Lights out! Who's next?

How to anticipate the next "cyber-blackout"

Authors

Daniel Trivellato, PhD - Product Manager Industrial Line
Dennis Murphy, MSc - Senior ICS Security Engineer

4 February 2016

Contents

Preface

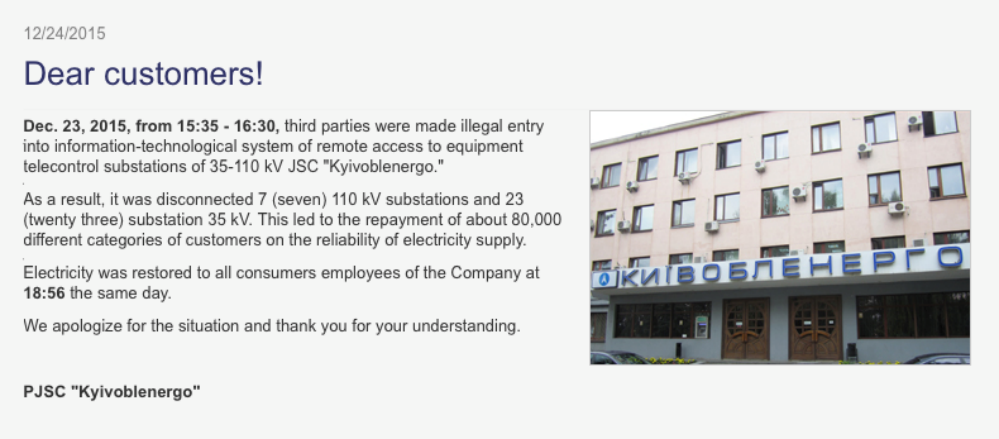
On December 23rd, 2015, for the first time in history, a major cyber-attack to a country's critical infrastructure has significantly affected the civilian population. As reported by several sources [1, 5], hundreds of thousands of inhabitants of the Ukrainian Ivano-Frankivsk region were left without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

Researchers and analysts of the major cyber-security players worldwide are currently analyzing the incident in detail [1, 5, 2, 4, 8, 7]. While there are still a lot of open questions about the origins and dynamics of the incident, all these sources agree that behind the big blackout there is the clear mark of a coordinated intentional (cyber-)attack against multiple Ukrainian utilities.

This short paper presents the current knowledge and 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.

The coordinated attack on the Ukrainian power grid

We begin our analysis of the attack to the Ukrainian power grid by analyzing the facts occurred on 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 1).



12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Figure 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 impeded to several customers to contact the utility staff during the blackout (Figure 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

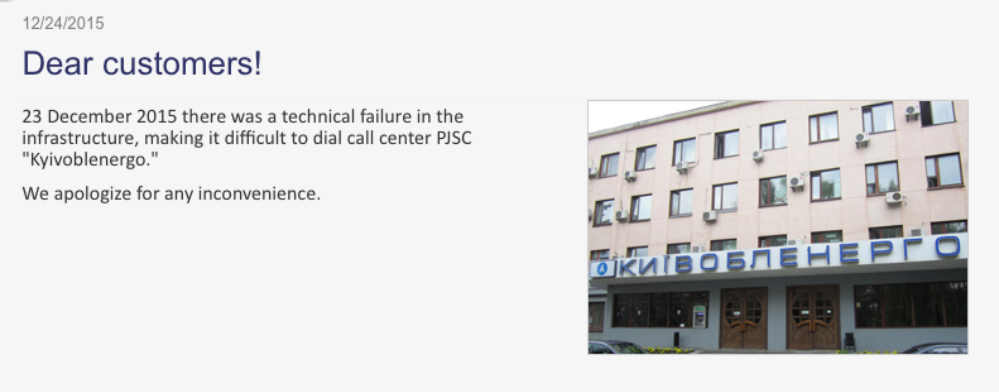


Figure 2: Public update of the problems to Kyivoblenergo's call center [2]

of SANS ICS [2] and ESET [1] (a Bratislava-based security software firm) mentions in particular the Western Ukrainian power authority Prykarpattyaoblenergo.

