

Lights out! Who's next?

Analysis and detection of the Ukrainian “cyber-blackout”

Authors

Daniel Trivellato, PhD - Product Manager Industrial Line

Dennis Murphy, MSc - Senior ICS Security Engineer

6 May 2016

Version 2.0 – UPDATED to include latest findings

Contents

1	Preface	2
2	The coordinated attack on the Ukrainian power grid	3
2.1	The steps of the attack	4
2.2	The role of the malware	5
2.3	Attribution	7
3	Could it be avoided?	8
3.1	Network monitoring with SilentDefense	8
3.2	Detection of the Ukrainian attack	9
4	Conclusions and recommendations	12
4.1	Testimonials	12
4.2	About SecurityMatters	13
4.3	About the Authors	13

1 Preface

On December 23rd, 2015, for the first time in history, a major cyber-attack to a country's critical infrastructure significantly affected the civilian population. As reported by several sources [1, 5], hundreds of thousands of inhabitants of the Ukrainian Ivano-Frankivsk region were left without electricity for about six hours.

Over the past few months, researchers and analysts of the major cyber-security players worldwide have been analyzing the incident in detail [1, 2, 4, 5, 6, 8, 9]. While there are contrasting opinions about the origins and dynamics of the incident, all these sources agree that behind the big blackout there is the clear mark of an extremely well-coordinated cyber-attack against multiple Ukrainian utilities.

This short paper presents the main results of investigations on the incident, and discusses how the key part of this attack could have been timely detected by applying appropriate network monitoring measures to the core parts of utility networks.

2 The coordinated attack on the Ukrainian power grid

We begin our analysis of the attack to the Ukrainian power grid by analyzing the facts surrounding the events of December 23rd, 2015. Between 15:35 and 16:30 local time, the Ukrainian utility Kyivoblenergo suffered an intrusion by third parties into their ICT infrastructure. During this breach, seven 110 kV substations and twenty-three 35 kV substations were "disconnected", leading to an outage for about 80,000 different categories of customers. This breach was reported by Kyivoblenergo through a public update on its website (Figure 2.1).

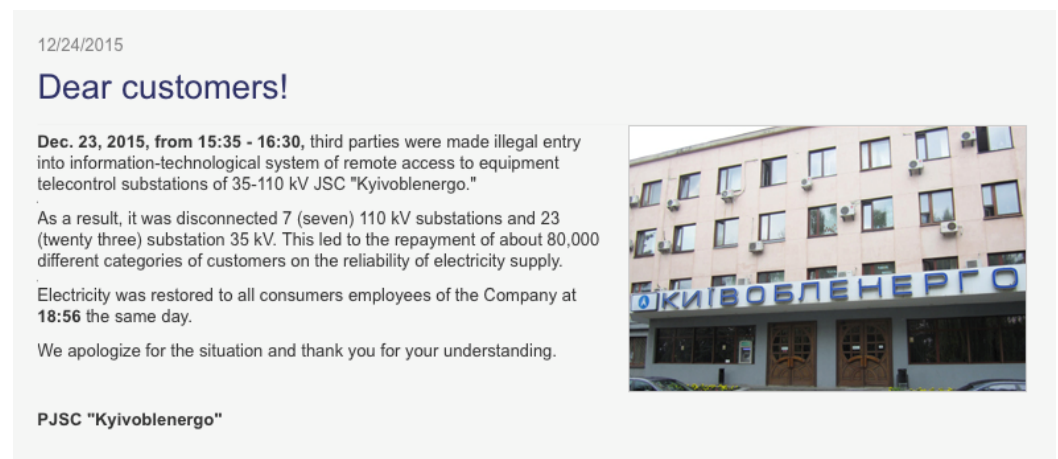


Figure 2.1: Public update of the breach by Kyivoblenergo [2]

According to the post, electricity was restored to all customers approximately three hours later, at 18:56 local time. On another public update, Kyivoblenergo also reported another technical failure in the call center infrastructure, which prevented customers from contacting the utility's staff during the blackout (Figure 2.2).

