

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Descontrol industrial, el enemigo invisible



- Aarón Flecha Menéndez
- s21sec
- aflecha@s21sec.com



Índice

- 1. Ataques recientes**
- 2. Debilidades en la red**
- 3. Defendiendo la red**
- 4. DEMO**

ATAQUES RECIENTES





BlackEnergy

EVOLUCIÓN



Segunda versión del Malware con **nuevas funcionalidades** (rootkits, robo de datos, envío de spam, etc.)

BlackEnergy última versión
Nuevas funcionalidades con características destructivas y de sabotaje (KillDisk).

Ciberataque a Ucrania

23/12/2015



2007

2008

2010

2014

2015

DETECTADO

Malware creado con el **objetivo de realizar ataques DDoS.**

Sus objetivos principales fueron **Europa del Este y Norteamérica.**

C&C detectados en Rusia



BlackEnergy Lite y BlackEnergy Big

Modificación del método de carga para dificultar su detección

Publicación de vulnerabilidades asociados a Office

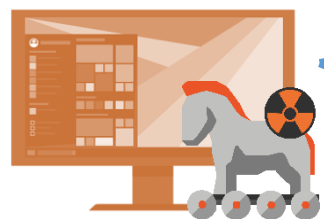
CVE-2014-4114 (Powerpoint)

CVE-2014-1761 (Word)





BlackEnergy



Aplicación
troyanizada

msiexec.exe



Componente
persistente



Aplicación
sin infección

msiexec.exe



Componente
persistente



Instalador
falso



Componente
NO
persistente



Documento
troyanizado

Documento
señuelo



Dropper
malware

msiexec.exe



Componente
persistente

Documento
señuelo





Troyano

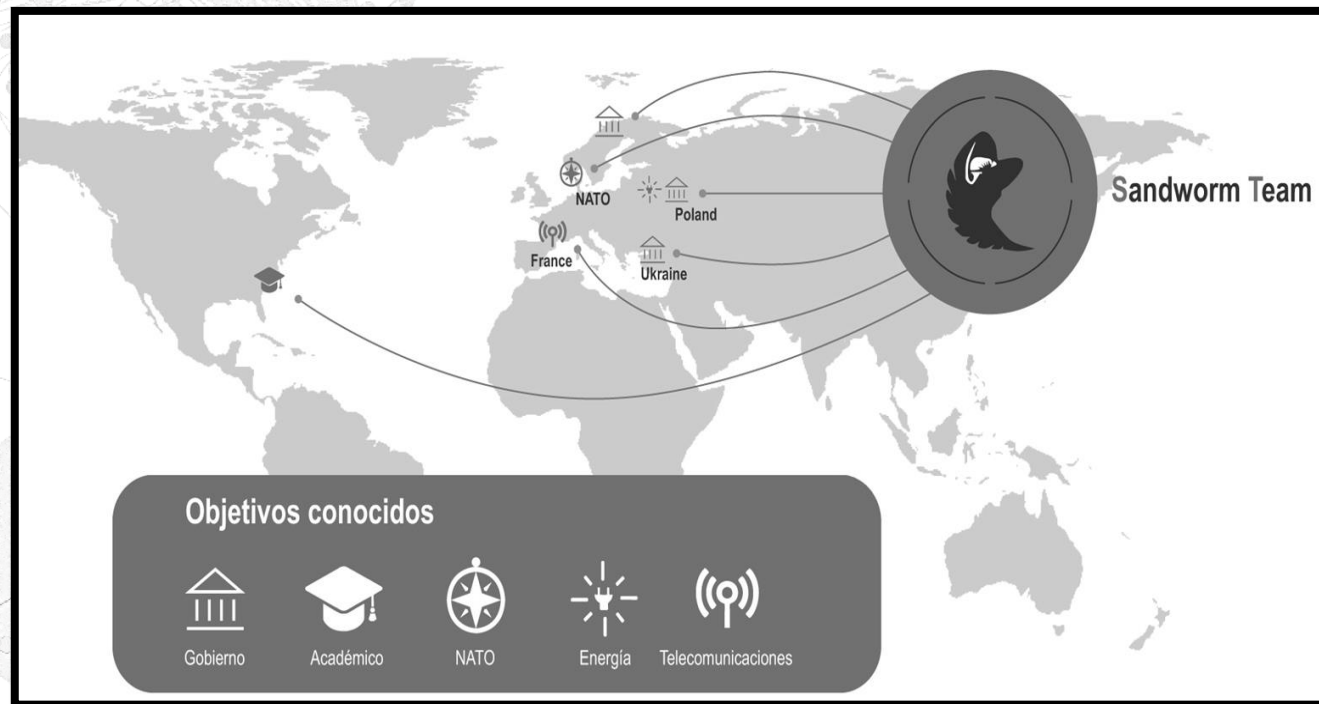
Evolución sufrida



APT

Extensiones de archivos afectados

Files
.crt .bin .exe .db .db .pdf .djvu .doc .docx .xls .xlsx .jar .ppt .pp
.tx .tib .vhd .iso .lib .mdb .accdb .sql .mdf .xml .rtf .ini cfg .boot
.txt .rar .msi .zip .jpg .bmp .jpeg .tiff



 **SandWorm**
(a.k.a. Electrum)


**Grupo de
cibercriminales
asociado a Rusia**

**Además de poseer un amplio
conocimiento en desarrollo
malware, también poseen
conocimiento sobre
infraestructuras críticas
(especialmente las existentes
en el sector eléctrico)**





<https://www.certs.es/blog/blackenergy-sistemas-criticos>




TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

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

BLACKENERGY & QUEDAGH

The convergence of crimeware and APT attacks

TLP: WHITE

CONTENTS

Introduction	2
Attack overview	2
Infection vectors	3
Target details	4
2008 cyberattacks on Georgia?	4
Ukraine-related proxies	4
Timeline	6
Technical details	8
UAC bypass during installation	8
Driver signing policy bypass	8
Hijacking existing drivers	9
Driver component	9
Main DLL component	10
BlackEnergy 3	10
Information-stealing plugin	11
Network traffic	12
Conclusions	13
Appendix A Samples	14

BlackEnergy is a toolkit that has been used for years by various criminal outfits. In the summer of 2014, we noted that certain samples of BlackEnergy malware began targeting Ukrainian government organizations for information harvesting. These samples were identified as being the work of one group, referred to in this document as "Quedagh", which has a history of targeting political organizations.

