bsi.

...making excellence a habit.™

Examining the vulnerabilities of Industrial Automation Control Systems (IACS)

An analysis of a real cyberattack on a Ukrainian energy distribution company

Executive summary

This paper depicts the real incident of a cyberattack on a Ukrainian energy distribution company; Ukrainian Kyivoblenergo, to demonstrate how vulnerable Industrial Automation Control System (IACS) are without a clearly defined Supervisory Control and Data Acquisition (SCADA) cyber security system.

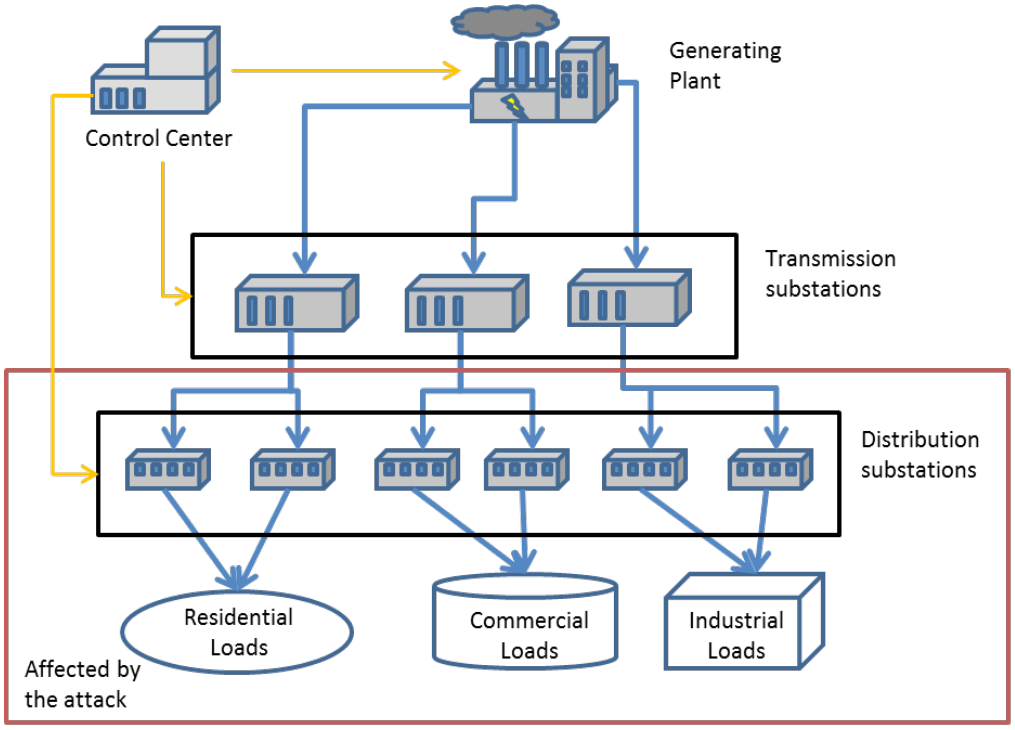
This paper is not intended to criticize or blame the actions of Kyivoblenergo. This type of coordinated attack was the first of its class and the Kyivoblenergo remediation was reasonably good, considering the circumstances. It is important to note that Kyivoblenergo was not without a cybersecurity system, however, the cybersecurity they had in place and its related policies, processes, and controls were designed from an IT perspective and not from a SCADA perspective.

The first part of this paper describes the incident and subsequent consequences to the nation. This is followed by an in depth technical analysis of the phases throughout the incident, including a complete breakdown of the technical components utilized and chronological order of events. From this analysis, cyber security mitigation practices that could have prevented this incident are presented. In conclusion, a gap analysis of the current system is conducted against a proposed system.

Scenario overview and incident description

On December 23 2015, Ukrainian Kyivoblenergo, reported a service outage to their customers. Shortly after that report, it was discovered that three more energy distribution companies were also affected, in a large and coordinated attack that targeted Ukrainian energy critical infrastructure, causing energy outage to more than 225,000 customers all over Ukraine, lasting for three hours.