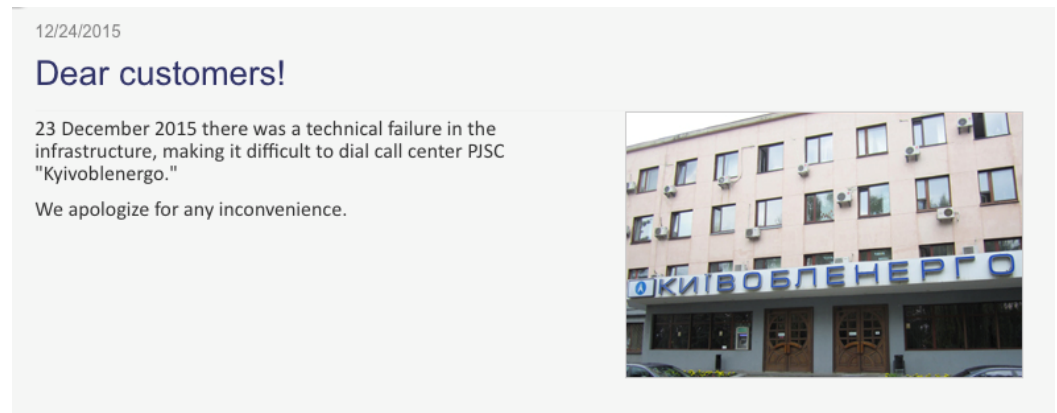


Figure 2.2: Public update of the problems to Kyivoblenergo's call center [2]

At the same time of the incident at Kyivoblenergo, other Ukrainian utilities have suffered breaches and malfunctions. The analysis published by TrendMicro [5] reports that two other utilities were targeted by the attackers, and in accordance to the reports of SANS ICS [2] and ESET [1] (a Bratislava-based security software firm) it mentions in particular the Western Ukrainian power authority Prykarpattiaoblenergo.

According to ESET [1], around 700,000 people in the Ivano-Frankivsk region of Ukraine (half of the local population) suffered from the blackout; most of the other reports assess to 225,000 the number of customers victim of the attack.

2.1 The steps of the attack

All researchers and analysts involved in the analysis of the incident have agreed from day one that the blackout is the result of an extremely well-coordinated cyber-attack. Whereas initial reports [1, 2, 5] were still vague concerning the exact dynamics of the attack, the latest document published by SANS ICS [6] clearly identifies the “weapons” used by the attackers to cause the blackout. In particular, the attack was made up of the following ingredients:

- **Spear phishing e-mails** to individuals in the administrative and IT network of the targeted utilities.
- Different **malware components** for information gathering, gaining remote access to the victims' ICS network and damaging their SCADA system and other key components, with the goal of delaying process restoration and complicating forensic analysis. Some of the malware used in the attack was targeted to the specific ICS vendors used by the victims [1, 9, 6].
- The **opening of substation breakers** to cause the outage. Most likely, the attackers opened the breakers by remotely operating the operators' HMIs.
- A **denial of service** to the utilities' call center, during which the attackers flooded the target infrastructure to prevent customers from successfully reporting the outage.

These components were carefully put in place by the attackers and orchestrated in precise steps in order to cause the biggest possible damage to the electricity distribution process. The scenario of the incident reconstructed by SANS ICS [6] and the steps followed by the attackers are the following:

1. The attackers penetrated the IT network of Kyivoblenergo, Prykarpattiaoblenergo and a third utility by means of malware hidden in e-mail attachments sent to the utilities' staff.

2. The attackers used the malware to move horizontally within the IT network and harvest credentials required to gain access to ICS networks. Evidence shows that the attackers' information gathering activity started more than six months prior to the incident.
3. Exploiting the harvested credentials and VPN tunnels connecting IT with ICS networks, the attackers gained access to the latter and started deploying their weapons. In at least one of the targeted utilities, they discovered a network connected to a UPS and reconfigured it to shut down the power also in the utility's buildings and data centers following the induced blackout. They then developed and deployed malicious firmware for the serial-to-ethernet devices used by the victims' SCADA system for remote communication with substations. Finally, they installed malware across the environment in order to wipe the evidence of their actions and make some of the systems unusable (e.g. HMIs).
4. When every ingredient was in place, the attackers gained control of the operators' workstations and issued a command to open breakers of various substations, causing the blackout. The operators were "blindfolded and handcuffed" by the malware components, which even made the keyboards and mice unusable on their workstations, preventing them from assessing or reacting to the attackers' action.
5. To conclude, the attackers initiated a denial of service to the utilities' call center, limiting the targets' awareness of the consequences of their action and frustrating the customers trying to report the outage.

Given the circumstances, the utilities victim of the attack have been extremely quick and effective in restoring the provision of electricity to their customers. In fact, due to the impossibility of controlling the process remotely and automatically through their SCADA system, they had to deploy field staff at all impacted substations in order to manually re-close the open breakers and return the system to a functioning state. For some time after the incident the entire distribution process has been run in a sort of "emergency mode", as the SCADA system was still unusable.