The Quedagh-related customizations to the BlackEnergy malware include support for proxy servers and use of techniques to bypass User Account Control and driver signing features in 64-bit Windows systems. While monitoring BlackEnergy samples, we also uncovered a new variant used by this group. We named this new variant BlackEnergy 3.

The use of BlackEnergy for a politically oriented attack is an intriguing convergence of criminal activity and espionage. As the kit is being used by multiple groups, it provides a greater measure of plausible deniability than is afforded by a custom-made piece of code.

F-SECURE LABS SECURITY RESPONSE
Malware Analysis
Whitepaper



https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

SentinelOne

Analyzing a New Variant of BlackEnergy 3

Likely Insider-Based Execution

By Udi Shamir

EXECUTIVE SUMMARY

Note - While writing this report (1/26/2016) a new attack has just been detected, targeting a Ukrainian power facility. The attack vector appears to be the same variant analyzed in this report. We'll provide more details in a subsequent analysis.

BlackEnergy was first reported in 2007 (named BlackEnergy 1) and at the time was a relatively simple form of malware that generated random bots to support Distributed Denial of Service (DDoS) attacks. A few years later, in 2010, BlackEnergy 2 emerged with some significant capabilities that extended beyond DDoS - most notably a new plugin architecture that allowed BlackEnergy to subvert system resources and perform other activities such as data exfiltration, and network traffic monitoring. It was at this time that many began to associate BlackEnergy with crimeware. Our analysis of a new BlackEnergy 3 sample has led us to conclude that this latest rootkit is in fact the byproduct of a nation-sponsored campaign, and likely the work of multiple teams coming together. It should be noted that Eight Partners has already validated a link between BlackEnergy and the Sandworm Team. Therefore, this conclusion in and of itself is not necessarily noteworthy, rather it's the discover of a new tactic that's now been employed targeting specific individuals running Microsoft Office.

In this particular sample the actor appears to have advanced a method used back in 2014 against Industrial Control Systems systems deployed in NATO countries, and more broadly across the European Union. At that time the actor used a vulnerability, CVE-2014-4114, in the OLE package 2 (package.dll) in the way it parses INF files. Each binary was compiled using different compiler versions, which led us to conclude that different groups are in fact directly involved in this campaign - much like a typical R&D project supported by different engineering teams who each follow their own unique development characteristics. These different characteristics have established unique fingerprints that ID each of the individual group's traits.

Traditional antivirus software vendors would have a difficult time detecting this particular type of attack given the constantly changing attack vectors even though they are still rooted to the same core components. For example, the actor can choose to drop the same binaries packed with different FUD (Fully Undetected) using different Excel documents.

It's expected that this particular sample is already resident in many systems across the Ukraine, and likely other nations in Europe which could lead to more blackouts and "mysterious" malfunctions within major utilities, transportation systems, and even healthcare institutions. There may be different variants of BlackEnergy used within each of these environments, but they all originate from the same common core.

INTRODUCTION

Execution of this particular BlackEnergy 3 attack vector is likely the work of an internal actor, especially in the case of SCADA systems. This is due to the fact that Office 2013 has already been patched against CVE-2014-4114. The only two options then to carry out the attack is - target a victim's machine that was not patched, or get an internal employee to either accidentally or deliberately execute the infected Excel documents causing the malware to propagate inside the network. At this point it would be highly unlikely that organizations have not deployed the patch against CVE-2014-4114, thus the most likely conclusion is use of an internal actor.

WHITEPAPER

©2016 SentinelOne. All Rights Reserved.

https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf



Dragonfly 2.0



```
const usage = `\\ \\ \\ \\ \\ 0
| \\  o  \\  o  _ _ _ / _ ( ) _ / _ _ _ _ _
> _ (( < _ o0 / _ \\ _ \\ / _ _ \\ _ \\ _ / _ /
| / \\ _ + _ / / _ / / / / / ( _ ) / / _ / / / /
| / _ / / _ / _ _ / _ / _ / _ / _ / _ / _ /
/_ / Basic Auth Credential Harvester ( _ /
    with Word Doc Template Injector

Start the server : phishery -s settings.json -c credentials.json
Inject a template : phishery -u https://secure.site.local/docs -i good.docx -o bad.docx

Options:
-h, --help      Show usage and exit.
-v              Show version and exit.
-s              The JSON settings file used to setup the server. [default: "settings.json"]
-c              The JSON file to store harvested credentials. [default: "credentials.json"]
-u              The phishery URL to use as the Word document template.
-i              The Word .docx file to inject with a template URL.
-o              The new Word .docx file with the injected template URL.
-k              Disable TLS support.
```

