

XI
JORNADAS
STIC
CCN-CERT

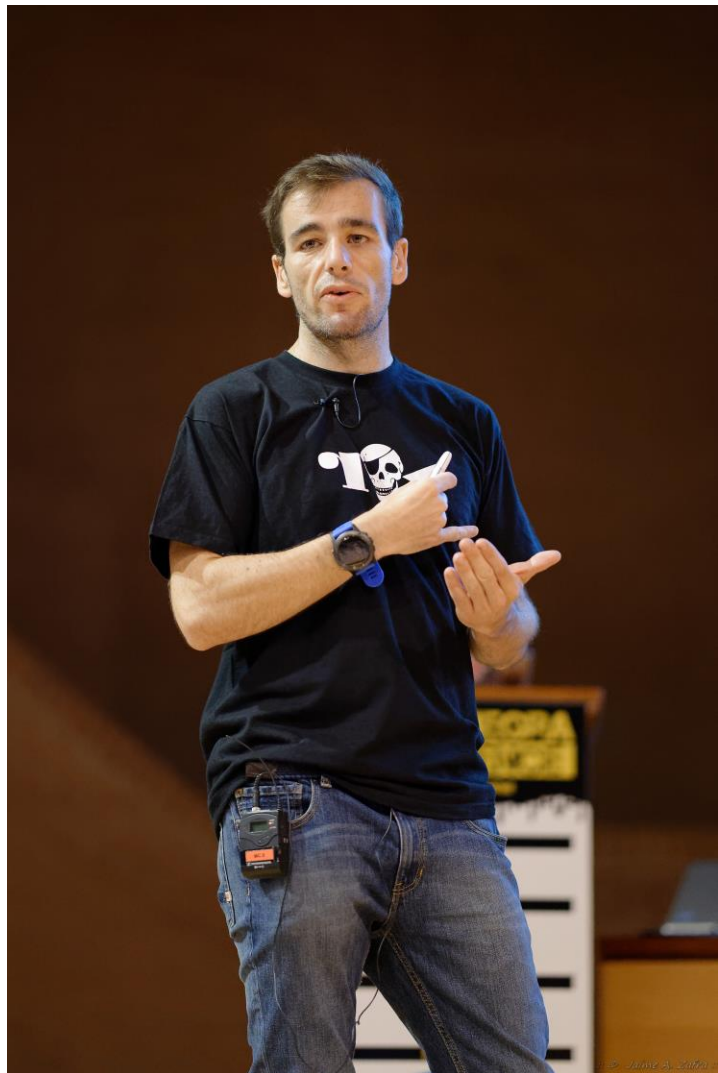
Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Radiografía de un ataque al suministro eléctrico

MANUEL BERMÚDEZ CASADO

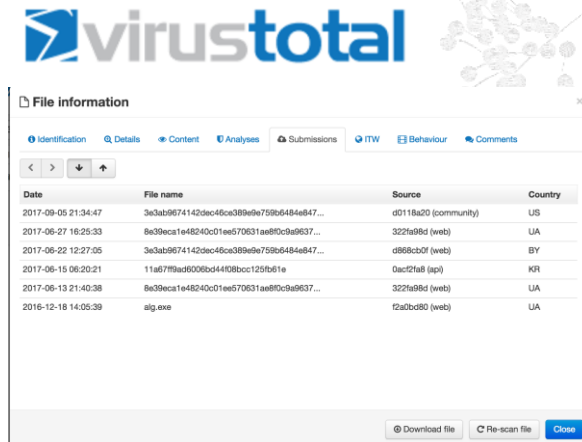
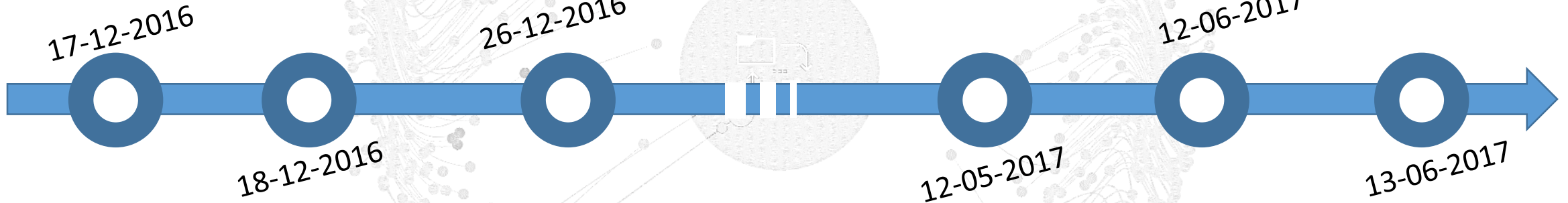


- Manuel Bermúdez Casado
- Enagás
- mbermudez@enagas.es

Agenda

- Timeline del ataque
- Descripción de un sistema Scada de los Grandes
 - Descripción del ataque
 - PoC1 Tomando el control del Backdoor
- PoC2 Apagando interruptores con IEC104