2.2 The role of the malware

In this section we present the results of the analysis of the different pieces of malware identified in the utilities' networks and their role in the attack. According to information first published by ESET [1] and TrendMicro researchers [5] and later confirmed by SANS ICS [6], the victims were infected by malware belonging to the **BlackEnergy** campaign, which was delivered via phishing emails with a macro-enabled Microsoft Office document attached (Figure 2.3). Once executed, this document would download the appropriate components for persistence on the infected machines.

The newly installed BlackEnergy malware would first of all contact its Command & Control (C&C) server to receive instructions on how to proceed. In the six months preceeding the blackout, the attackers used BlackEnergy as a backdoor to gain access to the utilities network, move laterally throughout the environment, and gather key information that was later used for the attack. Among the information exfiltrated by the attackers there are passwords used for VPN connections with the ICS network, as well as ICS manufacturers and models used by the victims.

The next clear demonstration of the skills of the attackers is represented by the fact that, based on the intelligence gathered in the initial stages, they developed **malicious firmware** specifically targeted to the serial-to-ethernet devices used by the target utilities. These devices are key network components that enable interrogations and remote operation of substation control systems. By compromising these devices, the attackers basically prevented the utilities' operators to see what was going in their substations and send corrective commands from a central location.

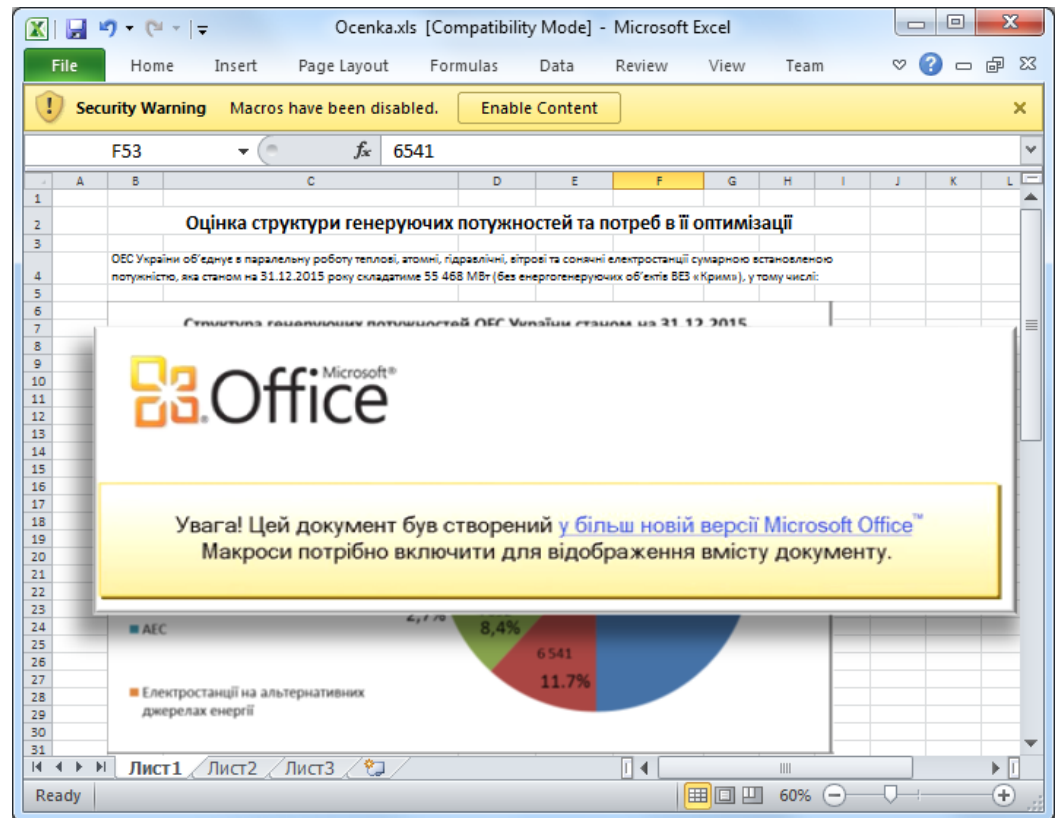


Figure 2.3: The infected macro-enabled Microsoft Excel document [10]

Finally, the last piece of malicious software used in the attack is a customized version of a known malware called “KillDisk”. This is the malware responsible for taking control of the operator workstations and locking them out of their systems, as well as of wiping some key SCADA components of the targeted utilities.

The December 2015 blackout was not the first cyber-warfare operation against Ukrainian companies seeing KillDisk as a malware component. The following is an extract from ESET's report [1]:

“The first known link between BlackEnergy and KillDisk was reported by the Ukrainian cybersecurity agency, CERT-UA, in November 2015. In that instance, a number of media companies were attacked at the time of the 2015 local elections. The report claims that a large number of video materials and various documents have been destroyed as a result of the attack.”