<https://github.com/ryhanson/phishery>

Family	MD5	Command & Control
Backdoor.Dorshel	b3b5d67f5bbf5a043f5bf5d079dbcb56	hxxp://103.41.177.69/A56WY
Trojan.Karagany.B	1560f68403c5a41e96b28d3f882de7f1	hxxp://37.1.202.26/getimage/622622.jpg
Trojan.Heriplor	e02603178c8c47d198f7d34bcf2d68b8	
Trojan.Listrix	da9d8c78efe0c6c8be70e6b857400fb1	
Hacktool.Credrix	a4cf567f27f3b2f8b73ae15e2e487f00	
Backdoor.Goodor	765fcd7588b1d94008975c4627c8feb6	
Trojan.Phisherly	141e78d16456a072c9697454fc6d5f58	184.154.150.66
Screenutil	db07e1740152e09610ea826655d27e8d	

<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>

Motivaciones de los ataques:



Sabotaje



Obtención de información sensible

Vectores de ataque utilizados:



Spear Phishing



Software troyanizado



Watering Hole



Dragonfly 2.0

Países 2011



EE.UU.



Canadá

Sectores afectados



Defensa



Aviación

Países 2014



Italia



EE.UU.



Francia

Sectores afectados

Energía



Países 2017



EE.UU.



Suiza



Turquía

Sectores afectados

Energía



RESUMEN



OBJETIVOS



Dragonfly

(a.k.a. Energetic Bear)



**Grupo de
ciberdelinquentes
asociado a Rusia**

🎯 **Sector transporte (aviación)– EE.UU. y Canadá (2011)**

🎯 **Sector defensa– EE.UU. y Canadá (2011)**

🎯 **Sector energía– EE.UU. y Europa (España, Francia, Italia, Alemania, Turquía, Polonia)**

- Operadores de redes eléctricas
- Principales empresas generadoras de electricidad
- Industria energética, empresas manufactureras que proporcionan dispositivos para Sistemas de Control Industrial (SCI)

Amplios conocimientos de desarrollo malware a medida (Oldred, a.k.a Havex) y de diferentes sectores industriales

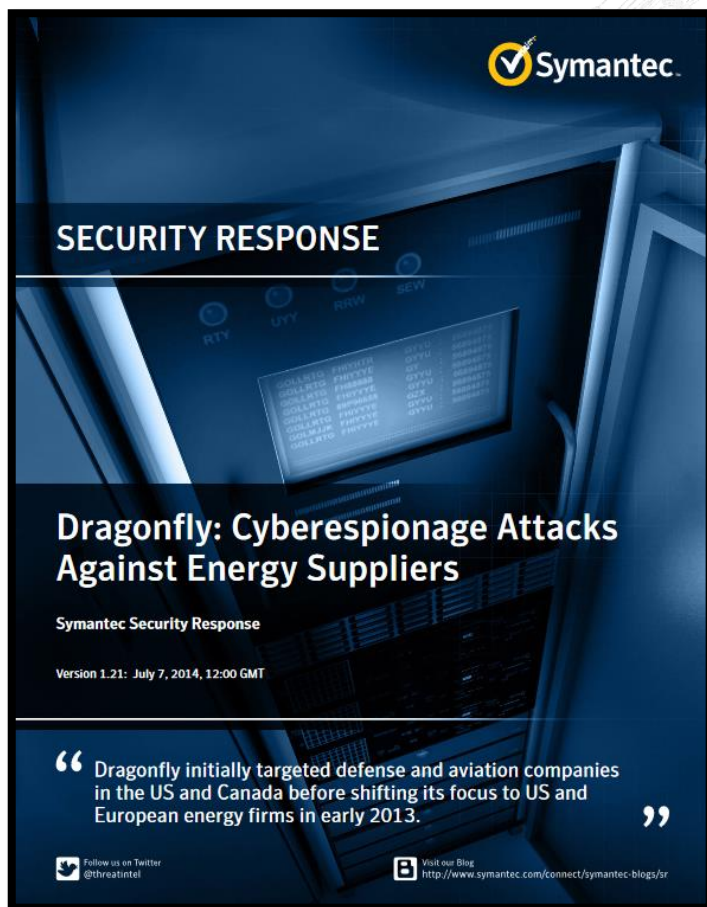
Más información sobre Havex



<https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf>



INFORMES



http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

NOTICIAS

Dragonfly: Western energy sector targeted by sophisticated attack group

Resurgence in energy sector attacks, with the potential for sabotage, linked to re-emergence of Dragonfly cyber espionage group.

<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>

Dragonfly 2.0: Hacking Group Infiltrated European and US Power Facilities

<https://thehackernews.com/2017/09/dragonfly-energy-hacking.html>

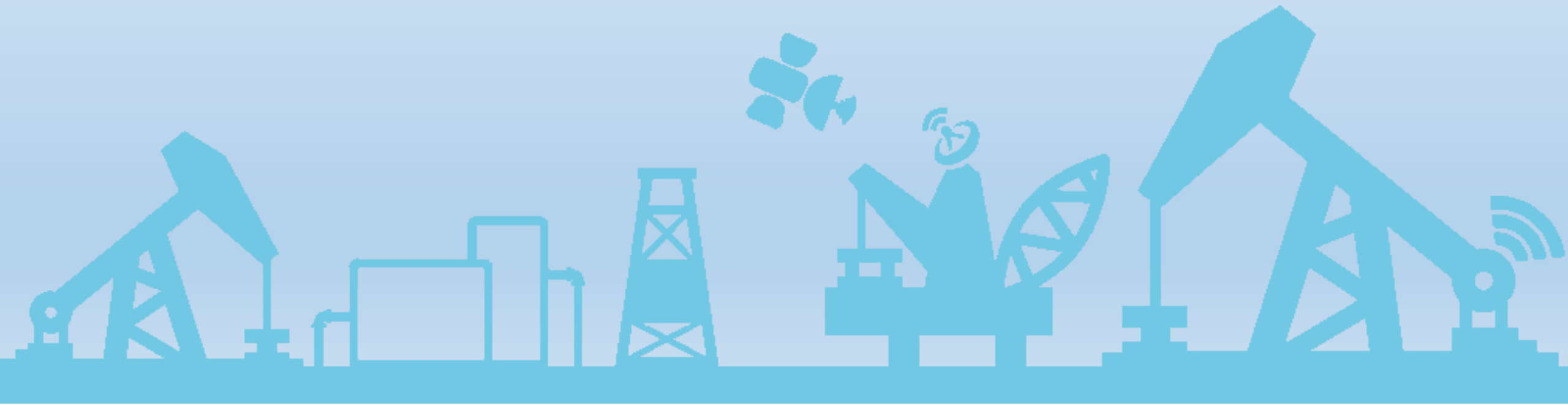
Dragonfly 2.0: nueva campaña de intrusión en sector eléctrico

