto de tecnologías de comunicación empleadas en el control del proceso del suministro eléctrico (redes, telemetría, aplicaciones de telecontrol y control de remotas).
- Medida remota en la última milla.
- Protección digital y sistemas safety (en productos como los PLC por ejemplo).
- Componentes de distribución DER (Distributed Energy Resources, Recursos de Energía Distribuida) preparados para futuras acometidas.

- Software, firmware y aplicaciones instaladas en sistemas anteriormente citados.

Tanto los sistemas puramente eléctricos (o electromecánicos) como los sistemas de telecomunicaciones quedan fuera de este estándar.

2.3.4 IEC 62351

El ámbito de actuación de la norma IEC 62351 es la seguridad en las operaciones de control del sector energético. El objetivo principal es acometer el desarrollo de estándares de seguridad para los protocolos de comunicaciones definidos por el grupo IEC TC 57, específicamente IEC 60870-5 (IEC101, IEC104, etc.), IEC 60870-6 (ICCP), IEC 61850 (MMS, GOOSE), IEC 61970 y IEC 61968.

La norma IEC 62351 se divide en 11 documentos independientes, siendo el primero la introducción a la norma, el segundo el glosario de términos y el resto el conjunto de medidas de seguridad, aplicadas por familias de protocolos. Los últimos documentos unidos a la norma definen la implementación de medidas como el control de accesos basado en roles (RBAC – Role Based Access Control), la gestión de claves, la definición de una arquitectura de seguridad o las medidas de seguridad para utilizar con ficheros XML.

Service	Applied Protocol (s) or Applications	Recommendations for security controls
Remote desktop	RDP	Use VPN or IPSec option. RDP has built-in encryption (RC4) and authentication from Windows operating system.
Web-monitor	HTTP	Application of HTTPS for secure Web access.
Web-monitor	Java Applets/Servlets	Application of HTTPS for secure Web access.
Reporting / MMS	IEC 61850	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Time synchronization	NTP	NTPv3 offers security. Can be deployed using auto-key for key management
Substation – control center communication	IEC 60870-5-104	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center communication	IEC 60870-6 TASE 2 (ICCP)	IEC/TS 62351-4 encompasses IEC 61850 and provides end-to-end security for IEC 61850. Alternatively a VPN may be deployed.
Control center and substation – control center communication	DNP3	Application of DNP3 security measures.
Network management	SNMP	Application of SNMPv3 security measures, support of IEC/TS 62351-7 defined NSM objects, SNMPv2 should only be allowed for monitoring.
File transfer	FTP	Use secure variants like SFTP instead of FTP.

Ilustración 8: Enfoques de seguridad para protocolos de comunicación en el sector energía.

2.3.5 IEC 62443

El estándar IEC 62443, elaborado por el grupo TC65 de la IEC, surge como evolución de la norma ISA 99, con la intención de completarla y ampliar sus

capacidades de actuación. Uno de los principales objetivos de seguridad de la IEC 62443 es la defensa en profundidad, profundizando en los conceptos planteados por ISA99 y extendiendo la seguridad a otros ámbitos desde los fabricantes hasta los operadores.

La seguridad en las redes industriales viene muy marcada por los diferentes niveles de la pirámide de automatización (ISA-95). Esta normativa creó la base para el estándar IEC 62443, evolución de la ISA99, en concreto el IEC-62443-3-2 "Standard addresses security risk assessment and system design for IACS", donde se introducen los conceptos de "zonas" y "conductos" para una segmentación segura de las redes industriales aplicando la defensa en profundidad¹³¹⁴.

- Una **Zona** se define como la agrupación lógica o física de activos industriales (dichos activos pueden ser físicos, aplicaciones o información) los cuales comparten los mismos requisitos de seguridad.
- Un **Conducto** es un tipo particular de zona que agrupa las comunicaciones que permiten transmitir información entre diferentes zonas.

El estándar se compone de un total de 13 documentos, de los cuales algunos ya están publicados de forma oficial y el resto en estado de borrador. A su vez, los documentos se dividen en 5 informes técnicos, 1 especificación técnica y 7 guías, agrupadas en cuatro bloques según su contenido: General, Políticas y procedimientos, Sistema y Componentes.

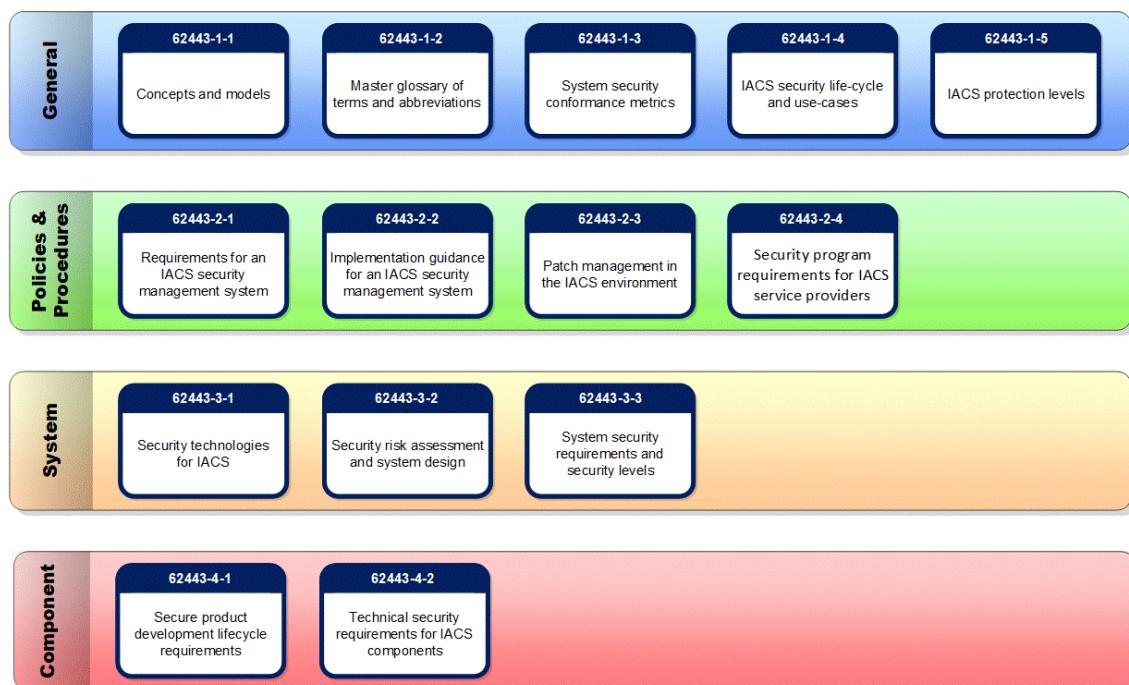


Ilustración 9: Documentos de los que se compone la IEC 62443

13 <https://www.cci-es.org/documents/10694/613683/Establecimientos+zonas+y+conductos.pdf/a479e3db-81f4-43c1-b5d1-f9e5f7754bcf>

14 <https://www.incibe-cert.es/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial>

2.3.6 NERC CIP

El NERC es el organismo regulador del sector Energía en el territorio estadounidense. Este organismo creó una serie de guías de control de obligado cumplimiento para poder valorar la seguridad de las instalaciones y del sector en general. Originalmente crearon 9 guías, de las que todas menos la primera, están relacionadas con la ciberseguridad, posteriormente ampliaron el número total a 12. Actualmente está en vigor la versión 5 y en desarrollo la versión 7 en algunas guías.

Este estándar reconoce los diferentes roles de cada entidad en la operación del sistema eléctrico, la criticidad y las vulnerabilidades de los activos que lo componen y los riesgos a los que están expuestos.

Entre los tipos de organizaciones que deben cumplir con el estándar, encontramos a empresas distribuidoras que tenga dentro de su red activos considerados dentro del estándar. Por lo que afectaría de forma directa a los objetivos que persigue este documento.

2.4 Amenazas en el sector eléctrico

La incorporación de nuevas tecnologías que permiten una monitorización mejor de las redes industriales y las diferentes soluciones defensivas que se están empezando a incorporar en el mundo industrial, facilitan la detección de malware. Tras las infecciones de Stuxnet, las diferentes empresas industriales han comenzado a desarrollar e incorporar medidas de ciberseguridad dentro de sus redes con el objetivo de evitar nuevas infecciones.

El reto que supone la defensa frente a una posible amenaza avanzada resulta bastante complejo ya que los atacantes utilizan técnicas bastante avanzadas que dificultan la detección de comportamientos anómalos.

Hace relativamente poco tiempo, han sido detectados una serie de piezas malware a nivel industrial cuyo objetivo era el sector eléctrico. Entre otras acciones las piezas de malware detectadas realizaban exfiltración de información, envío de tramas de control con protocolos industriales, etc. Cabe destacar que tras el análisis de estas piezas malware, se detectó un desarrollo bastante profesional dado que algunos de ellos eran modulares y estos módulos se cargaban mediante comunicaciones con el C&C (Centro de Control).

2.4.1 Actores y vectores de ataque en entornos industriales

Entre los diferentes actores que pueden originar un incidente industrial fruto de alguna motivación como pueda ser la venganza, terrorismo, espionaje industrial, sabotaje, etc. encontramos los siguientes actores:

- **Estados o naciones:** Sus objetivos están totalmente estudiados y son atacados por razones concretas como pasó en el caso de Stuxnet, para parar el programa nuclear iraní.
- **Insiders:** Empleados descontentos que buscan beneficios, principalmente económicos, mediante el uso de conocimientos que poseen de la red interna, dispositivos, etc. de la empresa en la que

trabajan. Estos empleados pueden actuar por cuenta propia o motivados por empresas externas que ofrecen dinero a cambio de información o sabotaje.

- **Terroristas:** Su principal objetivo es generar pánico social a través de ataques dirigidos a infraestructuras críticas utilizadas por gran parte de una población. Un ejemplo de este tipo de ataques se dio en Reino Unido en 2018 cuando el Estado Islámico, Daesh, intento modificar los parámetros de una central potabilizadora.
- **Cibercriminales:** El objetivo que buscan este tipo de actores es un beneficio económico a través de ataques como el uso de ransomware para pedir un rescate de los datos cifrados u originar anomalías dentro de las redes industriales. A veces estos grupos se mueven por ideales políticos o simplemente infectan redes industriales tras una gran campaña de infección en la red.

Ahora que ya conocemos algunos de los actores con mayor peso en los ataques a nivel industrial, es hora de conocer los vectores de ataque más utilizados en las campañas de malware donde se utilizan sobre todo APT (Amenazas avanzadas persistentes):

- **Adjuntos maliciosos:** prácticamente, la totalidad de los últimos malware detectados en sistemas de control industrial posee como vector de ataque un correo con adjuntos maliciosos. Gran parte de estos documentos adjuntos necesitan de funcionalidades como las macros de Office o la activación de JavaScript en documentos para infectar a la víctima.
- **Spear phishing:** variante de phishing que consiste en el envío de mensajes, generalmente correos electrónicos, específicos y personalizados a un grupo de personas determinado, con el objetivo de obtener información sensible o infectar la máquina utilizada por la víctima. Esta es la principal diferencia respecto al phishing tradicional por email, que consiste en el envío de un mismo correo electrónico de forma masiva y al azar a millones de usuarios.
- **Watering hole:** esta técnica consiste en realizar un estudio del perfil u organización a atacar con el objetivo de detectar las webs más consultadas por sus víctimas. Una vez detectadas, serán analizadas en busca de vulnerabilidades que poder explotar para comprometer el sitio web y poder así infectar a sus visitantes, mediante diferentes recursos existentes, URL maliciosas, etc.
- **Superficie de exposición elevada:** este vector de ataque suele venir acompañado de un desconocimiento de las redes y servicios publicados que tienen algunas organizaciones, aumentando su nivel de exposición en Internet. En otros casos como el de GreyEnergy con sus servidores web, la organización es consciente de que los servicios son públicos y accesibles desde Internet, pero no poseen todas las medidas de

seguridad que deberían con respecto a la segmentación o el hardening del host que tiene público un servicio.

2.4.2 BlackEnergy 3

Desde su primera detección en 2007, siendo este un troyano en sus inicios cuyo objetivo no era otro que infectar ordenadores para crear una botnet y realizar denegaciones de servicio distribuidas. BlackEnergy ha evolucionado hasta convertirse en una Amenaza Persistente Avanzada (APT - Advanced Persistent Threat).

En el año 2014 surgen variaciones que limitan el modo kernel únicamente para la realización de la carga maliciosa o que directamente lo inhabilitan cargándolo mediante el proceso rundll32.exe, versión denominada BlackEnergy Lite.

Ya en el año 2015, BlackEnergy agrega las variaciones Win32/KillDisk.NBB, Win32/KillDisk.NBC y Win32/KillDisk.NBD y quedando en su versión final tal y como lo conocemos en el ataque que sufrió Ucrania a finales de este mismo año.

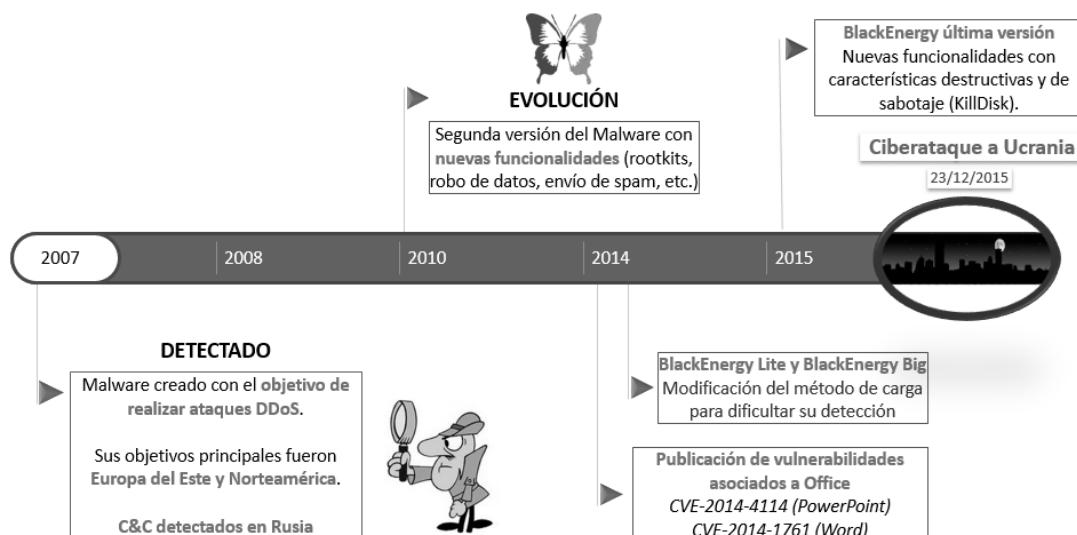


Ilustración 10: Evolución de BlackEnergy a lo largo del tiempo hasta el ataque en Ucrania

El vector de infección se originó gracias a un spear phishing simulando entidades gubernamentales ucranianas que enviaban correos con un adjunto malicioso. Este adjunto poseía una hoja Excel con una macro que se ejecutaba si se habilitaban las opciones de macro reconstruyendo un archivo ejecutable asociado al malware.

La carga maliciosa del dropper es una DLL que es ejecutada por el proceso rundll32 y crea el archivo LNK que permite la persistencia tras el reinicio. En el proceso de carga se realizar la conexión con el servidor C&C.

Una vez infectado su objetivo, el malware se propagó hasta la red de control donde originó un comportamiento anómalo abriendo y cerrando interruptores con comandos IEC-104 y llegando a dejar sin servicio una subestación eléctrica en pleno invierno¹⁵.

¹⁵ https://www.youtube.com/watch?v=634AdOAq_cM

2.4.3 CrashOverride/Industroyer¹⁶

Se trata de un malware modular focalizado en organizaciones que utilizan los protocolos IEC101, IEC104, IEC61850 y OPC. Esta focalización ya está indicando un claro objetivo sobre el sector eléctrico. A nivel de funcionamiento, CrashOverride, utilizaba funcionalidades previamente detectadas en los tres principales malware para sistemas de control aparecidos hasta la fecha (finales de 2017).

- Copia a STUXNET en la forma en que entiende y representa el conocimiento del proceso industrial, codificándolo para interrumpir operaciones.
- La arquitectura del sistema se mapea mediante el protocolo OPC, tal y como hizo HAVEX/ Dragonfly.
- Y también sigue la estela de BlackEnergy2 a la hora de revisar librerías y archivos de configuración de HMI para comprender el entorno y tratar de conectarse a internet cuando sea posible.

Entre otras capacidades, CrashOverride podía¹⁷:

- Enviar comandos directamente a las RTU utilizando protocolos industriales, entre los que se incluye la apertura y cierre de breakers (interruptores de las subestaciones) de forma rápida y continuada al igual que BlackEnergy.
- Bloquear los puertos serie de equipos Windows, impidiendo las comunicaciones de los dispositivos legítimos con los equipos afectados.
- Realizar un descubrimiento de red mediante el protocolo OPC y través de un escáner de puertos, mejorando notablemente la probabilidad de éxito.
- Tiene la capacidad para explotar una vulnerabilidad conocida de los relés de Siemens SIPROTEC, que puede provocar una denegación de servicio.
- Incluye un módulo wipe (elimina registros y cualquier otro fichero con el que pueda ser rastreado, o ficheros concretos) que deja los sistemas Windows inservibles y se requiere de una reconstrucción o de una copia de respaldo para volver a ponerlo en funcionamiento.