Timeline del ataque





DESCRIPCIÓN DE UN SISTEMA SCADA DE LOS GRANDES

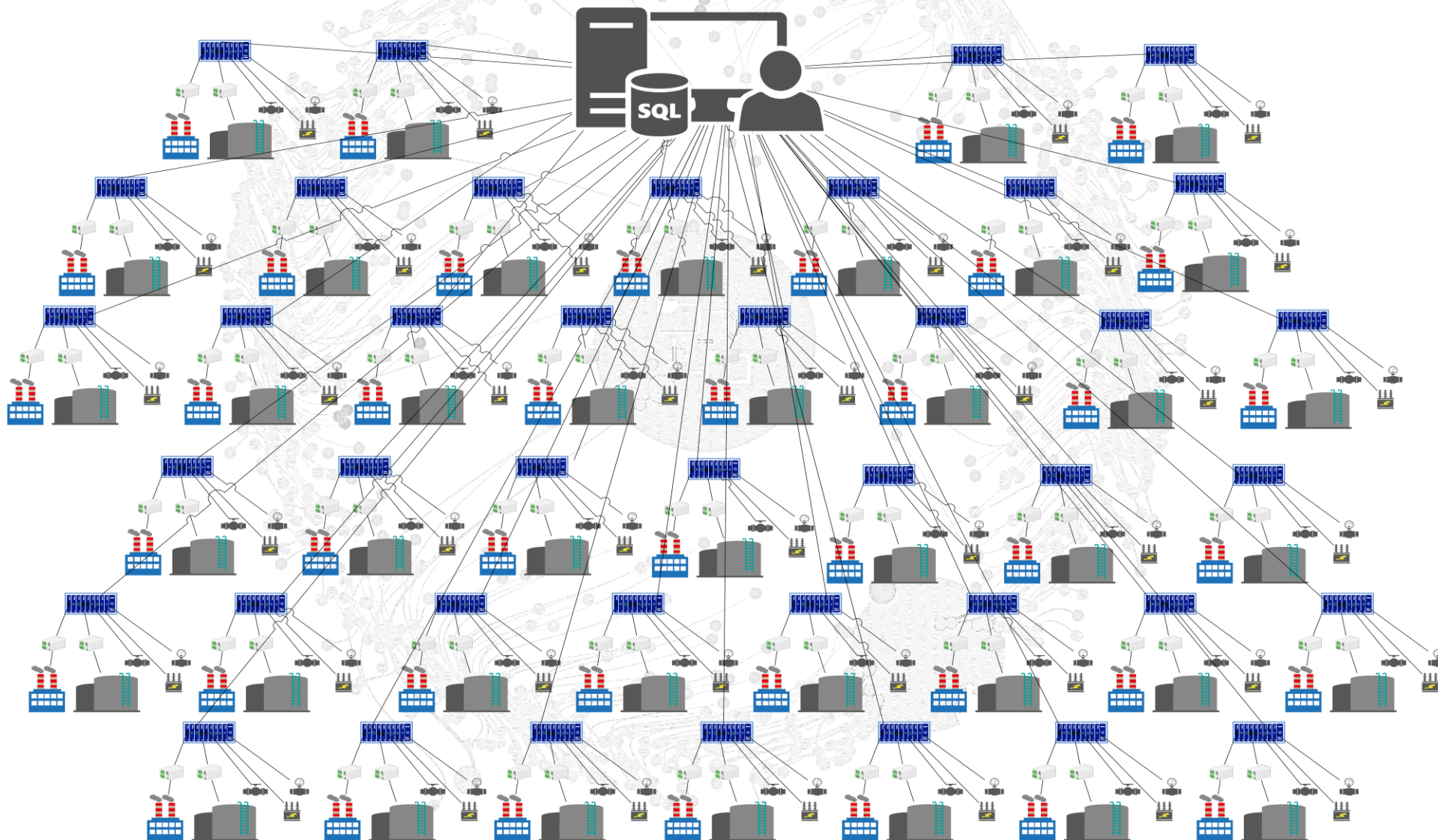
The diagram illustrates the architecture of a SCADA system, showing the flow of data and control signals between different components:

- SCADA (Supervisory Control and Data Acquisition):** The top-level system, represented by a computer icon and a database (SQL). It communicates with the RTU using protocols: IEC101, IEC 104, IEC 61850, and DNP3.
- RTU (Remote Terminal Unit):** The central unit that receives commands from the SCADA and manages the PLC. It supports various communication protocols: Modbus, Profibus, and Señales digitales. It is connected to the SCADA via Ethernet, Radio enlace, or Fibra optica.
- PLC (Programmable Logic Controller):** The unit that executes control logic. It is connected to the RTU via Ethernet Serie. It manages the simple devices.
- Dispositivos simples (Simple Devices):** These include basic components like valves, pumps, and sensors, which are connected to the PLC via simple wiring (Cableado simple) and simple signals (Señales simples).
- Dispositivos complejos (Complex Devices):** These include more sophisticated equipment like large storage tanks and industrial buildings, which are connected to the PLC via Ethernet Serie.

A screenshot of a SCADA software interface is shown on the right, displaying various process parameters, alarms, and control buttons.