06/09/2017

Una nueva campaña conocida como Dragonfly 2.0 está atacando con el objetivo de infiltrarse en infraestructuras del sector energético en Turquía, Suiza y Estados Unidos. La empresa de seguridad Symantec ha dado a conocer esta nueva versión de Dragonfly como ya ocurriera anteriormente, informando que esta nueva oleada lleva operativa desde diciembre de 2015. En esta campaña los atacantes están utilizando diferentes vectores para lograr acceso a las empresas del sector energético como por ejemplo emails maliciosos con los que realizan intentos de phishing o en los que adjuntar archivos que contienen troyanos. Además, se valen de "backdoors" instaladas previamente para tener acceso directo a los sistemas afectados, además de otros "toolkits" para gestionarlos

<https://www.certs.es/alerta-temprana/bitacora-ciberseguridad/dragonfly-20-nueva-campana-intrusion-sector-electrico>

DEBILIDADES EN LA RED





Historizador

Estación de ingeniería

HMI

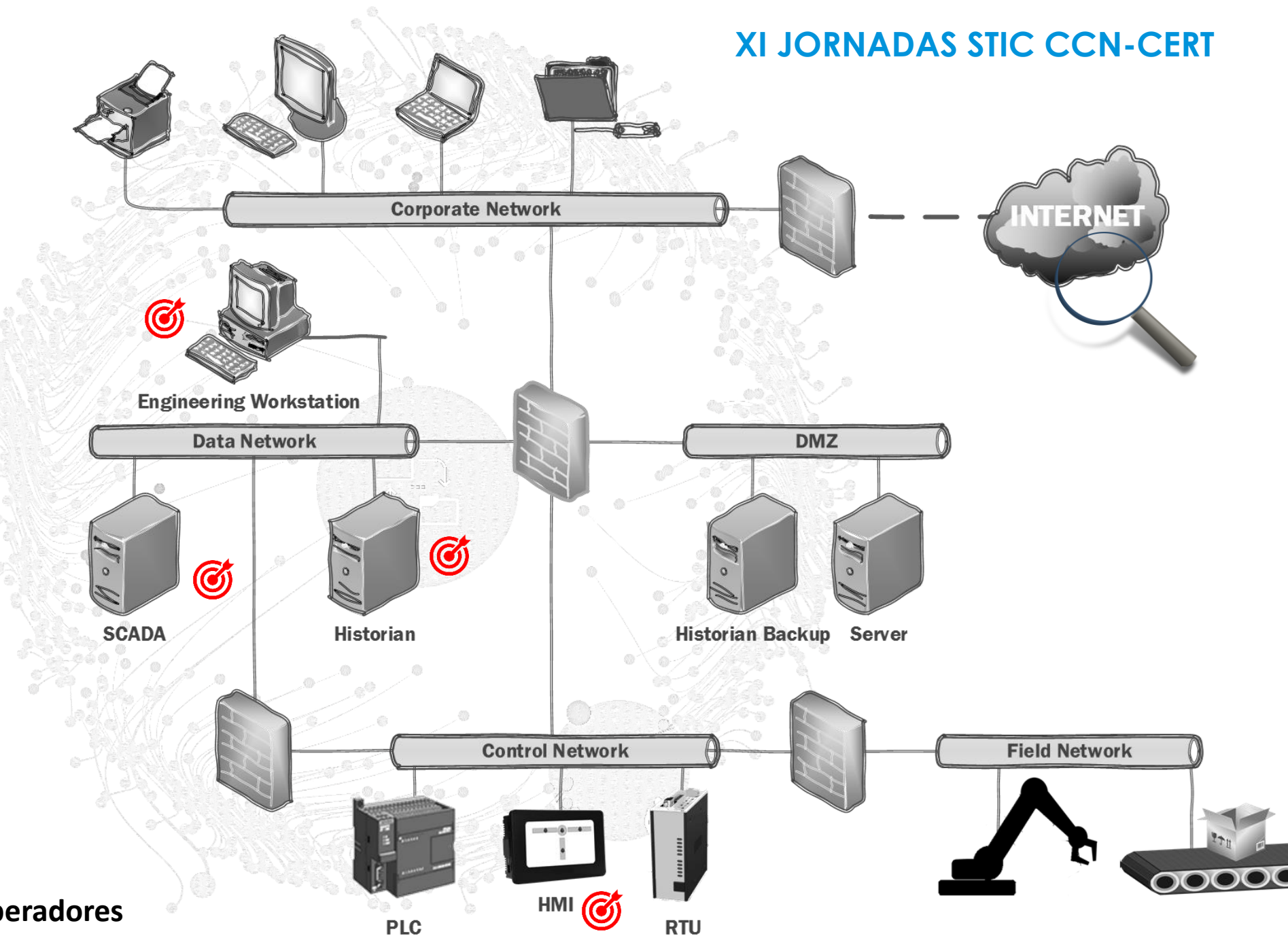
SCADA



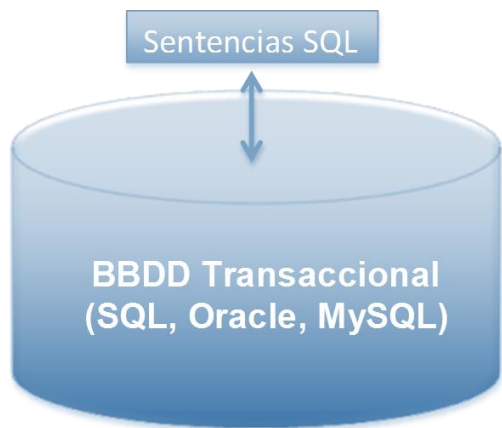
OTROS



Ordenadores de operadores

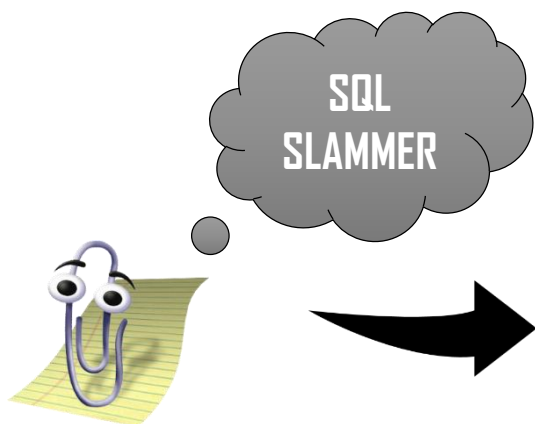


Historizador