¹⁶ <https://www.incibe-cert.es/blog/crashoverride-el-malware-sci-ataca-nuevo>

¹⁷ <https://www.cci-es.org/documents/10694/431723/10.+S21Sec+DEFENDIENDO+MI+ENTORNO+INDUSTRIAL.pdf/cb576393-8cc1-4dbe-bd65-5da3f56ec418;jsessionid=5096EFB8A58A12579C2F9D83E40CB8B8?version=1.0>

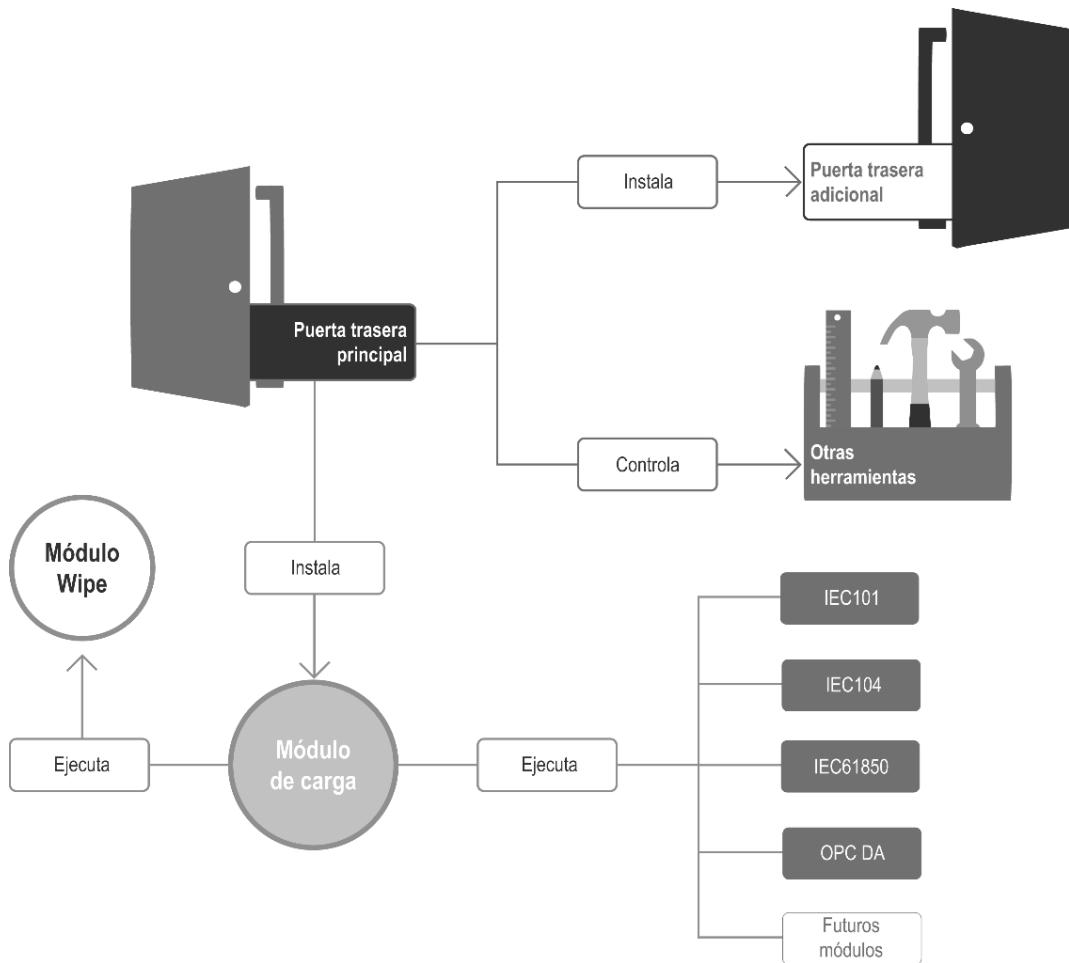


Ilustración 11: Funcionamiento de CrashOverride

2.4.4 DragonFly 2.0

Dragonfly 2.0 fue una campaña de malware a nivel industrial cuyo objetivo no era otro que el de infiltrarse en infraestructuras del sector energético. En esta campaña los atacantes utilizaron diferentes vectores de ataque para lograr acceso a empresas del sector energético entre los que se encontraba el envío de correos maliciosos (phishing) con adjuntos troyanizados. Además, utilizaban backdoors que permitían un acceso de forma continuada a las infraestructuras industriales pudiendo realizar modificaciones en las máquinas infectadas gracias a los Centros de Control que utilizaban (C&C).

2.4.5 GreyEnergy

Esta pieza de malware es considerada una evolución de BalckEnergy, de ahí su nombre. El vector de ataque, utilizado era el envío de correos a medida con adjuntos infectados (spear phishing), además, como novedad también comprometieron la web de la empresa para poder realizar entre otros, ataques de watering hole.

Tras una infección inicial con un mini dropper llamado GreyEnergy Mini, este abría paso para realizar nuevas infecciones y posteriormente descargar el malware en su totalidad, GreyEnergy.

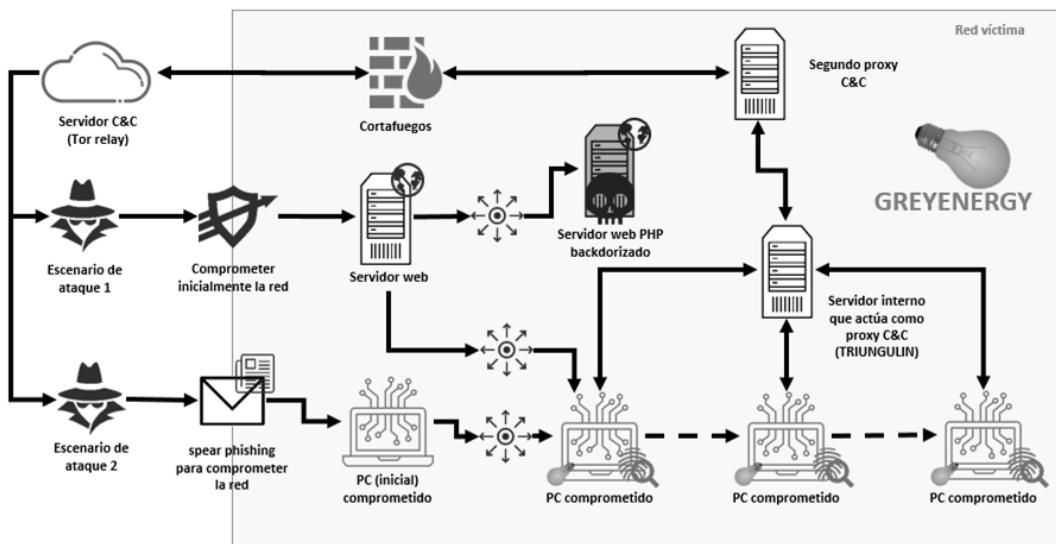


Ilustración 12: Proceso de infección de GreyEnergy

En la investigación de ESET¹⁸ sobre esta pieza malware, no se observó ningún módulo específicamente para Sistemas de control industrial (ICS). Sin embargo, sí que se detectó que los atacantes de GreyEnergy, han estado apuntando estratégicamente a las estaciones de trabajo relacionadas con entornos ICS que ejecutaban software relacionado con SCADA. Estas estaciones o servidores suelen ser sistemas críticos que nunca fueron desconectados, excepto en casos de mantenimiento.

¹⁸ https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

3 Taxonomías de ataque, Cyber Kill Chain y CAT

Una taxonomía de ataque puede describirse como un conjunto de fases o etapas que permiten analizar un ciberataque sufrido por un entorno en concreto. Este análisis en profundidad permite a los equipos de respuesta ante incidentes poder actuar en base a la gravedad del ciberataque y de las acciones que se ejecutan dentro del mismo.

3.1 Cyber Kill Chain (CKC)

Dentro de las estas taxonomías, destaca la acuñada por Lockheed Martin Corporation, Cyber Kill Chain (CKC). Esta taxonomía se compone de una secuencia de siete fases, que caracterizan las diferentes fases de un ataque avanzado. Este modelo, identifica los pasos que deben completar los adversarios para alcanzar su objetivo, centrándose en la red, en la exfiltración de datos y cómo mantener la resiliencia en la organización.

Dado que todas las intrusiones dejan algún tipo de rastro, es importante detectarlos y clasificar todas las acciones para poder aprender de ellas. A nivel forense, existe un principio bastante conocido llamado “Locard’s Exchange Principle”, dicho principio sostiene que, en todo crimen, el perpetrador del mismo siempre introducirá un elemento y se llevará algo de él. Por ello, ambos elementos servirían como evidencias. Extrapolando este principio a un ciberataque, tendremos que los atacantes dejarán evidencias (logs, modificación de registros, comunicaciones, etc.) y se irán con información u otros elementos que posteriormente les delatarán.

Una vez conocidos estos conceptos y volviendo a la taxonomía Cyber Kill Chain, estas son las fases que posee dicha cadena:

- **Reconocimiento (Reconnaissance):** Búsqueda, investigación, identificación y selección del o los objetivos. Esta fase puede consistir en un reconocimiento con técnicas pasivas de análisis de código abierto o un reconocimiento activo de los sistemas accesibles desde Internet para detectar posibles vulnerabilidades.
- **Preparación (Weaponization):** Incluir o enmascarar malware para permitir el acceso remoto a los atacantes y que puedan cargar exploits o módulos interesantes que se utilizarán en la fase de explotación. Normalmente suelen utilizarse documentos de la suite de Office o documentos PDF maliciosos para lograr este objetivo.
- **Distribución (Delivery):** El envío y recepción del payload es una fase importante en esta taxonomía. Las vías de entrega más utilizadas suelen ser correos electrónicos con documentos adjuntos, sitios web maliciosos o medios extraíbles como dispositivos USB.
- **Explotación (Exploitation):** La explotación ejecuta el payload que previamente ha sido enviado a la víctima. Dicha fase puede apuntar a una

vulnerabilidad concreta, características específicas de una aplicación o del sistema operativo utilizado, etc. La explotación también puede involucrar técnicas de ingeniería social para atacar un objetivo muy concreto directamente.

- **Instalación (Installation):** La instalación de un troyano o puerta trasera para acceder de forma remota en el sistema permite al o los atacantes mantener cierta presencia en el entorno atacado. En esta fase se suelen utilizar técnicas de persistencia en memoria para evitar perder comunicaciones si el sistema comprometido es reiniciado.
- **Comando y Control (Command & Control):** Comunicaciones salientes de un servidor controlado tras la infección y que posee salida a Internet directa o indirectamente para establecer un canal de Comando y Control (C&C). Este canal permitirá a los atacantes tener acceso remoto al sistema comprometido, cargar módulos que mejoren la amenaza persistente, etc.
- **Acciones sobre el objetivo (Action on Objectives):** Esta es la última fase de la taxonomía en la que se ejecutarán acciones concretas sobre el objetivo como la extracción de datos confidenciales, modificación de información, comprometer sistemas adicionales, movimientos laterales dentro de la red, etc.

Existen diferentes variantes a la cadena anteriormente comentada. Una de ellas es la versión extendida que incluye:

- **Reconocimiento interno:** Fase en la que el atacante tiene acceso a un dispositivo que se encuentra desplegado en la red interna de la organización atacada. Gracias a este acceso el atacante puede analizar ficheros locales, tráfico de red intercambiado, historial del navegador, contraseñas almacenadas, etc. El objetivo de este reconocimiento es averiguar cómo el dispositivo infectado podría ayudar a mapear la red interna de la organización y permitir atacar objetivos más interesantes.
- **Explotación interna:** Utilizando la información obtenida del sistema víctima, el atacante puede aprovechar una falta de parches contra vulnerabilidades concretas, vulnerabilidades en protocolos utilizados o en aplicaciones concretas, etc. para realizar movimientos laterales entre redes o dispositivos de una misma red, escalar privilegios o manipular los sistemas.

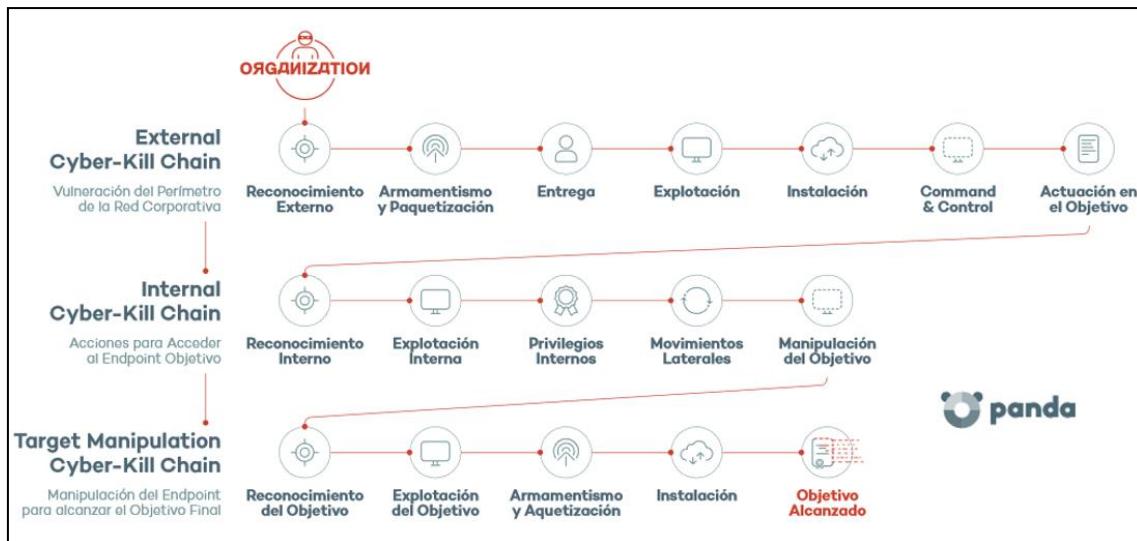


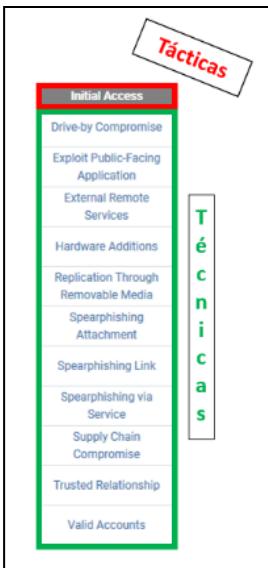
Ilustración 13: Taxonomía Cyber-Kill Chain Extendida¹⁹

Además de la taxonomía acuñada por Lockheed Martin Corporation, existen otros modelos que permiten entender los ataques, cada uno con sus particularidades y etapas.

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Laliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control		18			5	7	9	8	8	8	8	8
9	Pivoting				11	13	11	9	9	9	9	9	9
10	Discovery				14	10	10	11	11	11	11	10	10
11	Privilege Escalation				17	14	14	10	10	10	10	11	11
12	Execution				18	12	12	14	14	14	12	12	12
13	Credential Access					15	13	12	12	12	13	13	13
14	Lateral Movement					16	17	13	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

Ilustración 14: Diferentes modelos desarrollados a partir de la taxonomía CKC o derivados de la misma, fuente: The unified kill chain

¹⁹ https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/11/Adaptive_Defense-Understanding_CyberAttacks-es.pdf



Uno de los modelos más utilizados hoy en día y que muchas empresas están empezando a incorporar en sus ejercicios de respuesta a incidentes a la hora de modelar algunos ataques, es el desarrollado por MITRE²⁰, dicho modelo se denomina MITRE ATT&CK²¹. Este modelo se basa en una matriz (Enterprise) que contiene tácticas y técnicas actuales utilizadas por atacantes a la hora de desarrollar amenazas persistentes. Es importante comentar que, aunque es llamada matriz, simplemente se trata de una serie de columnas cuya fila inicial contiene el nombre de la táctica y las filas posteriores contienen las técnicas.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	File Structure Wipe	
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Endpoint Denial of Service	
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Command and Control Channel	
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dyno Hijacking	Complete After Delivery	Forced Authentication	Network Shifting	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Inhibit System Recovery	Scheduled Transfer
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels	Network Denial of Service	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware		Hooking	Control Panel Items	Kerberoasting	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
Local Job Scheduling	Launchd	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multibind Communication		Storage Data Manipulation
	Create Account	Launch Daemon		DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
Malta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Shifting	Security Software Discovery	Third-party Software			Port Knocking		
	PowerShell	Dyno Hijacking		Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		

Ilustración 15: Parte de la matriz MITRE (Enterprise) donde se pueden observar las técnicas y tácticas de los adversarios

Además de la matriz Enterprise, MITRE actualmente dispone de otras:

- **PRE-ATT&CK²²**: Esta matriz es un resumen de las tácticas y técnicas descritas en el modelo PRE-ATT&CK. Alinea visualmente las técnicas individuales bajo las tácticas en las que se pueden aplicar. Algunas técnicas abarcan más de una táctica porque pueden usarse para diferentes propósitos.