According to ESET [1], around 700.000 people in the Ivano-Frankivsk region of Ukraine (half of the local population) suffered from the blackout; TrendMicro [5] more generically reports that "hundreds of thousands" of homes were victim of the attack.

The steps of the attack

It is still early to determine the exact dynamics of the incident. However, all researchers and analysts involved in the analysis agree that the blackout is the result of an extremely well-coordinated attack. As described by SANS ICS [2], the attack consisted of at least three components:

- A **malware** component, which possibly enabled access to the network to the attackers and acted to damage the SCADA system of the targeted utilities, with the goal of delaying process restoration and complicating forensic analysis. The malware variant used in the attack contained code specifically intended to sabotage industrial systems [1, 8].
- A **denial of service** to the utilities' call center, during which the attackers flooded the target infrastructure to prevent customers to successfully report the outage.
- The **opening of substation breakers** to cause the outage. This is still the most mysterious piece of the puzzle. Most likely, the opening of the breakers resulted from a direct command issued by the attackers rather than activity of the malware found in the victims' network.

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. A possible scenario of the incident and the steps followed by the attackers are the following:

1. The attackers infected the main servers controlling the electricity distribution process of Kyivoblenergo and two other utilities with malware.
2. They infiltrated in the victims' network (possibly using a malware backdoor) and issued a command to open breakers of various substations.
3. The malware acted to "blind and handcuff" the utility staff – i.e. to prevent them from seeing and reacting to the command issued by the attackers – by terminating and making impossible to restart some key services of the SCADA system.
4. The attackers initiated the denial of service to the call center, limiting the targets' awareness of the consequences of their action.

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 infected.

The role of the malware

In this section we present the results of the analysis of the malware identified in the utilities' networks and its role in the attack. According to ESET [1] and TrendMicro researcher [5], the victims were infected by malware belonging to the BlackEnergy campaign, which was delivered via phishing emails with a macro-enabled Microsoft Excel document attached (Figure 3). Once executed, this document would download the appropriate components for persistence on the infected machines. The specific malware component that was responsible for wiping the SCADA system of the targeted utilities is called "**KillDisk**". 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."