➡ Guarda y almacena todos los datos del proceso, estados de variables (digitales y analógicas) y en general, cualquier tipo de información que sea generada en un proceso industrial.

➡ Algunas empresas basan sus producciones en la información que recopila el historizador día a día.



Sistemas afectados:

- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000
- Any application that includes MSDE



- Central nuclear de Davis-Besse en Ohio
- Compañía de ferrocarriles CSX en EE.UU



Estación de ingeniería



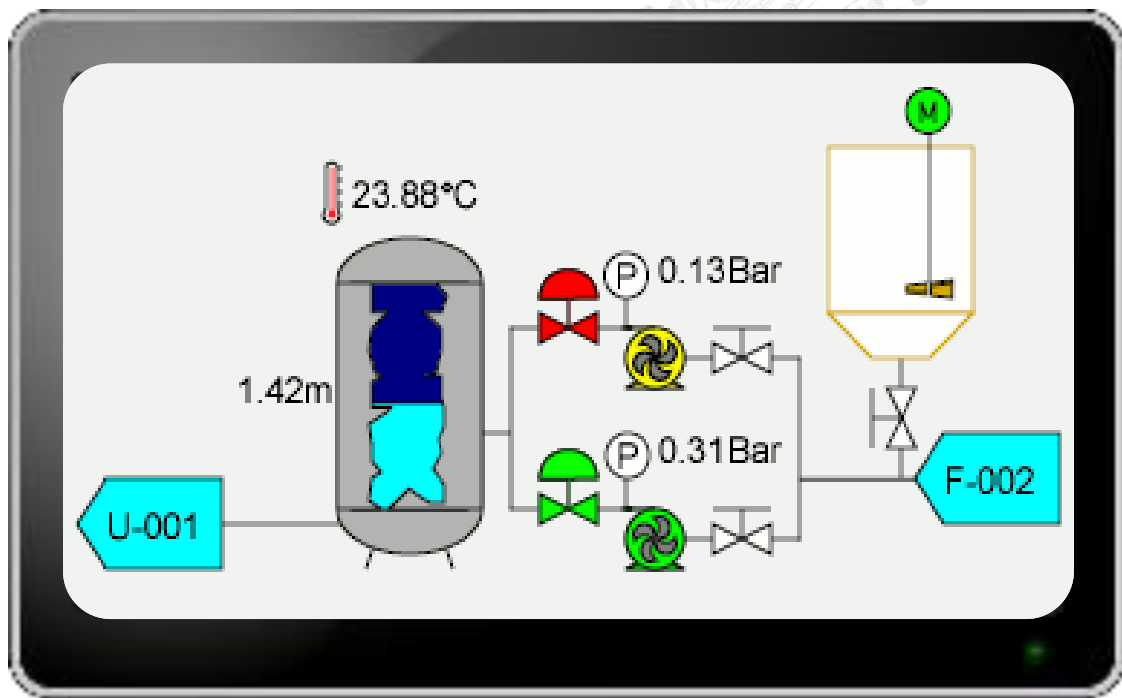
➡ **Control sobre la programación que se posee de los PLC, RTU, HMI y otros dispositivos.**

➡ **Almacenamiento de ficheros de configuración que poseen la programación de muchos dispositivos.**

➡ **Estación de ingeniería / Equipos de programación**

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.

Información de interés:

<https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf>

Supervisory Control and Data Acquisition system



- ➡ Realiza acciones de supervisión, control y gestión de información en tiempo real.
- ➡ Permiten una centralización de señales generadas por uno o varios procesos industriales (control de alertas).
- ➡ Se comunica con multitud de dispositivos ubicados en la red de control (PLC, RTU, HMI, etc.)