20 <https://www.mitre.org/>

21 <https://attack.mitre.org/>

²² <https://attack.mitre.org/matrices/pre/>

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities
Assess KITs/KIIs benefits	Assign KITs, KIIs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review log and residual traces
Assess current holdings, needs, and wants	Receive KITs/KIIs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability evade automated mobile application security analysis performed by app stores
Assess leadership areas of interest	Submit KITs, KIIs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callబ functional
Assign KITs/KIIs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malwa in various execution environments

Ilustración 16: Matriz que cubre las primeras fases de un ataque

- **Mobile**²³: Son 2 matrices ATT&CK específicas para dispositivos, una para tácticas y técnicas relacionadas al acceso a dispositivos, y otra para efectos originados en la red que pueden ser utilizados por adversarios sin acceso a dispositivos.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Effects	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Encrypt Files for Ransom	Abuse Accessibility Features	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Calendar Entries	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery		Lock User Out of Device	Access Call Log	Standard Application Layer Protocol	Standard Application Layer Protocol

Ilustración 17: Matriz relacionada con acceso a los dispositivos

Network Effects		Remote Service Effects	
Downgrade to Insecure Protocols		Obtain Device Cloud Backups	
Eavesdrop on Insecure Network Communication		Remotely Track Device Without Authorization	
Exploit SS7 to Redirect Phone Calls/SMS		Remotely Wipe Data Without Authorization	
Exploit SS7 to Track Device Location			
Jamming or Denial of Service			
Manipulate Device Communication			
Rogue Cellular Base Station			
Rogue Wi-Fi Access Points			
SIM Card Swap			

Ilustración 18: Matriz relacionada con los efectos originados por un ataque en la red (dispositivos)

Este modelo, al igual que otros muchos, está orientado hacia el mundo de las tecnologías de la información y por ello, no es totalmente adecuado para los sistemas de control industrial, debido a la naturaleza de los sistemas y la tipología de los ataques. No obstante, existen adaptaciones que permiten su aplicación en entornos industriales.

Al igual que el modelo elaborado por MITRE, la taxonomía de ataque de Lockheed Martin Corporation se pensó orientada al mundo TI. No obstante, a finales del año 2015, SANS Institute publicó un informe²⁴ adaptando el modelo Cyber-Kill Chain a los sistemas de control. En este informe se detalla la expansión de las fases que posee la Intrusion Kill Chain original para adecuarlos mejor a las características de los entornos industriales, además de dividirla en dos etapas.

23 <https://attack.mitre.org/matrices/mobile/>

24 <https://www.sans.org/reading-room/whitepapers/ics/paper/36297>

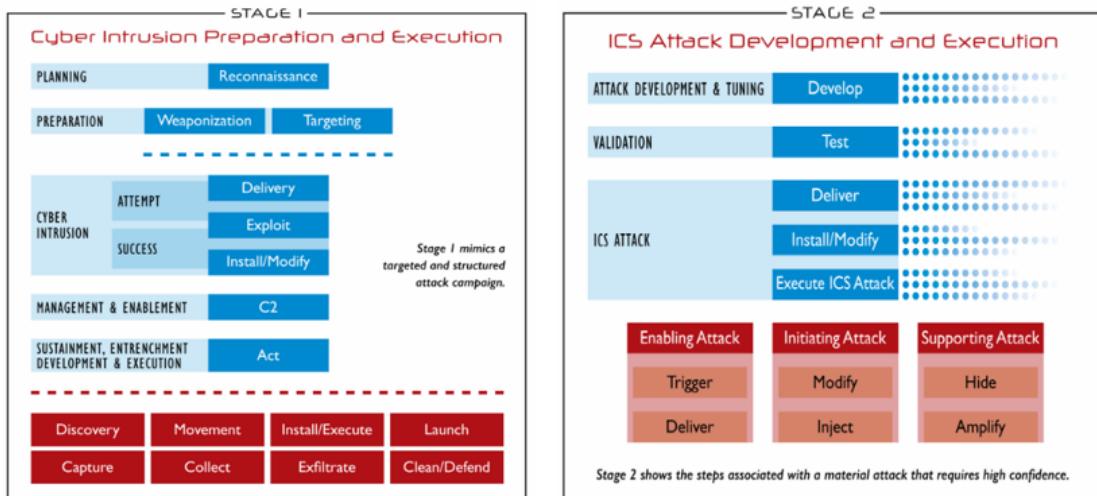


Ilustración 19: Adaptación del modelo CKC a los sistemas de control, fuente: SANS

La primera etapa, bastante similar al modelo original ya explicado, se corresponde con lo que tradicionalmente se ha clasificado como espionaje u operaciones de inteligencia.

Por su parte, en la segunda etapa, se saca partido al conocimiento recogido en la primera etapa para elaborar un ataque dirigido, no siendo necesaria la sucesión inmediata tras la primera etapa, sino que puede existir un retardo entre ambas. Las fases típicas del segundo escenario en este Cyber Kill Chain orientado a entornos industriales son:

- **Desarrollo y ajuste del ataque:** Con esta fase se comienza la segunda etapa en la que el atacante trata de crear una nueva capacidad (procedimiento, herramienta, método, etc.) que afecte específicamente al sistema de control objetivo. El desarrollo de este ataque, posiblemente se llevará a cabo gracias a los datos exfiltrados y a la recopilación de información realizada durante un largo tiempo sobre el entorno industrial víctima. Es por este hecho que también puede existir demoras en las operaciones maliciosas a ejecutar.
- **Validación:** La fase de validación pretende certificar la nueva capacidad en un entorno similar o igual al que se pretende atacar. Habitualmente, el atacante adquiere hardware específico para llevar a cabo esta fase. Dentro de esta fase, un atacante realiza simulaciones del ataque que desea llevar a cabo. Esto supone un gran reto, dada la complejidad de simular un sistema completo por tratarse de entornos industriales.
- **Ataque al sistema de control industrial:** En última instancia, la última fase es el ataque al sistema de control industrial. Aquí, el atacante trata de distribuir la capacidad desarrollada, instalarla o modificar el comportamiento del sistema a explotar y ejecutar el ataque. Las consecuencias habituales que se dan en un ataque sobre sistemas de control son la pérdida de datos o de control, la denegación de servicio y la manipulación de datos, visualizaciones, etc.

Al igual que la taxonomía de ataque Cyber Kill Chain, por su parte la matriz Enterprise desarrollada por MITRE también dispone de una adaptación para entornos industriales. Dicha adaptación se compone de técnicas y tácticas extraídas de algunos ataques a nivel industrial como los definidos en el punto de “Amenazas en el sector eléctrico”. Estas amenazas avanzadas permiten especificar técnicas y tácticas que se utilizan sólo en entornos industriales a la hora de elaborar un ataque. No obstante, algunas técnicas son compartidas con entornos más corporativos ya que, en la industria, pueden encontrarse tecnologías similares o directamente las mismas que podemos encontrar en redes corporativas pero adaptadas al mundo industrial.

Un ejemplo de esta matriz puede verse a continuación con el malware CrashOverride:

Persistence	Privilege Escalation	Defense and Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Efiltration	Command and Control	Disruption	Destruction
External Remote Service	Exploitation of Vulnerability	Alternate Modes of Operation	Brute Force	Account Enumeration	Default Credentials	API Interaction	Automated Collection	Automated Efiltration	Commonly Used Port	Alternate Modes of Operation	Alternate Modes of Operation
Firmware	Loadable Module	Block Comm Port	Create Account	Control Process	Exploitation of Vulnerability	Alternate Modes of Operation	Data Staged	Data Compressed	Communication Through Removable Media	Block Comm Port	Block Command Message
Interactive Service	Valid Account	Block Reporting Message	Credential Dumping	File and Directory Enumeration	External Remote Service	Command-Line Interface	Data from Local System	Data Encoding	Connection Proxy	Block Command Message	Block Reporting Message
Loadable Module	Web Shell	Code Signing	Credentials in Files	I/O Module Enumeration	Man in the Middle	Exploitation of Vulnerability	Data from Network Service	Data Encrypted	Custom Command and Control Protocol	Block Reporting Message	Command-Line Interface
Modify Control Logic		Exploitation of Vulnerability	Default Credentials	Local Service Enumeration	Remote File Copy	Graphical User Interface	Data from Network Share	Data Transfer Size Limit	Custom Cryptographic Protocol	Command-Line Interface	Device Shutdown
Modify System Settings		File Deletion	Exploitation of Vulnerability	Location Identification	Replication Through Removable Media	Interactive Service	Data from Removable Media	Efiltration Over Alternative Protocol	Data Encoding	Device Shutdown	Exploitation of Vulnerability
Module Firmware		Inhibit Security Tools/System	Input Capture	Network Connection Enumeration	Taint Shared Content	Loadable Module	Screen Capture	Efiltration Over Command and Control Channel	Data Obfuscation	Exploitation of Vulnerability	Firmware
Non-Interactive Service		Man in the Middle	Intercept Multi-Factor Authentication	Network Enumeration	Third-party Software	Modify System Settings	Video Capture	Efiltration Over Other Network Medium	Efiltration Over Command and Control Channel	Firmware	Man in the Middle
Rootkit		Masquerading	Modify Account	Network Service Enumeration	Valid Accounts	Non-Interactive Service	Web Service	Efiltration Over Physical Medium	Fallback Channels	Man in the Middle	Masquerading
Scheduled Task		Memory Residence	Network Sniffing	Network Sniffing	Virtual Terminal Services	Scheduled Task		Scheduled Transfer	Multi-Stage Channels	Masquerading	Modify Control Logic
Valid Accounts		Modify Control Logic	Password Manager	Role Identification		Scripting		Virtual Terminal Services	Multihand Communication	Modify Control Logic	Modify Parameter
Web Shell		Modify Event Log	Private Keys	Serial Connection Enumeration		Third-party Software			Multilayer Encryption	Modify Parameter	Modify Physical Device Display
		Log Settings				Virtual Terminal Services			Remote File Copy	Modify Physical Device Display	Modify Reporting Message
		Modify HM/Historian Reporting				Web Shell			Standard Application Layer Protocol	Modify Reporting Message	Modify Reporting Settings
		Modify Parameter							Standard Cryptographic Protocol	Modify Reporting Settings	Modify Tag
		Modify Physical Device Display							Standard Non-Application Layer Protocol	Modify System Settings	Module Firmware
		Modify Reporting Message							Uncommonly Used Port	Modify Tag	Rootkit
		Modify Reporting Settings							Virtual Terminal Services	Module Firmware	Spoof Command Message
		Modify Security Settings							Web Services	Rootkit	Spoof Reporting Message
		Modify System Settings									Spoof Command Message
		Modify Tag									Spoof Reporting Message
		Rootkit									
		Spoof Reporting Message									

Ilustración 20: Modelado de CrashOverride con la matriz de MITRE

3.2 CAT – Cyber Attack Taxonomy

En este trabajo, se introduce la taxonomía de ataque CAT. Esta taxonomía nace fruto de un proyecto open source bajo licencia Creative Commons Attribution 4.0 International²⁵, por ello, tanto la documentación como cualquier tipo de información sobre la taxonomía está liberada y accesible por Internet.

Esta taxonomía se encuentra actualmente en desarrollo y fue creada por Mildrey Carbonell Castro y Francisco Luis de Andres Perez. En ella, se definen una serie de estrategias, tácticas, técnicas y procedimientos que permitirán tener una visión más completa de los ciberataques.

²⁵ <https://creativecommons.org/licenses/by/4.0/>



Ilustración 21: Fases de CAT, fuente: S21sec

CAT cuenta con 7 fases que permiten el modelado del ataque. Este modelado permite, entre otras cosas, entender los ataques que se ejecutan hoy en día por los criminales y proporciona a los equipos de respuesta a incidentes una potente herramienta para entenderlos.

1. **Perfilado del Objetivo:** Fase inicial de la taxonomía donde se analiza el objetivo elegido por los atacantes. En esta fase se tendrá en cuenta el grado de exposición que posee el objetivo seleccionado por los atacantes y las posibles vías de entrada a la hora de poder realizar un primer acercamiento para posteriormente ejecutar el ataque.

Esta fase se fundamenta en dos tipos de análisis:

- **Análisis Macro o PESTLE²⁶:** Consiste en el estudio Político, Económico, Social, Tecnológico, Legal y de Entorno (PESTLE) asociado al objetivo. Enumera las amenazas actuales a las que está sometido, el sector a atacar o las localizaciones geográficas donde se encuentra ubicada entre otros. Este tipo de análisis, permite replicar técnicas de atacantes y permite obtener el conocimiento suficiente para replicar los mismos.
 - **Análisis Micro:** Centrado exclusivamente en el análisis de exposición del objetivo. Se analizan los tres factores fundamentales de exposición: las personas, los procesos y las tecnologías. En este análisis hay que tener siempre en cuenta que las personas suelen ser el eslabón más débil de la cadena a la hora de elegir un objetivo.
2. **Compromiso del Objetivo:** En esta fase, el o los atacantes intentan obtener un vector de ataque gracias al cual, podrán infiltrarse o simplemente explotar una vulnerabilidad para originar acciones como denegaciones de servicio, ejecución de código remoto, etc.

²⁶ https://es.wikipedia.org/wiki/An%C3%A1lisis_PESTEL

En los malware anteriormente comentados que afectan a los sistemas de control industrial, lo normal es utilizar ingeniería social mediante el uso de phishing, spear phishing (engaños más a medida), watering hole, etc.

Esta fase puede constituir también el inicio y el fin de un ataque, pasando directamente desde la fase de compromiso a la fase de ejecución del objetivo, como es el caso de los ataques DoS o DDoS, donde la disponibilidad del sistema es comprometida (objetivo final) pero el atacante no tiene ningún interés en acceder a los sistemas de su víctima (no se infiltra). Este tipo de ataques también se dan en los sistemas de control industrial, pero dan a entender que el atacante no utiliza técnicas muy avanzadas o simplemente, puede ser una distracción para ejecutar un ataque más elaborado.

3. **Infiltración:** El éxito de esta fase, depende directamente de la fase de compromiso. Si el compromiso inicial resulta exitoso, el atacante puede empezar a realizar acciones para, entre otras cosas, obtener un canal directo de comunicación con el objetivo sin ser detectado y así seguir realizando las acciones maliciosas que considere pertinentes. Entre estas acciones se encuentra la instalación de backdoors, uso de troyanos, etc.

De igual forma que en las anteriores, esta fase puede ser el final de un ataque, dañando la confidencialidad, integridad o disponibilidad del activo, como ejemplos, la modificación de una web, la modificación de datos de una BBDD, el reinicio de los sistemas, los cambios de configuraciones que generan un mal funcionamiento, etc.

4. **Persistencia:** Una vez comprometidos el o los objetivos, muchas piezas de malware utilizan técnicas de ocultación para evitar ser detectados por los sistemas de protección. El uso de herramientas de monitorización es bastante común y por ello, los atacantes suelen invertir bastante tiempo en el desarrollo de esta fase.

La persistencia en memoria o el uso de módulos wipe para la eliminación de pistas, suelen ser algunas de las técnicas utilizadas en esta fase. Recordemos que, en el mundo industrial, se están detectando piezas de malware que llevaban años activas. En esta línea, los atacantes cuyo objetivo son los entornos industriales, utilizan el conocimiento de estos entornos para seleccionar activos como estaciones de ingeniería o dispositivos PLC entre otros dado que el apagado de estos equipos no suele ser muy común. Muchos equipos industriales llegan a durar años sin ser apagados y sólo se apagan para ejecutar acciones de mantenimiento.

5. **Reconocimiento Interno:** Esta es una fase importante si el atacante desea conocer bien el entorno que rodea al dispositivo víctima que ya ha sido comprometido. En esta fase, un atacante puede empezar a detectar todos los dispositivos de red que existen, activos que se encuentran en la

misma red que el dispositivo víctima, dispositivos similares al ya vulnerado para tener un mayor número de víctimas, etc.

En los sistemas de control industrial suelen utilizarse técnicas como la captura de tráfico o la consulta de tablas ARP con el objetivo de obtener el mayor número de información sin levantar sospechas. De esta forma, los atacantes van recopilando información para seguir infectando activos sin levantar sospechas.

- 6. Movimientos Laterales:** Es la fase en la que el atacante, en base a los resultados obtenidos en la fase anterior, va infectando nuevos objetivos que se encuentren en la misma red que el activo ya vulnerado o intenta infectar otros dispositivos de otras redes.

Es muy común que, en el uso de malware industrial, la infección comience por el entorno corporativo, se obtenga información sobre los dispositivos de red existentes (routers, switches, cortafuegos, etc.) y se intente llegar al entorno industrial por la falta de segmentación o alguna comunicación directa entre red corporativa y red industrial sin controlar. En muchos casos, es mayor el conocimiento que tienen algunos atacantes de la red víctima que el que pueda tener la propia empresa atacada.

- 7. Ejecución de objetivos:** El objetivo final que suelen perseguir los ataques es provocar el mayor impacto a su víctima. Al igual que se persigue este objetivo, también es común que el impacto genere cierto beneficio a los atacantes o a terceros. Por ejemplo, el malware Stuxnet sirvió para parar el desarrollo del programa nuclear iraní, BlackEnergy llegó a dejar sin servicio una subestación eléctrica en Ucrania, etc. Algunos factores que suelen influir en este impacto son el espionaje industrial, ciberterrorismo, fuga de información, pérdida de confianza por parte de los clientes que pueda llegar a tener la víctima, etc.