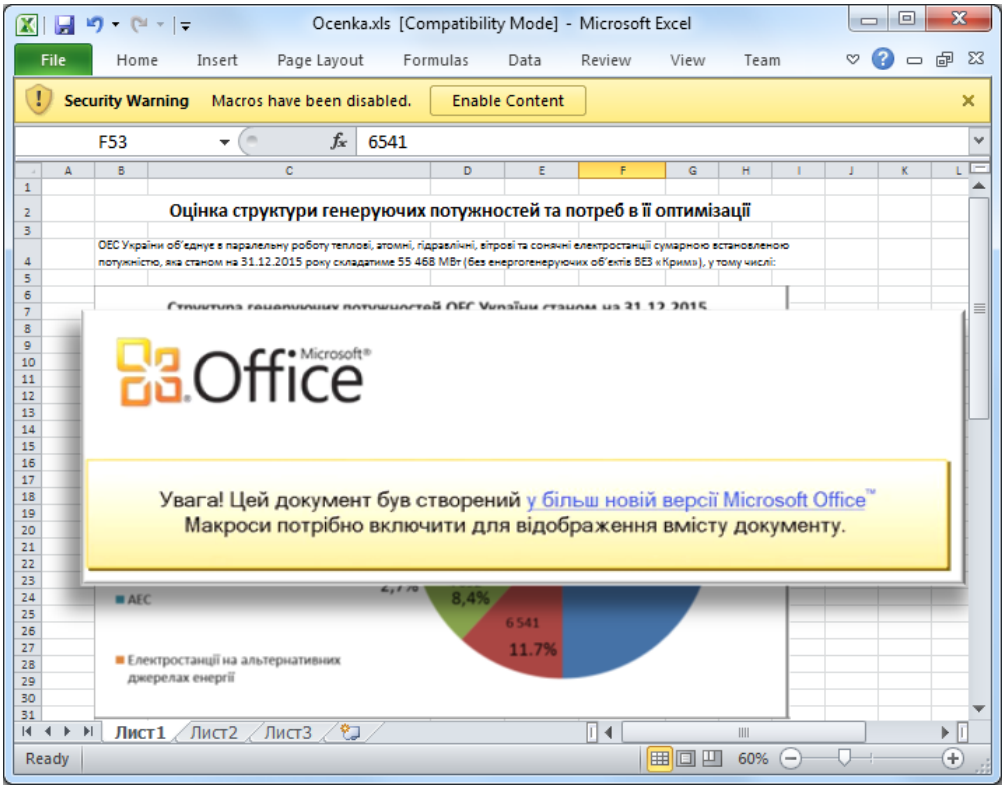


Figure 3: The infected macro-enabled Microsoft Excel document [9]

A comprehensive analysis of the KillDisk component can be found in the report published by Symantec [8]. In this report, KillDisk (detected 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."*

The extensive analysis of a malware sample by SentinelOne [7] indicates that further 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 is sent to the malware Command & Control (C&C) server via HTTP messages.

Despite these results, the exact role and impact of the malware in the attack is still to be confirmed. SANS ICS [1] states that next to the researchers that deem BlackEnergy and KillDisk fully responsible for the incident, there is a stream of thought according to which the malware found in the utility networks is not necessarily related to the outage (in other words, the malware just happened to be there and acting on the network at the same time of the outage). The position of SANS ICS is somehow in between: the malware was just an enabler rather than the executor. It allowed the attackers to gain access to the utility networks and was responsible for the disruption to the SCADA system after the attack; but the actual command that caused the blackout – i.e. the opening of multiple substation breakers in a short time interval – was **manually issued** by the attackers themselves.

Attribution

Current 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, 8]. Although not mentioning Russia, SentinelOne [7] 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 explicitly states in both its reports [2, 3] that it is far too early in the technical analysis to determine whether the attack can be linked to the BlackEnergy campaign. Also the latest issue of the SCADASEC mailing list by Ray Parks [6] dedicates particular attention to the attribution of the attack. 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.

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 [8] 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 [7].

Two steps of the attack that could have certainly been detected as they happened are (a) communications between infected machines and the malware C&C server to report intelligence gathered through the traffic capture capability; and (b) the action performed by the attackers to remotely open the substation breakers, action which caused the actual outage. Their detection would have been possible by monitoring the utility SCADA networks with SecurityMatters' network monitoring platform SilentDefense, which exploits a built-in capability to understand industrial communications and SecurityMatters' exclusive **Industrial Threat Intelligence** library to report in real-time every activity that could harm the stability of industrial processes.

SilentDefense

SilentDefense is an advanced network monitoring and intelligence platform used by critical infrastructure operators worldwide to preserve the stability of their ICS/SCADA networks. 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 Intelligence library, and reports in real-time problems and threats to the ICS/SCADA 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 4). These graph 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 capture of the traffic related to the event. The latter is fundamental in case of complex scenarios such as zero-day attacks, when this traffic capture can be forwarded to specialized security vendors such as Symantec, McAfee, etc. and can become fundamental for further analysis.

