INDUSTROYER
CRASHOVERRIDE

Zero Things Cool About a Threat Group Targeting the Power Grid
Robert Lipovský
Senior Malware Researcher
@Robert_Lipovský

Anton Cherepanov
Senior Malware Researcher
@cherepanov74
Robert M. Lee
CEO
@RobertMLee

Ben Miller
Director, Threat Operations Center
@electricfork

Joe Slowik
Senior Threat Research Analyst
@jfslowik
• ICS-targeting malware
• The story of INDUSTROYER: Ukrainian blackout
• INDUSTROYER analysis
• CRASHOVERRIDE impacts
• Predictions moving forward
ICS-targeting malware
ICS
MALWARE
OPERATOR
INTERNET
POWER DISTRIBUTION COMPANY
European Gas Conference 2012
Jan 24-27, 2012 in Vienna (Austria)

The European Gas Conference 2012 is the only event to unite the commercial and policy makers 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 move on natural gas, the challenges of unblocking Europe’s international pipeline projects, the implementation of Russia in European natural gas supply, new developments and arbitrations and legal implications.

Don’t miss this unique opportunity to join the industry European natural gas market at European Gas Conference 2012.

Why Attend European Gas Conference 2012:
• Networking: meet the Ministers designing European projects from across Europe
• Learning: hear the latest from all the major European projects
• News: understand how long the downgrading of oil and gas your business
• Comprehensively encroaching North East, Gas South. What can ensure security of supply – contribute to the facilitation of the market
• Global context: understand how developments in North America will impact the European market
• Capitalize: claim market share by testing your concepts and Skal gas opportunity

European Gas Conference 2012 will be held in Vienna, Austria 24-27 January 2012.

EU chief Barroso to snub Euro 2012 in Ukraine

Reuters By Timothy Larsen

Protests show EU chief Barroso will not attend 2012 European soccer championships in Ukraine

EU chief Barroso to snub Euro 2012 in Ukraine

EU chief Barroso was due to attend the 2012 European soccer championships in Ukraine next year but will now miss the opening match.

The European Commission on Tuesday said it had decided not to travel to Ukraine for the opening match of the 2012 European soccer championships.

The commission said in a statement that it had decided not to travel to Ukraine for the match in Donetsk on June 8 because of “the climate of tension and instability” in the region.

The statement said that the commission was not able to participate in the event due to “the risk of a security incident.”

The European Commission has already decided not to travel to Russia for the opening match of the 2014 World Cup in June.

The commission said that it would not travel to the opening match of the 2014 World Cup in Brazil in June because of the “risk of a security incident.”
on December 23, 2015
in Ukraine
BlackEnergy

- Network Scanner
- File Stealer
- Password Stealer
- Keylogger
- Screenshots
- Network Discovery
17 Dec 2016

Blackout in Ukraine

18 Jan 2017

ESET begins analysis

A few days later

12 Jun 2017

Initial report finished

Finished report shared with Dragos

8 Jun 2017

Further research

Industroyer report goes public
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute process</td>
<td>Execute process</td>
</tr>
<tr>
<td>Execute process using specified user account</td>
<td>Execute process using specified user account</td>
</tr>
<tr>
<td>Download file from C&amp;C server</td>
<td>Download file from C&amp;C server</td>
</tr>
<tr>
<td>Copy &amp; upload file</td>
<td>Copy &amp; upload file</td>
</tr>
<tr>
<td>Execute shell command</td>
<td>Execute shell command</td>
</tr>
<tr>
<td>Execute shell command using specified user account</td>
<td>Execute shell command using specified user account</td>
</tr>
<tr>
<td>Quit</td>
<td>Quit</td>
</tr>
<tr>
<td>Stop service</td>
<td>Stop service</td>
</tr>
<tr>
<td>Stop service using specified user account</td>
<td>Stop service using specified user account</td>
</tr>
<tr>
<td>Start service using specified user account</td>
<td>Start service using specified user account</td>
</tr>
<tr>
<td>Replace &quot;Image path&quot; registry value for specified service</td>
<td>Replace &quot;Image path&quot; registry value for specified service</td>
</tr>
</tbody>
</table>
Start service using specified user account

