

**XIII
JORNADAS
STIC
CCN-CERT**



**Estrategias de ataque
para el sector
eléctrico**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Jacinto Moral Matellán
S21sec
jmoral@s21sec.com



Aarón Flecha Menéndez
S21sec
aflecha@s21sec.com



Índice

Introducción

CAFFEINE

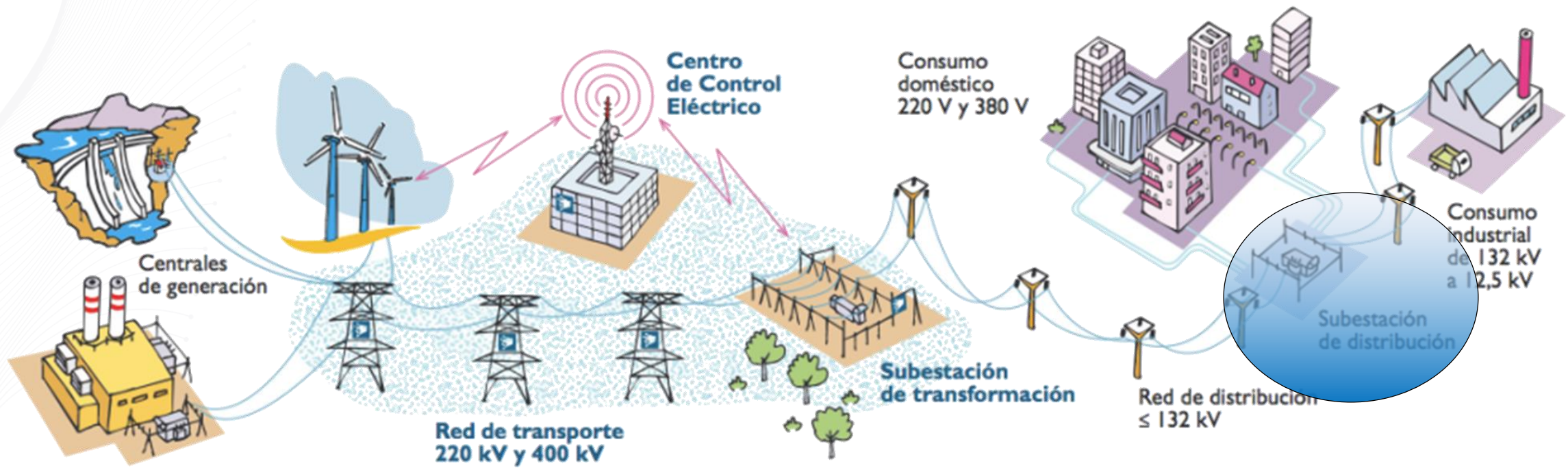
Detección de TTP

DEMOS

Introducción

Introducción

Sector eléctrico



Introducción

BlackEnergy - 2015

Primera detección.
Funcionamiento principal, DDoS.
(2007)

Evolución con una segunda
versión añadiendo nuevas
capacidades (2010)

Black Energy Lite y Black Energy
Big (2014)

Última versión del malware
(2015)

CrashOverride/Industroyer - 2017

Malware modular que permitía envío de comandos directamente a RTU utilizando protocolos industriales (IEC104, IEC101, IEC61850, OPC DA, etc.)

Descubrimiento de dispositivos a través del protocolo OPC y escáner de puertos.

Bloqueo de puertos serie para impedir comunicaciones legítimas.

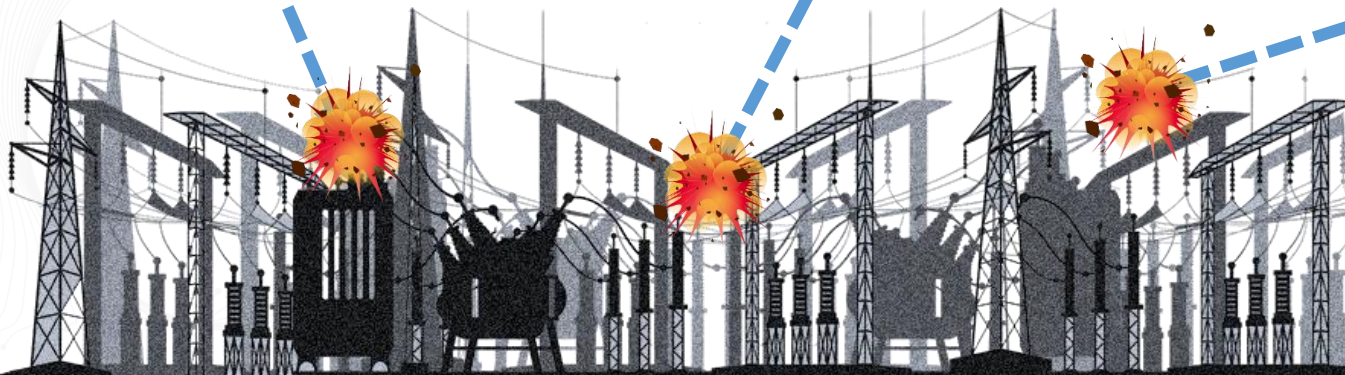
Vulnerabilidad de Siemens en dispositivos SIPROTEC (CVE-2015-5374).

Módulo *wipe*. Eliminación de registros y otros ficheros.