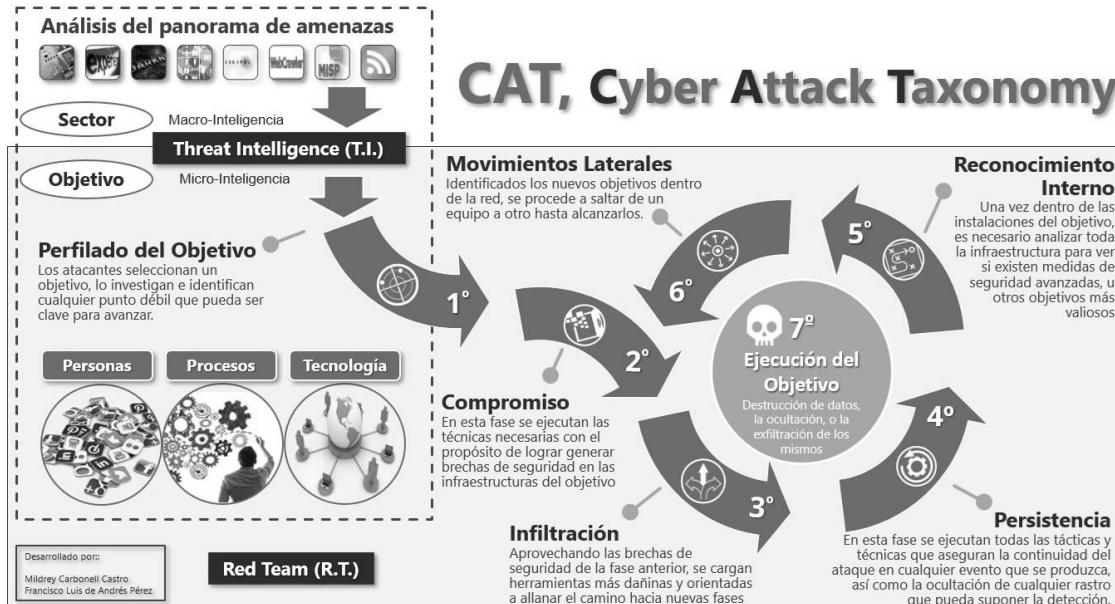


Ilustración 22: Fases de la taxonomía CAT

Esta taxonomía se ha desarrollado para que pueda ser adaptada a cualquier entorno, ya sea corporativo o industrial. A lo largo de este proyecto, se podrá observar una serie de adaptaciones utilizando CAT con alguno de los incidentes industriales más conocidos y que guardan estrecha relación con el sector eléctrico, concretamente en la parte de distribución.

CAT está basado en un modelo DML (Detection Maturity Levels). Este modelo fue utilizado originalmente para describir la madurez de una organización en lo que se refiere a su madurez a la hora de tratar y actuar sobre una información de una amenaza dada. Esta información puede incluir Indicadores de Compromiso (IoC), Técnicas, Tácticas y Procedimientos (TTPs), informes de inteligencia y mucho más. Este modelo enfatiza en el nivel de abstracción de los equipos de respuesta a incidentes y su nivel de madurez combinado con las habilidades técnicas que puedan llegar a tener.

Otro de los puntos importantes a tener en cuenta sobre CAT es que se enriquece con otros modelos como el desarrollado por MITRE o el de Pwnwiki. Gracias a este enriquecimiento, CAT es capaz de definir estrategias, tácticas, técnicas, procedimientos y herramientas profundizando aún más a nivel técnico y ayudando tanto a equipos de ataque como de defensa ya que igual están más acostumbrados a utilizar la matriz de mitre o Pwnwiki.



Ilustración 23: Planteamiento de la metodología CAT siguiendo el modelo DML, fuente: Modelado de escenarios de ataque con metodología CAT, Hack&Beers Alicante vol.5

3.3 Cyber Kill Chain vs. CAT

Ambas se definen como taxonomías de ataque, pero la realidad es que, el modelo planteado por Lockheed Martin además de poseer más antigüedad que la taxonomía CAT, también ha generado gran controversia dado que se han detectado algunas deficiencias. Este hecho, puede verse como una ventaja para la taxonomía CAT ya que, al ser un modelo más moderno, se han tenido en cuenta detalles que el modelado planteado en Cyber Kill Chain no.

Uno de los grandes problemas detectados en el modelado Cyber Kill Chain es precisamente el concepto de cadena. Hablamos de un planteamiento lineal sin bucles en el que se sigue una estructura prefijada y presupone que todos los ataques seguirán la misma estructura ya sea hasta el final de las fases o quedará en una fase previa.

Por otro lado, y siguiendo la argumentación de problemas relacionados con el modelo Cyber Kill Chain, la fase de preparación (*weaponization*) no tiene mucho sentido si tenemos en cuenta que no puede ser utilizada a la hora de plantearse medidas defensivas. Esta fase depende totalmente del atacante ya que es este el que realizará el desarrollo del malware y elegirá tanto las herramientas como cualquier otro detalle a utilizar. Si tenemos en cuenta la adaptación realizada para los entornos industriales, algunas de las fases añadidas en la segunda etapa, además de la ya comentada de la primera etapa, tampoco tienen sentido a nivel defensivo.

Tanto la fase de desarrollo y ajuste del ataque como la fase de validación, por tratarse de fases totalmente relacionadas con el atacante o con la evolución que pueda realizar el mismo para los entornos industriales, no tienen aplicación a nivel defensivo. En la fase de desarrollo y ajuste del ataque, el atacante crea nuevas capacidades que afecten especialmente a los entornos industriales. Por su parte, en la fase de validación, se verifica el desarrollo a medida realizado para el entorno industrial simulando el ataque en un entorno lo más similar posible al que será objetivo. En esta fase se utilizan por ejemplo dispositivos que posee la víctima desplegados en su red industrial.

Otra deficiencia detectada en el modelo Cyber Kill Chain original es la inexistencia de una fase que tenga en cuenta los movimientos laterales. En la actualidad prácticamente todas las piezas de malware incorporan esta fase gracias a la cual consiguen una mayor propagación e impacto dentro de la organización víctima. Es cierto que algunas variantes del modelo original planteado por Lockheed Martin si incorporan los movimientos laterales, pero no son modelos oficiales ni registrados por lo que no se tendrán en cuenta.

Cyber Kill Chain (CKC)	Cyber Attack Taxonomy (CAT)
Concepto de cadena, ataques lineales que siguen unas fases muy marcadas y preestablecidas.	Posibilidad de crear bucles y no seguir un camino lineal para modelar un ataque.
Fases como <i>weaponization</i> que no permiten un planteamiento defensivo frente al modelado que se ofrece.	Muestra de todas las fases de forma coherente gracias a la incorporación de la parte estratégica que proporciona una coherencia a todos los movimientos descritos que podría ejecutar un malware.
El modelo oficial registrado no tiene en cuenta los movimientos laterales de forma correcta.	CAT permite una vez más gracias a la parte estratégica detectar ver los movimientos laterales y permite una mejor representación visual.
Posee variantes para el sector industrial pero no son específicas de sector y se	Posee un framework específico para el sector eléctrico (<i>caffeine</i>). Además

basan en un pensamiento heredado de TI.

incorpora nuevas tácticas y técnicas para entornos industriales.

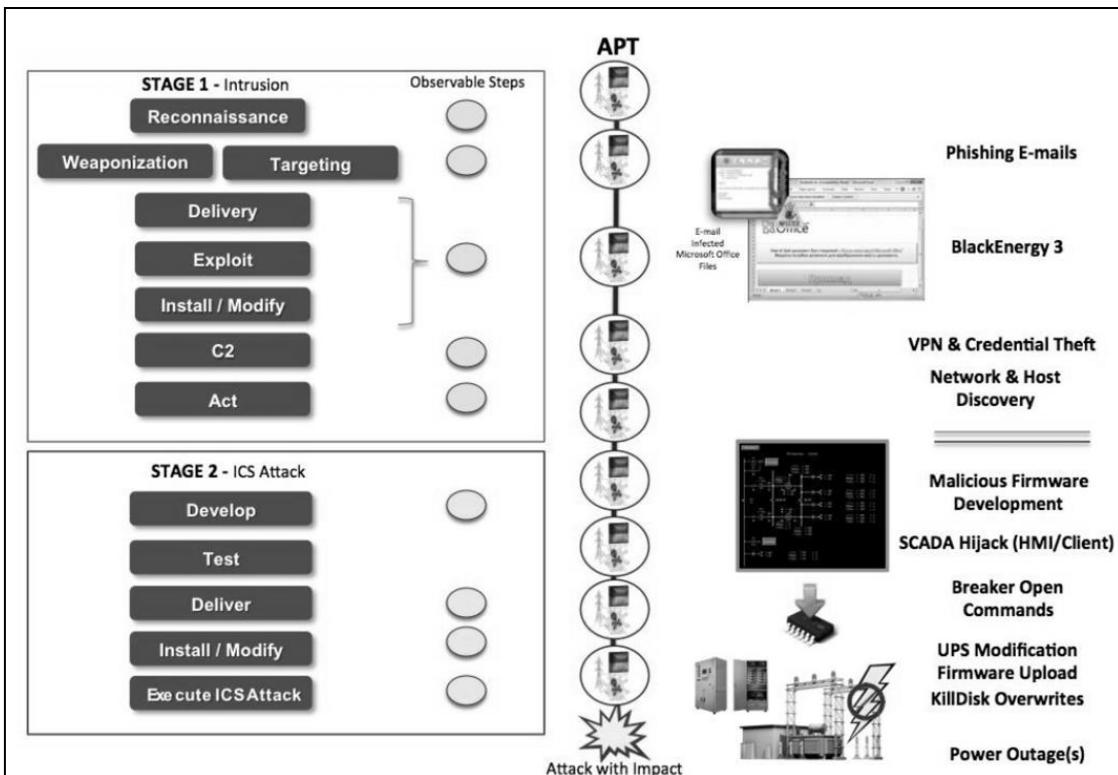


Ilustración 24: Mapeo de BlackEnergy con el modelado Cyber Kill Chain para sistemas de control industrial, fuente: Analysis of the Cyber Attack on the Ukrainian Power Grid²⁷

Ya para finalizar, y como otro problema bastante comentado relacionado con el modelado planteado por Lockheed Martin. Los ataques originados a nivel interno por posibles insiders²⁸, empleados descontentos con poder y conocimiento suficiente de la red y los recursos de la organización como para ejecutar un ataque, no pueden ser representados fácilmente.

Uno de los casos más conocidos a nivel industrial de este tipo de ataques originados internamente por un empleado descontento sucedió en una planta de tratamiento de aguas en Australia²⁹. En este caso, el empleado descontento utilizó un ordenador portátil provisto con un software de control adecuado y un módem de radio. La forma de acceder al sistema consistía en conectar el ordenador al sistema de estación de bombeo tratando de no ser detectado. El resultado de estas intrusiones fueron litros y litros de aguas residuales vertidas en ríos y parques, además de la pérdida de imagen de la empresa encargada de gestionar el alcantarillado. El empleado fue condenado a 2 años de cárcel por el acceso ilegal al sistema de control de alcantarillado del Condado, práctica que realizaba por el descontento que tenía tras ser despedido de la empresa para la que trabajaba.

²⁷ https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

²⁸ <https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado>

²⁹ <https://es.slideshare.net/sommerville-videos/maroochy-water-breach>

Por su parte, CAT al tratarse de un modelo bastante actual, pero con gran base argumental, actualmente no tiene grandes críticas salvo las que se plantean sus propios desarrolladores o las personas que ayudan a su desarrollo.

CAT pretende no sólo cubrir la parte estratégica como taxonomía de ataque para fases estratégicas y metodología, sino que, CAT pretende tener una parte de framework para unir tácticas, técnicas y procedimientos al igual que hace MITRE. La novedad en este aspecto es la incorporación de la estrategia. Definida como la planificación y desarrollo de operaciones que posteriormente usarán las tácticas. La incorporación de la estrategia es muy importante ya que los grupos de atacantes, hoy en día están bastante organizados y jerarquizados. Los ataques a entornos industriales son muestra de que este hecho es real ya que, para el desarrollo del malware utilizado en estos entornos, es necesario un equipo multidisciplinar que tenga sendos conocimientos en diferentes ámbitos y especialidades.

Podría decirse que el crimen organizado cada vez se parece más a una empresa donde existen diferentes roles con jefes de equipo, desarrolladores, etc. Además, si a todo esto sumamos el hecho de que algunos ataques están motivados por intereses de naciones, el dinero invertido para desarrollar un malware puede ser bastante considerable.

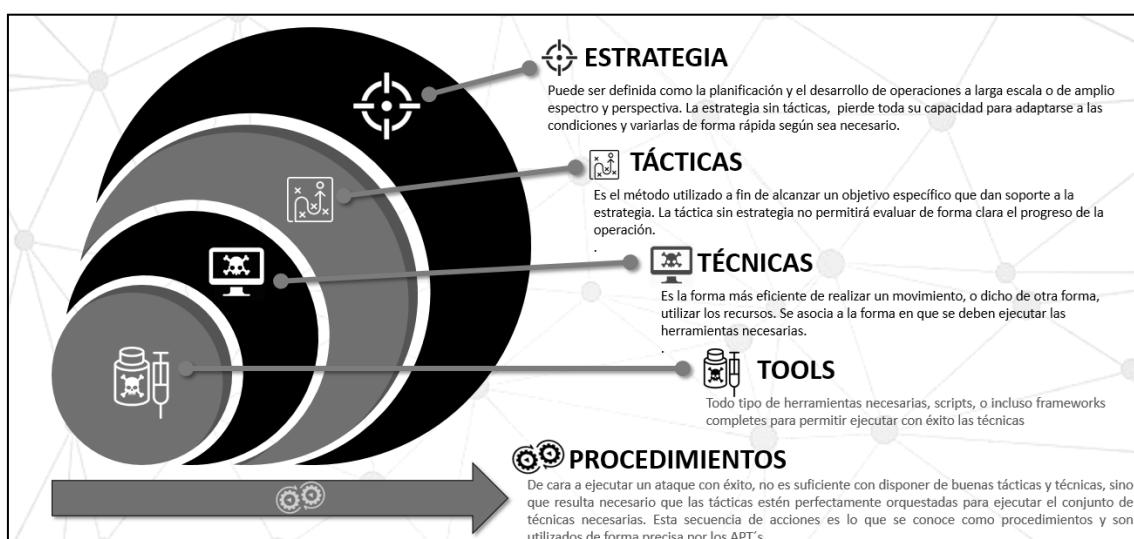


Ilustración 25: Estrategia, tácticas, técnicas y procedimientos de CAT, fuente: Modelado de escenarios de ataque con metodología CAT, Hack&Beers Alicante vol.5

4 Framework de Ataque para el Sector Eléctrico

El desarrollo de este framework, pretende facilitar las labores de los equipos orientados al mundo ofensivo dentro de la ciberseguridad en entornos industriales y, concretamente, en el sector energía y el subsector electricidad (distribución). Al tratarse de entornos en producción, y, dado que en la industria prima la disponibilidad y la seguridad de las personas (safety), es importante tener en cuenta ciertas pautas antes de realizar alguna tarea ofensiva en estos entornos.

- **Impacto bajo o cero en la disponibilidad del proceso.** Las empresas industriales suelen ser bastante cautelosas en este aspecto dado que, por ejemplo, una parada de una subestación eléctrica que proporcione energía a una gran zona habitada supondría grandes pérdidas económicas y pérdida de imagen frente a los clientes. Por ello, en el planteamiento de este framework se aconseja realizar las tareas ofensivas en estas 2 situaciones:
 - **Descargas:** Situación en que se encuentra una instalación de la red (línea, transformador, barra, etc.) cuando está desconectada del resto del sistema eléctrico y, por lo tanto, no puede circular potencia eléctrica a través de ella. Esta práctica es utilizada cuando se requiere dejar una parte de la instalación eléctrica sin tensión, y en condiciones de seguridad para poder trabajar en ella o en sus inmediaciones.
 - **Balanceo de nodos:** Esta práctica es utilizada en el sector eléctrico para equilibrar el suministro eléctrico en las subestaciones dependiendo de las necesidades de los consumidores. La gestión de la electricidad en estos casos suele estar relacionada con temas ambientales (excesivo frío, altas temperaturas, etc.) y por demanda.
- **Equipamiento de protección para el equipo ofensivo.** Dentro de una subestación eléctrica son obligatorias ciertas medidas de seguridad para evitar accidentes laborales. Por ello, el equipo ofensivo debe cumplir estas medidas. El uso de calzado reglamentario, casco, guantes, etc. son algunas de estas medidas de seguridad. En las reuniones previas a ejecutar pruebas ofensivas, el equipo que ejecutará dichas pruebas tendrá que ser informado por el cliente para que todo el mundo cumpla las medidas de seguridad.
- **Conocer bien el entorno a atacar.** Todo el equipo ofensivo debe ser consciente del entorno que va a atacar, los diferentes dispositivos existentes dentro de una subestación eléctrica, protocolos intercambiados y normativas que afectan a dicho sector. Gran parte de esta información puede consultarse en los apartados 2.1 Dispositivos y Sistemas, 2.2 Comunicaciones o 2.3 Normativa y estándares.