Replace "Image path" registry value for specified service
**Main Backdoor**

**Additional Backdoor**

**Port Scanner**

**DOS Tool**

```cmd
C:\> port.exe
Error params Arguments!!!
Example: 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
Malware impact: PAYLOADS
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], 18h
call   ds:SystemTimeToFileTime
lea    eax, [esp+50h+FileTime]
push   eax     ; lpFileTime
push   eax     ; lpLocalFileTime
call   ds:LocalFileTimeToFileTime
```
• Serial
• IOA (Information Object Address) ranges
  • single command (C_SC_NA_1)
  • double command (C_DC_NA_1)
• OFF -> ON -> OFF
104 Payload

- TCP/IP
- Modes:
  - Range
  - Shift
  - Sequence
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
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
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: 15 Starting only success:
Done: 10
Done: 11
Done: 13
Done: 14
Done: 15
Switch value: OFF
Done: 10
Done: 11
Done: 13
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
- 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)
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)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>FC</th>
<th>Value/Value range</th>
<th>M/O</th>
<th>OPC Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctlSelOn</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlSelOff</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlOperOn</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlOperOff</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlCan</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlOper</td>
<td>AbbCommand-Bitmask</td>
<td>M</td>
<td></td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>lastApplError</td>
<td>ApplicationErrorCode</td>
<td>M</td>
<td>Refer to 5.2.22, Application error codes</td>
<td>M</td>
<td>VT_I4</td>
</tr>
<tr>
<td>ctlVal</td>
<td>BOOLEAN</td>
<td>CO</td>
<td>off (FALSE)</td>
<td>on (TRUE)</td>
<td>M</td>
</tr>
</tbody>
</table>
**AbcCommandBitmask**

The following table defines the mapping of AbcCommandBitmask. 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>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value/Value range</th>
<th>M/O/C</th>
<th>Bit Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>NormalControl</td>
<td>1bit</td>
<td>FALSE (0)</td>
<td>TRUE (1)</td>
<td>M</td>
</tr>
<tr>
<td>InterlockOverride</td>
<td>1bit</td>
<td>FALSE (0)</td>
<td>TRUE (1)</td>
<td>M</td>
</tr>
<tr>
<td>SynchrocheckOverride</td>
<td>1bit</td>
<td>FALSE (0)</td>
<td>TRUE (1)</td>
<td>M</td>
</tr>
<tr>
<td>TestCommand</td>
<td>1bit</td>
<td>FALSE (0)</td>
<td>TRUE (1)</td>
<td>M</td>
</tr>
<tr>
<td>Originator</td>
<td>4bit</td>
<td>not-supported(0)</td>
<td>bay-control(1)</td>
<td>station-control(2)</td>
</tr>
<tr>
<td>ControlValue</td>
<td>nbit</td>
<td></td>
<td>M</td>
<td>8-31</td>
</tr>
</tbody>
</table>

