MANAGING MALWARE
CRASH OVERRIDE/INDUSTROYER MALWARE ASSESSMENT
CONTENTS

• STATE OF THE HACK: CRASHOVERRIDE/INDUSTROYER
• THE ATTACK LANDSCAPE
• RECOMMENDATIONS

• APPENDIX
  - CRASHOVERRIDE/INDUSTROYER MALWARE SAMPLES
  - CVE-2015-5374—Siemens AG SIPROTEC 4 and SIPROTEC Compact Products Input Validation Error DoS Vulnerability
STATE OF THE HACK:
CRASHOVERRIDE/INDUSTROYER

When the lights went out in Ukraine’s capital, Kiev, in December 2016, it seemed an unwelcome inconvenience that resembled some issues Ukraine had experienced a year earlier. But further examination of what happened in the region by cybersecurity companies Dragos Inc. and ESET has uncovered something altogether more threatening about the outage. The two independent companies have identified a malware framework, known as CRASHOVERRIDE or INDUSTROYER which targeted the electrical infrastructure of the Ukrainian grid via its Industrial Control Systems (ICS). The sophistication and high impact of this apparent cyber-attack has serious implications globally—and the potential to visit more than a power grid near you sometime soon.

The continued deployment of digital technologies for enhanced automation has greatly increased the attack surface for hackers to target. What is more, due to the life expectancy of such field level assets supporting critical infrastructure, many of these devices were designed and deployed potentially decades ago and not necessarily architected with cybersecurity in the forefront of everyone’s mind. CRASHOVERRIDE/INDUSTROYER targeted circuit breakers and switches hijacking electrical systems from a distance by taking advantage of standard device level communication protocols, making it almost completely undetectable in the power infrastructure, and potentially in some water and gas systems used all over the world.

While there are suggestions that a specific nation state is behind the Kiev incident, there is little doubt that the CRASHOVERRIDE/INDUSTROYER malware could be used as a blueprint of sorts, modified and used in a more widespread and longer-lasting attack. The potential to disrupt energy, water supplies and other critical industries using ICS for automation, in an economic context, could be highly damaging to a company, municipality or nation for a sustained time.

CURRENT ASSESSMENT

Based on the compilation time, and early submissions of the files to public repositories such as VirusTotal, iDefense assesses the attack initiated in mid-November 2016, and lasted until mid-December 2016. Early location of malware submissions were from Eastern Europe, and notably Ukraine.

iDefense has evaluated the unique TTPs, features and comparisons with other destructive malware as follows:

- Malware analysis indicates that the CRASHOVERRIDE/INDUSTROYER samples, although well designed, were not nearly as sophisticated when compared against Stuxnet and similar ICS/SCADA malware. For example, the Stuxnet code contained multiple zero-days and the threat actors employed multiple layers of code obfuscation to evade detection and basic analysis. By contrast, CRASHOVERRIDE/INDUSTROYER leverages Internet communications, does not use major encryption to hide malware functionality and exploits only one vulnerability, which is already publicly disclosed.
Probably part of a coordinated series of attacks, the CRASHOVERRIDE/INDUSTROYER operation would have taken time to prepare. It was unlikely to be set off by near-term events, but rather part of a focused operation. Reinforcing this assertion that this was likely not an opportunist attack is the fact the attackers had significant knowledge of the security flaws in the victim’s defensive posture. It is probable the threat actors performed substantial targeting recon leading up to the attacks during November 2016. The attack on the electric grid came at the end of two weeks of attacks on Ukrainian infrastructure. It is possible that these operations were part of an ongoing nation state’s attempt to accomplish two things: first, to inflict harm against the Ukrainian government for regional geo-political gain, and second, test and showcase this potential nation state’s ability to launch coordinated attacks against the infrastructures of entire countries.

All the recovered command-and-control (C2) servers for the analyzed malware samples were internal IP addresses or TOR exit nodes at time of compromise. It is probable that some time before the incident, the threat actors took the time to set up TOR exit relays and pushed these attack-relay nodes into official/publicly available list of nodes, whereby maintaining those attack-relay nodes so they could capture the receiving traffic. From a defensive stand point, iDefense highly recommends blocking access to TOR or any anonymity service that threat actors could leverage to facilitate the communication. TOR nodes that are baked into malicious software to facilitate the communication with infected systems can leverage the strong encryption of TOR platform, and make detection and attribution extremely difficult.

**COMPARISON WITH STUXNET**

As we have stated, malware analysis indicates that the samples are not as sophisticated when compared against Stuxnet and similar ICS/SCADA malware, specifically the code did not include code obfuscation; however, it is evident that the threat actors performed targeted reconnaissance before conducting the cyber attack since the attackers were aware of the shortcomings and flaws in the victim’s defensive posture. Further, Stuxnet was created in a way to have worm functionality, self-propagate, and spread through air-gapped networks. The Stuxnet code contained multiple zero-day vulnerabilities and the threat actors employed several layers of code obfuscation to evade detection and basic analysis. Whereas the analyzed CRASHOVERRIDE/INDUSTROYER samples rely on the Internet for communications, they did not use major encryption to hide the true nature of malware functionality and relied on only one vulnerability, which was already publicly disclosed. Since some of the analyzed samples show slight modifications in comparison to supposedly initial malware builds, it is evident that threat actors were inside the compromised network and over time tweaked the malware to not only delete traces of suspicious file presences of the system, but also modified the malware to function and operate in the desired way.

**WHAT’S IN A NAME?**

The malware identifies itself as "crash," hence Dragos’ choice of the term CRASHOVERRIDE/INDUSTROYER. Whoever developed CRASHOVERRIDE/INDUSTROYER may have been paying homage to, or making fun of, the previously known hacker who used the name "Cr4sh". This hacker was credited with developing the first version of **BlackEnergy** during the mid-2000s. It is believed that the individual who used the name Cr4sh currently works as an exploit-seller in Southeast Asia. Current information supports that this hacker and has denied any responsibility for later versions of BlackEnergy and their abuses.

Managing Malware | Crashoverride/Industroyer Malware Assessment
THE ATTACK LANDSCAPE

The attack on the electric grid was the culmination of a series of attacks on key Ukrainian financial and physical infrastructure. On December 6, 2016, visitors to the Ukrainian State Treasury website were redirected to the site www.whoismrrobot[.]com, a site created by an American multinational media conglomerate to promote a television show with a plot about an anti-social computer programmer who works as a cybersecurity engineer during the day, but at night he is a vigilante hacker. Ukrainian news sites soberly reproduced the text currently visible on the website as if it were a message directed at the Ukrainian government: “We lit the fuse of revolution. Now we decide if it sputters and dies, or truly ignites. Our real work is just beginning.” Soon other attacks occurred involving the following entities:

- December 6: Ukrainian State Treasury and Finance Ministry
- December 7: Ukrainian Pension Fund
- December 12: Volya Kabel Internet provider; State Executive Service, a Justice Ministry agency responsible for administering fines and imprisonment.
- December 13: Defense Ministry
- December 15: Ukrainian Railways railroad ticketing system
- December 16: Infrastructure Ministry
- December 17 to 18: Just before midnight on December 17, the Northern electrical generating substation Ukrainian: Pivnichni in the Kyiv suburb of Novyye Petrovtsy lost power.¹

This rash of outages represented a peak in an already high level of attacks. Before December 2016, 247 attacks were revealed against Information and Communications Technology (ICT) systems of diplomatic organizations, law enforcement, critical infrastructure elements and other state ICT resources, according to the Ukrainian Security service. A Ukrainian state agency employee said that in one day alone his agency had repelled 322 attempts to guess e-mail passwords.

Likely coming as part of a coordinated series of attacks, the CRASHOVERRIDE/INDUSTROYER operation would have taken time to prepare. It was probably not set off by particular near-term events, but was rather part of a long-hatched plan; however, its timing may have responded to or been pegged to short-term stimuli. As such, it is worth looking at the landscape for at least the previous several months.

The attacks coincided with many regional and global geo political events, so the timing seems suspicious. More details on these notable but not directly linked events that may imply a nation state’s intention to be disruptive in the region are available in a non-disclosed briefing.

¹ See: iDefense intelligence Alert “December 2016 Ukrainian Electrical Outage Was Part a two-week Campaign Against Ukrainian Financial and Physical Infrastructure” for more
iDefense recommends the following actions for affected organizations:

**ASSESS AND ISOLATE:** There is nothing to suggest that the specific devices targeted in this cyber attack have design flaws or limitations. However, organizations should determine if they have the specific ABB or Siemens SIPROTEC switches/breakers whose communications protocols use the below standard. If so and if possible that organization should isolate/segment them from all network paths using air-gaps or hardened jump-boxes. Protocols identified:

- IEC 60870-101
- IEC 60870-5-104
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

**MONITOR AND DETECT:** Deploy Intrusion Detection Systems equipped with signatures for CRASHOVERRIDE/INDUSTROYER and/or capable of anomaly detection in network traffic going to and from the breakers.

**PLAN AND PREPARE:** Plan for and replace legacy devices and review and redesign network paths to the control rooms, if financially feasible.

**MITIGATE RISK:** For the switches and breakers targeted by this attack, ICS-CERT suggests the following mitigation methods:

- Configure firewall rules to appropriately restrict traffic to affected devices on Port 50000/UDP. Monitor traffic to affected devices on Port 50000/UDP with an intrusion detection system (IDS).
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as VPNs, recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. In addition, recognize that VPNs are only as secure as the connected devices.

---

**IDEFENSE UNDERGROUND ANALYSIS**

In addition to technical analysis of malware associated with CRASHOVERRIDE/INDUSTROYER and ELECTRUM, iDefense’s Threat Analysis and Reconnaissance (TAR) unit has conducted an analysis of chatter on criminal underground sources regarding available technical indicators. As of June 14, 2017, iDefense has not identified any threat actors or groups on the cyber-criminal underground that appear to be associated with the malware samples identified. This is consistent with iDefense’s assessment that ELECTRUM is likely to be a nation state-sponsored cyber-espionage group with sophisticated operational security procedures.

---

The attack on the electric grid was the culmination of a series of attacks on key Ukrainian financial and physical infrastructure. On December 6, 2016, visitors to the Ukrainian State Treasury website were redirected to the site www.whoismrrobot[.]com, a site created by an American multinational media conglomerate to promote a television show with a plot about an anti-social computer programmer who works as a cybersecurity engineer during the day, but at night he is a vigilante hacker. Ukrainian news sites soberly reproduced the text currently visible on the website as if it were a message directed at the Ukrainian government: “We lit the fuse of revolution. Now we decide if it sputters and dies, or truly ignites. Our real work is just beginning.” Soon other attacks occurred involving the following entities:

- December 6: Ukrainian State Treasury and Finance Ministry
- December 7: Ukrainian Pension Fund
- December 12: Volya Kabel Internet provider; State Executive Service, a Justice Ministry agency responsible for administering fines and imprisonment.
- December 13: Defense Ministry
- December 15: Ukrainian Railways railroad ticketing system
- December 16: Infrastructure Ministry
- December 17 to 18: Just before midnight on December 17, the Northern electrical generating substation Ukrainian: Pivnichni in the Kyiv suburb of Novyye Petrovtsy lost power.

This rash of outages represented a peak in an already high level of attacks. Before December 2016, 247 attacks were revealed against Information and Communications Technology (ICT) systems of diplomatic organizations, law enforcement, critical infrastructure elements and other state ICT resources, according to the Ukrainian Security service. A Ukrainian state agency employee said that in one day alone his agency had repelled 322 attempts to guess e-mail passwords.

Likely coming as part of a coordinated series of attacks, the CRASHOVERRIDE/INDUSTROYER operation would have taken time to prepare. It was probably not set off by particular near-term events, but was rather part of a long-hatched plan; however, its timing may have responded to or been pegged to short-term stimuli. As such, it is worth looking at the landscape for at least the previous several months.

The attacks coincided with many regional and global geopolitical events, so the timing seems suspicious. More details on these notable but not directly linked events that may imply a nation state’s intention to be disruptive in the region are available in a non-disclosed briefing.

### APPENDIX

#### CRASHOVERRIDE/INDUSTROYER MALWARE SAMPLES

Following the reports published by ESET and Dragos, iDefense captured the following sets of malware samples related to this incident:

#### SET 1: COMMUNICATION MODULES

**SAMPLE CM-1**

- MD5: F67B65B9346EE75A26F491B70BF6091B
- Size: 10,752 Bytes
- Time Date Stamp: 0x00000000 / Modified
- Compiler/Linker: MASM / Microsoft Linker(14.0)[EXE32]

Sample CM-1 communicates with the internal IP address 10.15.1.69:3128 sending POST commands using the default user-agent setting of the infected system. If the malware could not find the default value, then it will use the following hard-coded user-agent string:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)

The malware then communicates with the following external IP address that supposedly was a TOR exit node at the time of infection:

- 5.39.218.152

**SAMPLE CM-2**

- MD5: FC4FE1B933183C4C613D34FFDB5FE758
- Size: 10,752 Bytes
- Time Date Stamp: 0x58551BF6 (12/17/2016 4:05:26 AM)
- Compiler/Linker: MASM / Microsoft Linker(14.0)[EXE32]

Similarly, sample CM-2 has the same functionality; it is apparent that the CM1 sample has been slightly modified (the compilation time has been removed), and minor changes were made to fit the specification of the targeted system.
SET 2: SERVICE INSTALLER MODULES

SAMPLE SI-1

- MD5: F9005F8E9D9B854491EB2FBBDO6A16E0
- Size: 74,240 Bytes
- Time Date Stamp: 0x00000000 / Modified
- Compiler/Linker: Microsoft Visual C++ 9.0 - Visual Studio 2008 (E8) / Microsoft Linker(14.0)[EXE32]

The SI-1 sample installs a fraudulent Windows service under the name of defragsvc

Sample SI-2

- MD5: F9005F8E9D9B854491EB2FBBDO6A16E0
- Size: 88,576 Bytes
- Time Date Stamp: 0x585536EB (12/17/2016 6:00:27 AM)
- Compiler/Linker: Microsoft Visual C++ 9.0 - Visual Studio 2008 (E8) / Microsoft Linker(14.0)[EXE32]

The SI-2 sample installs a fraudulent Windows service under the name of tiering. The SI-2 sample, similar to CM-1 and CM-2, communicates with internal IP address 10.15.1.69:3128 sending POST commands using default user-agent setting of the infected system. If the malware could not find the default value, then it will use the following hard-coded user-agent string:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)

The malware then communicates with the following external IP address that supposedly was a TOR exit node at the time of infection:

- 93.115.27.57

Sample CI-3

- MD5: FF69615E3A8D7DDC4B7BF94D6C7FFB
- Size: 89,088 Bytes
- Time Date Stamp: 0x58539EF2 (12/16/2016 12:59:46 AM)
- Compiler/Linker: Microsoft Visual C++ 9.0 - Visual Studio 2008 (E8) / Microsoft Linker(14.0)[EXE32]

The SI-3 sample installs a fraudulent Windows service under the name of TieringService. The SI-2 sample similar to CM-1 and CM-2, communicates with internal IP address 10.15.1.69:3128 sending POST commands using default user-agent setting of the infected system. If the malware could not find the default value, then it will use the following hard-coded user-agent string:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)

The malware then communicates with the following external IP address that supposedly was a TOR exit node at the time of infection:

- 195.16.88.6

A comparison of SI modules indicates that SI-1 is a modified version while SI-2 and SI-3 incorporate the same functionality of CM-1 and CM-2 modules.
Set 3: WIPER MODULES

Sample WP-1

- MD5: AB17F2B17C57B731CB930243589AB0CF
- Size: 75,776 Bytes
- Time Date Stamp: 0x00000000 / Modified

The SI-1 sample installs a fraudulent Windows service under the name of defragsvc

Sample WP-2

- MD5: 7A7ACE486DBB046F588331A08E869D58
- Size: 76,800 Bytes
- Time Date Stamp: 0x00000000 / Modified

The wiper modules perform a process enumeration, and terminate the following running processes:

- audiodg.exe
- conhost.exe
- csrss.exe
dwm.exe
- explorer.exe
- lsass.exe
- lsm.exe
- services.exe
- shutdown.exe
- smss.exe
- spoolsv.exe
- svchost.exe
- taskhost.exe
- wininit.exe
- winlogon.exe
- wuautil.exe

The wiper modules then crawl all the internal hard drivers, and attached network drives (from C to Z), to find the following file, and file extensions. The targeted files will be overwritten with random data, making them irrecoverable.

- SYS_BASCON.COM,
- .v
- .PL
- .paf
- .XRF
- .trc
- .SCL
- .bak
- .cid
- .scd
- .pcmp
- .pcmi
- .pcmt
- .ini
- .xml
- .CIN
- .prj
- .cxml
- .elb
- .epl
- .mdf
- .ldf
- .bk
- .bkp
- .log
- .zip
- .rar
- .tar
- .7z
- .exe
- .dll
SET 4: RECON MODULE (PORT SCANNER)

SAMPLE RM-1

- MD5: 497DE9D388D23BF8AE7230D80652AF69
- Size: 174,080 Bytes
- Time Date Stamp: 0x582E4566 (11/17/2016 5:03:50 PM)
- Packer/Compiler/Linker: UPX(3.91)[NRV,best]/Microsoft Linker(14.0)[EXE32,console]

The recon module is a custom port scanner, and apparently was leveraged after initial infection for lateral movement and finding other systems on the infected network.
CVE 2015 5374 SIEMENS AG SIPROTEC 4 AND SIPROTEC COMPACT PRODUCTS INPUT VALIDATION ERROR DOS VULNERABILITY

Remote exploitation of an input validation error vulnerability in Siemens AG’s SIPROTEC 4 and SIPROTEC Compact products could allow attackers to create a denial of service (DoS) condition on the targeted host. An input validation error vulnerability has been identified in SIPROTEC 4 and SIPROTEC Compact products. The error occurs with the EN100 module as included in the products. The module fails to properly handle specially crafted packets destined for UDP port 50000.

An attacker can successfully exploit this DoS vulnerability by submitting a specially crafted packet for the host to process. Once an attacker has successfully exploited this vulnerability, a full reboot is required to put the appliance back into service.

SIEMENS HAS GIVEN THE FOLLOWING EXPLANATION ON THE PRODUCTS:

SIPROTEC 4 and SIPROTEC Compact devices provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application. The EN100 module is used for enabling IEC 61850 communication with electrical/optical 100 Mbit interface for SIPROTEC 4 and SIPROTEC Compact devices.

The malware has a component within which when given the IP address of the victim, will exploit the vulnerability by sending crafted UDP packets to port 50000 of that victim machine.

According to ESET, the malformed UDP packet contains only 18 bytes: 11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E.

iDefense considers this a MEDIUM-severity vulnerability because a remote DoS condition is possible. ICS-CERT suggests the following mitigation methods:

- Configure firewall rules to appropriately restrict traffic to affected devices on Port 50000/UDP.
- Monitor traffic to affected devices on Port 50000/UDP with an intrusion detection system (IDS).
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. In addition, recognize that VPN is only as secure as the connected devices.
Following the reports published by ESET and Dragos, iDefense captured the following sets of malware samples related to this incident:

**SET 1: COMMUNICATION MODULES**

**SAMPLE CM/hyphen.uc1**
- **MD5:** F67B65B9346EE75A26F491B70BF6091B
- **Size:** 10,752 Bytes
- **Time Date Stamp:** 0x00000000 / modified
- **Compiler/Linker:** MASM / Microsoft Linker(14.0)[EXE32]

Sample CM/hyphen.uc1 communicates with the internal IP address 10.15.1.69:3128 sending POST commands using the default user-agent setting of the infected system. If the malware could not find the default value, then it will use the following hard-coded user-agent string:

- **Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)**

The malware then communicates with the following external IP address that supposedly was a TOR exit node at the time of infection:

- **5.39.218.152**

**SAMPLE CM/hyphen.uc2**
- **MD5:** FC4FE1B933183C4C613D34FFDB5FE758
- **Size:** 10,752 Bytes
- **Time Date Stamp:** 0x58551BF6 (12/17/2016 4:05:26 AM)
- **Compiler/Linker:** MASM / Microsoft Linker(14.0)[EXE32]

Similarly, sample CM/hyphen.uc2 has the same functionality; it is apparent that the CM1 sample has been slightly modified (the compilation time has been removed), and minor changes were made to specify the specific of the targeted system.