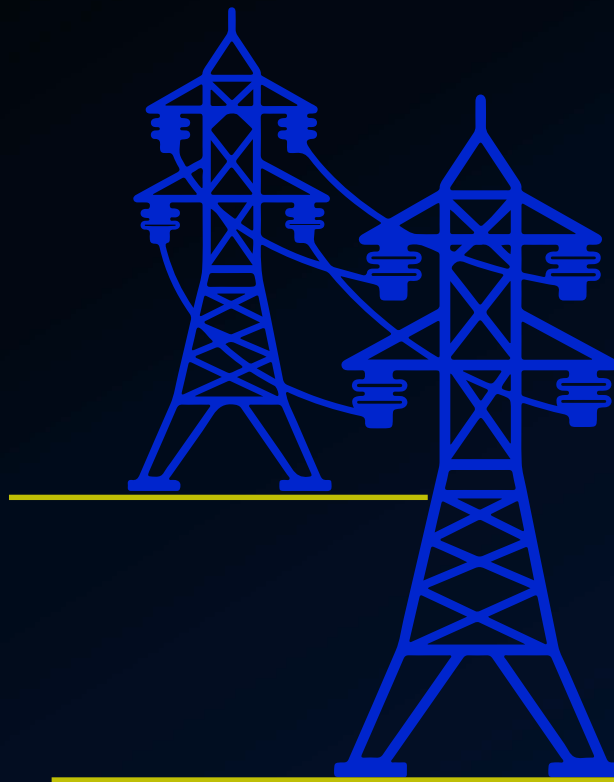


Radiflow

Analysis of the Ukraine Cyber Attack: Causes, Process and Mitigation

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER-RESEARCH TEAM



Analysis of the Ukraine Cyber Attack

Causes, process and mitigation



Description of the Case

On Dec. 23, 2015, at about 13:00, a power outage occurred at western Ukraine's local energy provider Prykarpattyaoblenergo. It cut the power to 80,000 customers for about six hours. During that time, costumers failed to report the outage, due to technical failures in the call center.

After analyzing the information obtained by researchers thus far, it is clear that cyber attacks were directly responsible for power outages in Ukraine.

From what has been revealed by now, it seems that the attackers used at least one malware for damaging the operational network servers and have demonstrated spreading capabilities inside the target network.

The leading theory is that in order to launch the attack the attackers connected online to the operational network, which allowed them to exactly time the command sequence that caused the power outage.

In the next sections, we will describe the phases of the campaign, the lessons learned, and how Radiflow's products can mitigate this risk.

Penetrating the Network

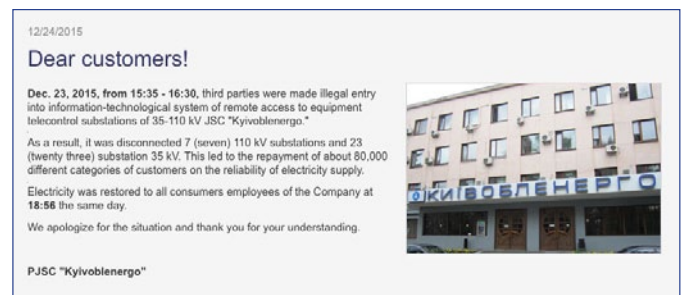
The targets of the attack were multiple regional distribution power companies. The attacks were coordinated, to achieve higher probability of creating the outage. The reports in the media explicitly named specific utilities that were attacked, including Prykarpattyaoblenergo and Kyivoblenergo.

The exact timeline of the attack and the sequence of events are still unclear and are currently being analyzed. What is known is that Kyivoblenergo provided public updates to customers, indicating that an unauthorized intrusion had occurred, which disconnected seven 110kV substations and twenty three 35kV substations, leading to an outage that affected 80,000 customers.

The attack vector, while not confirmed, involved a connection to the internet, either through remote

access or another unprotected route. It is known that the attacker use a corrupted version of a remote-access software that was installed in the operators network.

In addition, it is known the attackers gained persistency in the network, due to a change they have done in one of the HMI files. Then, when the operator updates the software, an infected file is downloaded, which contain the attacker's malware.



Message sent by the energy provider Prykarpattyaoblenergo to its customers following the attack

Lateral Movement

After infiltrating the network the attackers started to infect workstations and servers. According to publicly-available information, they proceeded to spread in the network, where their targets were the servers responsible for controlling the field devices and reflecting the devices' state to the operator.

This allowed the attackers, upon completion of the execution stage, to hide the exact state of the distribution network and to delete forensic data.

These two actions increased the time it took the distribution companies to react to the cyber attack; moreover, even now these actions are still preventing the research community from tracing the exact attack steps.

It is still not clear which method and vulnerabilities were used for spreading the malware and moving around in the network. As mentioned above, it is known that the attackers changed executable files related to the HMI software.

Executing the Attack

What's most interesting about the attack is that current evidence and analysis indicate that the attackers interacted directly with the network (perhaps by means of malware, but not necessarily).

By interacting with the network they were able to send the relevant commands to the field devices and to time those commands to cause the attack.

Analysis of the attack reveals that at least two pieces of malware were associated with the outage. The first, 'KillDisk', was probably used to erase some of the servers.

This piece of malware probably did not directly cause the outage, since the attacker's actions took into consideration timing, sites and impact, which is not the typical MO of 'KillDisk'.

It is not clear if exact goal of the 'KillDisk' malware was to delete forensics data, to increase recovery time from the attack, or another function. It probably was used to delay the restoration of service by wiping SCADA servers after they caused the outage.

Another malware that was reported is related to the BlackEnergy campaign. It is still not clear if this malware was used to gather information and to spread in the network, or to directly execute the attack.

Using this malware the attacker downloaded and activated the 'KillDisk' software.

Another piece of software that the attacker used is an SSH backdoor, probably for communicating within the network and from the network to the Command and Control Servers.

During the attack phase, the attackers issued "denial of view" commands to system dispatchers and attempted to deny customer calls that would have reported the power outage.

The Takeaway

The Ukrainian case illuminates several points regarding SCADA Cyber Attack Campaigns:

1. The coordination required to achieve a significant effect: to cause a full-on outage, hackers would typically need to infiltrate several networks and even different organizations. In addition, they would have to coordinate their commands to the field devices.

2. The least protected company is the one most prone to be attacked: eventually, there are many ways to cause an outage.

Assuming the attackers' goal was just to cause a mass outage in Ukraine, rather than target specific households, they would logically go after the most exposed and least secure targets.

Therefore we can expect to find similar malicious activities in other Ukrainian companies, which have been more secure and have mitigated their risks on time.

3. The use of the supply-chain as an attack vector: it is clear that the attackers manipulated legitimate files used by the operator. When the operator downloaded a file from what was supposed to be the operator's website, what was actually downloaded was a file containing the malware. This attacker vector has been increasingly become a threat to ICS networks.

4. Hiding the damage: as we described in our August post, "Designing an ICS attack Platform," an attacker will typically attempt to hide the damage he has caused. The reasons we presented also hold in the Ukrainian case: increasing the operator's mitigation time and complicating post-attack research.

5. Massive network anomaly behavior: according to the information available to date, it seems that the attackers presented capabilities to move between stations within the network, send commands, change server configuration and open connections from the outside.




This behavior should increase, among operators, the motivation to deploy network security tools such as firewalls and industrial Intrusion Detection Systems.

6. Preventing SCADA Cyber Attacks is indeed possible! Once the targeted companies found out about the malicious activity, they initiated their mitigation programs, which mainly focused on moving to manual control on the operational network.

This step proved to be efficient, but unfortunately too late – since they detected the attack only after it had been launched and already cause the outage.

The first conclusion is that had the operators detected the attack in its initial stages they'd stand a better chance in preventing the outage.

Early detection is key in thwarting cyber attacks, taking advantage of the fact that it takes time for the attacker to launch an attack, and that it creates significant abnormal network behavior.

	Penetrating the network <ul style="list-style-type: none">• Breach in the segregation of the OT/IT• Update of an HMI software
	Lateral Movement <ul style="list-style-type: none">• Compromising Remote Access software for backdoor and C&C• Spreading to multiple servers• Use of SSH-Backdoor
	Attack Execution <ul style="list-style-type: none">• Synchronized commands• "Kill-Disk"

Mitigation

The Ukrainian Outage could have been prevented at multiple points along the "Kill-Chain."

At the Network Penetration phase, effective segregation of the OT network would have enabled detecting the attacker's attempts to penetrate the network. This type of 'ICS Internal Zoning' segregation has already been suggested by the ICS-CERT in August 2014. All it requires is deploying firewall protection between sites.

Radiflow's Secure Gateway was designed exactly for this purpose. With extensive VPN and authentication capabilities, as well as a native Deep-Packet-Inspection (DPI) Industrial Firewall, it is the most suitable product for achieving effective segregation. In addition, the

gateway is capable of self-learning DPI Rules, which helps the operator to easily deploy multiple Secure Gateways with minimal configuration.

That said, while network segregation is an extremely important measure, as it would have enabled detecting and preventing the next attack phases, even without it, the Ukrainian operators could have still detected the attack.

At the Lateral Movement stage, Radiflow's Industrial IDS provides the highest level of protection. Using the Network Visibility package, the Ukrainian operators would have been able to see that the attackers had opened an SSH connection between different stations in their network. In addition, the operator could have detected the communication channel to the attackers' Command-and-Control servers.

Another important package included within Radiflow's IDS is the Cyber Attack package, a signature-based detection engine that allows detecting known malware that communicate inside the network. It is known that the Ukraine attackers used the Black-Energy malware as well as known SSH-Backdoors. Both have signatures, and both could have been detected.

Finally, at the Attack stage, the operator could have seen the exact commands that were sent by the attacker. In the aftermath of the Ukraine attack there was a big problem conducting forensics research due to lack of data. Using Radiflow's Industrial IDS the operators could have analyzed the traffic that caused the outage and track all of the attackers' actions. This would have made the forensics and the mitigation stages much easier and shorter.

About Radiflow

Radiflow is a leading provider of industrial cyber security solutions for critical business operations. Our comprehensive portfolio of cybersecurity solutions empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent threat management for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment.

The Radiflow team consists of professionals from diverse backgrounds, from veterans of military cyber and communications units to former employees of leading players in the industry. Founded in 2009, Radiflow's first solutions were launched in late 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at radiflow.com.