**NormalControl**: True = normal operation, false = inverse operation (for example, On > Off).
<table>
<thead>
<tr>
<th>Object</th>
<th>Object Identifier</th>
<th>Signal Text</th>
<th>Block/Bit addr.</th>
<th>Station</th>
<th>IN</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2BQ0.P10</td>
<td>STA2. STA2B2</td>
<td>Breaker position indication</td>
<td>1/2</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.stVal</td>
</tr>
<tr>
<td>S2BQ0.P11</td>
<td>STA2. STA2B2</td>
<td>Breaker open select command</td>
<td>5</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.ctSelOff</td>
</tr>
<tr>
<td>S2BQ0.P12</td>
<td>STA2. STA2B2</td>
<td>Breaker close select command</td>
<td>6</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.ctSelOn</td>
</tr>
<tr>
<td>S2BQ0.P13</td>
<td>STA2. STA2B2</td>
<td>Breaker open execute command</td>
<td>7</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.tOperOff</td>
</tr>
<tr>
<td>S2BQ0.P14</td>
<td>STA2. STA2B2</td>
<td>Breaker close execute command</td>
<td>8</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.tOperOn</td>
</tr>
<tr>
<td>S2BQ0.P16</td>
<td>STA2. STA2B2</td>
<td>Breaker open interlocked</td>
<td>0/16</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.Seld</td>
</tr>
<tr>
<td>S2BQ0.P17</td>
<td>STA2. STA2B2</td>
<td>Breaker close interlocked</td>
<td>0/16</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.ctCan</td>
</tr>
<tr>
<td>S2BQ0.P18</td>
<td>STA2. STA2B2</td>
<td>Cause of interlocking</td>
<td>0</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>S2BQ0.P19</td>
<td>STA2. STA2B2</td>
<td>Breaker selection on monitor</td>
<td>0</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>S2BQ0.P20</td>
<td>STA2. STA2B2</td>
<td>Breaker command event</td>
<td>0/16</td>
<td>41</td>
<td>IEC61850 Subnetwork.REF542_41.LD1.Q0CSW11.Pos.StVal</td>
</tr>
</tbody>
</table>
# IDAPython script for OPC DA binaries

```python
id = GetStrucIdByName('IID')
if id == BADADDR:
    id = AddStrucEx(-1, 'IID', 0)
    id = GetStrucIdByName('IID')
    AddStrucMember(id, 'Data1', 0x0, FE_FWD, -1, 4)
```

Github: [https://github.com/eset/malware-research/tree/master/industroyer](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
mov eax, [ebx+1Ch]
lea edi, [ebx+4]
push edi
push offset unk_429840
push [ebp+arg_C]
mov ecx, [eax+4]
lea eax, [ebx+18h]
push eax
push 0
lea eax, [ebp+arg_10]
mov edx, [ecx]
push eax
movzx eax, [ebp+arg_4]
push 0
push 0
push [ebp+arg_8]
push eax
push esi
push ecx
call dword ptr [edx+0Ch]
test eax, eax
jns short loc_40885E
push eax
push offset aErrorCodeAt
; "Error code: %d\n"
call sub_407B60
mov    eax, [ebx+1Ch]
lea    edi, [ebx+4]
push   edi           ; ppUnk
push   offset IID_IOPCGroupStateMgt ; riid
push   [ebp+pRevisedUpdateRate]   ; pRevisedUpdateRate
mov    ecx, [eax+4]
lea    eax, [ebx+18h]
push   eax           ; phServerGroup
push   0             ; dwLCID
lea     eax, [ebp+pPercentDeadband]
mov     edx, [ecx]
push   eax           ; pPercentDeadband
movzx   eax, [ebp+arg_4]
push   0             ; pTimeBias
push   0             ; hClientGroup
push   [ebp+dwRequestedUpdateRate] ; dwRequestedUpdateRate
push   eax           ; bActive
push   esi           ; szName
push   ecx           ; This
call   [edx+IOPCServerVtbl1.AddGroup]
test   eax, eax
jns    short loc_40885E
push   eax
push   offset aErrorCodeD ; "Error code: %d\n"
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 vulnerability, if exploited, could result in denial-of-service conditions.
DENIAL OF SERVICE