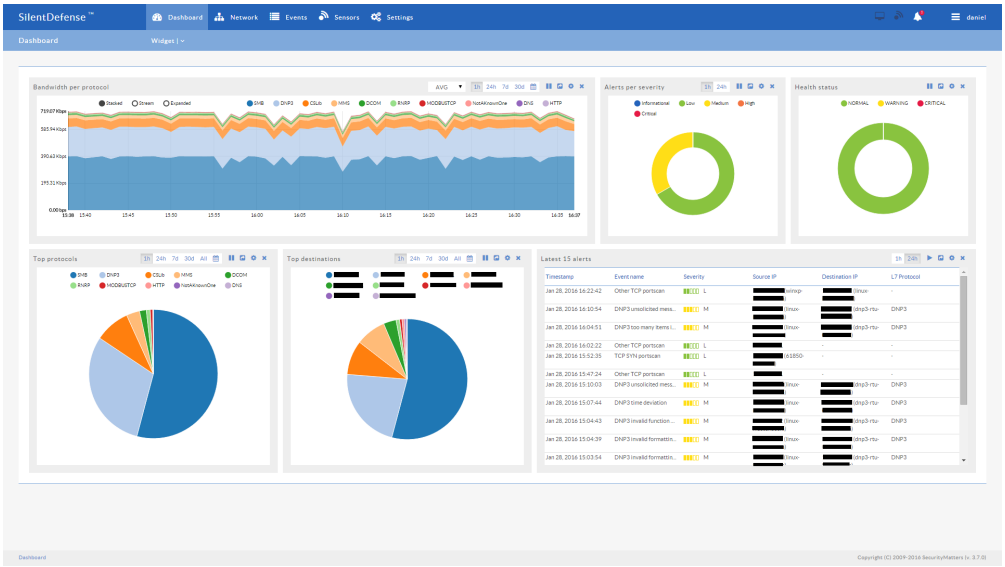


Figure 4: The SilentDefense dashboard combines a set of preconfigured widgets

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

Detection of the Ukrainian attack

SilentDefense leverages different complementary detection engines to achieve the detection of problems and threats described above. 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 blueprints** for defining legitimate network devices, communication patterns, protocols and commands and detecting the presence of unknown network devices, insecure protocols and undesired operations.
- Automatically generated **protocol blueprints** for defining desired process operations and detecting unexpected process deviations.
- A **network intelligence framework** consisting of SecurityMatters' Industrial Threat Intelligence library and that further enables the specification of arbitrary 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 previously validated communication blueprints, SilentDefense would have immediately identified and reported communications between the infected machines and the malware C&C server. In particular, it would have notified the Ukrainian utilities' staff that a local server was communicating with an external unknown device (Figure 5). Although one might argue that this type of threat can be mitigated by existing firewall and intrusion prevention systems, we have seen in several circumstances that these systems are misconfigured or overlooked.