A comprehensive analysis of the KillDisk component can be found in the report published by Symantec [9]. In this report, KillDisk (identified by Symantec as Trojan.Disakil) is regarded as a highly destructive multi-stage Trojan, which renders the infected system unusable by overwriting its Master Boot Record and other key files with junk data. But the most interesting finding in the variant of the malware found at the Ukrainian utilities is that it contained code specifically targeted at the **disruption of industrial processes**. In particular, this KillDisk variant

“attempts to stop and delete a service named sec_service. This service appears to belong to 'Serial to Ethernet Connector' software by Eltima. This software allows access to remote serial ports over network connections. A lot of legacy SCADA systems still use serial ports for RTU communications. [...] If an attacker knew that their target was using this

software for communicating with their legacy SCADA devices, stopping the service and any communications would increase the potential for damage within their environment.”

This finding clearly links the customization of KillDisk with the malicious firmware developed by the attackers for the serial-to-ethernet devices: basically, the attackers “broke” the communication with substation control systems both at the workstation and at the connector level.

The extensive analysis of a KillDisk malware sample by SentinelOne [8] further indicates that in addition to the wiping routine, the malware features code for subverting and capturing traffic from network interfaces of the infected machines, including wireless adapters. All the information gathered was sent to the malware Command & Control (C&C) server via HTTP messages. This indicates that KillDisk might have been a precious weapon of the attackers also for information gathering.

Based on all this evidence, it is clear that malware components have played a major role in the attack: from providing the attackers with the information required to access and attack the network, to preventing operators from responding to the blackout, thereby delaying restoration efforts. However, as SANS ICS highlights [6], neither BlackEnergy, nor KillDisk nor the malicious firmware were primarily responsible for the outage. The actual cause of the outage was a **direct action of the attackers** who took control of the HMIs and opened multiple substation breakers in a short time interval.

2.3 Attribution

Available reports of researchers and analysts provide different opinions concerning who is behind the attack. Ukraine’s security service (SBU) was quick in pointing the finger to Russia, and so were the analysts of iSIGHT Partners [4]. This is mainly due to the presence of the BlackEnergy malware in the network of the Ukrainian utilities targeted by the attack. Behind BlackEnergy there is the Moscow-based group **Sandworm**, which has a history of targeting organizations in Ukraine, a number of Western countries, and companies operating in the energy sector [4, 9]. Although not mentioning Russia, SentinelOne [8] is sure that this latest variant of the malware is the by-product of a nation-sponsored campaign, and “likely the work of multiple teams coming together”.

Other researchers are more cautious or at least less direct in attributing the attack to known and state-sponsored players. For instance, SANS ICS does not take a clear position on the matter in any of its reports [2, 3, 6]. On the other hand, one of the latest issues of the SCADASEC mailing list by Ray Parks [7] dedicates particular attention to the attribution of the attack, playing down the “international cyber-warfare” scenario. In his analysis, Ray Parks points out that state-backed attacks would normally aim big (e.g. the Stuxnet worm, which aimed at slowing down the Iranian nuclear program) or at very targeted strategic objectives (e.g. turn off a critical radar site). The Ukrainian utility that suffered most from this attack is in the Western part of Ukraine, so it is unlikely that the attack was aimed at strategic (military) objectives. Ray Parks’ conclusion is thus that the attack was more likely carried out by a group with *some* ties to a nation-state (demonstrated by the use of special tools), but that acted on its own for personal motives.

3 Could it be avoided?

The answer is *maybe not*, but some symptoms of the attack and actions of the attackers could have been detected earlier in the process. For example, antivirus and intrusion prevention systems such as Symantec [9] already feature signatures capable of detecting the KillDisk malware component. It is arguable, however, whether these signatures would have detected the specific variant of the malware found at the Ukrainian utilities [8].

Two steps of the attack that could have certainly been detected as they happened are (a) communications between machines infected by BlackEnergy and KillDisk and the malware C&C servers to report intelligence gathered on the victims' network; and (b) the action performed by the attackers to remotely open the substation breakers, which was the actual cause of the outage. Furthermore, the upload of new (malicious) firmware to the serial-to-ethernet devices could have also been noticed, if performed at unusual times or from unusual workstations.

The detection of these activities would have been possible by monitoring the utilities' ICS/SCADA network with SecurityMatters' network monitoring platform SilentDefense, which exploits a built-in capability to understand industrial communications and SecurityMatters' exclusive **Industrial Threat Library** to report in real-time every activity that could harm the stability of industrial processes.