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.

```c
ip_addr = htonl;
memset(&WSADat); 0x00; 0x98u); *to.sa_data[8] = 0;
*to.sa_data[12] = 0;
to.sa_family = AF_INET;
*to.sa_data[0] = 0164;
*to.sa_data[0] = htons(port); // port 50000
if (WNSAStartup(0x202u, &WSADat))
{
  s = socket(SOCK_DGRAM, AF_INET, 0);
  if (s)
  {
    for (; ip_addr <= 03; ++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);
  }
  WSCleanup();
}
```
Malware impact: DATA WIPER
dd offset a_v
dd offset a_pl
dd offset a_paf
dd offset a_v
dd offset a_xrf
dd offset a_trc
dd offset a_scl
dd offset a_bak
dd offset a_cid
dd offset a_scd
dd offset a_pcm
dd offset a_pcmi
dd offset a_pcmt
dd offset a_ini
dd offset a_xml
dd offset a_cin
dd offset a_ini
dd offset a_prj
dd offset a_cxm
dd offset a_elb
dd offset a_epl
dd offset a_mdf
dd offset a_ldf
dd offset a_bak
dd offset a_bk
dd offset a_bkp
dd offset a_log
dd offset a_zip
dd offset a_rar
dd offset a_tar
dd offset a_7z
dd offset a_exe
dd offset a_dll
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

Edison Electric Institute

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.
<table>
<thead>
<tr>
<th>Activity Group</th>
<th>ELECTRUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Name</td>
<td>CRASHOVERRIDE</td>
</tr>
</tbody>
</table>
| Capabilities   | ▪ Manipulation of Control  
                  ▪ Denial of Control  
                  ▪ Denial of View  
                  ▪ Data wiping |
Stage 1 - Intrusion

Reconnaissance

Weaponization

Targeting

Delivery

Exploit

Install / Modify

C2

Act

Stage 2 – ICS Attack

Develop

Test

Deliver

Install / Modify

Execute ICS Attack

Enabling

Initiating

Supporting

Trigger

Modify

Hide

Deliver

Inject

Amplify

Cleanup & Defend

Exploit

Install & Execute

Collect

Exfiltrate

Launch

Discovery

Movement

Capture
Stage 1 - Intrusion

- Reconnaissance
  - Weaponization
  - Targeting
  - Delivery
  - Exploit
  - Install / Modify
    - C2
  - Act

Stage 2 – ICS Attack

- Develop
- Test
- Deliver
- Install / Modify

Execute ICS Attack

- Enabling
- Initiating
- Supporting
- Trigger
- Modify
- Inject
- Hide
- Amplify

- Discovery
- Movement
- Install & Execute
- Launch
- Capture
- Collect
- Exfiltrate
- Clean & Defend
# Payload Modules

## CRASHOVERRIDE

### MODULES and IMPACT

<table>
<thead>
<tr>
<th>Loss of Control</th>
<th>Payload Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IEC-101</td>
<td>Manipulates substation devices through value modification via serial*</td>
</tr>
<tr>
<td></td>
<td>IEC-104</td>
<td>Manipulates substation devices through value modification via TCP/IP</td>
</tr>
<tr>
<td></td>
<td>IEC-61850</td>
<td>61850 driver identifying devices and modifying values**T</td>
</tr>
<tr>
<td></td>
<td>SIPROTECT Denial of Service</td>
<td>Uses CVE-2015-5374 to cause a denial of service against SIPROTECT digital relays*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss of Visibility</th>
<th>Payload Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OPC DA</td>
<td>Identifies OPC servers and sets all addresses to ‘out of bounds’ preventing status reports*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destruction</th>
<th>Payload Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Wiper</td>
<td>Stops all process, destroys all data in local and network connected drives</td>
</tr>
</tbody>
</table>

* 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
IEC 104 Module Configuration File

- 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
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
WHO WANTS TO KNO
Learning from CRASHOVERRIDE

```latex
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" ncase wide ascii
        $s2 = " MSTR \rightarrow SLV" ncase wide ascii
        $s3 = " MSTR \leftarrow SLV" ncase wide ascii
        $s4 = "Unknown APDU format !!!" ncase wide ascii
        $s5 = "iec104.log" ncase wide ascii

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