GreyEnergy - 2018

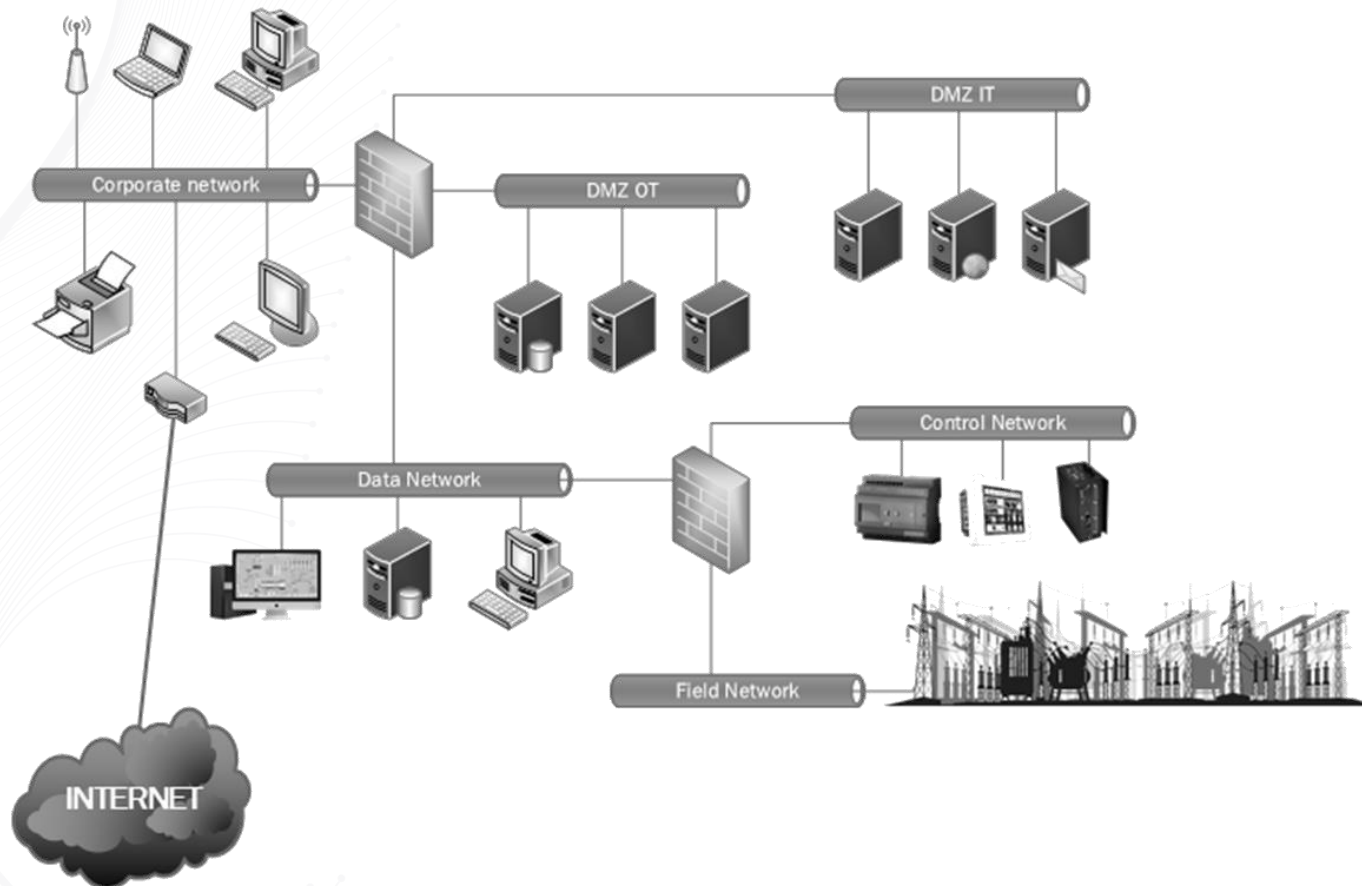
Objetivos principales de espionaje y reconocimiento. Afectaba a:

- Estaciones de trabajo que ejecutaban software SCADA
- Servidores clasificados como sistemas esenciales y sólo eran desconectados en tareas de mantenimiento



Introducción

Aplicando herramientas a entornos específicos (I/II)

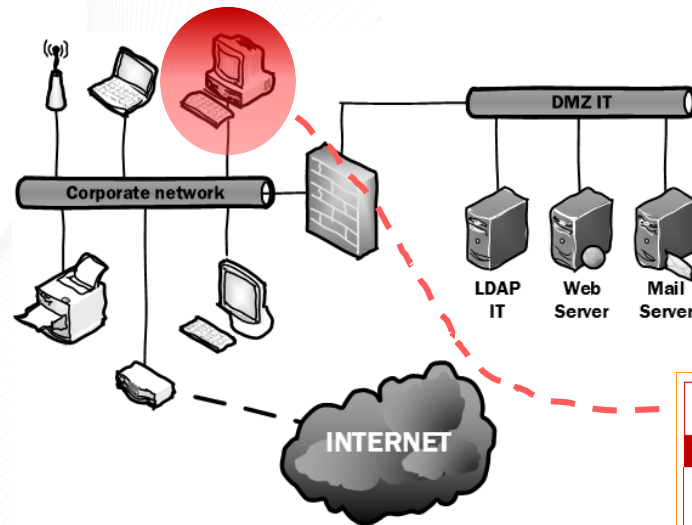


- **Analizar en profundidad las vulnerabilidades** que afectan a nuestro entorno.
- **Siempre valorar el impacto de las vulnerabilidades** en los dispositivos de nuestros entornos y proponer mitigaciones en el caso de no existir soluciones.
- **Conclusión:** Los análisis previos ejecutados permiten realizar un mejor modelado en caso de incidente y detectar de manera más eficiente las TTP.

MUY IMPORTANTE: ESTRATEGIA

Introducción

Aplicando herramientas a entornos específicos (II/II)



Campaña activa que explota vulnerabilidades concretas y afectar a dispositivos con conexión entre la red corporativa e Internet.

Objetivo: Infectar con ransomware.

ccn-cert
centro criptológico nacional

ALERTAS

Vulnerabilidad crítica en RDS de Microsoft

Fecha de publicación: 16/05/2019
Nivel de peligrosidad: Crítica

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, alerta de la publicación de una vulnerabilidad crítica en el servicio **RDS** (Remote Desktop Services) de **Microsoft**, la cual permitirá la ejecución remota de código, sin ser necesario ningún tipo de autenticación.

Vulnerabilidad

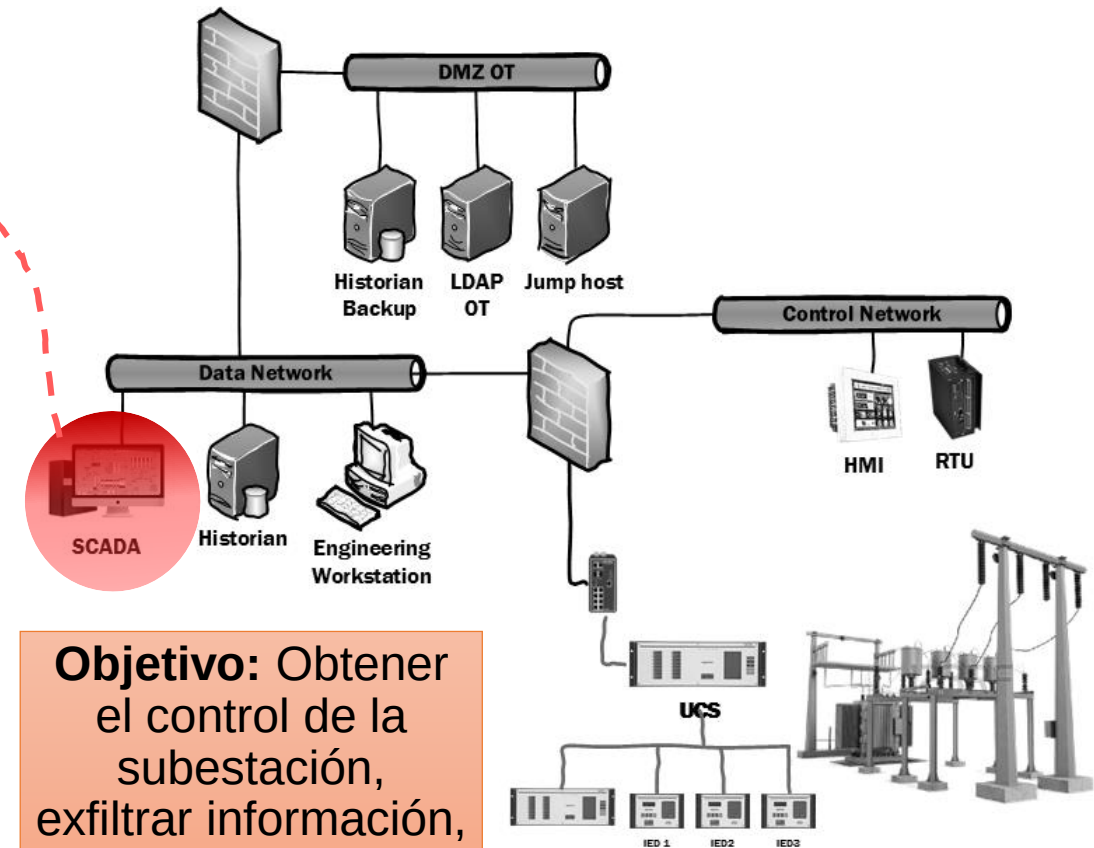
- **CVE-2019-0708:** Esta vulnerabilidad permitirá la ejecución remota de código en el servicio RDS (antiguamente conocido como "Terminal Services") sin autenticación previa y sin interacción por parte de un usuario. Un atacante podría enviar solicitudes especialmente diseñadas que provocarían la ejecución de comandos como usuario privilegiado, pudiendo instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas de usuario.