DEFENDIENDO LA RED





**Actualizaciones y
aplicación de parches
de seguridad**



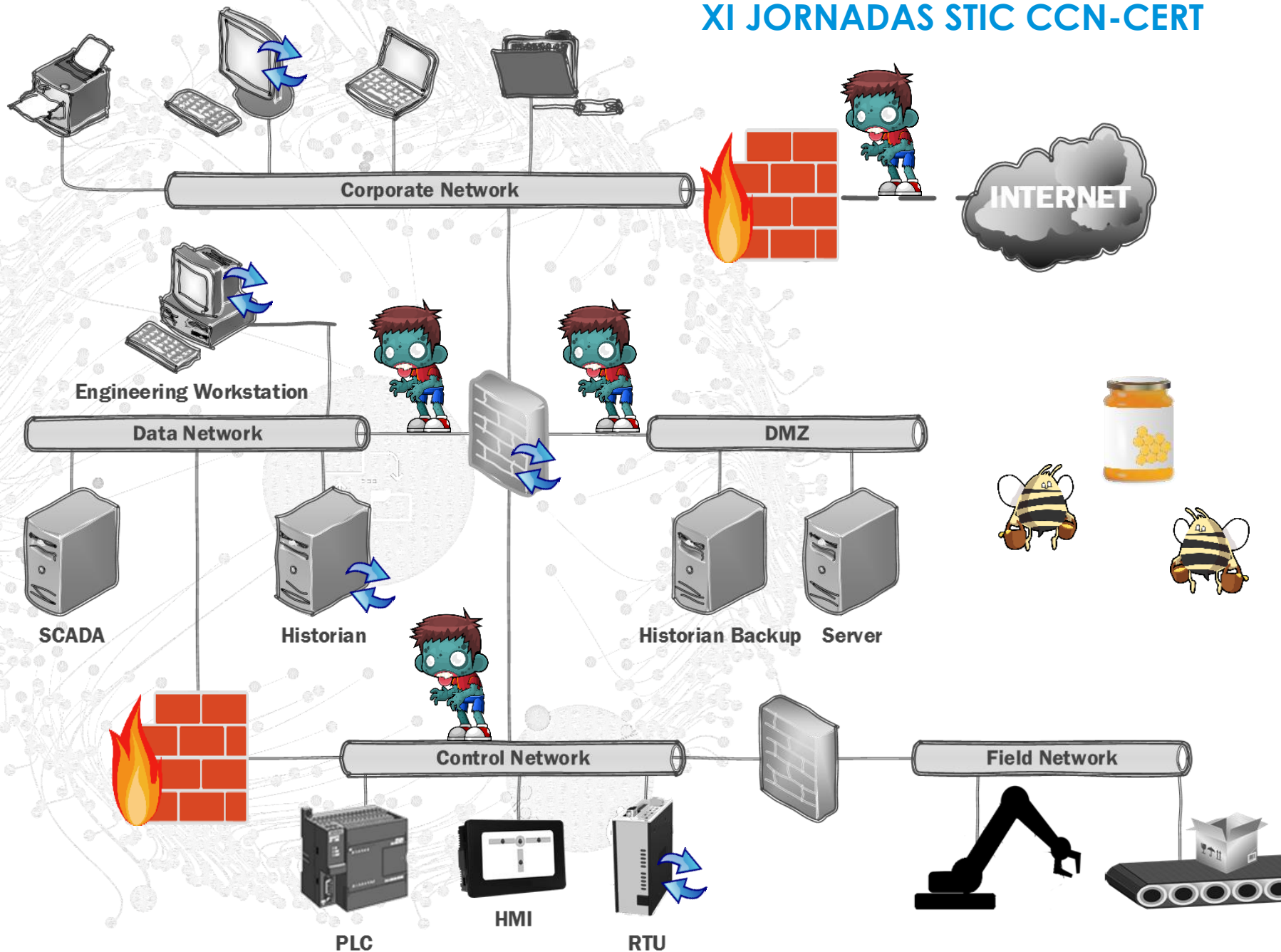
Honeypots



**Uso de dispositivos
(Firewalls, IDS,
Diodos de datos, etc.)**



**Prevención
Antimalware
(sandboxing,
reputación de IPs o
dominios, whitelisting
de aplicaciones, etc.)**



Herramientas de monitorización proactivas



Sonda ubicado para obtener información de la red (port mirror o TAP) y enviarla a un panel central

Concienciación a los empleados

ESTRATEGIAS DE DEFENSA FRENTE A CIBERATAQUES EN SISTEMAS DE CONTROL Y AUTOMATIZACIÓN INDUSTRIAL **S21 SEC**

Conozca de primera mano las amenazas que afectan a los sistemas de control industrial y aprenda qué herramientas y estrategias le ayudan a asegurarlos teniendo en cuenta su particular naturaleza.

A QUIEN VA DIRIGIDO

Curso orientado principalmente a técnicos de seguridad de la información y personal técnico responsable de la seguridad lógica de los sistemas de automatización y control. Este curso también está indicado para profesionales como ingenieros de red, ingenieros SCADA/IACS, e integradores SCADA/IACS, con un background técnico de seguridad de la información y que quieran capacitarse en la seguridad digital de los sistemas de automatización y control.