The ultimate cause of the power outage was traced to the circuit breakers being opened in several substations, shutting off power to the end users. In addition the UPS (Uninterrupted Power Supply) systems covering the affected substations were hacked, preventing them from acting whenever the nominal power was stopped. A general overview of the electric system with the affected areas is shown in the following figure.



Incident Summary

The following descriptions detail the complex and highly coordinated nature of this attack, exposing the different tools the threat actors used to perform the attack and then summarizing the chronological evolution of the attack itself. Further in this paper, each of the attack steps are confronted with the hypothetical situation of having a proper IACS cyber security system in place.

Technical components mapping

- Spear phishing: emails pretending to be from a trusted domain or person, used to gain access to the business network.
- Infected Microsoft Office files, asking the user to enable the macros when a user opens them, but instead installing malware on the system
- BlackEnergy 3 Malware (embedded in the corrupted office files)

"BlackEnergy is a trojan that is used to conduct DDoS attacks, cyber espionage and information destruction attacks. In 2014 (approximately) a specific user group of BlackEnergy attackers began deploying SCADA-related plugins to victims in the ICS (Industrial Control Systems) and energy markets around the world. This indicated a unique skillset, well above the average DDoS botnet master.

Since mid-2015, the BlackEnergy APT group has been actively using spear-phishing emails carrying malicious excel documents with macros to infect computers in a targeted network. However, in January this year, Kaspersky Lab researchers discovered a new malicious document, which infects the system with a BlackEnergy Trojan. Unlike the Excel documents used in previous attacks, this was a Microsoft Word document.

Upon opening the document, the user is presented with a dialog recommending that macros should be enabled in order to view the content. Enabling the macros triggers the BlackEnergy malware infection." [1]

BlackEnergy is a trojan malware used to gather information on the target system. In the Ukrainian incident, it was use to steal credentials in the business network, and then, to gather information of the assets and the architecture of the SCADA network.

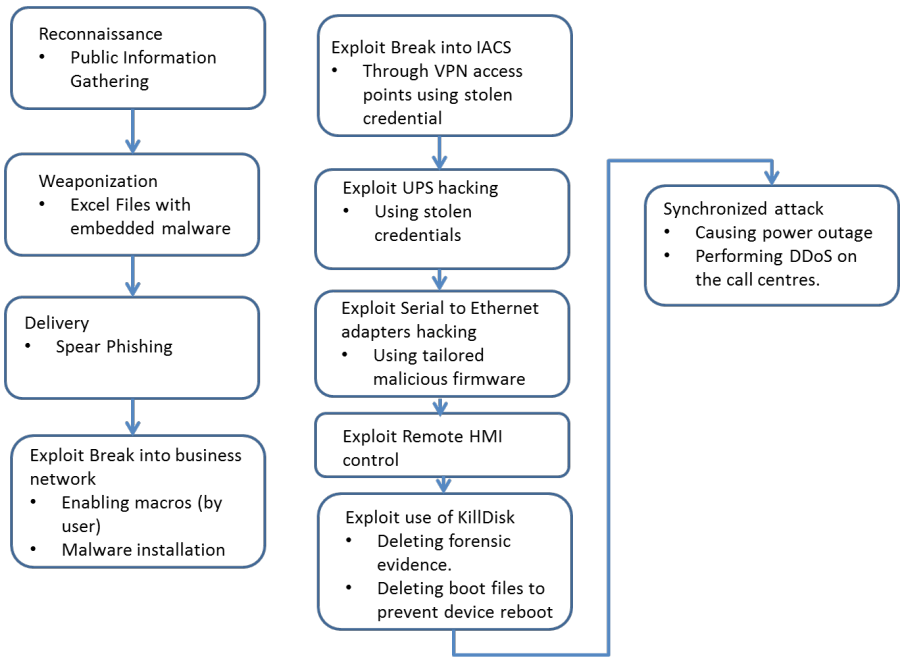
Apart from the use of BlackEnergy, the Ukrainian attacks included multiple tools to exploit the IACS systems in multiple ways, conforming complex threat scenarios, briefly described in the following list:

- A modified version of KillDisk malware was used to erase system logs and the boot files, reducing the traceability of the attack and also preventing some SCADA devices from rebooting normally. In addition, this tool was used to change some system registry, allowing the accounts to be locked up and preventing the real operators from entering the system.
- Credential theft from the company business network, using the mentioned BlackEnergy malware, among others
- Use of Virtual Private Networks (VPN) to enter the IACS
- Use of remote access tools to gain control of the IACS. Two vectors for the remote control have been documented in the incident
- Use of a rogue client that connects to the SCADA server through a VPN and using previously stolen credentials, gains control of the SCADA server:
    - Use of a "phantom mouse" tool, gains remote control of the mouse of a SCADA workstation (through a VPN)
    - Serial-to-ethernet communication devices impacted at firmware level
- UPS configuration to secure the power outage
- Telephone version of DDoS (Distributed Denial of Service) attack, overwhelming the call centre with fake calls and preventing any real calls to be processed (preventing awareness and analysis of the power outage)

1 Source: Kaspersky

Technical components mapping

The following figure and description establishes a chronological analysis of the different phases of the Ukraine cyberattack. This analysis is used further in this paper to hypothesize the outcome with SCADA's dedicated processes and controls.



- **Reconnaissance:** there is no evidence of this phase prior to the attacks, but due to the nature and complexity of the attack, it is difficult to believe that the attacks were that fortuitous. In this phase, all available public information of the target systems is gathered
- **Weaponization:** in the Ukrainian attack, some office files (Word and Excel files) were embedded with BlackEnergy 3 Malware
- **Delivery:** this phase occurred in the spear phishing campaign, attaching the infected files in the documents. The most common targets for these types of campaigns are high level company management.
- **Exploit. Break into business network[1]:** when the files attached in the mail were opened, a popup was displayed encouraging the enablement of the macros in the document. Doing this allowed the malware to exploit office macro functionality to install BlackEnergy 3 in the workstation. Once installed, the malware connected to certain command and control (C2) IP addresses to enable communication with the threat actors. Then the malware starts gathering information from the system, harvesting credentials, escalating privileges, but also moving away from the initial foothold and vulnerable C2, trying to blend into the target's systems as authorized users
- **Exploit. Break into the IACS:** with the information already gathered, the threat actors were able to identify VPN connections to the IACS and with the relevant credentials they were able to break into the IACS
- **Exploit. UPS hacking:** once inside the IACS, the threat actors accessed the UPS systems and managed to change the user configuration, making them unable to provide power when the circuit breakers of the substations were opened. The discovered evidence shows that the threat actors simply used stolen credentials to access the configuration of the UPS
- **Exploit. Serial-to-ethernet devices:** at this point, the threat actors were able to develop malicious firmware

1 There is evidence that shows that the threat actors were gathering information from the Ukrainian networks at least 6 months prior to the attacks.

especially for the detected serial-to-ethernet devices. There is evidence that supports the fact that the threat actors were able to test the developed firmware previous to its implementation in the Ukrainian company (in other words, it is probable that the threat actors had enough infrastructure to test the tools they developed prior to their implementation in the target system)

- **Exploit. Remote control of HMI (Human Machine Interface):** using the two mentioned remote control tools, the threat actors took control of the HMI that interacted directly with the field actuators (the circuit breakers of the substations)
- **Exploit KillDisk:** use of the previously mentioned tool to reduce the forensic evidence of the attack and to lock the operators out of the system
- **Exploit. Synchronized attack:** the threat actors used the remote control over the HMI to open the circuit breakers, causing the power outage. At the same time they uploaded the malicious firmware to the serial-to-ethernet devices, preventing the remote commands from bringing the substations back online. Finally, synchronized with the other actions, the threat actors started a telephonic denial of service attack, to prevent real customers alerting the companies of the power outage

IACS Cybersecurity system hypothesis

The following lists some characteristics of a properly assessed cybersecurity system designed for an IACS. It is not the purpose of this paper to make a complete and general cyber risk assessment applied to this incident but to highlight key points that could significantly improve the studied IACS.

- **System modelling. Domains and conduits:** using the approach exposed by the ISA 62443-1-1 Standard, this paper recommends the modelling of the whole IACS using the domain and conduit concepts. We can consider a domain as a defined zone in the IACS where all the physical and logical assets contained share the same security level. All the information transactions between the elements of the same domain are permitted without compromising the systems cyber security. The only way to transfer information between different domains is with a conduit. Modelling a system with these two concepts implies that all the possible information transactions are known and therefore we can define the required level of control of each of them, depending on the defined "critical level" of the information contained in the two domains that each conduit connects.[1] The Segmentation Model (named by ISA 62443-1-1) also provides a clear view of the IACS that allows us to reduce the conduits to the minimum required number, as having more conduits than necessary increases the vulnerability level of a system
- **Network monitoring:** this can be applied to the IT network (business network) and to the OT network (Operations Technology - IACS). The network monitoring should be improved with some kind of SIEM (Security Information and Event Management) in line with rules tailored for the IACS. In this incident case a useful set of rules could be:
  - Raise an alarm if a certain number of circuit breakers open at the same time
  - Raise an alarm if the UPS does not begin working when the corresponding circuit breaker opens
  - Raise an alarm if the call centre is handling an excessive number of calls
  - Raise an alarm if the remote control VPN is activated
- **Authentication:** where possible, a two factor authentication should be implemented in the IACS.
- **Remote control limitation:** the remote control capability should be enabled only when it needs to be used (in many situations the remote control operations are scheduled) and disabled when it is clearly not going to be used[2]
- **Remote control whitelisting:** a control should be enabled to allow only an approved list of devices/users to perform remote controls. Also, if the IACS permits, a double authentication for the remote control actions should be enabled[3]

1 Refer to ISA 62443-1-1 for more information on the segmentation model (domains and conduits).
2 Obviously this cannot be a general rule, because many IACS need total availability of remote control, due to inherent process needs.
3 Again, in many cases this may not be possible, but a possible example is the need to make a phone call to a security central to confirm that the remote control is authorized.

- **User privileges:** each HMI control privileges should be limited to the normal area of interaction. Also, some type of actions, like write/change certain configuration files, or even upload new firmware version for any IACS asset, should be disabled for certain users if possible, or implement a two factor authentication if the incidence in the system performance is acceptable (i.e. requiring a phone confirmation by the operator after login with the proper credentials when a major change is to be made)
- **Policies:** raise employee's awareness of cyberthreats, scheduling training programmes for all employees to mitigate the people vulnerability to phishing and social engineering

Benchmarking of incident key points with the hypothetical cybersecurity system

The scope at this point of the paper is to confront the major points of the Ukrainian attack with the related aspects of the hypothetical cybersecurity system exposed in the previous step.

- **Spear phishing:** the impact of spear phishing can be reduced by two different aspects of the cybersecurity system
  - **Raising awareness:** the best way to reduce the risk of common threat vectors like spear phishing is conducting periodical training for all company personnel. This training will enable employees to distinguish between trustworthy emails and emails containing malicious software
  - **Segmentation model:** with the classification of a system into domains and conduits, all services (like mail services) that are not 100% trusted can be positioned into a special domain called a DMZ (Demilitarized Zone). The conduit that connects that domain with others should be considered critical and as a critical conduit, the type and number of controls included on it should be thoroughly designed
- **Credential theft:** in the Ukrainian incident, the tool used to perform the credential theft was BlackEnergy 3 malware[1]. There are three ways the hypothetical cybersecurity system can minimize the risk of credential theft:
  - **Antimalware network monitoring:** since the incident, many anti-malware detection and removal tools have evolved to detect BlackEnergy 3 malware. Including an updated version of an anti-malware tool as a control in the required conduits which can significantly reduce the chances of the same malware penetration[2]
  - **Process:** the periodical mandatory change of user credentials, and policies that ensure the use of a secure password for each user, will minimize the time that a threat actor can use a stolen credential
  - **Segmentation model:** if the segmentation model is properly defined, certain conduits will have controls that check things like, the times of using the conduit by a user (the time of the day, but also the number of times). Also, if possible, two factor authentications can reduce the impact of credential theft
- **Data exfiltration:** during the "exploring" phase and using the credentials stolen with BlackEnergy 3, the threat actors gathered information about the IACS architecture and all the assets contained on it. The cybersecurity system can reduce the impact on this in the following ways:
  - **Segmentation model:** ensuring through the conduit controls and procedures that the information containing the IACS architecture, or list of assets has a high enough level of protection against disclosure by external sources. For example, controls that limit the users/applications that perform an automated asset discovery with the "whitelisting" method can be a good preventative measure

1 BlackEnergy malware uses keystroke loggers to get the credentials of users.

2 This paper has to remark that malware like BlackEnergy is continually evolving. Newer versions are likely to go under the radar of any anti-malware control. However, having updated controls will prevent older versions of the malware to perform a successful attack, which is also an important way of reducing the risk.

- **Network monitoring:** performing extensive IACS network monitoring (whenever the delay introduced in it is acceptable for their required performance) is a good tool that helps to recognize when an automated asset discovery has been performed (and was not scheduled)

- **VPN access:** the malicious access through the VPN is hard to prevent, because the threat actors used stolen credentials. However, there are measures that can help to effectively reduce this risk:
  - **Two factor authentication:** if possible, two factor authentication should be implemented. This will at least complicate access through the VPN, forcing threat actors to find a way to pass through the second authentication
  - **Segmentation model:** when the segmentation model is defined, one of the key points is to reduce the conduits to the minimum number required. Doing this reduces the attack surface to a minimum
- **Workstation remote access:** in general, remote control is a critical process and the cybersecurity system has to ensure the correct level of security
  - **Segmentation model:** controls can be implemented in the conduits that prevent the remote control being controlled from certain domains of the system (for example, when it is controlled from the DMZ). A whitelist can also be implemented for the remote control
  - **Enable/Disable:** certain rules may be implemented to get the remote control capability enabled only when it needs to be used and the capability disabled when the authorized use is finished. If a non-scheduled use is needed, a two factor authentication may be implemented
- **HMI Control:** usually it is hard to limit HMI control actions, as these are standard operations for the control operators of IACS. However, the cybersecurity system can assure that each HMI control privileges are limited to the minimum necessary area of the process. Also two factor authentication can be enabled for some major changes performed by HMI (like changing the configuration of the UPS)
- **Phone DDoS:** the simple fact of receiving an abnormal high amount of calls at the same time is reason enough to raise an alarm in order to check if it is a DDoS attack (and be on alert that this can be part of a complex attack scenario)

Conclusion

This paper is not intended to transmit the idea that the Ukrainian incident could have been easily avoided by having a normal cybersecurity system in place.

An APT attack, like the one Ukrainian Kyivoblenergo experienced, which targets the critical infrastructure of a country, is generally well funded and supported by an extended operating infrastructure. These types of attacks are hard to avoid, even for well-defended systems that require a lot of resources, man-hours, time and sophisticated skills.

The message this paper aims to highlight, is that with a robust cybersecurity system in place, it is much more difficult for threat actors to perform a successful attack. In addition, a good cybersecurity system provides the tools to supply forensic information for post-attack actions.

In summary and focusing on the threat scenario of the Ukrainian attack, the key points that a cybersecurity system should have are as follows:

- **Segmentation model:** a well-defined segmentation model can reveal many problems that are otherwise normally hard to notice
- **Monitor Network Traffic**
- **Strong credential policies:** ensure secure passwords and periodical change of credentials, this will limit the window to obtain and use stolen user credentials.
- **Control processes:** ensure that all the logical assets have implemented proper processes to handle their required maintenance functions (updating, maintenance, normal managing)
- **Log system:** in order to notice abnormal situations and to build a large historic data repository to enable automated controls
- **Raise user awareness:** people are a major access point for threat actors. Programming periodical training to raise employee's cyber security awareness will help reduce the risk of many threats.

References

- BlackEnergy APT Attacks in Ukraine; http://www.kaspersky.com/internet-security-center/threats/blackenergy

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 345 222 1711

Call IE: +353 1 210 1711

Visit: bsigroup.com