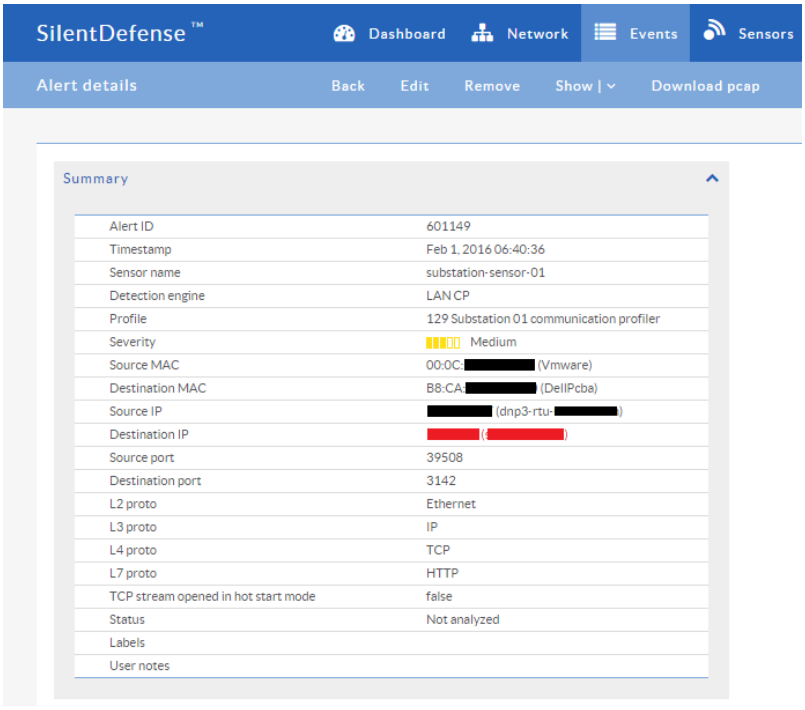


Figure 5: An alert generated in case of an unauthorized communication to an unknown device

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 cutomers' networks. SecurityMatters' Industrial Threat Intelligence 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 Intelligence 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 6 shows an example alert generated by the check.

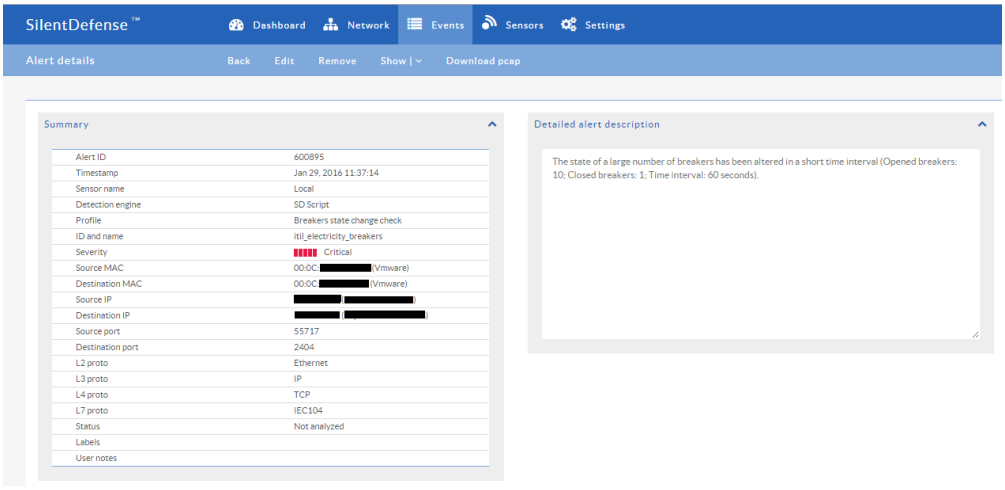


Figure 6: An alert generated when the state of several breakers changes in a short time interval

Note that here we are assuming the most likely case that the command opening the breakers was issued by the attackers to all substations from a remote workstation. In the less probable case that the attackers have connected to the targeted substations one by one and acted on the individual breakers to cause the outage, SilentDefense would have anyway reported the presence of unusual connections to field devices in a similar way as it would have reported communications to the malware C&C server (Figure 5).

As mentioned in the introduction of the section, most likely even the real-time detection of the attackers' action would not have prevented the incident. However, system dispatchers would have all the information required to immediately understand the cause of the outage and the substations targeted by the attackers, promptly directing field staff to fix the problem. In addition, with a network monitoring solution like SilentDefense still active in the network, the Ukrainian utilities would not have been completely blind about their network and process activities even after their SCADA system was down.

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 Industry 4.0 has brought a lot of risks next to evident advantages.

In looking at what should be done next, we agree with the view presented in the latest report by SANS ICS [3]: 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. T his 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.

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."

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.

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 distributer 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] Infracritical SCADASEC mailing list. New wave of attacks against ukrainian power industry. http://news.infracritical.com/mailman/listinfo/scadasec.

[7] SentinelOne. Sentinelone discovers a new delivery tactic for blackenergy 3. https://www.sentinelone.com/blog/sentinelone-discovers-a-new-delivery-tactic-for-blackenergy-3/.

[8] 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-organizatio

[9] ESET welivesecurity. New wave of cyberattacks against ukrainian power industry. http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/.