3.1 Network monitoring with SilentDefense

SilentDefense is an advanced network monitoring and intelligence platform used by critical infrastructure operators worldwide to preserve the stability of their ICS/SCADA network. SilentDefense constantly monitors and analyzes network communications, compares them with a baseline of legitimate/desired operations and with the "known bad" defined in SecurityMatters' Industrial Threat Library, and reports in real-time problems and threats to the network and process. Some examples include:

- Attempted and ongoing intrusions
- Misbehaving and misconfigured devices

- Undesired process operations
- Operational mistakes
- Known and zero-day attacks

These threats are detected and presented to the operator in two main formats:

- **Visual analytics:** The operator can benefit from a graphical representation of the network in all its aspects by means of different types of graphs and charts (see Figure 3.1). These graphs and charts are preconfigured to obtain at-a-glance insights into the most relevant aspects of current network activity, but can be fully customized by the operator to obtain different views. In fact, the visual analytics platform is built on top of a full-fledged data warehouse, which means that the operator is able to query and represent the network aspects of interest at any moment in time, giving him/her the possibility of both seeing what is currently happening, detecting strange network behavior, but also analyzing what happened in the past (e.g. in correspondence to a suspicious event).
- **Real-time alerts:** As soon as something bad or unexpected occurs in the network, SilentDefense notifies the operator and provides him/her with all the intelligence required to react on the event. This includes information about the source of the problem, the targeted device(s), the nature of the problem (e.g. an unknown device suddenly starts communicating with field devices, the SCADA server issues an undesired command, field devices become unresponsive or return unusual values, etc.) and even a packet capture of the traffic related to the event. The latter is fundamental in case of advanced threats such as zero-day attacks, when this traffic capture can be forwarded to specialized security vendors and organizations such as ICS-CERT, Symantec, Mandiant, etc. and can become a key input for further analysis.

