THREAT INTELLIGENCE REPORT

CYBERATTACKS AGAINST UKRAINIAN ICS

sentryo

BY VYTAUTAS BUTRIMAS

SUBJECT MATTER EXPERT, RESEARCH AND LESSONS LEARNED DIVISION, NATO ENERGY SECURITY CENTER OF EXCELLENCE[1]

FOREWORD

Since 2008 we have seen a steady progression in the severity and scale of cyberattacks on critical infrastructure.

In 2010 Stuxnet malware was placed at a nuclear enrichment facility in Iran that tampered with the control of equipment used in a critical process resulting in physical damage. In 2012, malware was used to erase the data on 30,000 computers belonging to one of the world's largest energy companies. Since 2011 malware has been found searching the Internet for locations of particular brands of industrial control equipment. In 2014 the control systems of a German steel mill were compromised denying view and control of equipment which also resulted in physical damage. In the spring of 2015 a sophisticated cyber-attack targeted the communications systems of France's national TV network TV5Monde.

The trend for increasing threats from cyberspace **is getting worse**. Cyber-attacks on critical infrastructure have also become associated with political and even military conflict. In 2008 cyber-attacks coincided with a traditional military operation for the first time in the Russian-Georgian War which arose out of a long political conflict between the two countries over separatists in the Georgian provinces of Abkhazia and South Ossetia.

The cyber-attack on Ukraine's power grid just before Christmas in 2015 also occurred in the same context of political-military conflict over Russia's illegal annexation of the Ukrainian province of Crimea. Of even greater concern is that these cyber incidents are suspected to have been caused **not by cyber criminals or student hackers but by state supported advanced and persistent threat (APT) actors**.

The successful cyber-attacks that took place against a Ukrainian regional power grid in December 2015 and the apparently even more sophisticated follow up attack on the Ukrainian capital nearly a year later is another serious wake-up call for security policy practitioners. All of these wake-up calls are taking place in an increasingly militarized cyberspace environment, with many nations treating it as a new domain for military operations. Until the international community recognizes **the seriousness of this new threat and organizes its response to manage this unsettling trend in cyberspace**, the operators of critical infrastructure can take steps to reduce the risk and potential for damage to their critical systems.

The cyber-attacks executed against the Ukrainian power grid and other sectors of critical infrastructure in 2015 are examined **with a purpose to derive some useful lessons learned that can be applied by operators of critical infrastructure**. In addition to technical solutions, this paper also stresses the importance of information sharing and proposes what policymakers can do to further support the technology based efforts of operators and industry at the international level.

[1] The views expressed by V. Butrimas are for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. These views do not represent the opinions or policies of NATO or NATO ENSEC COE or any other institution. The views presented in the articles are those of the authors alone.

INTRODUCTION

BY LAURENT HAUSERMANN
SENTRYO CO FOUNDER

Since Christmas 2015, the Sentryo Security Labs has analyzed in detail the various reports published by different actors in the cybersecurity world and the available information from malware feeds, technical blogs or social media regarding the Ukainian CyberAttacks. The resulting reports were part of the Threat Monitoring service offered to paying Sentryo customers. Following the second wave of attacks in December 2016, the Sentryo team has decided to publish a public version of this report to share this review. **This also includes a technical part on the newly found malware called INDUSTROYER/CrashOverride supposedly used during the second attack.** This article also includes a section about **the NotPetya attack** which recently targeted many Ukrainian businesses and companies doing business with Ukraine.

IT cybersecurity analysts tend to look at the attack vectors in depth. They provide great details about the way attacks are developed focusing on the technical perspective. **Is the design well made?** Does it embed lots of different hacking techniques (0day, obfuscation, etc.)? We think this approach is misleading in the growing field of OT Monitoring cybersecurity. Attack vectors are definitely part of the problem but their physical impact must be careful analysed. OT impacts safety, health and environment where IT is about data. OT impact is about casualties not only money and data losses.

Moreover, fear mongering (i.e. tricks to have fear drive the sales process) is not part of the Sentryo culture. That's why we are being **very careful and trying to distinguish what can be taken as true from what is**, because there is no other evidence, pure speculation. In this document, the reader will have **an overview of Facts and Claims made in the cybersecurity community and Sentryo's views on the subject**. Our goal is also to share our analysis to the whole SCADA/ICS/DCS/OT security community. Threat intelligence shall be seen as an ongoing public debate between **different skilled experts such as instrumentation engineers, control engineers, cybersecurity experts, CISOs, forensics gurus, etc**.

We welcome any feedback or updates to this document and will definitely include all evidence that is lacking in this version. This document also includes a great contribution that will stress the need for more Threat Information Sharing. We warmly thank its author.

To ease the reading and provide a quasi executive summary, we will start with a detailed potential scenario of the first 2015 attack which has been documented. Please note that 2016 incidents do not have enough documentation to provide such a scenario description. It should also be noted that the attack campaign has apparently continued **since early january 2017 with new technical elements coming to light regularly.** Check out the Sentryo website to download the latest version.

At Sentryo, we remain committed to helping industrial asset owners, including when they face a crisis. Do not hesitate to contact us!

SUMMARY

Les contributeurs :

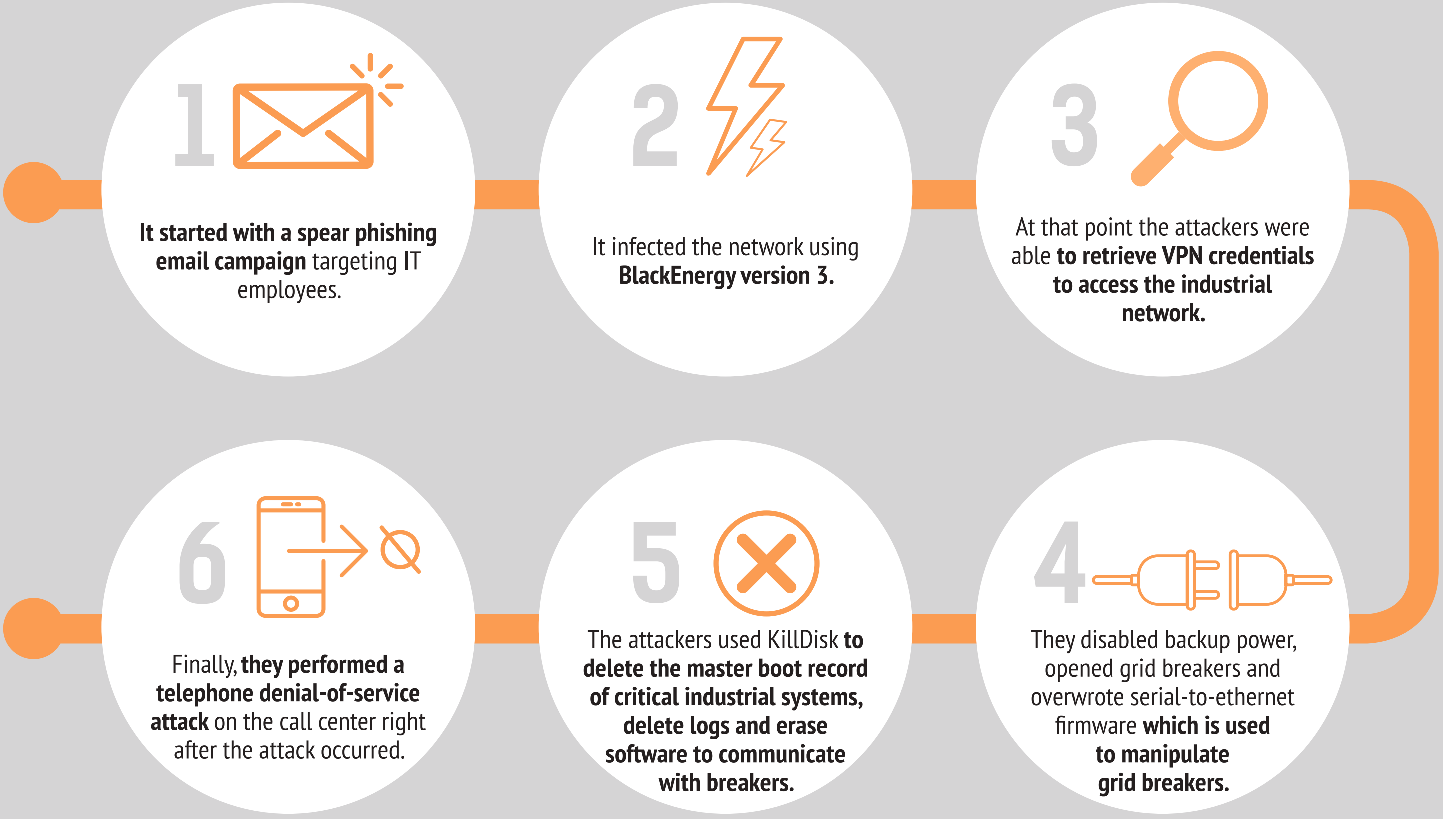
Laurent Hausermann - *Sentryo Co-founder & COO* / Patrice Bock - *Sentryo Customer Success Manager*
Romain Francoise - *Sentryo CTO* / Antoine de Nervaux - *Sentryo Security Engineer*

EXECUTIVE SUMMARY

POTENTIAL SCENARIO FOR THE FIRST ATTACK

2015 DECEMBER

DUE TO THE ANALYSIS AND DATA DEVELOPED IN THE PRESENT DOCUMENT, WE ARE ABLE TO DESCRIBE THE MOST PROBABLE ATTACK SCENARIO. INDEED, IT APPEARS THAT IT WAS TARGETING THE CORE OF THE INDUSTRIAL NETWORK:



1 **It started with a spear phishing email campaign** targeting IT employees.

2 It infected the network using **BlackEnergy version 3.**

3 At that point the attackers were able **to retrieve VPN credentials to access the industrial network.**

4 They disabled backup power, opened grid breakers and overwrote serial-to-ethernet firmware **which is used to manipulate grid breakers.**

5 The attackers used KillDisk **to delete the master boot record of critical industrial systems, delete logs and erase software to communicate with breakers.**

6 Finally, **they performed a telephone denial-of-service attack** on the call center right after the attack occurred.

- ✓ The scale of the attack was able to cut power **in a whole geographic area of Ukraine** as three independent electricity distributors were **simultaneously** attacked.
- ✓ They also used hacking techniques to support and amplify the cyberattack. Their goal was clearly **to stop, or at least slow down, operations during the power restore processes**.
- ✓ Finally, they performed **a telephone denial-of-service attack** on the call center. Citizens were not able to call their power operator thus amplifying an already **chaotic situation**.
- ✓ The impact of this attack was that **more than 50 substations went offline** and **more than 200,000 homesremained without electricity for a period of time**. Ukrainian operators were able to restore power **after 6 hours** using manual on-site switches like in “the old days”.

FACTS & REPORTS

2015 INCIDENT

THE DECEMBER 23 OUTAGE AT WESTERN UKRAINE'S PRYKARPATTYAOBLENERGO/ IVANO-FRANKIVSK PLANT CUT POWER TO MANY CUSTOMERS FOR ABOUT SIX HOURS. REPORTS VARY FROM 80,000 TO 1.4 MILLION CUSTOMERS IMPACTED.

VARIOUS ANALYSTS, INCLUDING ESET, A WELL KNOWN ANTIVIRUS VENDOR, HAVE PROVIDED DEEP ANALYSIS OF THE MALWARE.

THEY FOUND THAT:

① The malware was distributed by a "**dropper**". This dropper was an Excel macro embedded in **a malicious spreadsheet file.**

② An updated analysis found that there was also an alternate attack based on **a Microsoft Word Document embedding macros.**

③ In reports about the December 2015 attack, the "dropper" used a variant of **the Black Energy** (3rd version) trojan (also called Lancafdo by Symantec). Black Energy is not a new malware. It's been used since 2007 in various campaigns including a famous one in 2014 against energy companies. Black Energy enables attackers to control their malware via a control center (C&C or C2) and enables them to do horizontal propagation (moving from one computer to another).

④ In reports about a replica attack performed in January 2016 (see next page for more details), the compromission chain was different and Black Energy was replaced by **a custom-made malware payload based on a variant of the open-source gcat backdoor**. Incidentally, the spear phishing email contained an invisible PNG image to track when the victims viewed the email and the PNG was hosted on a server located in France and hosted by Online SAS. The IP pointed to a domain name associated with **a Hong Kong company** which was probably a collateral victim in this case (compromised web server).

⑤ In the December campaign the attackers launched a "wiper" named "**KillDisk**" or "**Disakil**". This wiper is a destructive malware. It is able to kill processes and services on a server and also wipe (i.e. format) the whole hard disk.

⑥ A known "feature" of Disakil is to stop and delete a named service and write its corresponding executable file on the hard drive with random data in order to make restoration of the system more difficult. Disakil was used against the service called "sec_service.exe". This service appears to belong to 'Serial to Ethernet Connector' software by Eltima. This software allows **access to remote serial ports over network connections**. These kinds of "remote serial" connections are used to pilot PLCs or RTUs which do not have a way to connect via Ethernet (via a dedicated module). This is quite common in old installations that were deployed **before 2000**.

⑦ As of April 2016, it is still unclear if the attack itself (breaker opening) was performed remotely using a digital / **computerized weapon or was the result of a human** and operational lapse but the likelihood of a digital weapon is high.

⑧ The organization NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) has published a book called "**Cyber War in Perspective: Russian Aggression against Ukraine**". From this book, a presentation at the BlackHat 2016 conference was performed: "**Cyber War in Perspective: Analysis from the Crisis in Ukraine**" by Kenneth Geers. This talk added some interesting points to this analysis. Mainly, the goal was also to steal VPN credentials to SCADA; to change passwords to access to the electric grid; to disable the backup power; to overwrite the serial-to-ethernet converter firmware; to open 3 circuit breakers; to launch the killdisk and to TDoS (Telephony Denial of Services) customer call center. The impact was **more than 50 substations offline and more than 200,000 homes without electricity**.

2016 INCIDENT

ON DECEMBER 18, 2016 THE SECOND POWER OUTAGE OCCURRED IN UKRAINE CAUSING SOME BLACKOUTS IN KIEV FOR LESS THAN ONE HOUR. THIS WAS THE TIME NEEDED FOR AN EXPERT TEAM TO GO ONSITE AND FIX THE PROBLEM USING A MANUAL PROCEDURE.

This second attack was targeting another grid company named **Ukrenergo**. This incident caused multiple blackouts in the Ukrainian capital - Kiev and a complete power loss for the northern part of Kiev on the right bank of the Dnieper river and the surrounding region.

Experts of the grid company were able to fix the situation **in less than 1 hour** with a manual procedure. This emergency response team was on site **30 minutes after the outage.**

The faulty component was **the automation control systems piloting a substation** in a village near the Kiev city. Automation systems in such substations control how power coming from power plants at high voltage is transformed to lower voltage for consumer and industrial use.

The main website of the power grid had been **unreachable** for a couple of days during and after the attack. The head of Ukrenergo had to publish a quick statement on Facebook (provided in the appendix).

When the situation had been recovered, the company published an official statement available on their website.

It states "Among the possible causes of failure are considered hacking and equipment malfunction (crashes). Timely police were involved and conducted a thorough investigation into the accident, which will be to inform the public. By the end of the official investigation into the case management of all objects SE 'NEC' Ukrenergo with automatic control system was transferred to the local level."

In the middle of January Ukrenergo confirmed that the source cause of this power outage was **malicious**. The authors are still undetermined.

Based on an article from Reuters, Ukrenergo said in comments emailed to Reuters: "Preliminary findings indicate that workstations and Supervisory Control and Data Acquisition (SCADA) systems, linked to the 330 kilowatt sub-station "North", were influenced by external sources outside normal parameters. [...] The analysis of the impact of symptoms on the initial data of these systems indicates **a premeditated and multilevel invasion**"

Law enforcement officials and cyber experts are still working to compile a chronology of events, draw up a list of compromised accounts, and determine the penetration point while tracing computers potentially infected with malware in sleep mode.

So far, no huge technical details related to the attack have been released publically. Indeed Marina Krotofil from Honeywell and Oleskii Yasinskiy from ISSP shared some information confirming the attack without going further c**oncerning technical details related to this attack**.

According to CyberX, a targeted malware campaign called **BugDrop** could have been performed in the reconnaissance phase. Indeed, the goal was to retrieve a maximum amount of information regarding the final target which was **the power grid. The complexity of the malware was quite impressive**. Once the target was infected through a targeted phishing campaign and the malware deployed, it retrieved a lot of information from the network and also screenshots, documents, passwords and audio recordings using the microphone. For each infected target, the data was encrypted with Blowfish using a "user-ID". **The exfiltration was performed through Dropbox services. The assumption linking this malware and the attack is detailed in the claims section below.**

2017 AN UPGRADED OT MALWARE

THE 12TH OF JUNE 2017, RESEARCHER ANTON CHEREPANOV FROM ESET PUBLISHED A COMPREHENSIVE TECHNICAL REPORT REGARDING THE MALWARE CALLED INDUSTROYER. DRAGOS HAS ALSO PROVIDED AN IN-DEPTH ANALYSIS UNDER THE NAME OF CRASHOVERRIDE.
THIS MALWARE IS PROBABLY LINKED TO THE DECEMBER 2016 UKRAINE ATTACK. INDEED, THIS MALWARE HAS BEEN DESIGNED TO DISRUPT THE WORKING PROCESS OF INDUSTRIAL CONTROL SYSTEMS USED IN ELECTRICAL SUBSTATIONS.

INDUSTROYER / CRASHOVERRIDE is the first OT malware designed specifically to attack electric grids.

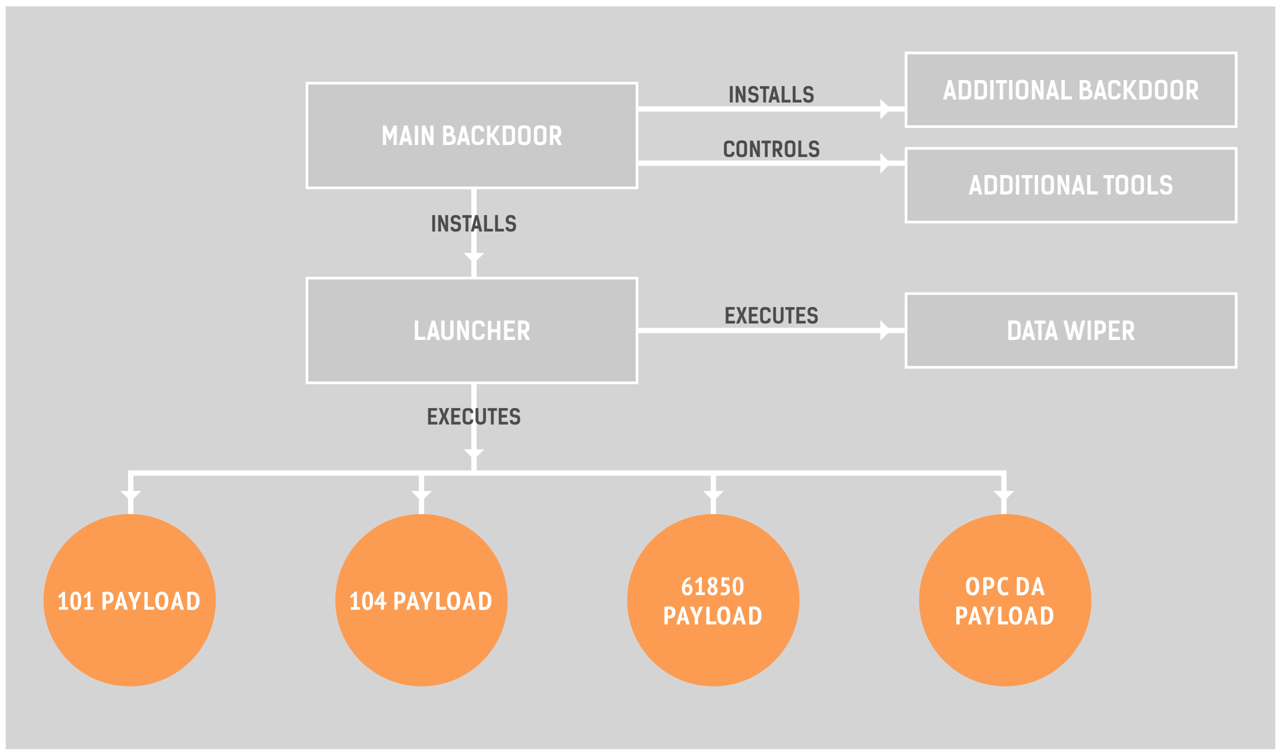
This malware supports four differents industrial protocols:

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

It is obvious that since the first 2015 attack (using Blackenergy and Killdisk) and this malware, there is a huge gap and attackers have **improved their capacities**. The malware is now able **to control switches and breakers**. ESET have seen indications that this malware could have been the tool used by attackers to cause the power outage in December 2016. **The infection vector remains unknown but the investigation is still ongoing**.

Before going deeper into the malware, let's have a look at embedded components. As we can see in the schematic below, the malware embeds:

✓ Two backdoors (C&C through HTTPS)
✓ A launcher
✓ A wiper
✓ Four differents payloads corresponding to four different industrial protocols



Source ESET: Simplified schematic of Win32 / Industroyer components

THE IT PART OF THE MALWARE

Regarding the C&C it is interesting to note that a local proxy configuration has been hardcoded in the malware. The local proxy is the way to access the Internet from the local network. This configuration is adapted to the local network. The fact that the local proxy has been **hardcoded in the malware**, means having technical knowledge about the target. Due to this, we can conclude that it was **a targeted attack**. In addition, without proper modification of the malware, it cannot be used on another target.

Another interesting thing is the way the malware deploys the backdoor to the victim to be able to spawn a shell, download a file and execute a program. At the beginning, when the backdoor is executed on the victim, it stays in RAM and starts communicating with the C&C. At this moment, through the C&C, information related to the victim is **exfiltrated and analyzed to find vulnerabilities on the targeted system**. Once found, the exploit is sent through **the backdoor** (still in ram) to perform a privilege escalation. **And now the fun part begins:**

- ✓ An initial persistent backdoor (the main) is deployed to replace **a non-critical Windows service**.
- ✓ A second persistent backdoor (the backup) is installed through a malicious Microsoft Notepad on the victim. Each time the Notepad is used **the backdoor is also executed**.

THE OT PART OF THE MALWARE

IEC 101 PAYLOAD COMPONENT

The payload uses the IEC101 protocol (IEC 60870-5-101) which is used for communications between industrial control systems and remote terminal units. If the target machine communicates with a RTU using IEC101, the IEC101 payload is used. It parses a configuration file created by the hacker to determine the process's target, it kills it and opens COM ports to communicate with the RTU and also to prevent the original process from communicating with the RTU. Once the communication has been established, the malware sends IEC101 C_SC_NA_1 and C_DC_NA_1 packets to switch off the RTU at the specified Information Object Address (IOA).

IEC 61850 PAYLOAD COMPONENT

This payload uses the IEC 61850 standard. This standard describes a protocol used for multi-vendor communication among devices that perform protection, automation, metering, monitoring, and control of electrical substation automation systems. The 61850 payload uses only a small subset of the protocol to produce its disruptive effect. The payload looks for a configuration file defining targets and commands as seen previously. If the payload does not find the file, it starts to scan the network for TCP port 102 (used by IEC 61850). Once found, the payload sends a connection request packet using the COTP protocol. If successful, it sends a InitiateRequest and a getNameList request to compile a list of targets, variables and contents. Afterwards, the payload parses received data for variables that contain the strings CSW (corresponds to logical nodes used to control circuit breakers and switches). For each of them it will try a read and a write order to change the position of the breaker.

IEC 104 PAYLOAD COMPONENT

This payload uses the IEC104 protocol (IEC 60870-5-104) which is used to send IEC101 on a TCP/IP network. Similar to the IEC101 payload, the DLL reads a configuration file containing information regarding the target including the IP address, the port, the ADSU (Application Service Data Unit) and the operation. The goal of this payload is to connect to a specified IP address and send packets with the ASDU address to interact with the IOA to switch it off. The OT impact is quite important. By using this payload, the malware is able to communicate on the OT network using the IEC104 protocol and to send orders to breakers. At the same time, the malware is also able to communicate on the IT network to receive orders from the C&C servers located outside of the target.

OPC DA PAYLOAD COMPONENT

This last payload implements a client for the OPC Data Access protocol. Once executed, the payload enumerates all OPC servers and OPC items and the server. In the payload source code, we can see that it is looking for specific strings in OPC item names (ctlSelOn, ctlOperOn...). These names may suggest an interest in ABB solutions such as the MicroSCADA range. For each of the found OPC items, the payload changes its states.

2017 ANOTHER MASSIVE INFECTION «NOTPETYA»

ON JUNE 27TH, THE UKRAINIAN RADIO HOLOS STOLYTSY WERE ABLE TO CONTINUE THE RADIO DIFFUSION USING AN ANALOG RADIO EMETOR: THEIR MAIN SERVER WAS INFECTED BY A MALWARE... NOTPETYA WAS BORN...

Still in 2017, **another massive attack has been performed against ukrainian critical infrastructure**. Although the payload did not include exploits targeting industrial systems, it did significantly impact manufacturing plants, as well in Ukraine as world-wide, with 6-figure losses at several european corporations.

What happened: on June 27th, the main server of the Ukrainian radio Holos Stolytsy was infected by a malware. The radio was only able to continue the diffusion using an analog radio emetor. **This was "NotPetya"'s first strike!** Soon after this first detection, other infections were quickly detected around the world. But NotPetya is not Petya: let's not mix the original 2016 Petya ransomware and the one we are talking about, which is not a ransomware, and therefore was named "NotPetya".

Basically, a ransomware is a malware that prevents file usage (e.g. using encryption) and requests a ransom to decrypt them. Petya is a ransomware published in March 2016. The one which started in June 27th is quite different although based on the ransomware Petya. The main difference is the fact that it is not a ransomware. Once NotPetya is executed on a platform, it encrypts the whole hard drive but does not exfiltrate or embed a method to decrypt stored data. **It means that NotPetya's authors were not interested in money.**

NotPetya embeds an effective infection method using the same exploits that Wannacry uses, targetting Windows SMB. Unlike Wannacry, NotPetya tries to exploit remote machines located on the same local network. But the main point is **NotPetya has functionalities to retrieve and exfiltrate passwords and some remote administration functionalities**.

We can directly conclude that NotPetya was not designed to make money or to control a BotNet but instead **to infect a precise target**. The initial infection vector came from a malicious update of the Ukrainian countability software M.E.Doc. Indeed, hackers took the control of a M.E.Doc's server update and infected an update with NotPetya.

This Ukrainian radio was not an isolated case. In fact, lots of Ukrainian institutions and companies have also been infected and, since NotPetya continued to spread itself through SMB, the infection rate was quite high. Several French companies, like Saint Gobain, have also been infected. As for previous attacks using the same vulnerability (Wannacry for instance), industrial systems were impacted, because of either direct network connections between IT and OT domains, or laptops or other equipments connected to both domains.

Determining the goal or attributing the malware to a country is quite hard. Russian Rosneft also has been impacted. The Ukrainian Cyber Police officially confirmed that M.E.Doc servers were backdoored on three different occasions. The total losses, due to the alleged negligence of Intellect-Service, might be in the range of **$1bn considering that St Gobain alone has declared a loss of $250M in revenue**.

CLAIMS

2015 & 2016 INCIDENTS

2015 INCIDENT

- Ukraine's state security service SBU has blamed Russia but the nation's energy ministry said it would hold off on attribution until after it finishes **a formal probe**.
- A press statement on the SBU website alleged the discovery of malicious software responsible for these outages on the networks of regional power companies. According to the SBU press statement, the cyberattack was accompanied **by a barrage of phone calls to their technical support telephone numbers which would have acted like a denial of service (DoS) attack**.
- The U.S. cyber intelligence firm iSight Partners said it has determined that a Russian hacking group known as **Sandworm** caused this unprecedented power outage in Ukraine. Many other US based companies are pointing to Sandworm as the “hacking” unit.
- Some press organizations are claiming this is the first known Grid hack. They should remember, even unconfirmed, that the 2003 blackout in the US east coast may have been caused by a cyberattack. Also, the FBI has already claimed that Daesh has tried unsuccessfully **to hack the national US power grid**.
- According to the SANS ICS blog, the attack was a coordinated effort which targeted several power sub-companies and included a flooding attack on their phone support systems to prevent legitimate customers from reporting a power cut which would alert the on-call personnel to the problem. According to the same source (unconfirmed), the staff in the affected companies **acted quickly to bypass the SCADA systems and run everything in manual mode by acting on the main breakers** which restored service in under 6 hours. This would not have been possible in a modern grid installation which relies heavily on automation and can't be run in “manual mode”.
- A Ukrainian telecoms engineer has raised doubts about the widely reported link between BlackEnergy attacks and power outages in his country. Named Illia Illin, per “**The Register**” article, he claims “First of all, there weren't any blackouts in Boryspil (KBP)”.
- An investigation team led by US government officials has released a report as part of the ICS-CERT initiative (see sources section). This report remains vague about the exact insertion methods and attacker techniques and focuses on proactive defenses that would have prevented the attack. Also, in the current political context, it's hard to imagine that interviews of Ukrainian operators by US government officials would be **100% factual and accurate**.
- SANS ICS has released a new detailed report which summarizes the information collected by the investigation team (see sources for “DUC5”). The report uses the Cyber Kill Chain framework to characterize the different phases of the attack. However, many technical details remain vague (especially concerning attacker reconnaissance and remote control by VPN). An analysis of the alleged malware used is provided. **The RAT tool used by the attacker is not mentioned.**

2016 INCIDENT

Several assumptions have been released since this second outage. For the time being, technical details regarding the attack have not been published. The only “technical” finding is **the threat vector.** Indeed, the SCADA stations had been compromised by an **external source**. Marina Krotofil, lead cyber-security researcher at Honeywell who assisted in the investigation, declared “It was an intentional cyber incident not meant to be on a large scale... they actually attacked more but couldn't achieve all their goals”. Also from Marina Krotofil, “hackers are thought to have hidden in Ukrenergo's IT network undetected for six months, acquiring privileges to access systems and figure out their workings, before taking methodical steps to take the power offline”. So far, we have no information confirming that the techniques used are the same or not.

According to CyberX, the malware used during the BugDrop operation detailed in the facts section **could have been used during the reconnaissance phase**. Indeed, the compilation date and some targets may lead to this conclusion. The malware was compiled several times **between June 2016 and end of October 2016**. Concerning identified targets here is the list:

- A company that designs remote **monitoring systems for oil & gas pipeline infrastructures.**
- **An international organization** that monitors human rights, counter-terrorism and cyberattacks on critical infrastructure in the Ukraine.
- **An engineering company** that designs electrical substations, gas distribution pipelines, and water supply plants.
- **A scientific research institute.**
- **Editors of Ukrainian newspapers.**

The assumption linking this malware and the attack is based on these targets mainly **located in Ukraine and linked to energy** but also due to techniques used like the reflective DLL injection (loading malicious code without calling the normal Windows API calls) which was used during the first attack. Another hint comes from the compilation time.

USING SENTRYO ICS CYBERVISION TO COPE WITH SUCH ATTACKS

SENTRYO ICS CYBERVISION OFFERS AN OT MONITORING SOLUTION THAT PROVIDES AN OPERATIONAL CAPACITY TO PREVENT, DETECT AND RESPOND TO CYBERATTACKS.

ICS CyberVision continuously listen communications between devices on the OT network and extract meaningful data. Those data are then used to create a behavorial «template» of the OT network which is then used as a white list to detect anomalies. ICS CyberVision use IA algorithms to caracterise and prioritize those anomalies in order to eliminate false positive and facilitate the remediation process. In addition scripts from Sentryo Security Labs are provided to ICS CyberVision users. These scripts use the CyberVision Center API to mine their CyberVision installations to check for some Indicators of Compromise (IOC).

In the case of organization is in the energy sector and may have been targeted by this new Black Energy campaign or the latest Grizzly Steppe (see the DHS report), **we strongly encourage them to run these scripts and check their ICS**.

Moreover, if ICS CyberVision had been deployed inside the process and control networks of an Energy corporation, it would have detected several weak signals enabling the local team to stop the attacks early:

- ✓ Regarding Black Energy, ICS CyberVision would have detected unknown connections to **a remote Internet website** (the C&C channels). These connections would have been seen as a change compared to the baseline (a set of given network behaviors) defined by plant operators.
- ✓ Regarding Industroyer/CrashOverride, ICS CyberVision would have detected any new connections to a remote Internet website (the C&C channels), and also new and strange behaviours on the OT networks like multiple OT network scans and critical OT communications like orders.
- ✓ Regarding the Disakil "wiper", ICS CyberVision would have detected the disappearance of TCP connections **between the SCADA stations and the PLCs / RTUs**. The defined baseline includes these connections and the fact that they stopped being active would have automatically been detected as a change **by the difference engine**.
- ✓ Regarding the breaker manipulation, ICS CyberVision would have analysed IEC 101 (serial over ethernet) flows and detected the order to open up the breaker and to switch off power. CyberVision would help **to trace down the hackers to particular infected machines**.
- ✓ Regarding the Siemens safety equipment DoS vulnerability used by Industroyer (CVE-2015-5374), **it will be detected by ICS Cybervision thanks to its Knowledge Database**. Back in 2015, Siemens provided a firmware update fixing this issue. It is even more important today to patch these equipments. Our solution can help by clearly identifying the potentially affected devices in the network.

The only vector which would have remained undetected by ICS CyberVision is the "**dropper**" i.e. an Excel spreadsheet or Word document in later case. It is the responsibility of an email gateway or an endpoint protection software to detect such attack vectors. The malware could also have been inserted via a malicious USB drive and only endpoint protection software can prevent these attacks.

Since Stuxnet, the malware Industroyer / CrashOverride is the first advanced and targeted industrial malware we have seen **with this level of maturity**. From a defense point of view, this malware also shows the need for an ICS network security monitoring capability to be able to detect these advanced attacks early in the kill chain.

Let's have look at the kill chain and the malware impact. This is important because investigations are still ongoing and some information may have not been communicated. **Because of this, Phase 1 and part of the Phase 2 are pure assumptions using our experience and external claims:**

PHASE 1

PREPARATION

1. **RECONNAISSANCE** › harvesting for email; industrial protocol used and target proxy configuration

2. **WEAPONIZATION** › development of the malware including the dropper, industrial payloads, the backdoor, the wiper and the C&C server

PHASE 2

INTRUSION

3. **DELIVERY** › probably an email with a link or an attachment to the dropper

4. **EXPLOITATION** › find and exploit a vulnerability on the victim's computer to be able to install the malware

5. **INSTALLATION** › install the malware as a non-critical Windows service program and install a new malicious Microsoft Notepad program

PHASE 3

ACTIVE BREACH

6. **COMMAND & CONTROL (C&C OR C2)** › communicate regularly with the C&C (the active period can be configured)

7. **ACTIONS AND OBJECTIVES** › scan the network using embedded payloads and configuration files dropped by the C&C; detect any breaker; turn it off and use the wiper.

THE NEED OF THREAT INFORMATION SHARING

BY VYTAUTAS BUTRIMAS - SUBJECT MATTER EXPERT,
RESEARCH AND LESSONS LEARNED DIVISION, NATO ENERGY
SECURITY CENTER OF EXCELLENCE[2]

Today's cyber attacker is several steps ahead of the defender. This is especially so in the case of a single operator trying to defend against a state resourced APT attacker. This is an unfair match, similar to a high-school soccer team's chances of defeating a FIFA World Cup contender. It is no contest unless the school team's capabilities are significantly enhanced. **It is important to realize that the operator-defender has a complex task of managing and protecting increasingly interconnected and sophisticated systems enabled with the latest advances in information and communications technologies (ITC).**

Technologies that in addition to providing new features and possibilities for remote management and control also introduce vulnerabilities for an adversary to exploit. The operator now faces a difficult challenge in managing systems that are vulnerable to not only intentional but also unintentional cyber incidents. Incidents that result from errors in managing interconnected and complex systems. The attacker needs only to find **a single weakness** in the design or exposed vulnerability in order to defeat all the wide-ranging efforts of the defender.

In order for the operator of critical infrastructure to avoid becoming an isolated target for an adversary that often is several steps ahead of the defender he must improve his relationship among operators of critical infrastructure, manufacturers, academia and Government institutions responsible for cybersecurity. The aim should be in **setting up a mechanism that will facilitate the timely sharing of information on cyber threats, coordinating a response to an incident and sharing lessons learned**. At the local level, National cybersecurity councils that represent the communities of interest (CoI) should be created as a first step in setting up a national cybersecurity capacity for protecting critical infrastructure from these advanced and persistent threats from cyberspace.

This is not an easy task since fear of lawsuits, embarrassment and concerns for confidentiality often make operators as well as manufacturers of control equipment reluctant to share the information needed to enhance resilience and enhance recovery capabilities. This lack of sharing can only contribute to making defenders more isolated and less aware of the significance of the problem. In addition to the high level National council a working level network for timely sharing of threat information and lessons learned should be created for dealing with immediate issues and facilitating coordinated effective response in times of emergency. **In summary it is only through cooperation and sharing of information among a community of interest that an operator-defender can hope to deal with today's advanced and persistent threats emanating from cyberspace.**

[2] The views expressed by V. Butrimas are for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. These views do not represent the opinions or policies of NATO or NATO ENSEC COE or any other institution. The views presented in the articles are those of the authors alone.

CONCLUSION

THIS CASE DEMONSTRATES THAT IS VERY HARD TO:

COLLECT ENOUGH DATA TO HAVE A DEEP TECHNICAL UNDERSTANDING OF THE HACKERS TECHNIQUES AND TACTICS,

ESTABLISH THE IDENTITY OF THE DIFFERENT ACTORS,

KNOW IF THE CYBERATTACK WAS SPECIFICALLY BUILT TO IMPACT ONLY THIS INDUSTRIAL FACILITY,

MAKING THE DIFFERENCE BETWEEN FACTS AND CLAIMS.

The case also demonstrates the absolute need for a monitoring capability on such ICS systems. Indeed, this kind of attack is quite hard to avoid when your IT network has been infected. Nevertheless, with adapted tools, hints of attack and / or compromission on the industrial network can be detected in order to prevent and / or mitigate the attack as soon as possible.

Everyone reading cybersecurity reports must keep in mind that Ukraine is at war with Russia. This tense international context probably explains the large number of different "statements" made by the Ukrainian and Russian governments.

In any case, this cyberattack should not be seen as a new Stuxnet. Black Energy is a quite old malware. No zero-day (i.e. unknown attack vector) was used. The destruction payloads, even if they are very impactful, are quite trivial without a fine-grained PLC reprogrammation. This attack underlines the extreme weakness of OT components which were never designed with maliciousness in mind.

As always, the Sentryo security team is deeply involved in the identification and analysis of the latest industrial threat vectors. We will follow the ongoing investigation related to the Ukraine attack.

FROM THE FOREWORD

Critical Infrastructure: "refers to assets of physical and computer-based systems that are essential to the minimum operations of an economy and its government. They include… telecommunications, energy, banking and finance, transportation, water systems and emergency services, both government and private."
http://www.infracritical.com/?page_id=73

Langner, R., To Kill a Centrifuge,
http://www.langner.com/en/wp-content/uploads/2013/11/To- kill-a-centrifuge.pdf

Rashid, F., Inside The Aftermath Of The Saudi Aramco Breach, Dark Reading, 8/8/2015
http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the- saudi-aramco-breach/d/d-id/1321676

Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) US ICS-CERT
https://ics-cert.us- cert.gov/alerts/ICS-ALERT- 14-281- 01B
Original release date: December 10, 2014

Sandworm and SCADA, Trend Micro
http://blog.trendmicro.com/sandworm-and-scada/ October 16, 2014

The State of IT Security in Germany 2014, Federal IT Department (BSI) Germany. p. 31.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany- 2014.pdf?__blob=publicationFile&amp;v=3

FIRST INCIDENT REPORTS

http://www.oe.if.ua/showarticle.php?id=3413

http://briz.if.ua/33432.htm

SECOND INCIDENT REPORTS

http://www.ukrenergo.energy.gov.ua/pages/en/detailsnew.aspx?nid=3387

http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

INTECH / ISA ANALYSIS

InTech, March/April 2017 issue, special section «Cybersecurity», a publication of the International Society of Automation
wwww.isa.org/intech

DETAILED ANALYSIS

http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations

http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf

https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

https://ics.sans.org/duc5

http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

https://motherboard.vice.com/en_us/article/there-will-always-be-internet-outages-so-buckle-up

https://www.youtube.com/watch?v=lTwsDLO3C44

https://motherboard.vice.com/en_us/article/who-hacked-the-lights-in-ukraine

CLAIMS

http://www.theregister.co.uk/2016/01/27/ukraine_blackenergy_analysis/

https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

http://in.reuters.com/article/ukraine-crisis-cyber-attacks-idINKBN1491QI

IOC

http://cert.gov.ua/?p=2464

GCAT C&C CONTROL USING GMAIL

https://github.com/byt3bl33d3r/gcat

NATO CCD COA

https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html

GRIZZLY STEPPE DHS

https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

SOURCES

BLACKHAT 2016 TALK

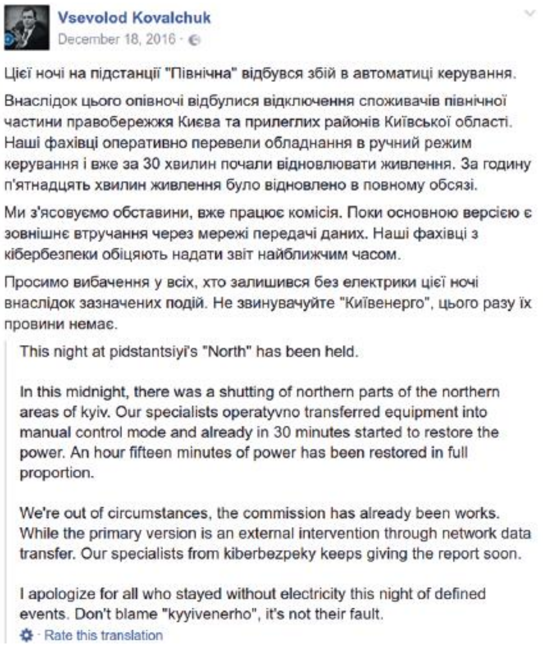
Author: Geers "Cyber War In Perspective Analysis From The Crisis In Ukraine"

Marina Krotofil at s4x17 Miam introducing the attack and the talk from Oleskii Yasinskiy: *https://www.youtube.com/watch?v=lTwsDLO3C44*

Oleskii Yasinskiy from *http://www.issp.ua/*

https://www.youtube.com/watch?v=3uPvps3l1Yc

VSEVOLOD KOVALCHUK'S FACEBOOK STATEMENT FOLLOWING THE SECOND ATTACK



Vsevolod Kovalchuk
December 18, 2016 ·

Цієї ночі на підстанції "Північна" відбувся збій в автоматиці керування.

Внаслідок цього опівночі відбулися відключення споживачів північної частини правобережжя Києва та прилеглих районів Київської області. Наші фахівці оперативно перевели обладнання в ручний режим керування і вже за 30 хвилин почали відновлювати живлення. За годину п'ятнадцять хвилин живлення було відновлено в повному обсязі.

Ми з'ясовуємо обставини, вже працює комісія. Поки основною версією є зовнішнє втручання через мережі передачі даних. Наші фахівці з кібербезпеки обіцяють надати звіт найближчим часом.

Просимо вибачення у всіх, хто залишився без електрики цієї ночі внаслідок зазначених подій. Не звинувачуйте "Київенерго", цього разу їх провини немає.

> This night at pidstantsiyi's "North" has been held.
>
> In this midnight, there was a shutting of northern parts of the northern areas of kyiv. Our specialists operatyvno transferred equipment into manual control mode and already in 30 minutes started to restore the power. An hour fifteen minutes of power has been restored in full proportion.
>
> We're out of circumstances, the commission has already been works. While the primary version is an external intervention through network data transfer. Our specialists from kiberbezpeky keeps giving the report soon.
>
> I apologize for all who stayed without electricity this night of defined events. Don't blame "kyyivenerho", it's not their fault.
>
>

ICS-CERT ALERT (TA17-163A) CRASHOVERRIDE MALWARE

https://www.us-cert.gov/ncas/alerts/TA17-163A

THE COMPLETE ESET REPORT

https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

THE DRAGOS REPORT

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

Other sources are confidential.

NOTES

sentryo

66 Boulevard Niels Bohr
Bâtiment CEI 1 CS 52132
69603 Cedex, Villeurbanne
09 70 75 34 80

www.sentryo.net
@sentryo