4.1 Uso del framework, ¿Y ahora qué?

En el apartado 3.2 CAT – Cyber Attack Taxonomy ya se introduce la taxonomía CAT para el modelado de ataques o planteamientos de red team. Esta taxonomía aporta ciertas ventajas frente a la planteada por Loocked Martin y por ello, ha sido la elegida para la elaboración de este framework. Pero, ¿qué aporta la taxonomía al framework? La respuesta es muy simple, proporciona las herramientas necesarias de clasificación con estrategias, técnicas, tácticas y procedimientos que permiten replicar ataques avanzados. En este punto encontramos 2 ventajas, una para los equipos que defienden (blue teams) y otra para los equipos que atacan (red teams). Desde el punto de vista defensivo, toda la información procesada en el modelado, y, acabando por la fase de compartición de información donde se elaboran indicadores de compromiso, reglas snort³⁰, reglas yara³¹, etc. permite la detección de amenazas iguales o similares a las ya analizadas. Por su parte, desde un punto de vista ofensivo, pueden llegar a replicarse las amenazas analizadas con el objetivo de poner a prueba los sistemas y dispositivos implicados en un proceso.

Dado que ya existen diferentes análisis tanto para modelados de ataques a nivel de TI como escenarios que pueden llegar a modelarse en un supuesto con diferentes taxonomías. El objetivo de este proyecto y que se desarrollará en los siguientes puntos es proporcionar una serie de pautas para atacantes que deseen realizar ejercicios de red team en subestaciones eléctricas y que el entorno sea real y en producción. Del mismo modo, se realizará un modelado de un ataque para mostrar todas las aplicaciones posibles de CAT en los entornos industriales.

4.2 CAT en los entornos industriales, *caffeine*

Dado que la metodología CAT ya posee un framework, pero este no está orientado a entornos industriales, la aportación de este proyecto es el framework caffeine (Cyber-Attack Framework for Energy Infrastructures). Dentro de este framework podremos encontrar estrategias, tácticas, técnicas y procedimientos tanto específicos de los sistemas de control industrial y, concretamente del sector eléctrico (distribución) como compartidos con el framework de CAT, la matriz de MITRE, PwnWiki, etc.

³⁰ <https://www.snort.org>

³¹ <https://yararules.com/>



Sobre todo, se plantearán técnicas específicas para la ejecución de ataques en entornos industriales. Un ejemplo de estas técnicas bajo la táctica de descubrimiento (TA0007) se puede ver de forma detallada a continuación:

Táctica	ID-Nombre	Nombre	Descripción
Descubrimiento (TA0007)	CAFT0001	Information through industrial protocols	<p>Envío de paquetes diseñados específicamente para utilizar protocolos industriales con el objetivo de obtener información sobre dispositivos industriales a través de la red como en los siguientes ejemplos:</p> <p>Ethernet/IP, obtención de información - Uso del protocolo industrial Ethernet/IP para la obtención de información por el puerto 44818 TCP y UDP.</p> <p>Modbus TCP, obtención de información - Uso del protocolo industrial modbus TCP para la obtención de información por el puerto 502 TCP.</p> <p>Factory Interface Network Service (FINS), descubrimiento y obtención de información - Uso del protocolo FINS para obtención de información de PLC en redes industriales. Este protocolo trabaja tanto bajo UDP como por TCP en el puerto 9600.</p> <p>S7, obtención de información - Uso del protocolo industrial S7 para la obtención de información por el puerto 102 TCP.</p> <p>IEC 61850-8-1, protocolo mms para obtención de información - Uso del protocolo industrial mms para la obtención de información por el puerto 102 TCP.</p>

			IEC 60870-5-104 para obtención de información - Uso del protocolo industrial IEC 60870-5-104 para la obtención de información por el puerto 2404 TCP.
--	--	--	--

Entre otras, las herramientas que pueden utilizarse para utilizar la técnica anteriormente comentada son:

Táctica	ID_técnica	herramienta	descripción
Descubrimiento	CAFT0001	enip-info.nse	<p>Script desarrollado en lua para nmap. Este script envía una petición al puerto 44818 TCP utilizado por el protocolo Ethernet/IP y parsea información como el tipo de dispositivo, el identificador del fabricante, nombre del producto, número de serie, estado del dispositivo, etc.</p> <p>Ejemplo de Uso <code>nmap --script enip-info -sU -p 44818 <host></code></p>
		modbus-discover.nse	<p>Script desarrollado en lua para nmap. Este script enumera los ID de los esclavos (sids) y recopila información del dispositivo.</p> <p>Ejemplo de Uso <code>nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host></code></p>
		omron-info.nse	<p>Script desarrollado en lua para nmap. Este script envía un paquete FINS al dispositivo que contiene un comando de control para lectura de parámetros. Si el comando es válido, el dispositivo responde con una información que es parseada por el script y mostrada por pantalla.</p>

			<p>Ejemplo de Uso</p> <pre>nmap --script omron-info -sU -p 9600 <host></pre>
		s7-info.nse	<p>Script desarrollado en lua para nmap. Este script permite enumerar los PLC Siemens S7 presentes en una red y obtener información sobre ellos.</p> <p>Ejemplo de Uso</p> <pre>nmap --script s7-info.nse -p 102 <host/s></pre>
		mms-identify.nse	<p>Script desarrollado en lua para nmap. Este script verifica que por el Puerto 102 TCP exista el protocolo IEC 61850-8-1 para, posteriormente, enviar una petición con el objetivo de extraer información del dispositivo.</p> <p>Ejemplo de Uso</p> <pre>nmap -d --script mms-identify.nse --script-args='mms-identify.timeout=500' -p 102 <host></pre>
		iec-identify.nse	<p>Script desarrollado en lua para nmap. Este script verifica que efectivamente por el Puerto 2404 se utiliza el protocolo IEC 60870-5-104 y realiza una prueba de comunicación contra el dispositivo para obtener información sobre las direcciones de objeto almacenadas.</p> <p>Ejemplo de Uso</p> <pre>nmap -sV --script=iec-identify <target></pre>

Lógicamente, existen alternativas a estas herramientas como PLCScan³² o mbtget³³.

³² <https://code.google.com/archive/p/plcscan/>

³³ <https://github.com/sourceperl/mbtget>

En el caso de querer enviar peticiones con IEC104, se podría utilizar un módulo de metasploit con este propósito³⁴ que permite establecer comunicaciones y enviar paquetes con el objetivo de interactuar con el dispositivo u obtener información.

El framework *caffeine*, al enmarcarse dentro de la metodología CAT, posee tanto tácticas y técnicas propias de entornos industriales y, concretamente del sector energía, subsector electricidad (distribución) como tácticas y técnicas de MITRE, PwnWiki, etc. Las técnicas y tácticas que son propias, se han creado con el objetivo de facilitar el modelado de un ataque a equipos de red team, por ello, si coinciden con algunas ya escritas, pueden ser utilizadas con el framework utilizando la nomenclatura de, por ejemplo, MITRE en la que las tácticas empiezan por *TAXXXX* como en el caso de las tácticas que siguen la nomenclatura *TXXXX*. Si por el contrario, las tácticas y técnicas son nuevas utilizadas exclusivamente en el framework *caffeine*, se utilizará la nomenclatura *CAFTXXXX* para tácticas y *CAFTXXXX* para técnicas.

4.3 Escenario de ataque y modelado con CAT para sector eléctrico (*caffeine*)

Se propone un ataque avanzado que permita modificar los parámetros recibidos por el centro de control en el SCADA mediante la suplantación de una RTU que envía comunicaciones IEC104. Para ello, el equipo red team ha podido introducir un dispositivo dentro de la subestación utilizando técnicas de ingeniería social y suplantando la identidad de supuestos operarios de la empresa a la que pertenece la subestación eléctrica. El dispositivo introducido en la red posee comunicaciones 4G que permiten un control en remoto y contiene una suite avanzada de herramientas relacionadas con el mundo industrial y concretamente con el sector eléctrico. Aprovechándose de vulnerabilidades 0-day en la RTU, han podido realizar las modificaciones necesarias para suplantar la RTU y enviar parámetros con el dispositivo introducido en la red.

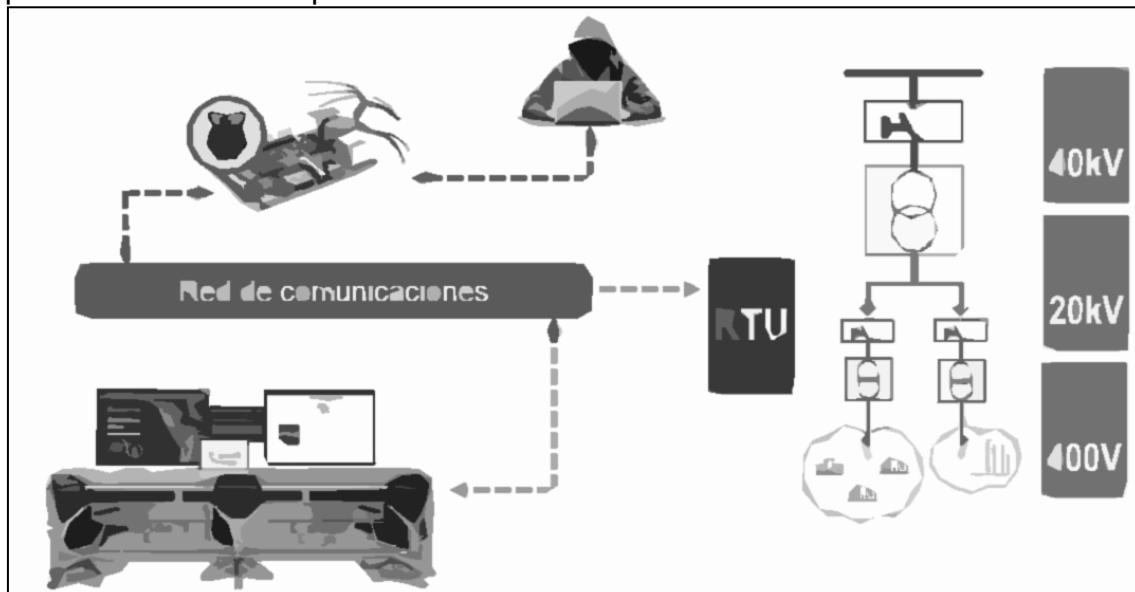


Ilustración 26: Situación que tendría la red del escenario propuesto

³⁴ <https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/client/iec104/iec104.md>

Este supuesto escenario se representaría con CAT de la siguiente forma:

Tácticas, Técnicas y herramientas

Fase CAT	Tácticas	Técnicas	Herramientas
Perfilado del objetivo	TA001:Target Selection	T1245: Determine approach/attack vector T1242: Determine operational element T1241: Determine strategic target	Buscadores que permiten obtener información en Internet como google, bing, etc. Búsqueda de información en foros especializados. Uso de herramientas como theharvester ³⁵ o shodan ³⁶ . Más herramientas: https://github.com/jivoi/awesome-osint
Perfilado del objetivo	TA0016 People Information Gathering	- T1266: Acquire OSINT data sets and information T1272: Identify business relationships T1268: Conduct social engineering T1273: Mine social media	Buscadores que permiten obtener información en Internet como google, bing, etc. Uso de Facebook, Instagram y Pinterest para obtener información. Uso de herramientas como theharvester ³⁷ o shodan ³⁸ . Más herramientas: https://github.com/jivoi/awesome-osint
Perfilado del objetivo	TA0017 Organizational Information Gathering	- T1300: Analyze organizational skillsets and deficiencies T1303: Analyze presence of outsourced capabilities	Búsqueda de información en foros especializados. Más herramientas: https://github.com/jivoi/awesome-osint
Perfilado del objetivo	TA0015 Technical Information Gathering	- T1247 - Acquire OSINT data sets and information T1249 - Conduct social engineering	Búsquedas específicas en foros y obtención de información gracias al diálogo y técnicas de ingeniería social.

³⁵ <https://tools.kali.org/information-gathering/theharvester>

³⁶ <https://www.shodan.io/>

³⁷ <https://tools.kali.org/information-gathering/theharvester>

³⁸ <https://www.shodan.io/>

Compromiso	TA0001 – Initial Access	T1200 Hardware Additions -	Uso de ganzúas para la ejecución de técnicas lockpicking. Uniforme de operario que trabaja en la empresa atacada. Finalmente, dispositivo a introducir (raspberry pi 3) en la red de la subestación eléctrica.
Infiltración	TA0011 – Command and Control	T1052 - Exfiltration Over Physical Medium	Instalación de un pincho 4G en el dispositivo introducido en la red de subestación para mantener comunicación y exfiltrar información.
Infiltración	TA0011 – Command and Control	T1043 Commonly Used Port T1105 - Remote File Copy	Consola de comandos como netstat, ifconfig, pas –aux, top, etc. con interprete sh, ash (común en busybox), bash, etc. Copia de información mediante FTP u otro protocolo con el uso del comando ftp o con programas como filezilla.
Persistencia	CAFTA001 - external power	CAFT003: use of external battery with solar cells	Para evitar posibles apagones por parte del dispositivo introducido en la red, utilizar baterías externas lo suficientemente potentes para aguantar todo el tiempo que se esté atacando al objetivo.
Reconocimiento interno	TA0007 Discovery. -	T1254 Technical Information Gathering CAFT0001 Information through industrial protocols T1254 - Conduct active scanning	mms-identify.nse y iec-identify.nse
Movimientos laterales	TA0008- Lateral Movement	T1078 - Valid Accounts T1037- Logon Scripts	Uso de documentación de los dispositivos donde aparece reflejada la contraseña por defecto o ataques de fuerza bruta muy controlados para evitar levantar sospecha. Diccionario a utilizar scadapass ³⁹
Ejecución del objetivo	CAFTA0002 - Cheat the control center	CAFT0002: Modification of parameters by industrial protocols	Uso de librería scapy para el envío de paquetes a medida, desarrollo de scripts específicos, uso del módulo de metasploit que soporta comunicaciones IEC104.

³⁹ <https://github.com/scadastrangelove/SCADAPASS>

			Simular comunicaciones de RTU para engañar al sistema SCADA o envío de peticiones single command/doublé command en IEC104.
--	--	--	--

Procedimientos

Se ha seleccionado una subestación estratégica de una empresa con sede en España catalogada como infraestructura crítica dado el gran territorio al que proporciona electricidad. También se sabe que es una infraestructura crítica porque entre los clientes a los que proporciona electricidad se encuentra uno de los hospitales más importantes y que más pacientes recibe en España.

1. Introducir el dispositivo malicioso previamente configurado en la subestación. Dentro del dispositivo, en este caso una raspberry pi 3, se encontrarán todo tipo de librerías y aplicaciones necesarias para ejecutar las pruebas que se deseen. A la hora de introducir el dispositivo es necesario conocer la red que posee la víctima ya que es posible que esta cuente con una red plana y el dispositivo a introducir no necesite introducirse directamente dentro de la subestación.
2. Obtener más información sobre la red y los dispositivos que habitan en ella gracias a la comunicación 4G entre el dispositivo introducido en la organización víctima (raspberry pi 3) y el ordenador del atacante.
3. Una vez detectado el dispositivo víctima, acceder y realizar las modificaciones pertinentes para poder suplantarla por nuestro dispositivo introducido. Este acceso puede realizarse gracias al conocimiento de vulnerabilidades sobre el dispositivo o gracias a la lectura de manuales que proporciona el fabricante donde aparecen reflejadas las credenciales por defecto del dispositivo. Si las credenciales se han modificado y ya no son por defecto, podrían realizarse ataques de fuerza bruta u otros más a medida.
4. Envío de señales erróneas y colapso del SCADA. Gracias al uso del protocolo IEC104 usado entre subestaciones eléctricas y redes de control, el atacante podrá enviar peticiones concretas que originarán una pérdida de visibilidad entre una RTU y el SCADA ubicado en el centro de control. Además, pueden enviarse comandos de control como single command o doublé command, dependiendo del tamaño de la información a enviar para interactuar con el sistema.