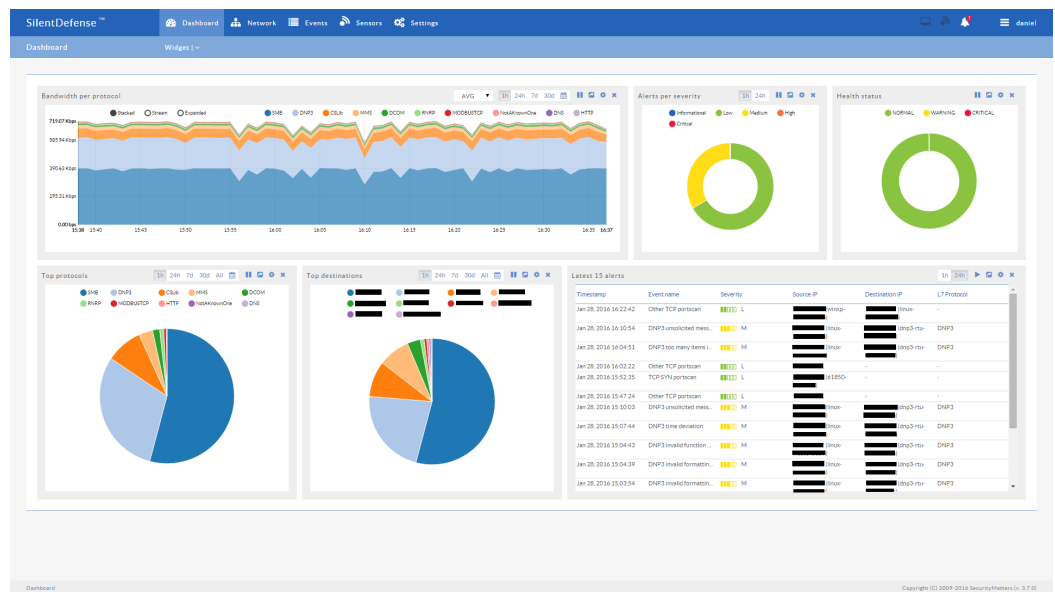


Figure 3.1: The SilentDefense dashboard combines a set of preconfigured widgets

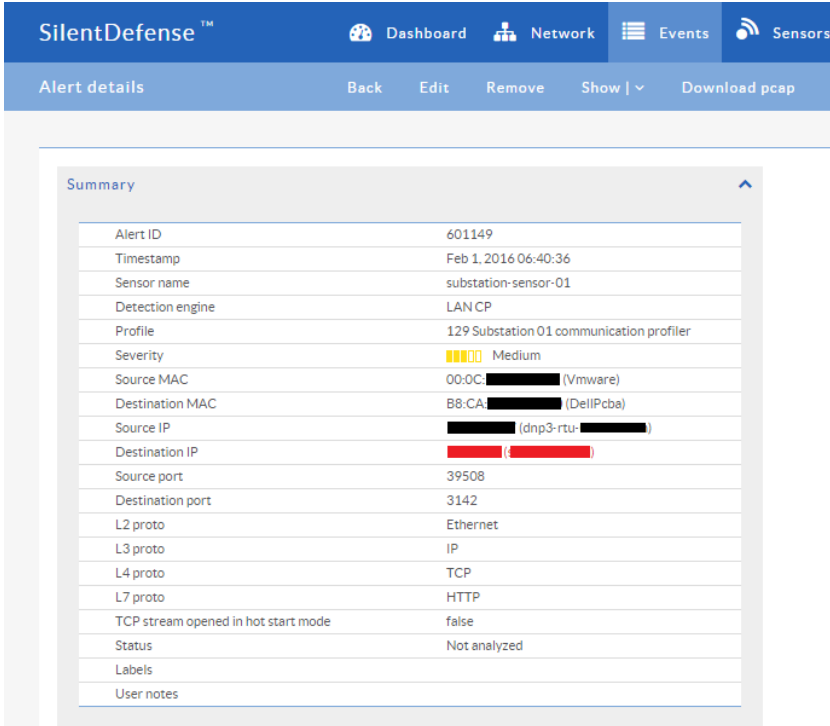
SilentDefense has already proven effective against intrusion attempts and ICS/SCADA-specific problems at different customers. Two of the latest examples of threats detected at our customers include a successful intrusion into our customer's network (exploiting a firewall misconfiguration) during which the attackers were caught probing the SCADA server with malformed protocol messages, and the instability of the power grid of a large region due to misconfigured devices, which was not revealed by the SCADA system.

3.2 Detection of the Ukrainian attack

SilentDefense leverages different complementary detection engines to achieve the detection of problems and threats to ICS/SCADA networks. In particular, operators can benefit from:

- **Built-in detection modules** for the detection of early stages of attacks (e.g. port scan and man-in-the-middle detection) and protocol compliance verification.
- Automatically generated **communication whitelists** for defining legitimate network devices, communication patterns, protocols and commands, and for detecting the presence of unknown network devices, insecure protocols and undesired operations.
- Automatically generated **protocol field whitelists** for defining desired process operations, parameters and values, and detecting unexpected process deviations.
- A **network intelligence framework** consisting of SecurityMatters' Industrial Threat Library and that further enables the specification of various ad-hoc network checks on the fly (e.g. detecting valves opened at undesired times, verifying that when a certain substation breaker is opened, another is closed, etc.)

By analyzing real-time network communications and comparing current traffic with validated communication whitelists, SilentDefense would have immediately identified and reported communications between the machines infected by BlackEnergy and KillDisk and the malware C&C servers. In particular, SilentDefense would have notified the Ukrainian utilities' staff that a local workstation was communicating with an external unknown device (Figure 3.2). Both BlackEnergy and KillDisk initiated this undesired communication in order to report the gathered intelligence to the attackers. Although one might argue that this type of threat can be mitigated by existing firewall and intrusion prevention systems, we have seen that sometimes these systems are misconfigured or not kept up-to-date.



Summary	
Alert ID	601149
Timestamp	Feb 1, 2016 06:40:36
Sensor name	substation-sensor-01
Detection engine	LAN CP
Profile	129 Substation 01 communication profiler
Severity	Medium
Source MAC	00:0C: [redacted] (Vmware)
Destination MAC	B8:CA: [redacted] (DellPcbe)
Source IP	[redacted] (dnp3-rtu- [redacted])
Destination IP	[redacted] ([redacted])
Source port	39508
Destination port	3142
L2 proto	Ethernet
L3 proto	IP
L4 proto	TCP
L7 proto	HTTP
TCP stream opened in hot start mode	false
Status	Not analyzed
Labels	
User notes	

Figure 3.2: An alert generated in case of an unauthorized communication to an unknown device

In a similar way, SilentDefense would have reported the upload of malicious firmware to the serial-to-ethernet devices, if such operation was performed from a workstation that was not normally used for maintenance operations. In addition, as firmware upload typically causes a higher bandwidth usage than other standard process operations (e.g. reading and writing of process values), the utilities' operators could have seen suspicious "peaks" in the visual analytics graphs related to bandwidth usage when the uploads took place. Figure 3.3 provides an example of what the operators could have been presented with.