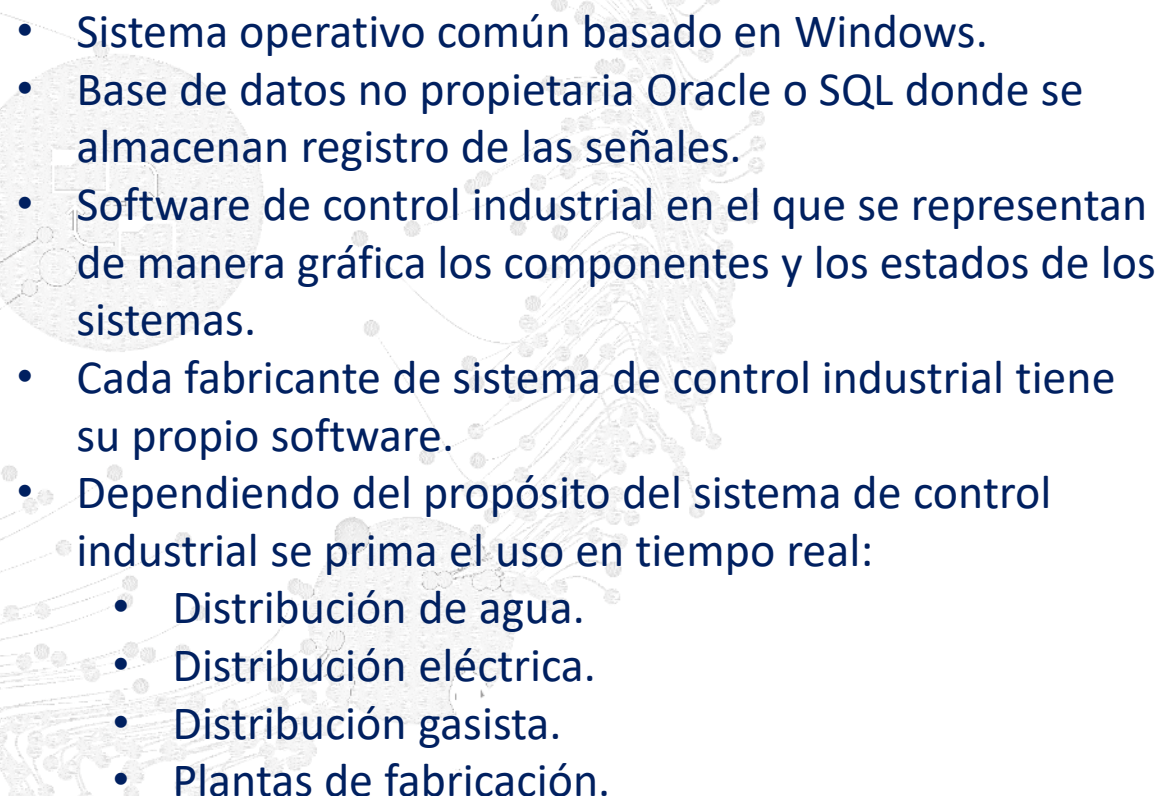
- Todas las señales se configuran manualmente.
- Las RTU soportan multitud de protocolos dependiendo de los módulos.

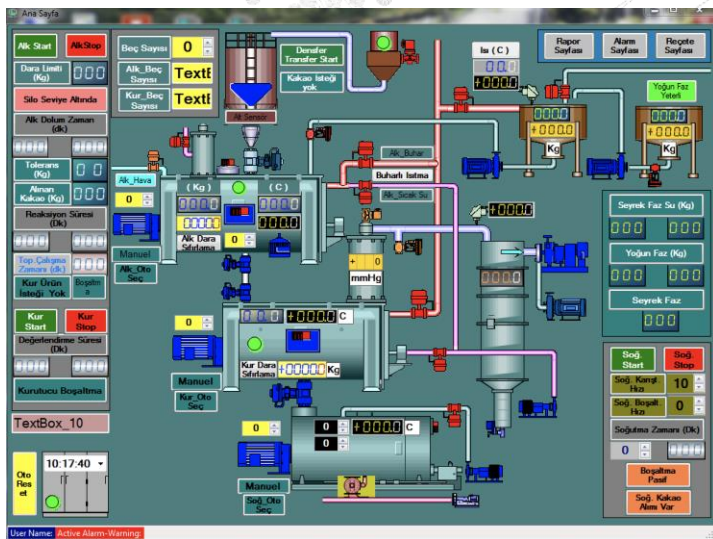
Arquitectura SCADA



Workstation & Servidor



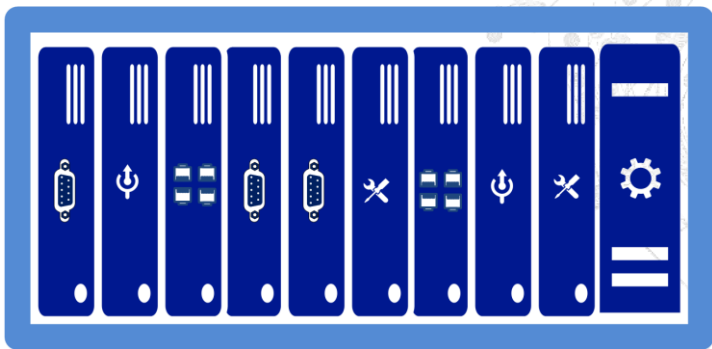
- 
- Sistema operativo común basado en Windows.
 - Base de datos no propietaria Oracle o SQL donde se almacenan registro de las señales.
 - Software de control industrial en el que se representan de manera gráfica los componentes y los estados de los sistemas.
 - Cada fabricante de sistema de control industrial tiene su propio software.
 - Dependiendo del propósito del sistema de control industrial se prima el uso en tiempo real:
 - Distribución de agua.
 - Distribución eléctrica.
 - Distribución gasista.
 - Plantas de fabricación.