SUMARIO

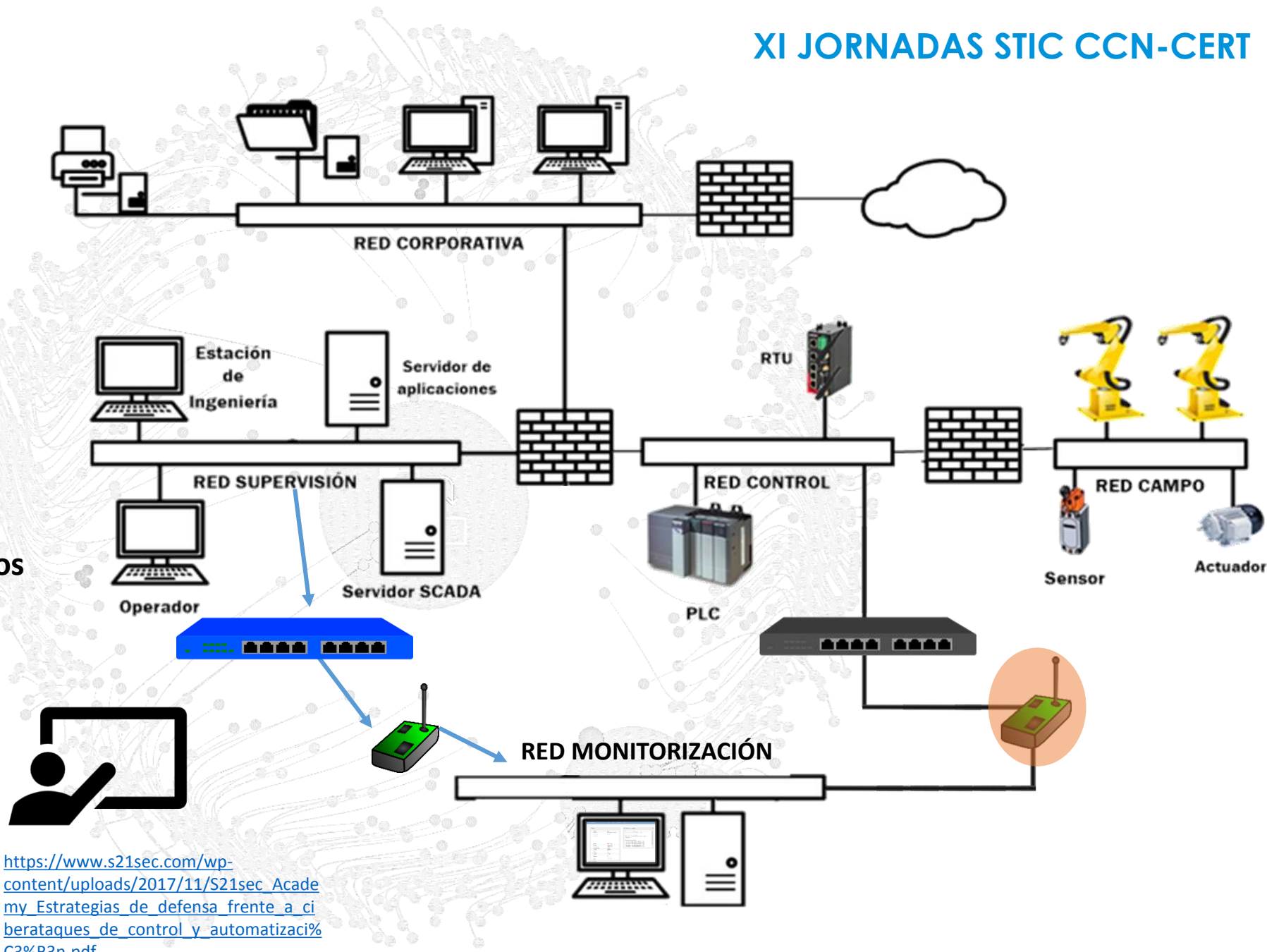
Curso de carácter técnico y práctico que se centra en los aspectos técnicos y tecnológicos más relevantes en la protección de aplicaciones, sistemas, infraestructura, y redes de control y automatización industrial.

En una primera fase se abordan los principales riesgos de seguridad que afectan a estas infraestructuras, tanto desde el interior como desde el exterior de las organizaciones. Se profundiza en el estudio de las principales vulnerabilidades a nivel de protocolos de control y automatización, de las arquitecturas de redes y sistemas, gestión y operación, así como en su diseño e implementación. La segunda fase de la formación aborda las distintas estrategias y requisitos de seguridad para el desarrollo e implementación de aplicaciones y sistemas de automatización y control industrial seguros teniendo en cuenta las buenas prácticas de ciberseguridad industrial, así como las distintas tecnologías de prevención, monitorización y protección específicamente diseñadas para estos entornos.

DURACIÓN DEL CURSO

4 días (24 horas).

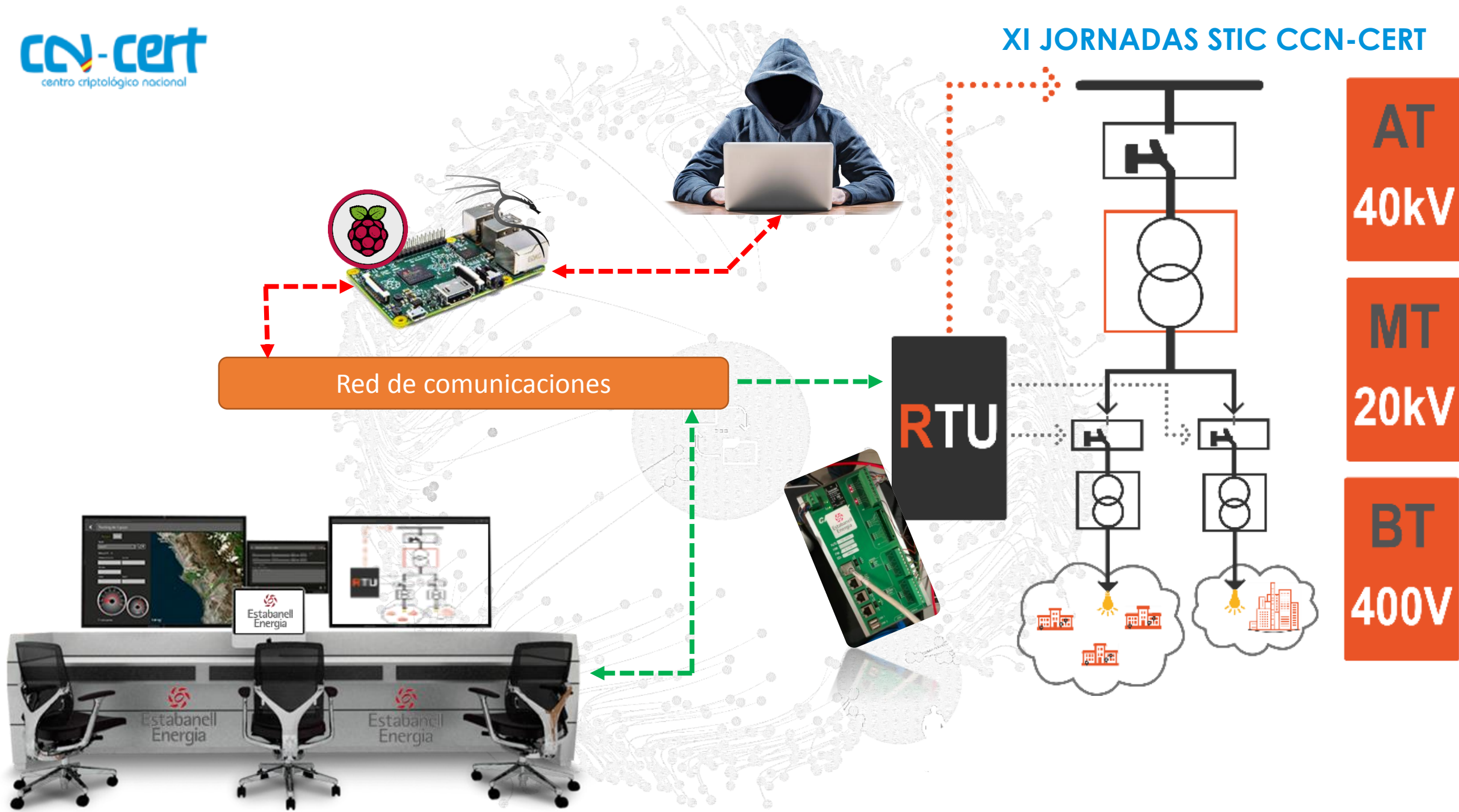
3 días (intensivo - 21 horas).

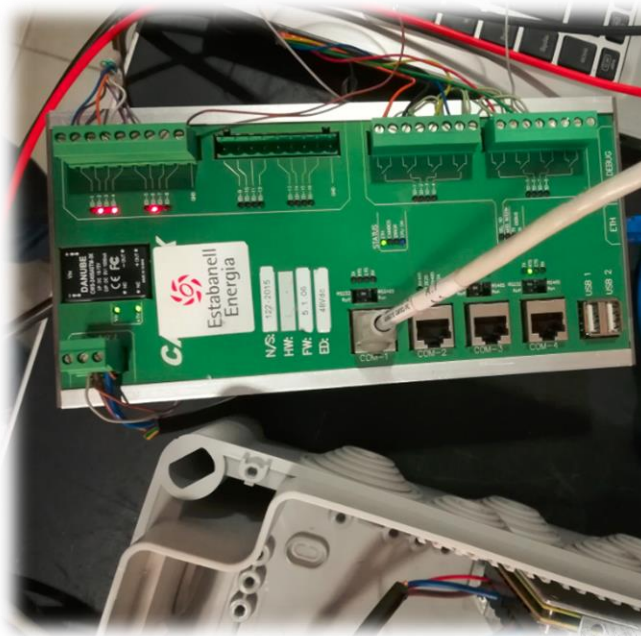


https://www.s21sec.com/wp-content/uploads/2017/11/S21sec_Academy_Estrategias_de_defensa_frente_a_ciberataques_de_control_y_automatizaci%C3%B3n.pdf



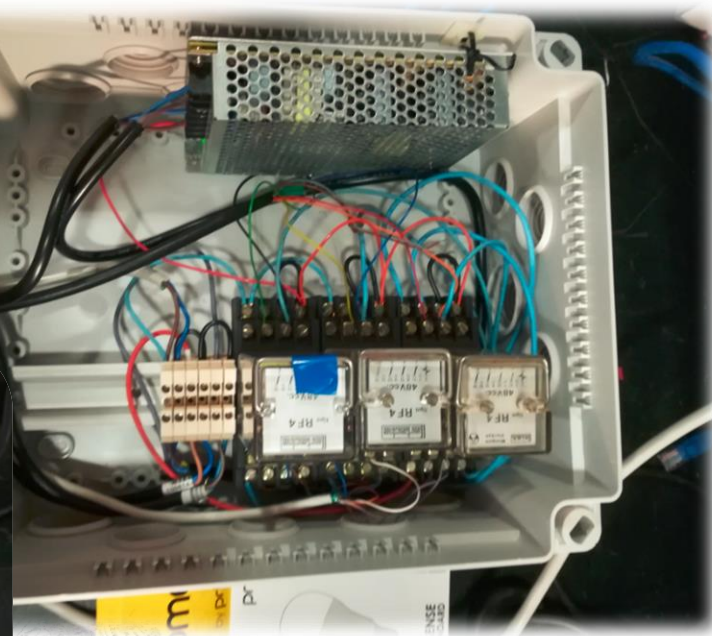
DEMO





León

Madrid



Granollers

Santander

Gijón

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