La vulnerabilidad ha sido identificada como **CVE-2019-0708** y calificada como "extremadamente crítica". Por el momento no se conoce la puntuación de su criticidad (CVSSv2) y **Microsoft** ha indicado que aún no ha observado ninguna evidencia de ataques explotando este fallo.

Recursos afectados:

- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Activos que poseen las mismas vulnerabilidades que explota la campaña activa pero se ubican en otras redes de la compañía.



Objetivo: Obtener el control de la subestación, exfiltrar información, etc.

Introducción

Diferencias entre taxonomías de ataque CKC vs. CAT

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 weaponization 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 basan en un pensamiento heredado de TI.	Permite adaptar nuevas TTP o incorporar frameworks específicos como el que se pretende incorporar en CAT con este proyecto (CAFFEINE).

CAFFEINE

Cyber-Attack Framework
for
Energy
Infrastructures

CAFFEINE



<https://github.com/fdeandres/CAT---Intelligence-Led-Cyber-Attack-Taxonomy>

CAFFEINE

TÁCTICAS - CAFTAXXXX

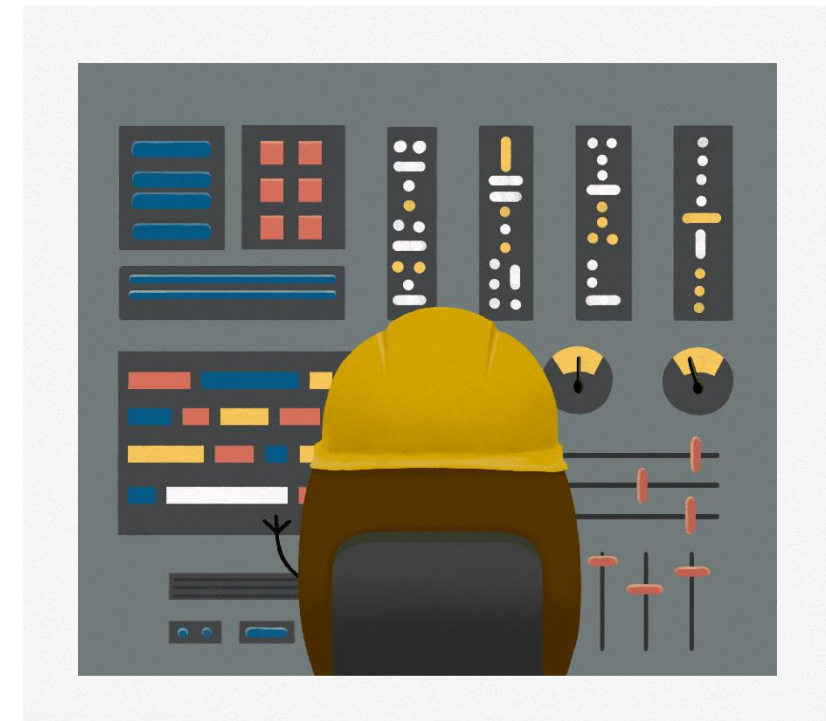
Método utilizado para alcanzar un objetivo específico y proporcionan soporte a la estrategia. La táctica sin estrategia no permitirá evaluar de forma clara el progreso de la operación.

TÉCNICAS - CAFTXXXX

Es la forma más eficiente de realizar un movimiento, o dicho de otra forma, utilizar los recursos. Se asocia a la forma en que se deben ejecutar las herramientas necesarias.

Herramientas

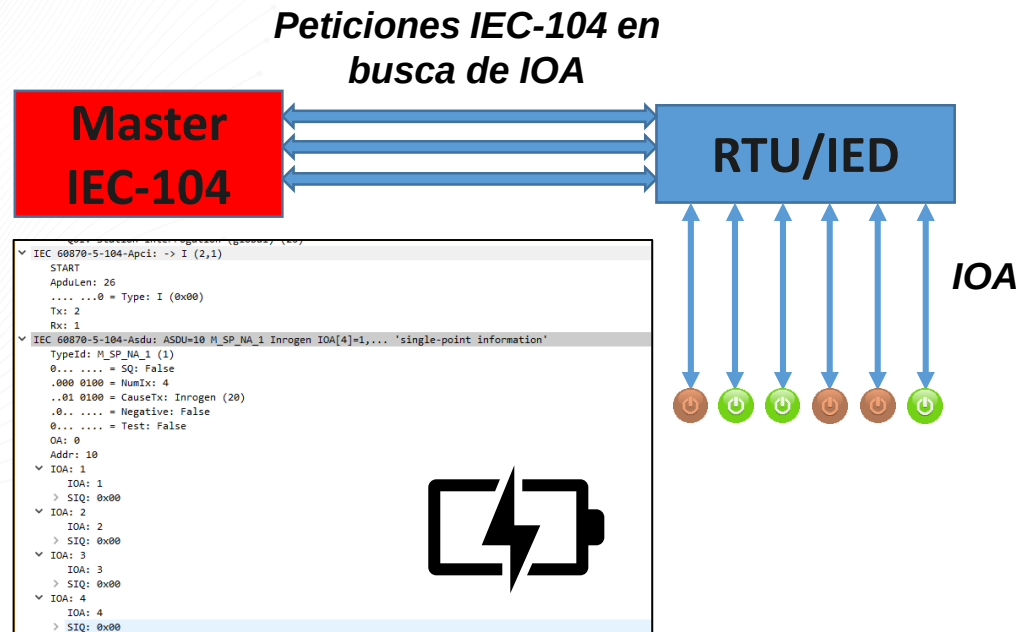
Scripts, herramientas de escritorio o incluso frameworks completos para permitir ejecutar con éxito las técnicas



CAFFEINE

IEC 60870-5-104

Alteración de valor en IOA



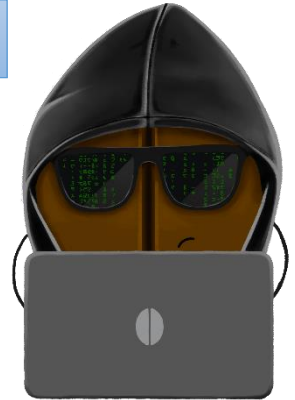
Estrategia: *Ejecución del objetivo*

Táctica: TA0040 - Impact

ID: CAFTXXXX

Técnica: Alteración de valor en IOA (IEC 104)

Descripción: Un potencial atacante con acceso a los activos que comanden o sean comandados mediante el protocolo IEC-104, podría alterar los valores que se encuentran tras las direcciones IOA de estos activos.