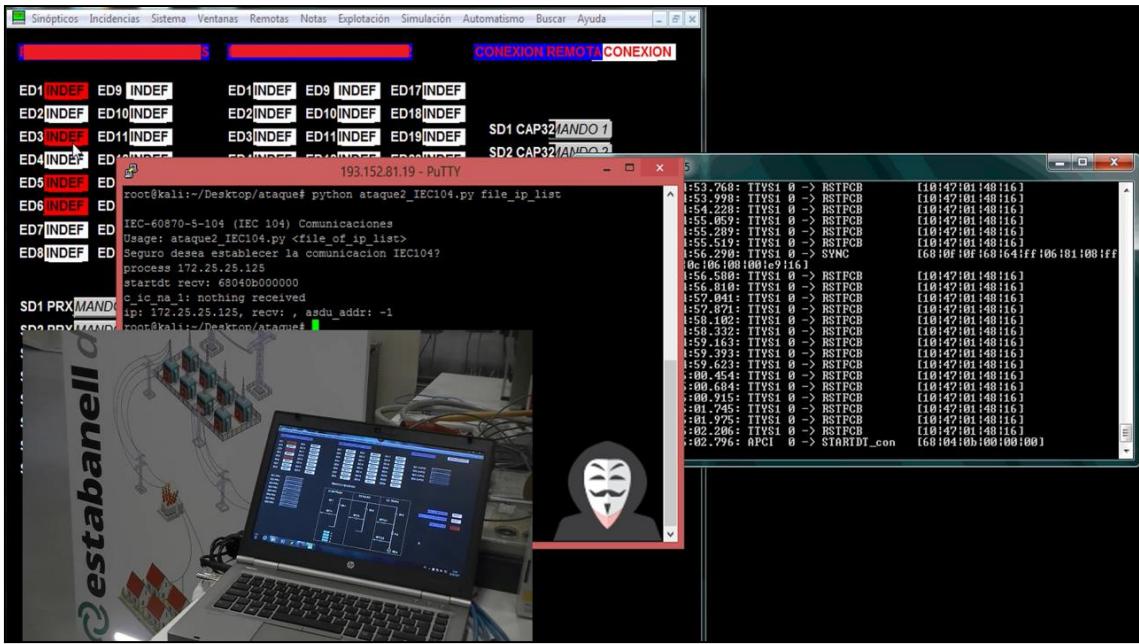


Ilustración 27: Ataque realizado utilizando comandos IEC-104 suplantando una RTU en sus comunicaciones hacia el SCADA

4.4 Desde el punto de vista defensivo...

El escenario anteriormente expuesto servirá principalmente a equipos ofensivos (red teams) pero esto no quiere decir que no puedan ser usados por equipos defensivos (blue team) con el objetivo de evitar o ya tener un plan de respuesta frente a escenarios anteriormente modelados gracias a Indicadores de Compromiso, reglas Yara, reglas snort, etc.

En este punto ha de tenerse en cuenta el cumplimiento regulatorio que afecta al sistema industrial al que se le presta soporte defensivo, en nuestro caso, el sector eléctrico y los procedimientos que se tienen frente a este tipo de ataques que afectan a un sector concreto.

Entre los puntos positivos que pueden extraerse desde el punto de vista defensivo de plantear escenarios para que equipos ofensivos ataquen tendremos:

- **Formación para equipos de respuesta a incidentes.** Gracias al análisis de diferentes escenarios que puede ejecutar un atacante o un equipo ofensivo, los equipos defensivos pueden tomarlo como ejercicios de formación. Con esta formación los equipos de respuesta a incidentes o blue teams, podrán mejorar su experiencia real de campo haciendo más eficiente su servicio frente a ataques reales.
- **Mejora de procedimientos y tiempos de respuesta.** Dado que es posible conocer tanto los pasos que ejecutaron los atacantes como el impacto que tendrá el ataque en los sistemas industriales a los que se presta soporte. Los equipos de respuesta a incidentes o blue teams

podrán mejorar los tiempos de respuesta y podrán procedimentar mejor las tareas a realizar dependiendo del tipo de ataque detectado.

Para el escenario de ataque anteriormente planteado, puede aplicarse una mitigación del mismo a nivel de red gracias al uso de un IDS como Snort.

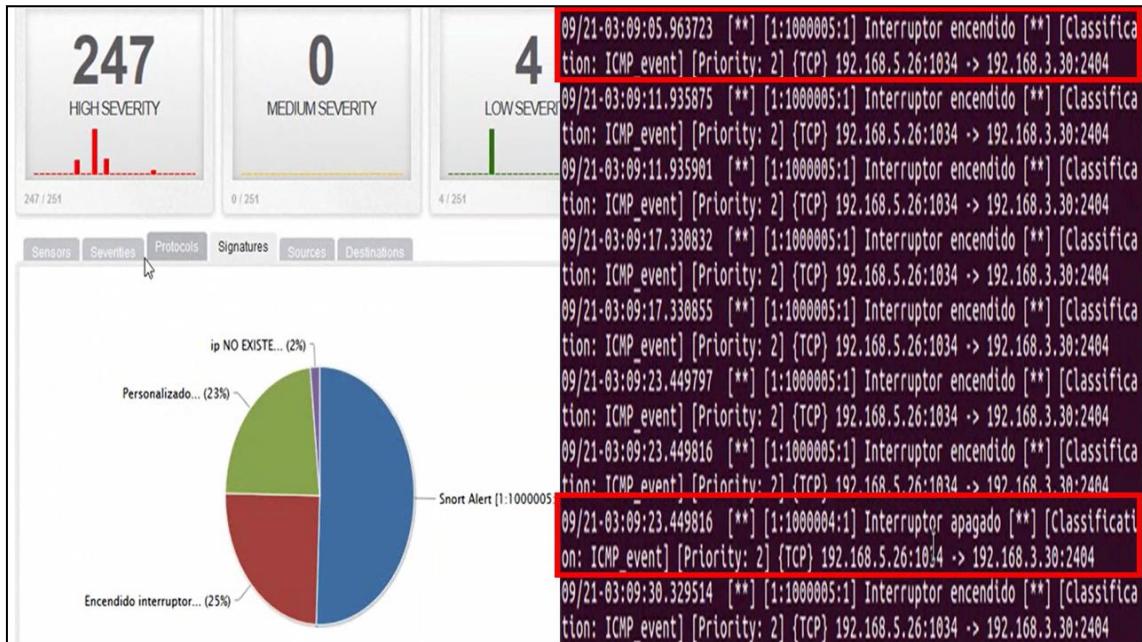


Ilustración 28: Ejemplo de implementar reglas Snort para la detección de anomalías con el envío de paquetes del protocolo IEC104. Uso de herramienta Snorby para mostrar las alertas

4.5 Modelado de un ataque, GREYENERGY

Como ejemplo final para mostrar las capacidades de la metodología CAT en entornos industriales, se ha modelado uno de los últimos ataques detectados en el sector energía y, concretamente, en el sector eléctrico. Dicho ataque fue GreyEnergy.

Con el objetivo de ver las diferencias entre ambos modelados, se ha analizado el ataque tanto con la matriz de MITRE como con la taxonomía de ataque CAT.

4.5.1 Matriz MITRE

ID	Táctica	Técnica	Uso (información del incidente)
T1193 CAPEC ID: CAPEC-163	Acceso inicial	Spearphishing con documentos adjuntos	Correos con documentos adjuntos. Los documentos enviados contenían macros que ejecutaban código malicioso al activarse. La infección inicial con estas macros era de GreyEnergy mini, también conocido como FELIXROOT . Más información sobre FELIXROOT . ESCENARIO 1
T1051 CAPEC ID: CAPEC-563	Acceso inicial	Servidores web comprometidos	El grupo de atacantes creador de GreyEnergy, utilizaba los servicios web publicados a

			Internet de la organización víctima. Dichos servicios se entraban alojados en servidores que tenían comunicación directa con la red interna de la propia organización víctima. ESCENARIO 2
<u>T1085</u> <u>CAPEC CAPEC-560</u>	Persistencia	Creación de entrada en menú de inicio para ejecución de proceso con DLL maliciosa como argumento	GreyEnergy mini (dropper) hace la descarga de una DLL maliciosa (%APPDATA%) y crea un fichero. LNK contra la propia DLL maliciosa, creando una entrada en el menú de inicio de Windows. La DLL descargada parece "legítima" para Windows.
<u>T1078</u> <u>CAPEC CAPEC-560</u>	Escalada de privilegios	Cuentas válidas	Gracias al uso de la herramienta <u>Mimikatz</u> , los atacantes eran capaces de obtener credenciales con privilegios de administrador.
<u>T1116</u>	Evasión del operador y defensas desplegadas	Firmado de código	GreyEnergy fue firmado digitalmente con un certificado pertenece a Advantech.
---	Evasión del operador y defensas desplegadas	Alojado en memoria	GreyEnergy se implementó de dos modos, sólo en memoria o utilizando la persistencia de DLL como servicio. El primer modo, se usa cuando los atacantes confían en que la implementación del malware no requiere ninguna persistencia (por ejemplo, servidores con mucha actividad); el segundo modo es se usa cuando el malware necesita poder sobrevivir a cualquier reinicio.
---	Evasión del operador y defensas desplegadas	Modificación de la configuración del sistema	---
---	Evasión del operador y defensas desplegadas	Modificación de parámetros	---
---	Evasión del operador y defensas desplegadas	Inhibición de herramientas de seguridad/sistemas	GreyEnergy utilizaba entre otras, técnicas Anti-reversing y anti-forensics para evitar tanto ser detectado como analizado. También poseía una característica de autoborrado en el caso de superar un número determinado de intentos de conexión fallida con el C&C.
<u>T1003</u> <u>CAPEC CAPEC-567</u>	Acceso de credenciales	Volcado de credenciales	Módulo <i>mimikatz</i> : Usa el software Mimikatz para recopilar credenciales de Windows.
	Descubrimiento	Enumeración de red	---
<u>T1087</u> <u>CAPEC CAPEC-575</u>	Descubrimiento	Enumeración de cuentas	Módulo <i>passwords</i> : Recoge las contraseñas guardadas de varias aplicaciones.
<u>T1007</u> <u>CAPEC CAPEC-574</u>	Descubrimiento	Listado de servicios locales	Módulo <i>info</i> : Recopila información sobre el sistema infectado, registros de eventos, SHA-256, etc.
---	Movimientos laterales	Cuentas válidas	---
---	Movimientos laterales	Servicios Remotos Externos	---

---	Ejecución	Scripting	GreyEnergy recibía comandos del servidor C&C. Entre ellos se encontraban los comandos: ID del comando = 3: ejecutaba un comando de Shell. ID del comando = 5: Descargaba y ejecutaba un archivo .BAT desde el directorio temporal.
---	Ejecución	Carga de módulos	Los atacantes no cargaban todos los módulos a la vez en la máquina comprometida. Mediante el uso de C&C descargaban y ejecutaban los módulos que eran necesarios para cada tarea.
<u>T1072</u>	Ejecución	Software de terceros	GreyEnergy usaba software legítimo de terceros en servidores Linux: <ul style="list-style-type: none">• 3proxy tiny proxy server• Dante SOCKS server• PuTTY Link (Plink)
<u>T1085</u>	Ejecución	Rundll32	Relacionado con la parte de persistencia y el modo de alojar el malware en el sistema afectado.
<u>T1005</u>	Recolección	Datos del sistema local	Comando con ID = 1, Recopilaba información sobre la máquina infectada. La información se recopilaba mediante el uso de WMI Query Language (WQL).
<u>T1113</u>	Recolección	Captura de pantalla	Módulo sshot
<u>T1125</u>	Recolección	Captura de vídeo	Módulo sshot
---	Recolección	Keylogger	Módulo keylogger – grabación de las pulsaciones de teclado.
<u>T1022</u>	Exfiltración	Cifrado de datos	Canales
<u>T1041</u>	Exfiltración	Exfiltración sobre canales de comando y control	Uso de proxies tanto internos como externos para comunicaciones con el C&C. (TRIUNGULIN)
<u>T1090</u>	Comando y Control	Conexión proxy	Es muy probable que cada servidor C&C tuviese una dirección .onion en Tor y que los atacantes la utilizasen para acceder, controlar o transferir datos. <i>Nota: Requisito de OPSEC, que agrega un nivel adicional de anonimato para los atacantes.</i>
<u>T1001</u>	Comando y Control	Ofuscación de datos	La mayoría de las muestras de GreyEnergy utilizaban un algoritmo de cifrado ligeramente diferente. Específicamente, los primeros cuatro bytes del bloque cifrado, se usan como clave de descifrado para la ejecución de T1001 operaciones XOR.
<u>T1102</u>	Comando y Control	Servicios web	La comunicación con el C&C se realizaba sobre HTTPS; sin embargo, en algunos casos también se usaba HTTP. En el mismo formato MIME se encapsulaban las solicitudes

			HTTP. Sin embargo, debe tenerse en cuenta que los datos se cifraban utilizando AES-256 y RSA-2048.
--	--	--	--

En su investigación, ESET no observó ningún módulo específicamente para Sistemas de control industrial (ICS). Sin embargo, sí que han observado que los atacantes de GreyEnergy, han estado apuntando estratégicamente a las estaciones de trabajo relacionadas con entornos ICS que ejecutaban software relacionado con SCADA. Estas estaciones o servidores, tienden a ser sistemas críticos que nunca fueron desconectados, excepto en casos de mantenimiento.

Análisis del backdoor FELIXROOT (mini GreyEnergy)⁴⁰:

Domain	ID	Name	Use
Enterprise	T1059	Command-Line Interface	FELIXROOT opens a remote shell to execute commands on the infected system. ^{[1][2]}
Enterprise	T1043	Commonly Used Port	FELIXROOT uses Port Numbers 443, 8443, and 8080 for C2 communications. ^{[1][2]}
Enterprise	T1022	Data Encrypted	FELIXROOT encrypts collected data with AES and Base64 and then sends it to the C2 server. ^[1]
Enterprise	T1107	File Deletion	FELIXROOT deletes the .LNK file from the startup directory as well as the dropper components. ^[1]
Enterprise	T1112	Modify Registry	FELIXROOT deletes the Registry key HKCU\Software\Classes\{Applications\rundll32.exe\shell\open\
Enterprise	T1027	Obfuscated Files or Information	FELIXROOT encrypts strings in the backdoor using a custom XOR algorithm. ^{[1][2]}
Enterprise	T1057	Process Discovery	FELIXROOT collects a list of running processes. ^[2]
Enterprise	T1012	Query Registry	FELIXROOT queries the Registry for specific keys for potential privilege escalation and proxy information. FELIXROOT has also used WMI to query the Windows Registry. ^{[1][2]}
Enterprise	T1060	Registry Run Keys / Startup Folder	FELIXROOT adds a shortcut file to the startup folder for persistence. ^[2]
Enterprise	T1105	Remote File Copy	FELIXROOT downloads and uploads files to and from the victim's machine. ^{[1][2]}
Enterprise	T1085	Rundll32	FELIXROOT uses Rundll32 for executing the dropper program. ^{[1][2]}
Enterprise	T1064	Scripting	FELIXROOT executes batch scripts on the victim's machine. ^[1]
Enterprise	T1063	Security Software Discovery	FELIXROOT checks for installed security software like antivirus and firewall. ^[2]
Enterprise	T1023	Shortcut Modification	FELIXROOT creates a .LNK file for persistence. ^[2]
Enterprise	T1071	Standard Application Layer Protocol	FELIXROOT uses HTTP and HTTPS to communicate with the C2 server. ^{[1][2]}
Enterprise	T1082	System Information Discovery	FELIXROOT collects the victim's computer name, processor architecture, OS version, volume serial number, and system type. ^{[1][2]}
Enterprise	T1016	System Network Configuration Discovery	FELIXROOT collects information about the network including the IP address and DHCP server. ^[2]
Enterprise	T1033	System Owner/User Discovery	FELIXROOT collects the username from the victim's machine. ^{[1][2]}
Enterprise	T1124	System Time Discovery	FELIXROOT gathers the time zone information from the victim's machine. ^[2]
Enterprise	T1047	Windows Management Instrumentation	FELIXROOT uses WMI to query the Windows Registry. ^[2]

Ilustración 29: Técnicas utilizadas por el backdoor FELIXROOT (Mini GreyEnergy), fuente: MITRE

Análisis del backdoor GreyEnergy⁴¹ por MITRE:

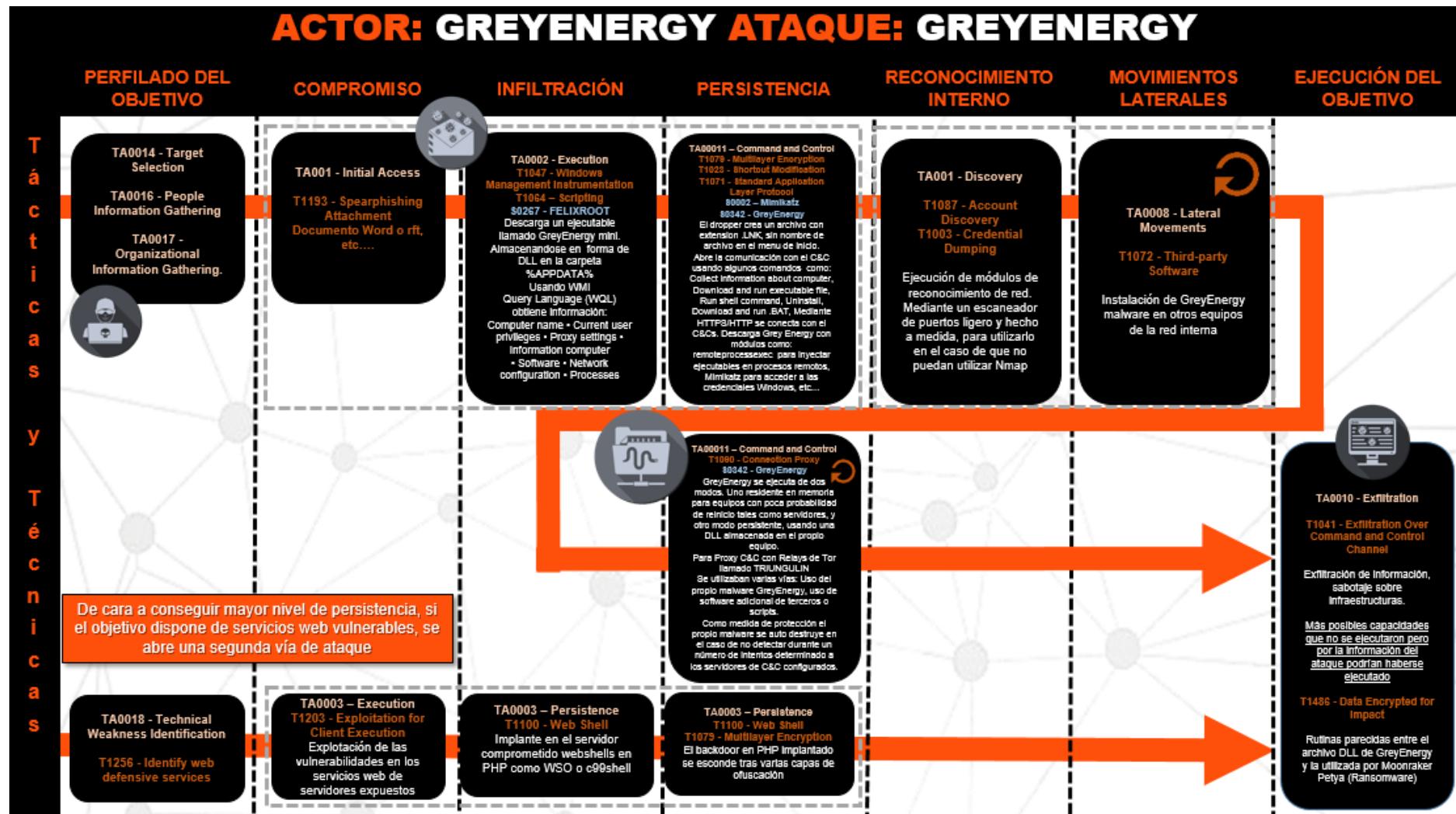
40 <https://attack.mitre.org/software/S0267/>

41 <https://attack.mitre.org/software/S0342/>

Domain	ID	Name	Use
Enterprise	T1116	Code Signing	GreyEnergy digitally signs the malware with a code-signing certificate. ^[1]
Enterprise	T1059	Command-Line Interface	GreyEnergy uses cmd.exe to execute itself in-memory. ^[1]
Enterprise	T1003	Credential Dumping	GreyEnergy has a module for Mimikatz to collect Windows credentials from the victim's machine. ^[1]
Enterprise	T1107	File Deletion	GreyEnergy can securely delete a file by hooking into the DeleteFileA and DeleteFileW functions in the Windows API. ^[1]
Enterprise	T1056	Input Capture	GreyEnergy has a module to harvest pressed keystrokes. ^[1]
Enterprise	T1031	Modify Existing Service	GreyEnergy chooses a service, drops a DLL file, and writes it to that serviceDLL Registry key. ^[1]
Enterprise	T1112	Modify Registry	GreyEnergy modifies conditions in the Registry and adds keys. ^[1]
Enterprise	T1188	Multi-hop Proxy	GreyEnergy has used Tor relays for Command and Control servers. ^[1]
Enterprise	T1027	Obfuscated Files or Information	GreyEnergy encrypts its configuration files with AES-256 and also encrypts its strings. ^[1]
Enterprise	T1055	Process Injection	GreyEnergy has a module to inject a PE binary into a remote process. ^[1]
Enterprise	T1105	Remote File Copy	GreyEnergy can download additional modules and payloads. ^[1]
Enterprise	T1085	Rundll32	GreyEnergy uses PsExec locally in order to execute rundll32.exe at the highest privileges (NTAUTHORITY\SYSTEM). ^[1]
Enterprise	T1045	Software Packing	GreyEnergy is packed for obfuscation. ^[1]
Enterprise	T1071	Standard Application Layer Protocol	GreyEnergy uses HTTP and HTTPS for C2 communications. ^[1]
Enterprise	T1032	Standard Cryptographic Protocol	GreyEnergy encrypts communications using AES256 and RSA-2048. ^[1]
Enterprise	T1007	System Service Discovery	GreyEnergy enumerates all Windows services. ^[1]

Ilustración 30: Técnicas utilizadas por el backdoor GreyEnergy escrito en C y compilado en Visual Studio, fuente: MITRE

4.5.2 Taxonomía CAT



5 Conclusiones

A continuación, se exponen una serie de lecciones aprendidas, críticas y líneas de trabajo futuras relacionadas con el proyecto desarrollado.

5.1 Lecciones aprendidas

- La complejidad a la hora de elaborar un modelado de un ataque de forma exhaustiva tanto a nivel técnico como a un alto nivel para que mucha gente pueda entender lo que sucede.
- Grandes cantidades de información disponible en Internet pero que no posee un orden a la hora de aplicar ciertos conceptos técnicos.

5.2 Reflexión crítica

- Todos los objetivos se han podido lograr y las tácticas y técnicas planteadas en el proyecto se encuentran en revisión por parte de la comunidad de CAT para su aparición en la página de github.
- En lo que respecta a la planificación, esta ha sido correcta. Se han podido desarrollar e investigar con tiempo los puntos expuestos en el proyecto.
- Se han introducido diferentes cambios de la planificación inicial sobre los puntos a tratar para evitar extender el proyecto mucho más. Con este hecho se pretende entregar un documento fácil de leer y con contenido interesante.

5.3 Futuras líneas de trabajo

- **Ejecución de las pruebas planteadas.** Ya se está trabajando en esta línea para aplicar los conceptos teóricos explicados en este proyecto.
- **Desarrollo de herramientas a medida** que permitan realizar ciertos ataques en los entornos industriales, concretamente en entornos de subestaciones eléctricas.
- **Modelado de más incidentes de ciberseguridad industrial** que vayan surgiendo a lo largo del tiempo.
- **Incorporación de más tácticas, técnicas y herramientas en el framework *caffeine*** que permitan realizar tanto un mejor modelado de los ataques como plantear nuevos escenarios de ataque para equipos de red team.

6 Glosario

6.1 Acrónimos

HMI: Human Machine Interface

IED: Intelligent Electronic Device

IDS: Intrusion Detection System

INCIBE: Instituto Nacional de Ciberseguridad Español

IT: Information Technology

LAN: Local Area Network

NIST: Instituto Nacional de Estándares y Tecnología de EE.UU

OSI: Open System Interconnection

OT: Operation Technology

PLC: Programmable Logic Controller

RTU: Remote Terminal Unit

SCADA: Supervisory Control And Data Acquisition

TTP: Técnicas, Tácticas y Procedimientos

UCS: Unidad Central del Sistema

6.2 Términos

- **Blue team:** Equipo de respuesta frente a incidentes en materia de ciberseguridad. Equipo defensivo.
- **Red team:** Equipo integrado por profesionales de hacking ético cuyo objetivo es la simulación de ataques reales en entornos normalmente en producción. Equipo ofensivo.

7 Bibliografía

- <http://pwnwiki.io/#!index.md>
<https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf>
<https://www.nist.gov/cyberframework/critical-infrastructure-resources>
https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf
<https://www.dsn.gob.es/sistema-seguridad-nacional/comit%C3%A9s-especializados/comit%C3%A9-seguridad-energ%C3%A9tica#collapseSix>
<http://www.proteccióncivil.es/catalogo/naturales/climaespacial/presentaciones/p31.pdf>
<http://www.seguritecnia.es/seguridad-publica/administraciones-publicas/plan-estrategico-sectorial-del-subsector-de-la-electricidad>
<https://www.larazon.es/espana/el-estado-islamico-intento-hackear-una-depuradora-y-envenenar-el-agua-de-miles-de-personas-en-inglaterra-CH20148208>
<https://dragos.com/wp-content/uploads/CrashOverride-01.pdf>
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
<https://github.com/rabobank-cdc/Blue-ATTACK/wiki>
<https://ieeexplore.ieee.org/document/5967924/references#references>
<https://cordis.europa.eu/es>
<https://cyberstartupobservatory.com/infographics/>
<https://www.nozominetworks.com/resources/>
<https://github.com/fdeandres/CAT----Intelligence-Led-Cyber-Attack-Taxonomy>
<https://github.com/NextronSystems/APTSimulator>
<https://github.com/snabbco/snabb>
<http://pwnwiki.io/#!index.md>
<http://www.addletters.com/image-list.php>
<https://github.com/nshalabi/ATTACK-Tools>
<https://github.com/hisanmehmood/Awesome-Red-Teaming>
<https://azeria-labs.com/tactics-techniques-and-procedures-ttps/>
<https://www.soc-cmm.com/>
<http://kinomakino.blogspot.com/>
<https://www.novainfosec.com/2016/02/12/the-dml-model/>
<https://elcomercio.pe/mundo/venezuela/venezuela-nicolas-maduro-rusia-asegura-apagon-pais-debio-ataque-proveniente-extranjero-estados-unidos-juan-guaido-noticia-nndc-616964>
https://www.researchgate.net/publication/319701970_Cyber_Threat_Intelligence_Model_An_Evaluation_of_Taxonomies_Sharing_Standards_and_Ontologies_within_Cyber_Threat_Intelligence
<https://www.endgame.com/blog/technical-blog/introducing-endgame-red-team-automation>
<https://ics.sans.org/blog/2016/12/27/one-cip-two-cip-red-cip-blue-cip>
<https://gitlab.com/d0ubl3g/industrial-security-auditing-framework>

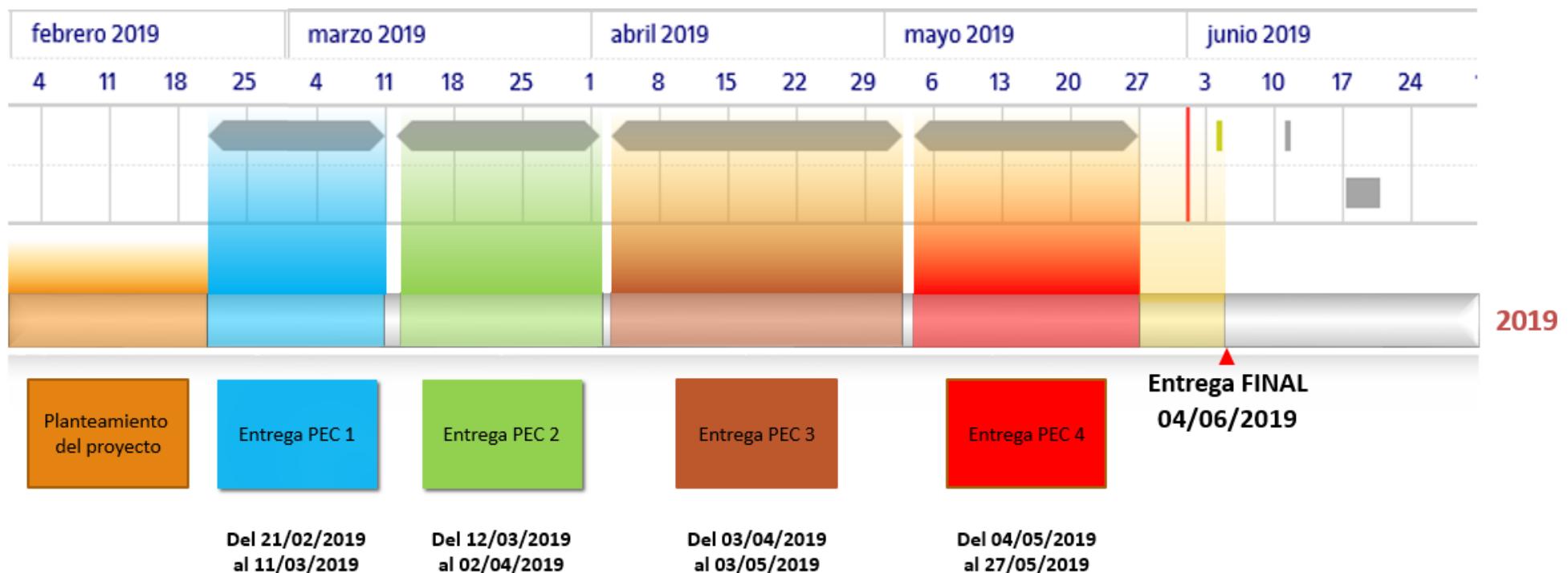
[https://www.researchgate.net/publication/330149899 Tools Techniques and Methodologies A Survey of Digital Forensics for SCADA Systems](https://www.researchgate.net/publication/330149899_Tools_Techniques_and_Methodologies_A_Survey_of_Digital_Forensics_for_SCADA_Systems)
https://www.nozominetworks.com/labs/?utm_campaign=2019-NN-Labs-Launch&utm_content=87238518&utm_medium=social&utm_source=twitter&hs_s_channel=tw-1340428902
<https://github.com/NozomiNetworks/greyenergy-unpacker>
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.html
<https://github.com/mitre/cti/blob/master/USAGE.md>
<https://federalnewsnetwork.com/strategic-threat-intelligence/2019/02/mitres-new-attck-tool-an-encyclopedia-of-cyber-threats/>
MIRAR WEBINARS DE SANS!!
<https://securelist.com/greyenergys-overlap-with-zebrcy/89506/>
<https://www3.corelight.com/l/420832/2019-01-17/gnz524>
<https://github.com/ITI/ICS-Security-Tools>

Lista numerada de las referencias bibliográficas utilizadas dentro de la memoria. En cada lugar donde se utilice una referencia dentro del texto, hay que indicarla citando el número de la referencia, por ejemplo: [7].

Es muy importante incluir **todas** las referencias utilizadas y citarlas apropiadamente, es decir, incluyendo toda la información necesaria para identificar la referencia. La información mínima que hay que incluir según el tipo de referencia es:

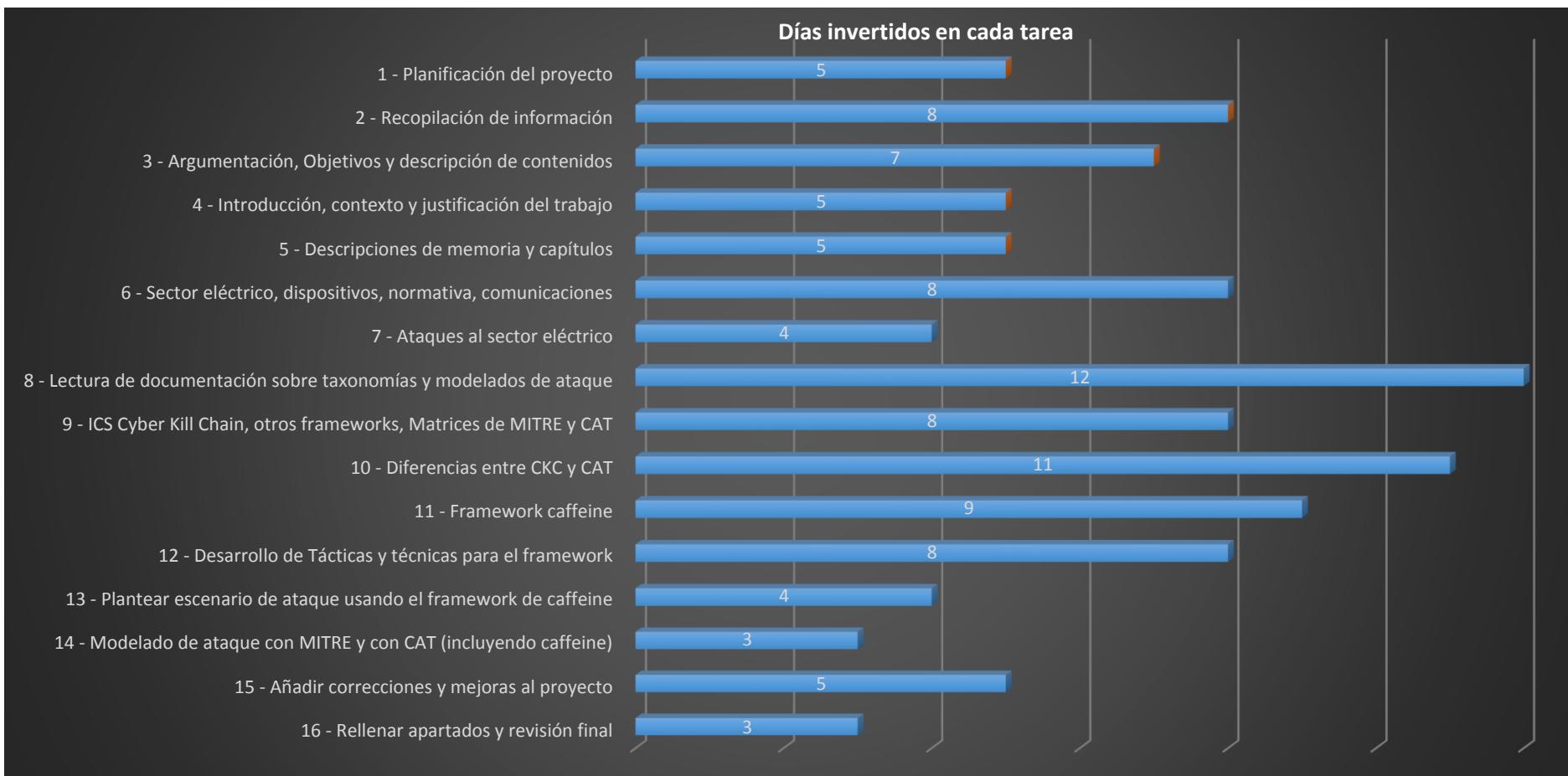
- **Libro:** Autores, Título, Edición (si se tercia) Editorial, Ciudad, Año.
- **Artículo de revista:** Autores, Título, Nombre de la Revista, Número de Página inicial y final, Número de la revista / Volumen, Año.
- **Web:** URL y fecha en que se ha visitado.

8 Anexo I – Diagramas de planificación



Información extra

PEC	Tarea	Fecha de inicio	Fecha de finalización	Hito o actividad	Inicio el día	Duración de la tarea
1	1 - Planificación del proyecto	21/02/2019	25/02/2019	Inicio	21/02/2019	5
1	2 - Recopilación de información	26/02/2019	04/03/2019	Actividad 2	26/02/2019	8
1	3 - Argumentación, Objetivos y descripción de contenidos	05/03/2019	11/03/2019	Actividad 3	05/03/2019	7
2	4 - Introducción, contexto y justificación del trabajo	12/03/2019	16/03/2019	Actividad 4	12/03/2019	5
2	5 - Descripciones de memoria y capítulos	17/03/2019	21/03/2019	Actividad 5	17/03/2019	5
2	6 - Sector eléctrico, dispositivos, normativa, comunicaciones	22/03/2019	29/03/2019	Actividad 6	22/03/2019	8
2	7 - Ataques al sector eléctrico	30/03/2019	02/04/2019	Actividad 7	30/03/2019	4
3	8 - Lectura de documentación sobre taxonomías y modelados de ataque	03/04/2019	14/04/2019	Actividad 8	03/04/2019	12
3	9 - ICS Cyber Kill Chain, otros frameworks, Matrices de MITRE y CAT	15/04/2019	22/04/2019	Actividad 9	15/04/2019	8
3	10 - Diferencias entre CKC y CAT	23/04/2019	03/05/2019	Actividad 10	23/04/2019	11
4	11 - Framework <i>caffeine</i>	04/05/2019	12/05/2019	Actividad 11	04/05/2019	9
4	12 - Desarrollo de Tácticas y técnicas para el framework	13/05/2019	20/05/2019	Actividad 12	13/05/2019	8
4	13 - Plantear escenario de ataque usando el framework de <i>caffeine</i>	21/05/2019	24/05/2019	Actividad 13	21/05/2019	4
4	14 - Modelado de ataque con MITRE y con CAT (incluyendo <i>caffeine</i>)	25/05/2019	27/05/2019	Actividad 14	25/05/2019	3
FINAL	15 - Añadir correcciones y mejoras al proyecto	28/05/2019	01/06/2019	Actividad 15	28/05/2019	5
FINAL	16 - Rellenar apartados y revisión final	02/06/2019	04/06/2019	Actividad 16	02/06/2019	3



9 Anexo II – Ciberataque a Venezuela, revisión técnica

Venezuela es un país tropical ubicado en el norte de América del Sur que posee alrededor de un 18% del petróleo mundial según antiguos datos. Aunque este porcentaje, actualmente es menor ya que se ha registrado una disminución en su producción de petróleo debido a influencias tanto políticas como de su situación internacional. Dada la cantidad de petróleo y recursos que posee para exportar, Venezuela podría llegar a ser un objetivo estratégico para otras naciones que quieran manipular de alguna forma sus recursos o guiar su desarrollo en una dirección concreta para obtener beneficio.

En la tarde del 7 de Mayo de 2019, Venezuela sufrió un apagón a gran escala que paralizó el país. Las infraestructuras críticas se vieron afectadas directamente y esto evolucionó en un malestar general por parte de la población que sufría apagones continuos quedándose sin forma de conservar alimentos, luz por la noche, etc. Además, a estos problemas hay que sumar los diferentes problemas que derivaron dada la situación como un gobierno desestabilizado y continuas trifulcas en las calles a lo largo de todo el país.

Tras unos días de continuos problemas, el presidente de Venezuela, Nicolás Maduro, anunció en diferentes medios públicos que los apagones habían sido originados por un ataque cibernético. En su discurso, el presidente señaló un posible culpable siendo EE.UU dicho culpable y el que atacó a todo el sistema eléctrico del país. Además, Nicolás Maduro añadió información sobre el ataque perpetrado por, supuestamente EE.UU el cual, se dividía en 3 fases o ataques:

- El primer ataque sería contra el sistema central informático que posee la empresa Corporación Eléctrica Nacional (Corpoelc) en la Central Hidroeléctrica Simón Bolívar (la tercera más grande del mundo), ubicada en la represa de El Guri. Este ciberataque afectaría también a la capital en Caracas. Es importante comentar que la hidroeléctrica Simón Bolívar, proporciona electricidad a un 80% de Venezuela y por ello, se catalogaría como una infraestructura crítica.
- Tras este supuesto primer ataque, el presidente comentó un posible ataque vía electromagnética con “*dispositivos móviles que interrumpen y revierten los procesos de recuperación*”. Parece que el presidente quería hacer referencia a inhibidores avanzados que impedían la transmisión de las comunicaciones de forma correcta.
- Finalmente, en un último ataque se realizarían quemas y explosión de subestaciones eléctricas fruto de sabotajes.

Como información extra, Maduro reveló que el ataque fue realizado desde dos ciudades estadounidenses, Houston y Chicago, y confirmó que ya se tienen pruebas de cómo se perpetró dicho ciberataque a la red eléctrica.

Pero, ¿se podría determinar si los apagones han sido originados realmente por un ciberataque? Existen algunas investigaciones técnicas enfocadas en esta línea por Internet y prácticamente todas llegan a la misma conclusión, no se puede determinar de manera rotunda si ha existido un ciberataque. Lo que si se puede afirmarse es que durante el periodo de los apagones, buscadores como shodan, zoomeye, fofa, etc. recibieron bastante afluencia de búsquedas, todas ellas focalizadas en Venezuela y su infraestructura.

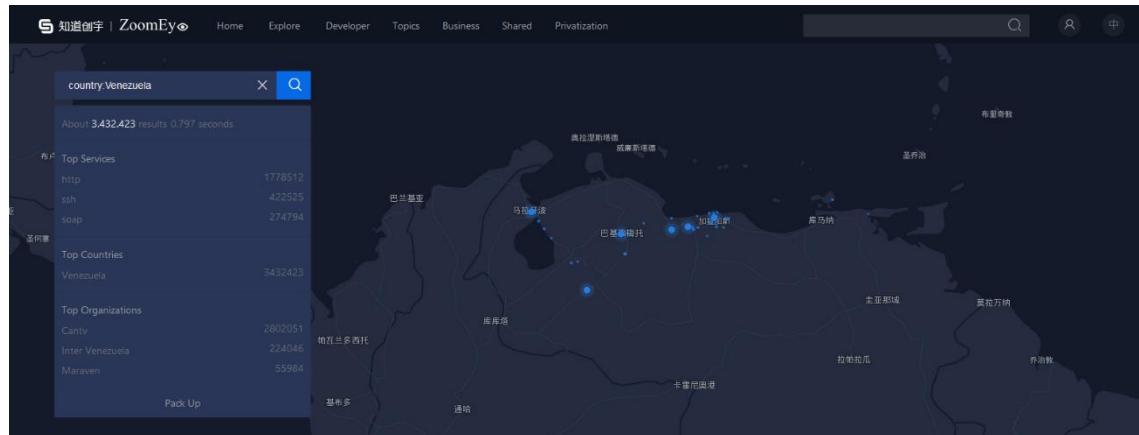


Ilustración 31: Búsqueda de dispositivos conectados a Internet desde ZoomEye ubicados en Venezuela

Tras el paso de estos ataques, se han realizado diferentes búsquedas en busca de dispositivos que siguen conectados a Internet y utilizan protocolos asociados al sector eléctrico. Teniendo en cuenta que el protocolo más extendido en América es el DNP3, se ha realizado una búsqueda de dispositivos que posean este puerto activo y este ha sido el resultado:



Ilustración 32: Uso de shodan para detectar posibles dispositivos con DNP3 en Venezuela

Se han detectado 53 dispositivos con el puerto 20000/TCP abierto. Dicho puerto es el utilizado por el protocolo DNP3 por defecto pero parece que algunos de

estos puertos no poseen un verdadero servicio DNP3 detrás sino otro servicio utilizado por otras comunicaciones.

Una búsqueda más avanzada con ZoomEye me ha permitido reducir los posibles falsos positivos y detectar 48 hosts que en un principio si son dispositivos industriales y utilizan el protocolo DNP3 de verdad.

Consulta enviada:

```
port:"20000"+country:"VE" +service:"dnp"
```

Por otro lado, también se realizó una búsqueda para el protocolo Modbus/TCP que utiliza el puerto 502/TCP por defecto.

[REDACTED]

The Houses Television C.A. (ConexTELECOM) Added on 2019-05-23 21:44:14 GMT Venezuela, Valencia	Unit ID: 0 -- Slave ID Data: (0900ff000800d203c000)
ics	Unit ID: 1 -- Slave ID Data: (0900ff000800d203c000)
	Unit ID: 2 -- Slave ID Data: (0900ff000800d203c000)
	Unit ID: 3 -- Slave ID Data: (0900ff000800d203c000)
	Unit ID: 4 -- Slave ID Data: (...)

[REDACTED]

Level 3 Communications Added on 2019-05-29 17:24:03 GMT Venezuela, Catia La Mar	Unit ID: 0
ics	Unit ID: 1 -- Device Identification: TELEMECANIQUE TWDLMDA20DRT 05.20
	Unit ID: 2

Ilustración 33: Búsqueda de dispositivos conectados a Internet con shodan que utilicen el protocolo Modbus/TCP (502/TCP)

En este caso, si parecen tratarse de dispositivos reales dadas las respuestas que se pueden captar por el puerto 502.

Además de todas estas búsquedas con protocolos relacionados con el sector eléctrico y con los sistemas de control industrial en general en el caso de Modbus/TCP. Se ha buscado información de los principales fabricantes o empresas que colaboraron en la hidroeléctrica que supuestamente sufrió el ataque. Dichas empresas son Edelca, Andritz, Alstom y ABB. Algunas de estas empresas como ABB son fabricantes industriales que proporcionan equipamiento a las infraestructuras y que poseen información pública de sus dispositivos por Internet.

Estructura general del sistema DCS

Interfaz hombre-máquina (HMI)
El sistema ABB de portales de generación de procesos (Process Generation Portal) se utilizará en las estaciones de operador. El sistema de consolas se basa en estándares industriales y en el sistema operativo Windows XP. Tiene una arquitectura abierta que permite utilizar numerosos protocolos de comunicaciones con capacidad para interconectar con programas y bases de datos de terceros.

TEI controlador AC800M



Protocolos y medios de soporte

El controlador utiliza los protocolos de comunicación y medios de soporte siguientes:

línea B, y si ambas líneas A y B se averían, entonces la estructura de anillo cambiará a una estructura de bus.

Comunicación a través de la red E/S

La red E/S conecta todos los dispositivos E/S de la planta con el controlador. Hay 3 tipos de protocolos de comunicación utilizados para la red E/S:

- ModuleBus, para comunicar directamente con los clusters E/S locales por cables de fibra óptica de plástico. ModuleBus soporta la funcionali-

Ilustración 34: Ejemplo de dispositivo desplegado por ABB en la hidroeléctrica de Simón Bolívar

Por Internet también se pueden encontrar videos públicos que muestran tanto el dispositivo de forma física como la forma de gestionarlo o programarlo.

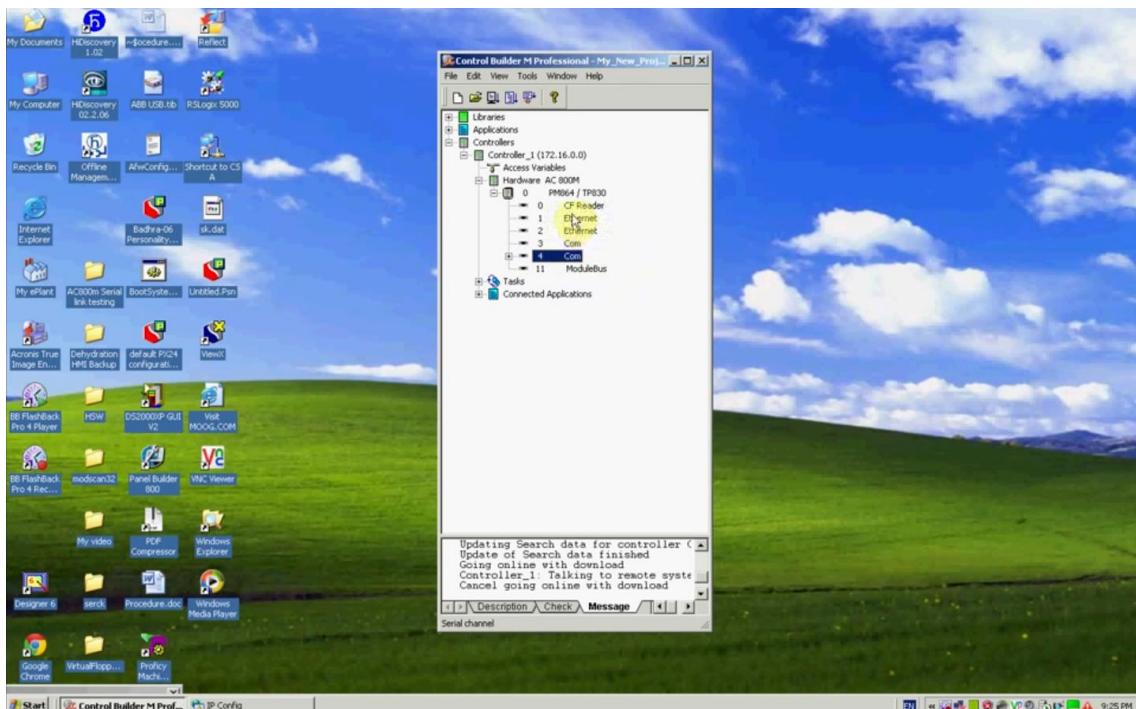


Ilustración 35: Captura del vídeo donde se muestra cómo programar el dispositivo ABB DCS AC 800M, fuente: YouTube

Si bien es cierto que una persona con acceso a Internet puede recabar tal cantidad de información sobre una infraestructura tan importante para Venezuela. Podría decirse que un ciberataque al sector eléctrico podría realizarse perfectamente si se cuenta con un equipo multidisciplinario de personas. También es cierto que detrás de estos ataques ha de encontrarse un estado u organización muy bien organizada y con muchos recursos para poder lograr que el ataque sea satisfactorio.

Que el supuesto ciberataque podría haberse ejecutado no cabe duda pero hasta que no salgan a la luz las pruebas, actualmente no se puede afirmar de manera rotunda que los hechos han sucedido de tal manera.

Por otro lado, lo que si podemos confirmar es que un ataque de estas magnitudes a una infraestructura crítica del sector eléctrico podría originar grandes problemas para un país hasta llegar a colapsarlo como pasó con Venezuela. De esta forma, la elección del sector eléctrico y concretamente en la parte de distribución en el proyecto cobra mucho más sentido tras ver estos sucesos que aunque no se han confirmado a nivel ciber, los problemas que se han detectado han sido más que notables.

Información de referencia utilizada

- <https://docplayer.es/10209350-Central-hidroelectrica-simon-bolivar-guri-marzo-2012.html>
- https://es.wikipedia.org/wiki/Central_Hidroel%C3%A9ctrica_Sim%C3%B3n_Bol%C3%ADvar
- http://interelectricas.co/pdf/ABB/03-2006/32-36%20M647_SPA72dpi.pdf
- <http://www.abb.com/cawp/seitp202/e3d432695eb75e8ac12572f800445309.aspx>
- <https://new.abb.com/news/detail/13622/abb-wins-us-28-million-contract-to-boost-venezuelan-electrical-transmission-system>
- <https://new.abb.com/news/detail/13649/abb-wins-us-41-million-in-orders-for-venezuelan-substation-and-transmission-lines>
- <https://www.telesurtv.net/news/venezuela-investiga-ciberataque-sistema-electrico-20190312-0032.html>
- <https://www.securityweek.com/venezuelas-maduro-says-cyber-attack-prevented-power-restoration>
- <https://www.ivcco.com/application/App%20Note%20-%20ABB%20Guri%20Dam.pdf>
- <https://www.reuters.com/article/us-venezuela-politics-russians/russian-deployment-in-venezuela-includes-cybersecurity-personnel-us-official-idUSKCN1R72FX>
- <https://paper.seebug.org/869/>
- <https://www.360enconcreto.com/blog/detalle/concreto-en-generacion-de-energia-central-hidroelectrica-simon-bolivar>
- <https://www.youtube.com/watch?v=pB4ullSa0zw>
- <https://fofa.so/>
- <https://www.zoomeye.org/>
- <https://www.shodan.io/>