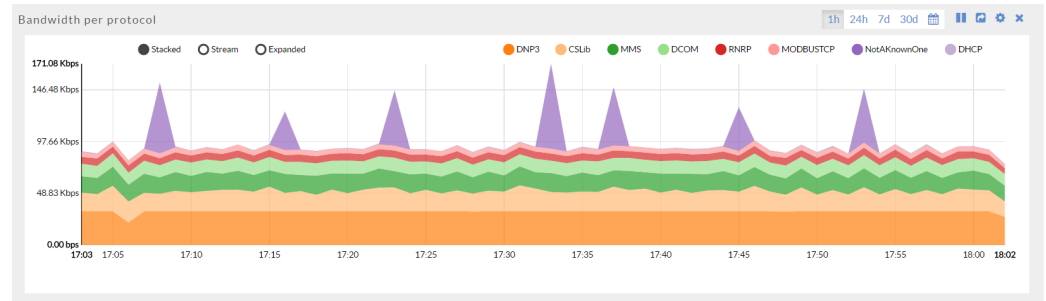


Figure 3.3: Peaks in the bandwidth usage that could be caused by firmware upload

The most noteworthy engine of SilentDefense for this specific use case, however, is the network intelligence framework. This engine is a unique feature of SilentDefense which has proven fundamental in the detection of a large number of problems in our customers' networks. SecurityMatters' Industrial Threat Library contains lessons-learned from different installations and heuristics from field experience translated into real-time network checks, which notify the operator as soon as something goes wrong.

One of the checks in our Industrial Threat Library would have **reported right away the action of the attackers** of opening the substation breakers. This check was developed following the request of a customer to report when their automatic fault isolation system would kick in, and was later generalized to cover the exact use case occurred in the Ukrainian attack. In fact, the fault isolation system would act similarly to the attackers of the Ukrainian power grid, i.e. would open/close a number of substation breakers in a short time interval. Figure 3.4 shows an example alert generated by this check.

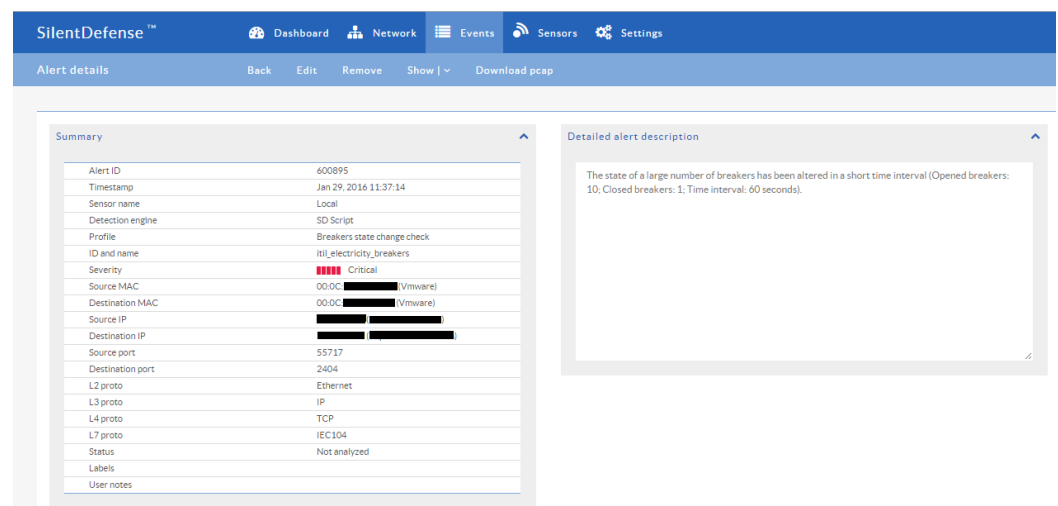


Figure 3.4: Alert generated when the state of several breakers changes in a short time interval

As mentioned in the introduction of this chapter, most likely even the real-time detection of the attackers' action would not have prevented the incident. However, system dispatchers

would have a record of the affected substations targeted by the attackers, enabling a prompt and clear reaction of field staff to fix the problem. In addition, with a network monitoring solution like SilentDefense, the Ukrainian utilities would have benefited from the forensics evidence retained by the system which in turn would reduce the analysis time required to understand the event and enable a more effective and focused DFIR (Digital Forensics and Incident Response) process.

4 Conclusions and recommendations

The Ukrainian blackout is the first instance of cyber-attack to critical infrastructure operators that directly impacts the civilian population. So far, this kind of scenario had been discussed only theoretically. Despite in small scale, this attack has demonstrated that motivated attackers have all the skills required to cause potentially catastrophic damages to the economy and public safety of a country. The biggest part of the problem is of course the fact that critical infrastructure organizations are still lacking behind in the protection of their ICS/SCADA network, possibly not fully realizing that the increased inter-connectivity between ICS/SCADA and corporate networks and the adoption of standard network communication technologies and protocols have brought a lot of risks next to evident advantages.