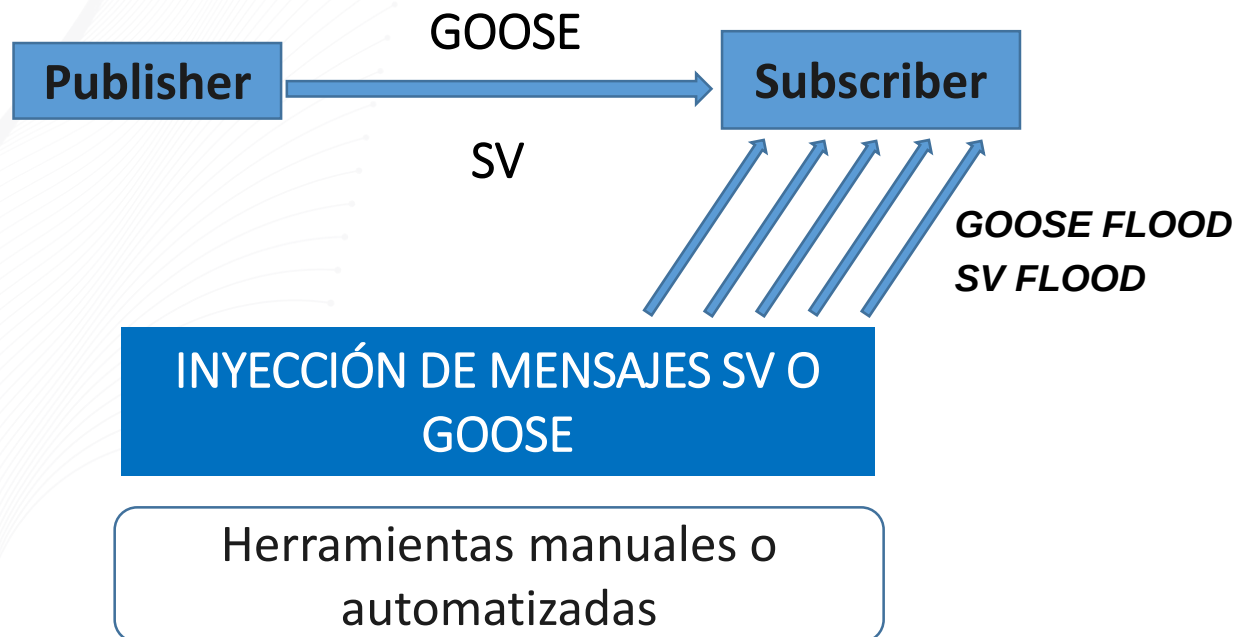


Herramientas: Modificación de librerías IEC-104 utilizadas por los dispositivos, scapy, tcpdump, herramientas específicas para comunicaciones IEC-104, etc.

CAFFEINE

IEC 61850

Inundación (Flooding)



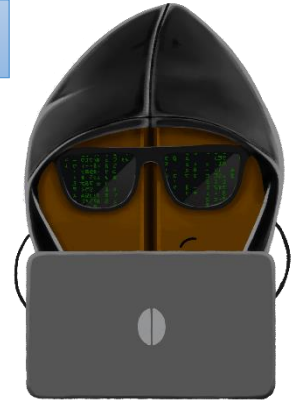
Herramientas: tcpreplay, scripting con scapy o nmap, etc.

Estrategia: *Ejecución del objetivo*

Táctica: TA0040 - Impact

ID: CAFTXXXX

Técnica: Inundación de paquetes (IEC 61850)



Descripción: Al tratarse de tramas *multicast*, cualquier trama que se envíe a través de la red y cumpla los requisitos del suscriptor, va a ser aceptada por este.

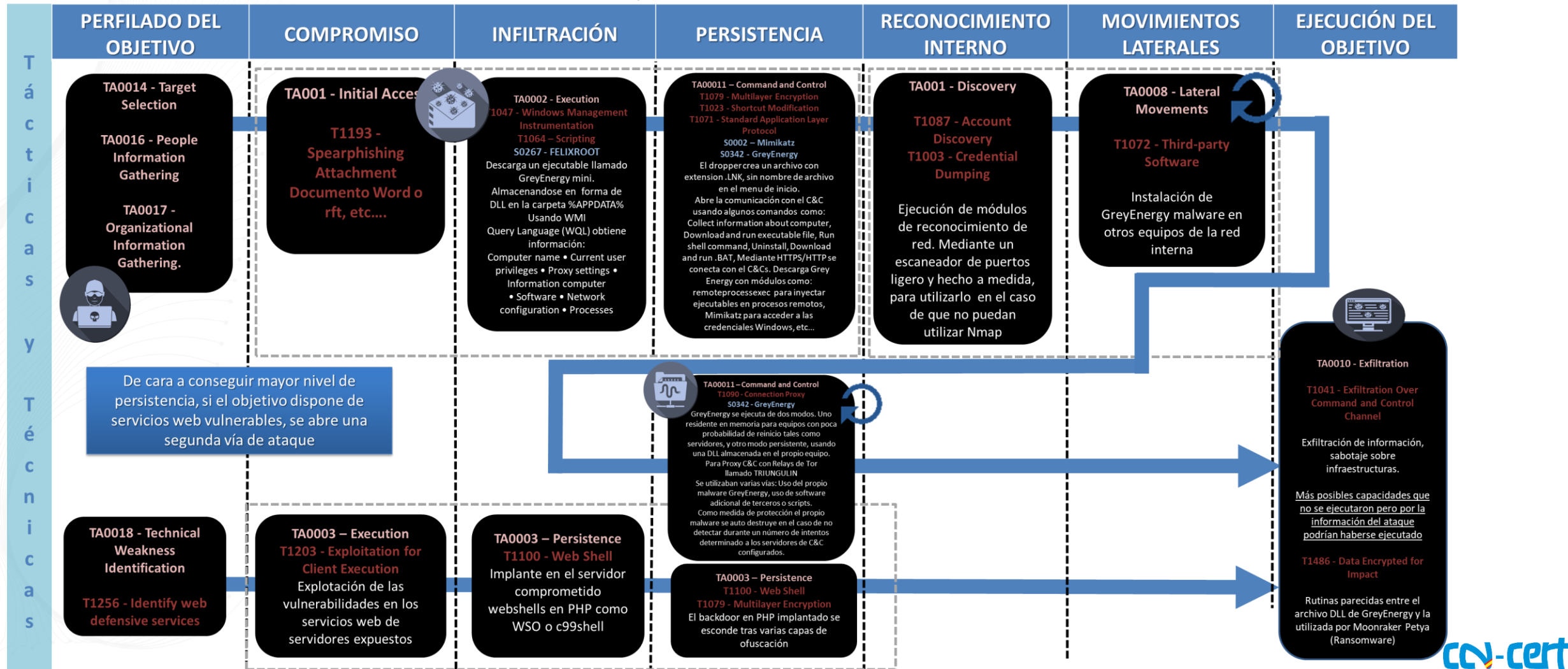
Un atacante con acceso al medio podría inundar la red con tramas especialmente diseñadas gracias al uso de diferentes herramientas. Este hecho podría originar una serie de estados como:

- Denegación de servicio.
- Desatención de tramas legítimas.
- Mediciones anómalas.

CAFFEINE – modelado de incidentes

EXAMPLE

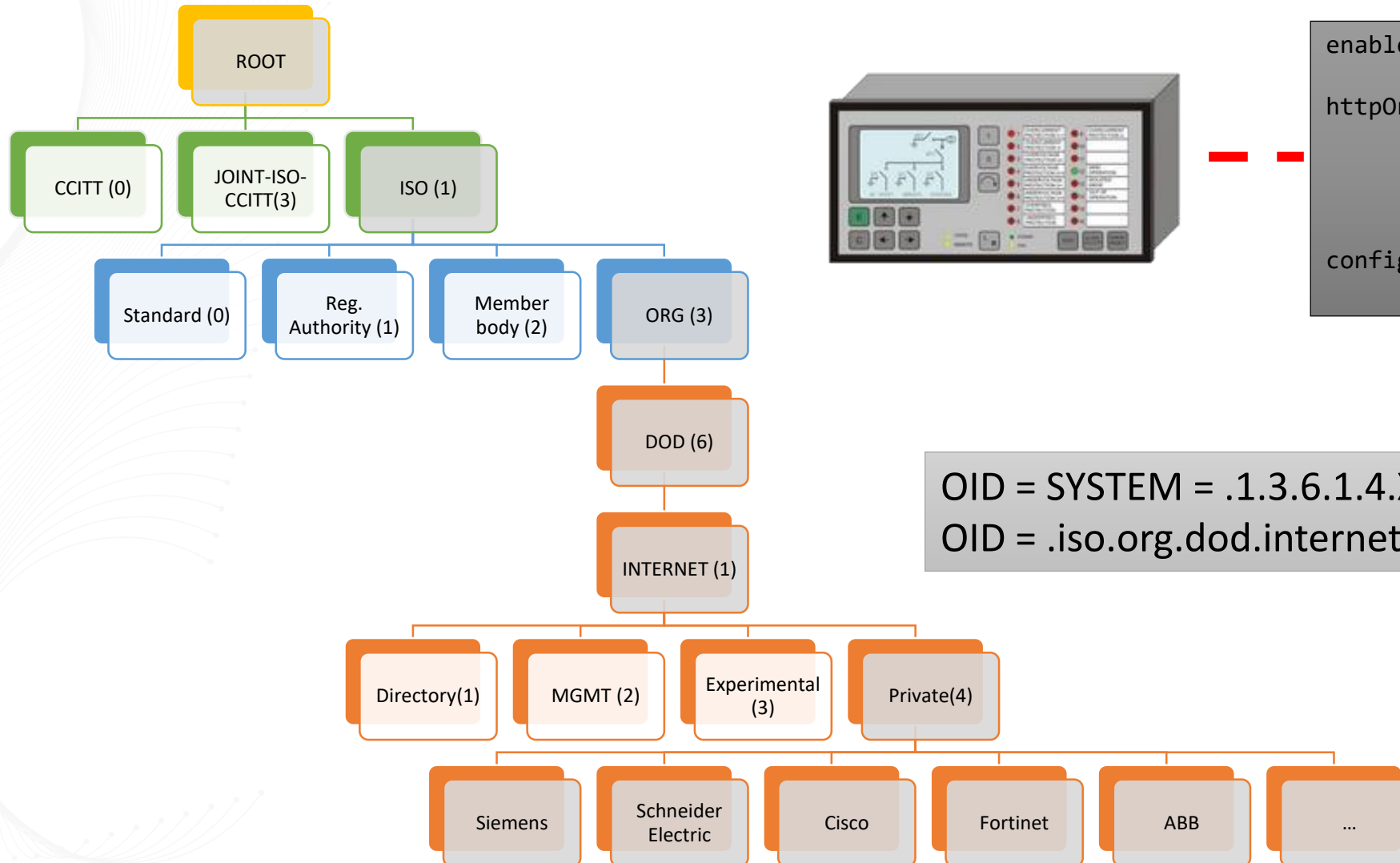
ATAQUE: GREYENERGY



Detección de TTP

Detección de TTP

Uso de SNMP para alteración de parámetros



```
enableWebXXXXXX OBJECT-TYPE
    SYNTAX INTEGER { disable(0),
httpOrHttps(1), httpsOnly(2) }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This enable the Web.
configuration function."
    ::= {xxxxxxx Y }
```

OID = SYSTEM = .1.3.6.1.4.XXXX.X

OID = .iso.org.dod.internet.private.ENTERPRISE.XXX

Detección de TTP

Uso de SNMP para alteración de parámetros

```

..
internet    OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
private     OBJECT IDENTIFIER ::= { internet(1) 4 }
Enterprise  OBJECT IDENTIFIER ::= { private(4) 1 }

```

El MIB nos indica la jerarquía o el path completo del OID, siguiendo los **OBJECT IDENTIFIER** 1.3.6.1.4.ENTERPRISE.1

```

...
command OBJECT IDENTIFIER ::= { enterprise 1 }
command OBJECT IDENTIFIER ::= { enterprise 2 }

```

...

```

reboot OBJECT-TYPE
    SYNTAX INTEGER {
        reboot (1) – reboot unit (using startup configuration)
    }

```

ACCESS read-write

STATUS current

DESCRIPTION

“Writing value ‘1’ will reboot the unit. (The unit will boot up using the startup configuration).