RTU

Remote Terminal Unit

- Pieza clave de un sistema industrial de gran escala.
- Recoge o establece señales de los dispositivos industriales.
- Pasa información de las señales al SCADA.
- Modulable, se pueden poner tarjetas para señales analógicas y/o digitales.
- Mediante las tarjetas se puede entender cualquier protocolo industrial.

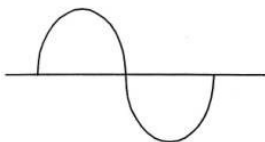


Dispositivos industriales simples

Simple

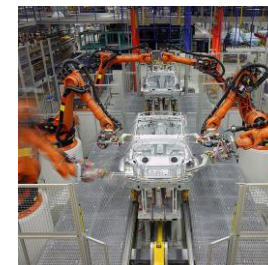
- Válvulas.
- Interruptores.
- Sensores sencillos.
- Alarmas.
- Cualquier dispositivo de estado ON/OFF.

SEÑAL ANALÓGICA



Complejos

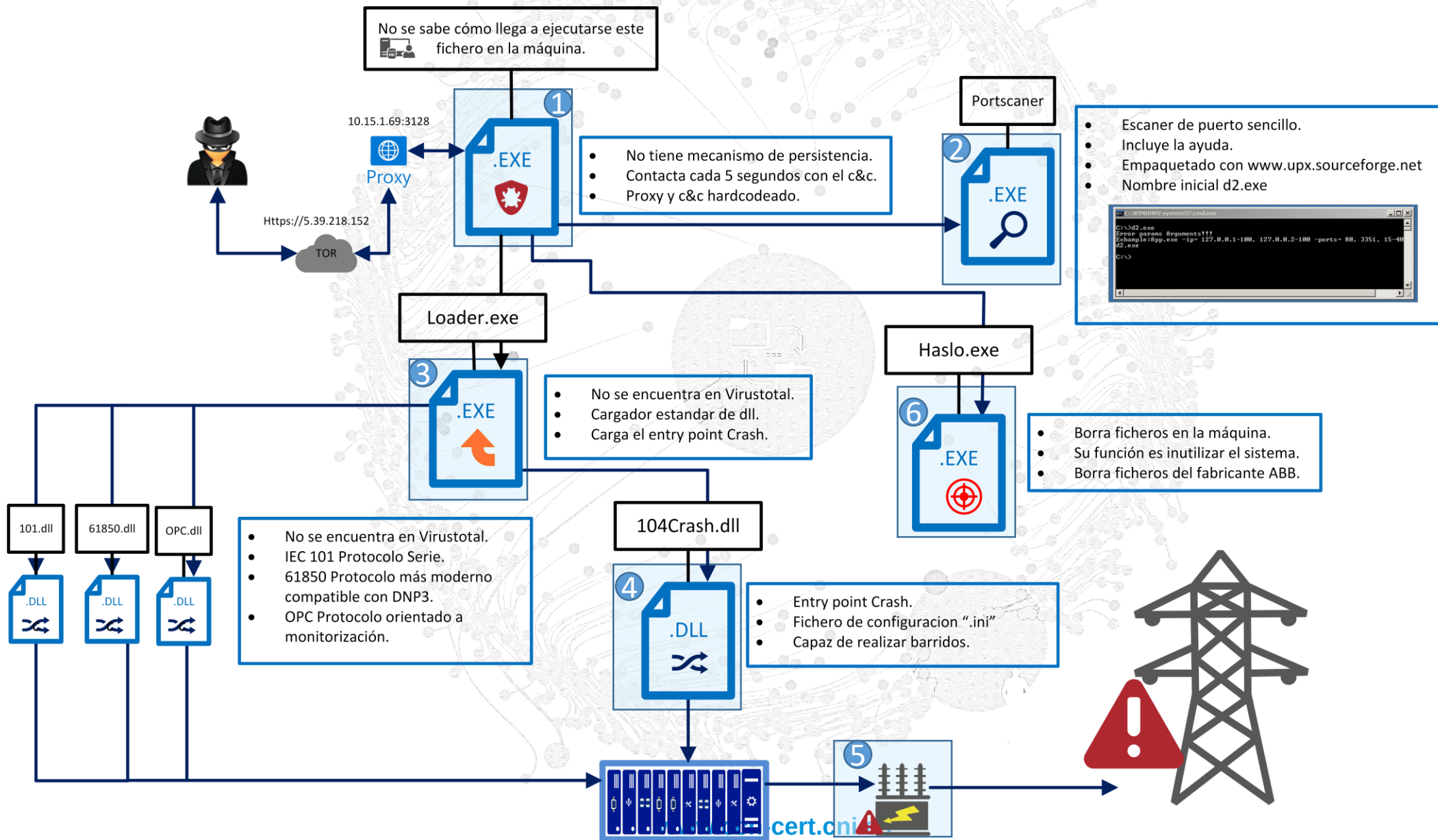
- PLC
- Brazos mecánicos.
- Sensores (temperatura, presión, caudal...).
- Motores.
- Sistemas de refrigeración.
- Comunicación serie o rj45.
- Protocolos Modbus profibus.