In looking at what should be done next, we agree with the view presented in one of the reports by SANS ICS [3] and further discussed in their latest document [6]: ICS facilities around the world need to **step up their defenses**, and in particular their capability to monitor their ICS/SCADA network and respond to threats. This is first of all a need to form teams with the right skillset and knowledge within each organization, a team capable of performing a first quick analysis and response to suspicious activity, and to define clear procedures to indicate who to contact to request for help in case the problem escalates. Secondly, these teams must be equipped with the right tools to monitor their network and detect when something goes wrong.

Adopting generic security solutions for this purpose would not help. As demonstrated by this whitepaper, the adoption of a solution specifically built for the ICS/SCADA domain such as SilentDefense is key to enable early detection of targeted threats. Such solution would additionally enable ICS/SCADA operators to have a complementary view of what is happening in their network independent from that of the SCADA system (or DCS) and HMIs, and would therefore guarantee visibility even when the main systems get corrupted.

4.1 Testimonials

Frank at US Independent System Operator:

"We found a misconfiguration that was directly affecting our bottom line revenue that essentially paid for SilentDefense many times over in the first few days of operation."

Jerry at a Major Industrial Control Security Integrator:

"Operational Technology security and monitoring needs to be able to adapt to rapid change, be self-sufficient and add value quickly and seamlessly. SilentDefense does all of these things for our customers."

4.2 About SecurityMatters

SecurityMatters is an international company with business in all major critical infrastructure and industrial automation sectors. Its network monitoring and intelligence platform SilentDefense ICS has been deployed for years at customers across multiple continents, providing daily value to operations and protecting their networks from emerging cyberthreats.

4.3 About the Authors



Daniel Trivellato Daniel Trivellato received his PhD in computer security from the Eindhoven University of Technology in 2012. During his PhD, he worked in collaboration with Thales Netherlands on the design and implementation of an access control framework for protecting confidential data in dynamic distributed systems. In 2012, Daniel joined SecurityMatters as a project leader; his responsibilities encompassed marketing and sales, account management, and the organization and management of deployment projects at customers. Since 2014, Daniel is product manager for SecurityMatters' Industrial Products portfolio, and is responsible for the evolution and commercialization of the line of products targeting the industrial control systems domain.



Dennis Murphy Dennis Murphy is a Sr. Cybersecurity Engineer at Security Matters. He has 12 years of experience in SCADA and ICS design, development and implementation and 10 years of experience in computer security as it applies to critical infrastructure networks. Mr. Murphy directed multiple SCADA security tests at Idaho National Labs Critical Infrastructure Test Range while he was a program manager at BAE Systems in their cybersecurity division in Merrimack, NH. During his tenure at a Wonderware distributor in New England, he designed, installed and supported dozens of different SCADA systems in the Electric Power, Water, Biopharmaceutical, Oil & Gas, Chemical, Food & Beverage and Pulp & Paper industries. He has a masters degree in Systems Engineering from Johns Hopkins University. He is a member of the Boston, MA chapter of the FBI's infragard program and he is a member of the Control System Integrator Association's Cybersecurity Best Practices Working Group.

Bibliography

- [1] ESET. Eset finds connection between cyber espionage and electricity outage in ukraine. <http://www.eset.com/int/about/press/articles/malware/article/eset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine/>.
- [2] SANS ICS. Confirmation of a coordinated attack on the ukrainian power grid. <https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid>.
- [3] SANS ICS. Potential sample of malware from the ukrainian cyber attack uncovered. <https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered>.
- [4] iSIGHT Partners. Sandworm team and the ukrainian power authority attacks. <http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/>.
- [5] Trend Micro. First malware-driven power outage reported in ukraine. <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/first-malware-driven-power-outage-reported-in-ukraine>.
- [6] Tim Conway Robert M. Lee, Michael J. Assante. Analysis of the cyber attack on the ukrainian power grid. Defense use case, SANS ICS, March 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- [7] Infracritical SCADASEC mailing list. New wave of attacks against ukrainian power industry. <http://news.infracritical.com/mailman/listinfo/scadasec>.
- [8] SentinelOne. Sentinelone discovers a new delivery tactic for blackenergy 3. <https://www.sentinelone.com/blog/sentinelone-discovers-a-new-delivery-tactic-for-blackenergy-3/>.
- [9] Symantec. Destructive disakil malware linked to ukraine power outages also used against media organizations. <http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations>.
- [10] ESET wlvivesecurity. New wave of cyberattacks against ukrainian power industry. <http://www.wlvivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/>.