Reading the reboot object will return ‘0’ (zero) ”

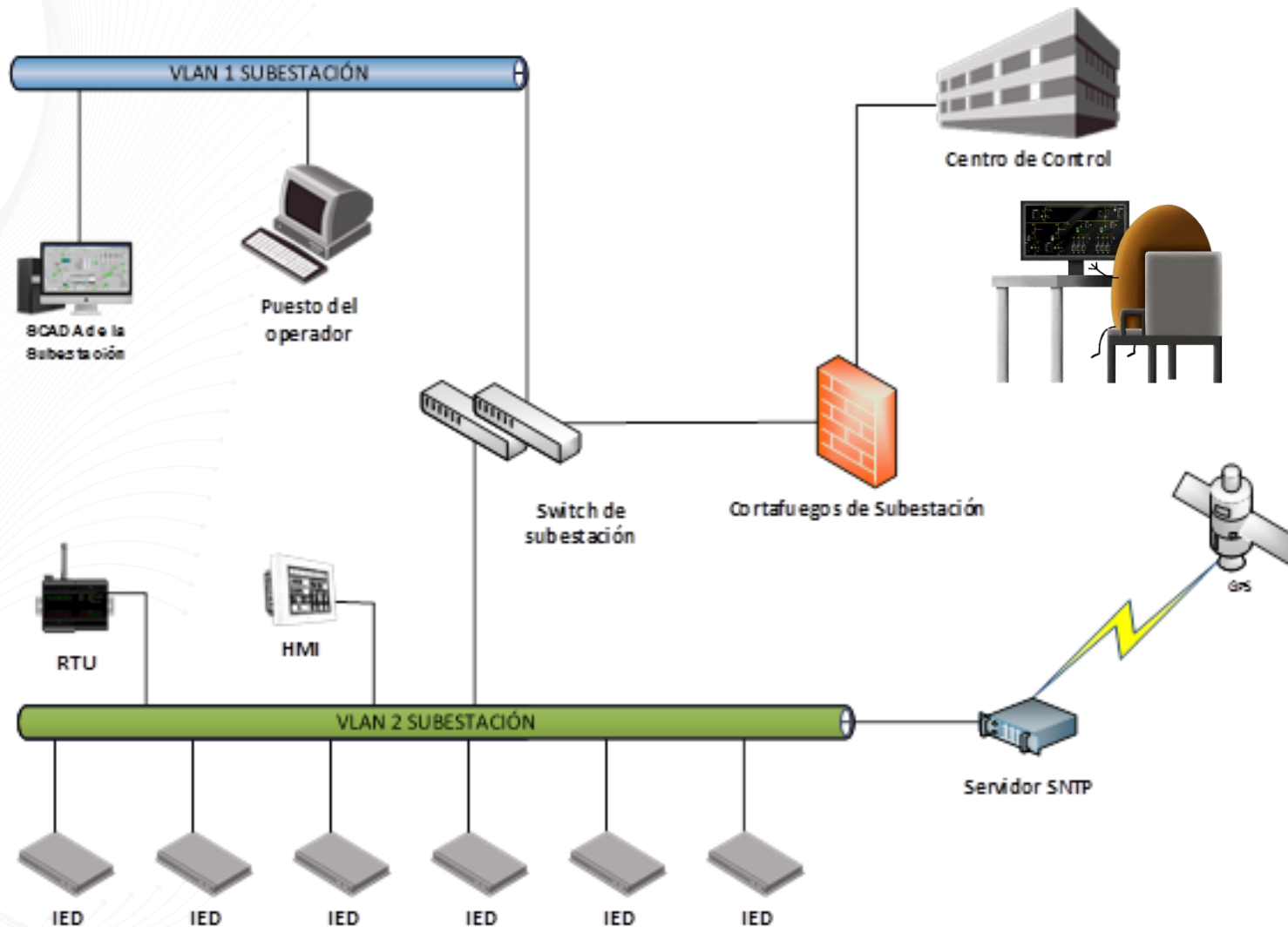
::= { command 1 }

Access ::= "read-write"
| "read-only"
| "write-only"
| "not-accessible"

Status ::= "current"
| "mandatory"
| "optional"
| "....."

Detección de TTP

Uso de SNMP para alteración de parámetros



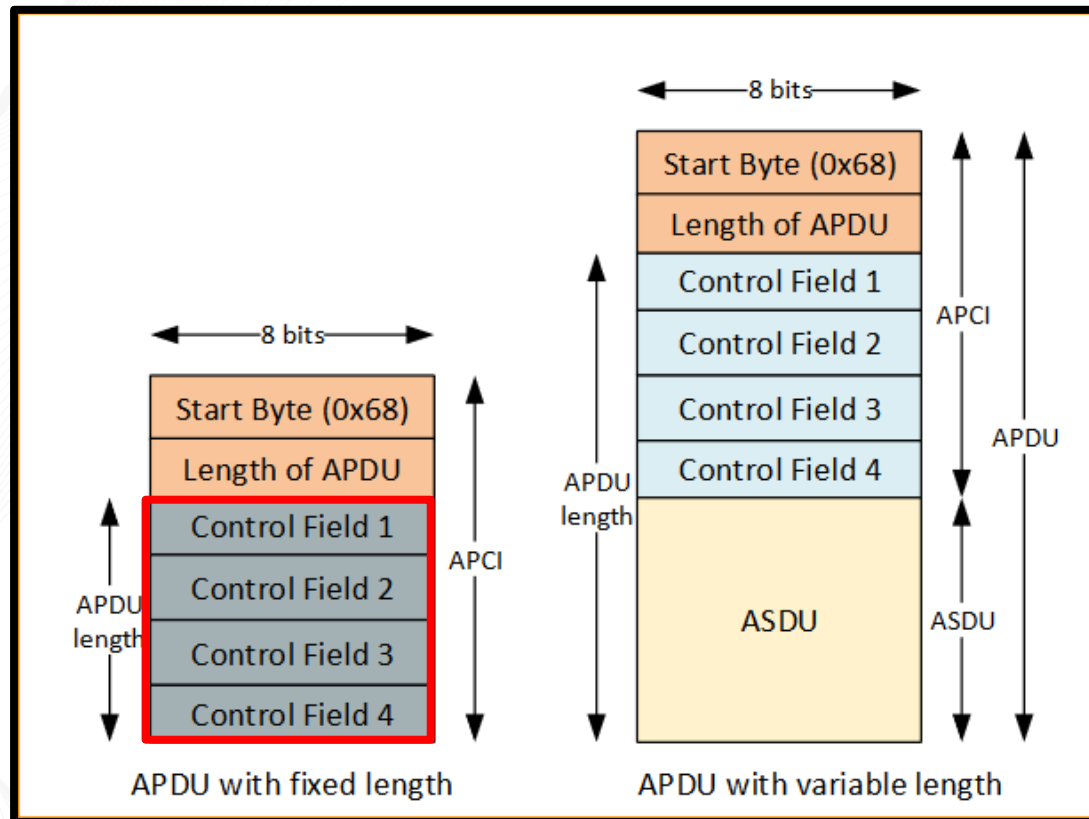
SNMP

-  Versión SNMP
-  Comunidad pública y privada
-  Árbol de MIB (Management Information Base)
-  Cambio de valor de en objetos OID
-  Exploits específicos