DESCRIPCIÓN DEL ATAQUE

Radiografía del ataque



Backdoor

CARACTERÍSTICAS

- No tiene mecanismo de persistencia.
- Contacta cada 5 segundos con el c&c aprox.
- Proxy interno e IP de c&c hardcodeado.
- Funcionalidades:
 - Ejecutar programa.
 - Lanzar un comando shell.
 - Subir un fichero.
- compiler-stamp, Sat Dec 17 12:05:26 2016
- debugger-stamp, Sat Dec 17 12:05:26 2016

PROXY

10.15.1.69 : 3128

Posiblemente SQUID

HTTP

<https://5.39.218.152>

/POST / HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322) Host: 5.39.218.152

Content-Length: 112

Connection: close

File information

SOLO 4 DE 55 LO DETECTABA COMO VIRUS

	Engine	Signature	Version	Update
2016-12-18 14:07:28 4/55	Ad-Aware	-	3.0.3.794	20161218
2016-12-25 14:07:55 4/56	AegisLab	-	4.2	20161217
2017-01-01 14:10:37 6/57	AhnLab-V3	-	3.8.2.16235	20161218
2017-01-08 16:39:30 15/55	ALYac	-	1.0.1.9	20161218
2017-06-12 14:50:30 28/61	Antiy-AVL	-	1.0.0.1	20161218
2017-06-12 15:24:32 27/60	Arcabit	-	1.0.0.791	20161218
2017-06-13 06:03:30 31/59	Avast	Win32:Evo-gen [Susp]	8.0.1489.320	20161218
2017-06-13 21:38:03 34/61	AVG	-	16.0.0.4739	20161218
2017-06-15 06:20:22 40/61	Avira	-	8.3.3.4	20161218
2017-06-15 18:20:26 41/62	AVware	-	1.5.0.42	20161218
	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9714	1.0.0.2	20161207

Download file Re-scan file Close

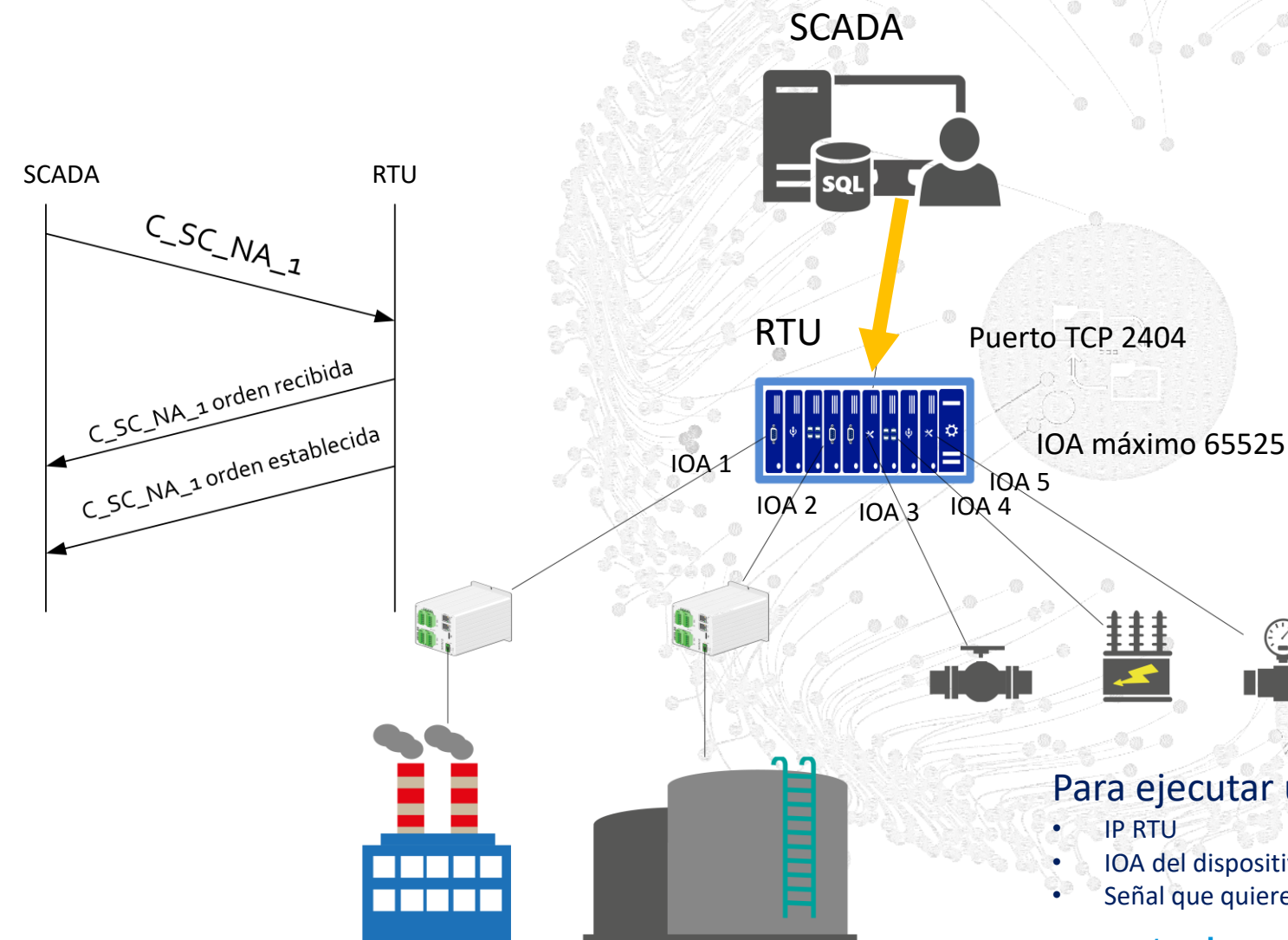
Date	File name	Source	Country
2017-06-27 16:21:39	ccccce62996d578b984984426a024d9b250237...	322fa98d (web)	UA
2017-06-27 16:15:22	ccccce62996d578b984984426a024d9b250237...	322fa98d (web)	UA
2017-06-22 12:27:28	6d707e64742711f4a7a9420188a8831f433a...	d868cb0f (web)	BY
2017-06-15 18:20:26	fc4fe1b933183c4c613d34fdb5fe758	0acf2fa8 (api)	KR
2017-06-15 06:20:22	fc4fe1b933183c4c613d34fdb5fe758	0acf2fa8 (api)	KR
2017-06-13 21:38:03	ccccce62996d578b984984426a024d9b250237...	322fa98d (web)	UA
2016-12-18 14:07:28	ws.exe	f2a0bd80 (web)	UA

EL DIA DESPUES DEL CORTE DE LUZ

UCRANIA

Download file Re-scan file Close

Crash104.dll Protocolo IEC 104



Nº ASDU	Descripción	Código
Monitorización:		
1	Single point information	M_SP_NA_1
...	...	...
21	Measured value, normalized value without quality descriptor	M_ME_ND_1
Monitorización con tiempos:		
30	Single point information with time tag CP56Time2a	M_SP_TB_1
...	...	...
40	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1
Cambio de estado:		
45	Single command	C_SC_NA_1
...	...	...
51	Bit string 32 bit	C_BO_NA_1
Cambio de estado con tiempo:		
58	Single command with time tag CP56Time2a	C_SC_TA_1
...	...	...
64	Bit string 32 bit with time tag CP56Time2a	C_BO_TA_1
Información del sistema:		
70	End of initialization	M_EI_NA_1
Información del sistema sobre señales:		
100	(General-) Interrogation command	C_IC_NA_1
...	...	...
113	Parameter activation	P_AC_NA_1
Transferencia de ficheros:		
120	File ready	F_FR_NA_1
...	...	...
127	QueryLog – Request archive file	F_SC_NB_1

Para ejecutar un comando o ASDU en un dispositivo necesitas:

- IP RTU
- IOA del dispositivo
- Señal que quieres establecer

Crash104.dll

- La DLL está malformada.
- Posiblemente la muestra sacada de Virustotal sea un dump de memoria.
- Da la posibilidad de parar un proceso.
- Incorpora todos los ASDU del protocolo IEC-104
- Hay que cargar un fichero de configuración “.ini”
- compiler-stamp, Thu Jan 01 01:00:00 1970
- debugger-stamp, Sun Dec 18 03:48:22 2016

```
-----FILE.INI-----
[STATION]
target_ip
target_port
Asdu
stop_comm_service
Change
first_action
Silence
Uselog
stop_comm_service_name
Timeout
socket_timeout
Range
command_type
Short
Long
Persist
Operation
Shift
sequence
```

File information

Identification Details Content Analyses Submissions ITW Comments

< > ↓ ↑

Date	File name	Source	Country
2017-07-31 13:55:12	7907dd95c1d36cf3dc842a1bd804f0db511a0...	5020ehec (web)	NL
2017-07-28 03:29:30	7907dd95c1d36cf3dc842a1bd804f0db511a0...	d8fde90a (web)	IN
2017-06-27 16:25:42	94488f214b165512d2fc0438a581f5c9e3bd4...	322fa98d (web)	UA
2017-06-22 12:27:35	7907dd95c1d36cf3dc842a1bd804f0db511a0...	d868cb0f (web)	BY
2017-06-16 02:27:29	7907dd95c1d36cf3dc842a1bd804f0db511a0...	4df93c1f (web)	US
2017-06-15 06:20:23	a193184e61e34e2bc36289deaafdec37	0acf2fa8 (api)	KR
2017-06-13 21:40:28	94488f214b165512d2fc0438a581f5c9e3bd4...	322fa98d (web)	UA
2016-12-19 10:06:04	104.dll	825716a1 (web)	UA

Download file Re-scan file Close

No.	Time	Source	Destination	Protocol	Length	...
304...	103681.2085...	10.15.1.128	10.15.1.69	TCP	66	2404 → 64424 [FIN, ACK] Seq=29 Ack=30 Win=65507 Len=0 TSval=1038855 TSecr=1061978568
304...	103681.2086...	10.15.1.69	10.15.1.128	TCP	66	64424 → 2404 [ACK] Seq=30 Ack=30 Win=131712 Len=0 TSval=1061979563 TSecr=1038855
304...	103682.2127...	10.15.1.69	10.15.1.128	104ap...	72	<- U (STARTDT act)
304...	103682.2157...	10.15.1.128	10.15.1.69	104ap...	72	-> U (STARTDT con)
304...	103682.2157...	10.15.1.69	10.15.1.128	TCP	66	64425 → 2404 [ACK] Seq=13 Ack=13 Win=131744 Len=0 TSval=1061980566 TSecr=1038865
304...	103684.2214...	10.15.1.128	10.15.1.69	104as...	82	<- I (0,0) ASDU=0 C_SC_NA_1 Act IOA=4
304...	103684.2224...	10.15.1.128	10.15.1.69	104as...	82	-> I (0,1) ASDU=0 C_SC_NA_1 ActCon IOA=4
304...	103684.2225...	10.15.1.69	10.15.1.128	TCP	66	64425 → 2404 [ACK] Seq=29 Ack=29 Win=131712 Len=0 TSval=1061982567 TSecr=1038885
304...	103686.2267...	10.15.1.69	10.15.1.128	TCP	66	64425 → 2404 [FIN, ACK] Seq=29 Ack=29 Win=131712 Len=0 TSval=1061984558 TSecr=1038885
304...	103686.2270...	10.15.1.128	10.15.1.69	TCP	66	2404 → 64425 [ACK] Seq=29 Ack=30 Win=65507 Len=0 TSval=1038905 TSecr=1061984558
304...	103687.2286...	10.15.1.128	10.15.1.69	TCP	66	2404 → 64425 [FIN, ACK] Seq=29 Ack=30 Win=65507 Len=0 TSval=1038915 TSecr=1061984558
304...	103687.2287...	10.15.1.69	10.15.1.128	TCP	66	64425 → 2404 [ACK] Seq=30 Ack=30 Win=131712 Len=0 TSval=1061985552 TSecr=1038915

Frame 30467: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0

Ethernet II, Src: Vmware_c0:00:04 (00:50:56:c0:00:04), Dst: Vmware_6c:81:d4 (00:0c:29:6c:81:d4)

Internet Protocol Version 4, Src: 10.15.1.69, Dst: 10.15.1.128

Transmission Control Protocol, Src Port: 64425, Dst Port: 2404, Seq: 13, Ack: 13, Len: 16

IEC 60870-5-104-Apci: <- I (0,0)

IEC 60870-5-104-Asdu: ASDU=0 C_SC_NA_1 Act IOA=4 'single command'

Haslo.exe

- El objetivo es inutilizar el sistema.
- Borra ficheros de configuración de sistemas industriales, va recorriendo todo el disco duro:
 - . *.pcmp*.pcmi*.pcmt
- Busca el fichero “SYS_BASCON.COM” (es un fichero de configuración de sistema MicroScada de ABB) y lo borra .
- Termina parando todos los procesos a los que tiene acceso.
- compiler-stamp,Thu Jan 01 01:00:00 1970
- debugger-stamp,Sun Dec 18 03:40:49 2016

```

;*****
; APPLICATIONS
;The usage of OI & OX -attributes
@SV(15) = LIST(-
    Process_Objects=LIST(- OI=LIST(-
        Title1=VECTOR("Substation"),-
        Title2=VECTOR("Bay"),-
        Title3=VECTOR("Device"),-
        Title4=VECTOR(""),-
        Title5=VECTOR(""),-
        Length1=10,-
        Length2=15,-
        Length3=5,-
        Length4=0,-
        Length5=0,- ...
    )
)

```

File information

[Identification](#)
[Details](#)
[Content](#)
[Analyses](#)
[Submissions](#)
[ITW](#)
[Behaviour](#)
[Comments](#)

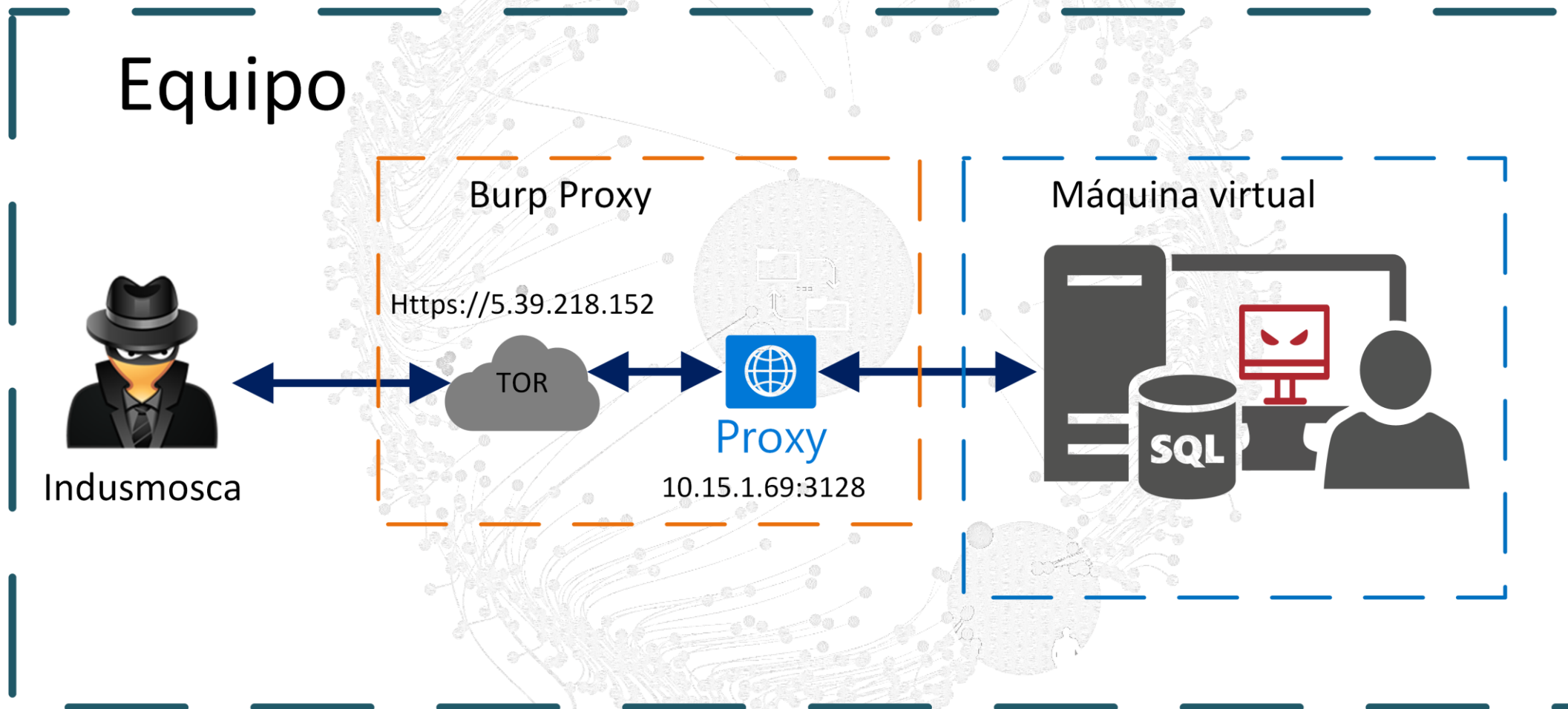
	Engine	Signature	Version	Update
2016-12-19 09:58:43 2/55	Ad-Aware	-	3.0.3.794	20161219
2016-12-26 09:59:03 10/56	AegisLab	-	4.2	20161219
2017-01-17 12:38:59 24/56	AhnLab-V3	-	3.8.2.16235	20161219
2017-01-25 08:32:46 37/57	ALYac	-	1.0.1.9	20161219
2017-01-25 10:10:23 36/57	Antiy-AVL	-	1.0.0.1	20161219
2017-02-15 11:11:34 39/59	Arcabit	-	1.0.0.791	20161219
2017-06-13 10:59:21 42/61	Avast	-	8.0.1489.320	20161219
2017-06-13 11:28:23 42/61	AVG	-	16.0.0.4739	20161219
2017-06-13 11:29:34 42/60	Avira	-	8.3.3.4	20161219
2017-06-13 21:37:18 43/61	AVware	-	1.5.0.42	20161219
	Baidu	-	1.0.0.2	20161207

[Download file](#)
[Re-scan file](#)
[Close](#)

PoC1

Tomando el control del Backdoor

Escenario PoC 1





PoC2 Apagando interruptores con IEC104

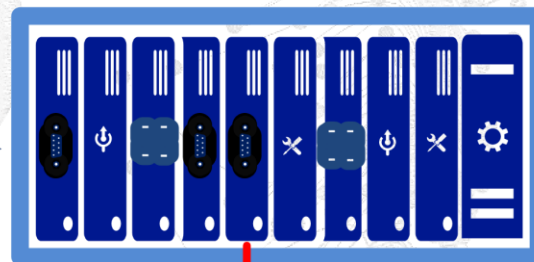
Escenario PoC 2

Equipo

CrazyScada



Máquina virtual



ENLACES

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

<https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>

HASHs

F6C21F8189CED6AE150F9EF2E82A3A57843B587D
CCCCE62996D578B984984426A024D9B250237533
8E39ECA1E48240C01EE570631AE8F0C9A9637187
2CB8230281B86FA944D3043AE906016C8B5984D9
79CA89711CDAEDB16B0CCCCFDCFB6AA7E57120A
94488F214B165512D2FC0438A581F5C9E3BD4D4C
5A5FAFBC3FEC8D36FD57B075EBF34119BA3BFF04
B92149F046F00BB69DE329B8457D32C24726EE00
B335163E6EB854DF5E08E85026B2C3518891EDA8

Yo



<https://github.com/manudbc>



<https://www.linkedin.com/in/manuel-bermúdez-20160b15/>



mbermudez@enagas.es



<https://twitter.com/ManuelDBC>

➤ 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