DEMO

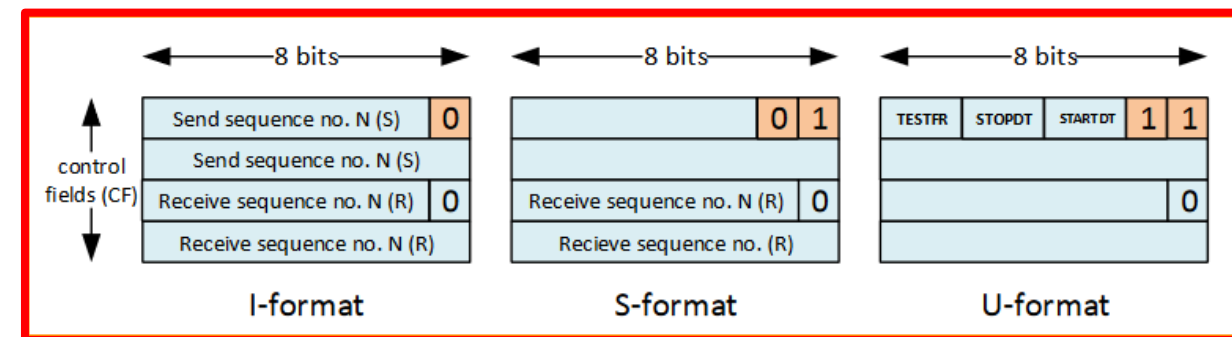
Detección de TTP



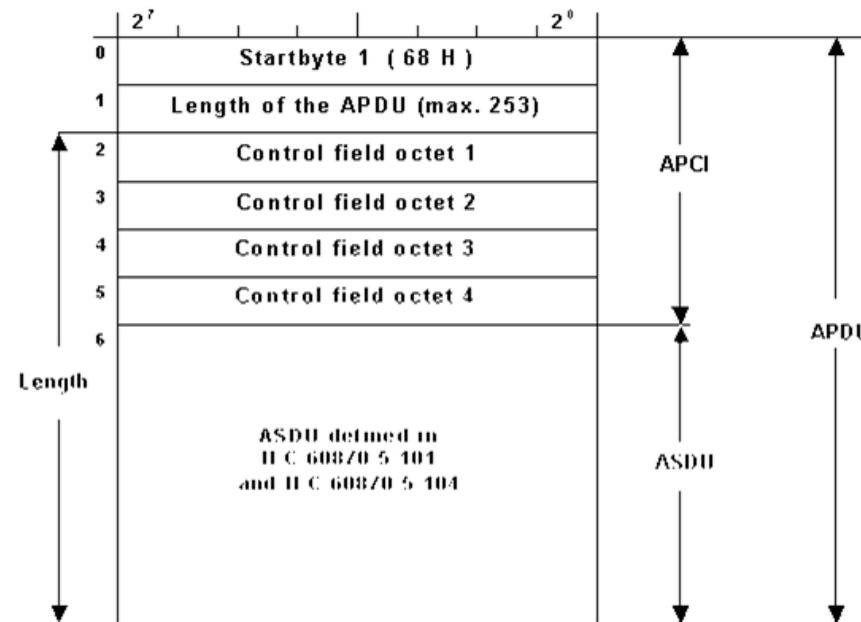
Selected application functions	User process
Selection of Application Service Data Units (ASDU) of IEC 60870-5-101 and 104	Application Layer (L7)
Application Protocol Control Information (APCI)	Transport Layer (L4)
Selection of TCP/IP Protocol Suite (RFC 2200)	Network Layer (L3)
	Link Layer (L2)
	Physical Layer (L1)

Existen 3 tipos de campo de control:

- **I-format** (trama con longitud variable)
- **S-format** (trama con longitud fija)
- **U-format** (trama con longitud fija para funciones *TESTFR*, *STOPDT* o *STARTDT*)



Detección de TTP

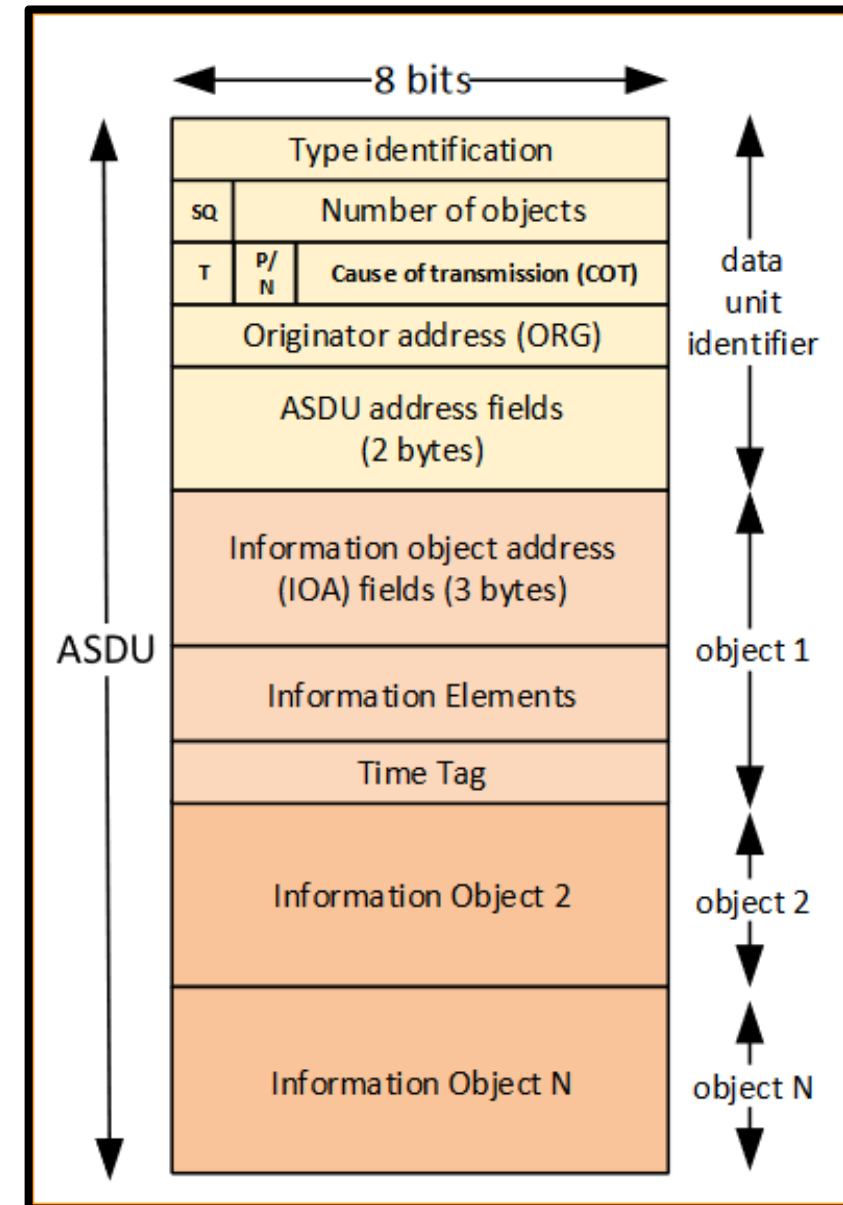


http://www.mayor.de/lian98/doc.en/html/u_iec104_struct.htm

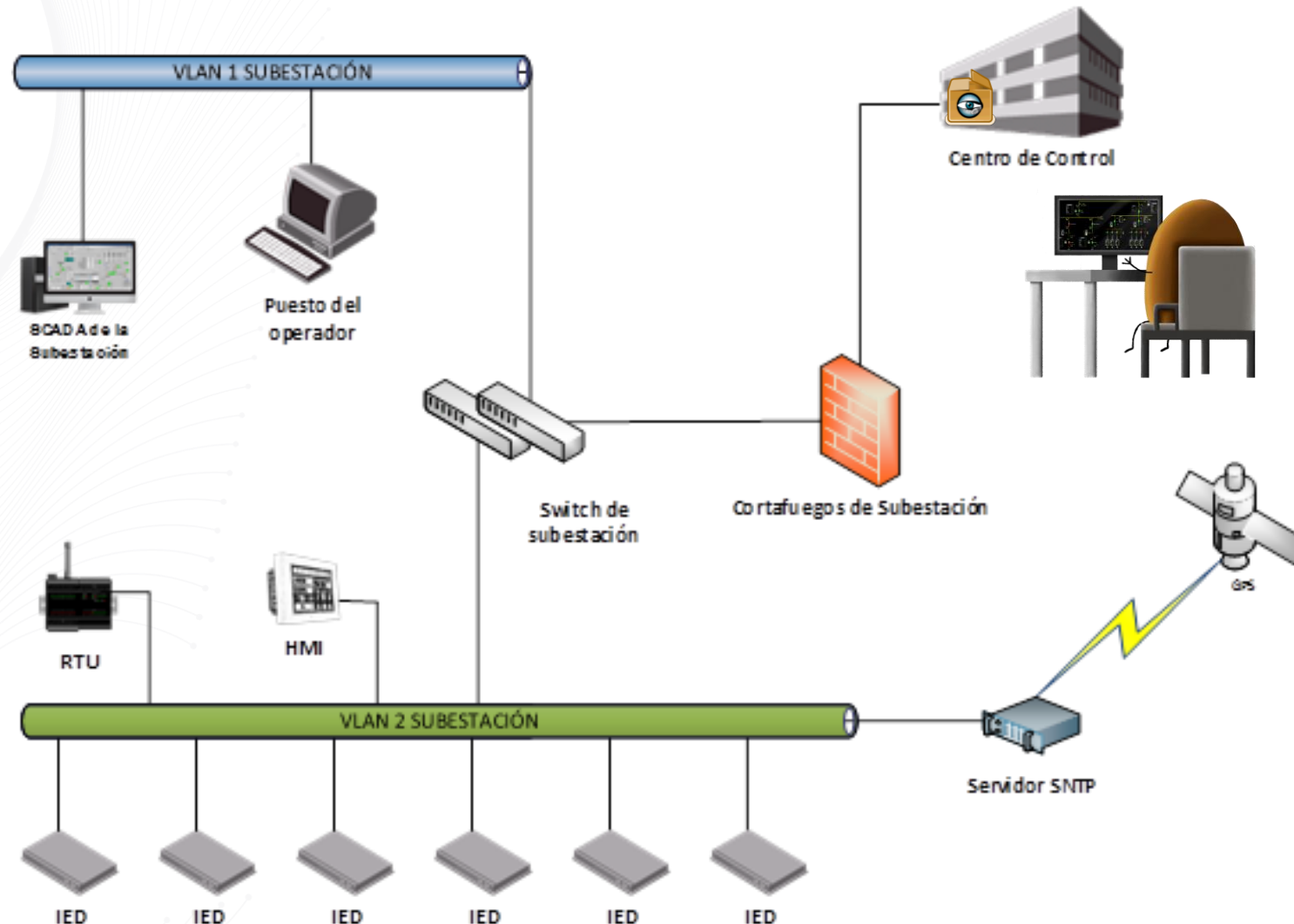
APCI - Application Protocol Control Information

APDU - Application Protocol Data Unit

ASDU - Application Service Data Unit

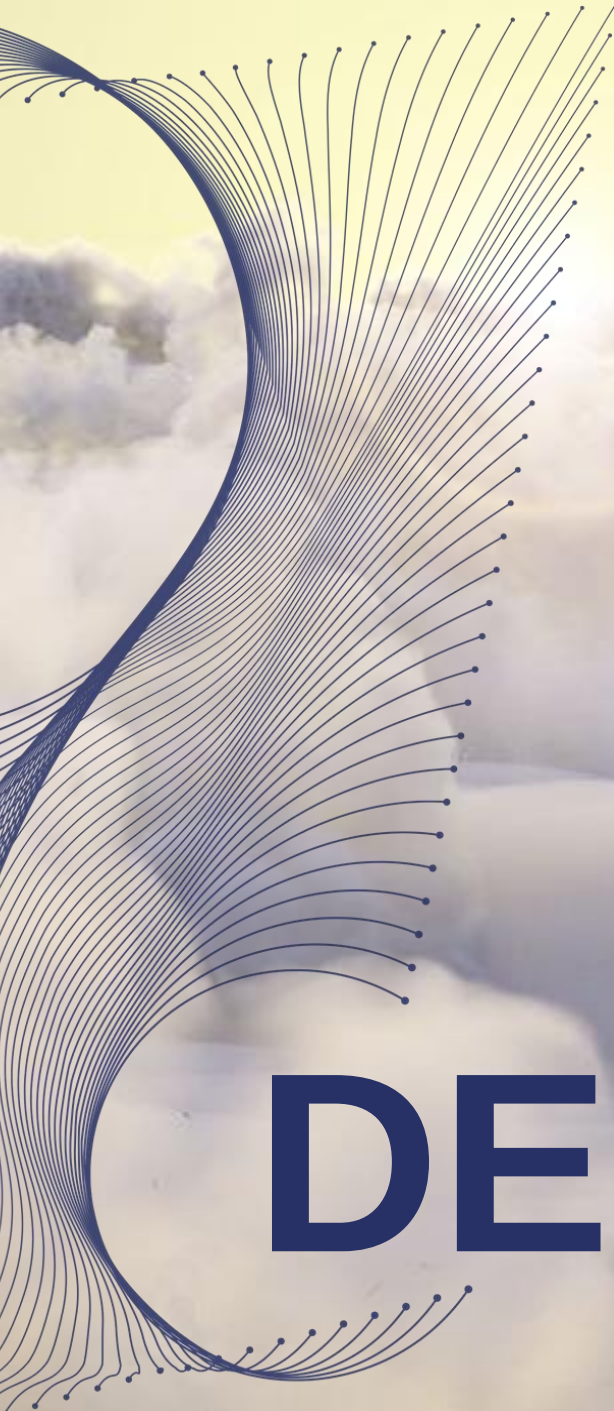


Detección de TTP



IEC-104

-  Reinyección de tramas
-  Denegaciones de servicio
-  Man in the Middle
-  Inyección de comandos
-  Ataques específicos con IOAs



DEMO

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional