Ukraine 2015 Power Grid Cyber Attack

ELEC-E7470 Cybersecurity L - Case Study

Group: Cyber Warriors

Sunny Vijay

Henriikka Hoikka

Blomqvist Kenneth

Introduction

On December 23rd 2015 a power outage occurred in Ivano-Frankivsk Oblast in Ukraine. This was the first known power outage caused by a cyberattack. Three power companies, Prykarpattyaoblenergo, Chernivtsioblenergo and Kyivoblenergo, were affected and they disclosed the source of the incident to be a cyber attack. Other power companies in Ukraine were reported to have similar problems that day but they did not admit being hacked. Consumers of the power company Prykarpattyaoblenergo were most severely affected. About 30 substations were switched off and 230 000 people were without power for a time span ranging from 1 to 6 hours. A estimated total amount of 73 MWh of electricity was not supplied as a consequence of the attack. [5, 6, 8]

The attack is believed to have been conducted by Russian advanced persistent threat group called "Sandworm" and occurred during an ongoing military and geopolitical conflict between Ukraine and Russia over Crimea [9]. "Sandworm" has recently targeted Europe and the United States [1]. There has been attempts to hack European Union institutions, American government entities, and NATO targets, and they have recently tried to hack for example European telecommunications companies repeatedly. "Sandworm" is known to use a distinctive hacking tool called BlackEnergy [9].

The attack

The attack consisted of several steps:

1. Compromising the network over email using BlackEnergy malware
2. Harvesting user credentials

3. Seizing the digital control system of the power plant by remotely switching off substations
4. Disabling IT infrastructure components
5. Destroying files that are stored on IT infrastructure using KillDisk malware
6. Deploying a denial-of-service attack on the company call center

Compromising the network

The BlackEnergy is a malware application that was originally developed in 2007 for distributed denial-of-service attacks. The malware was deployed using weaponized Microsoft Office files delivered to employee workstations by email. The Microsoft Office files included visual basic scripts that would download the malware and install it on the user's computer.

The BlackEnergy malware

BlackEnergy is a trojan malware application designed to perform actions on the host computer. The malware installer will attempt to bypass user account control but will prompt for administrative access if bypassing is not possible. The malware exploits a windows a backward-compatibility feature of Windows 7 and later allowing it to bypass default user account control settings. [4]

The malware targets solely the Windows operating system.

The installer sets up a windows driver that acts as the persistent component of the malware. Windows requires drivers to be signed in order to run. The malware exploits a developer feature which allows developers to run drivers during development. The feature is engaged using a boot configuration option which the installer switches on. When in this mode, the operating system will show a watermark on screen to prevent using this feature by such malware. BlackEnergy bypasses this watermark by modifying a dynamically linked system library. [4]

The driver component is designed to load plugins over the network. These plugins can then execute arbitrary tasks on the host computer allowing the botmaster to use malware for whatever they wish. [2, 4] In the Ukrainian power grid attack the BlackEnergy driver component was used in several stages of the attack, including harvesting user credentials [2].

Getting access to the control system virtual private network

The BlackEnergy malwares driver component detailed in the previous section was used to run plugins designed to harvest user credentials and stored passwords on employee workstations. The attackers managed to harvest credentials for the virtual private network used by employees to access the SCADA control system. Upon getting access to the VPN, the attackers were able to reconfigure an uninterruptible power supplies such that it would power off as a result of a power outage. [5]

It is speculated that in this stage of the attack, additional reconnaissance would have taken place. Such reconnaissance would include identifying devices on the network such as serial-to-ethernet devices used to interpret commands from the SCADA network as well as distribution management systems. [5]

In the final stages of the preparation of the actual attack, the attackers installed KillDisk malware on servers and workstations on the network rendering them completely inoperable.

The KillDisk malware

Several types of KillDisk malware have been found. The exact version used in the attack remains unclear. Variants of KillDisk malware that have been examined render the system it is run on unstable by overwriting critical system files. In addition they may overwrite other files on the system such as log files.

Attacking the industrial control system

Once the attackers gained access to the network, they were able to access operator's computers which they then used to take down the substations.

Right before shutting down the power grid, the attackers installed custom firmware on serial-to-ethernet gateway devices to ensure that remote commands could not be issued to the substations. This required the employees to physically visit the substations in order to flip the switches back on the substations, making the attack more severe. It is believed that the attackers had tested the firmware beforehand on their own hardware indicating that this was a highly targeted, skilled and intricately orchestrated attack. [5]

The denial-of-service attack on the call center

After the outage Prykarpattyaoblenergo and Kyivoblenergo were flooded with calls. However, these calls did not come from local customers, as one could assume, but they appeared to come from abroad - from Moscow. It turned out to be a telephone denial-of-service attack (TDoS), very much similar to distributed denial-of-service attack, where call center is bombarded with bogus calls to prevent actual customers calling in and reporting their power outs and getting information. [3][6] Later on, in the light of new evidence, it was analyzed that the TDoS attack was perhaps not carried out to prevent customers from reporting the outages but rather to frustrate the customers as they could not get clarity on the situation from the call center. The TDoS attack's purpose was to be a supporting attack. [5]

Aftermath

The intelligence community of Ukraine points finger at Russia for being the culprit for the attack but have not been able to provide full proof. It cannot be with full assurance who were the ones behind the attack but many signs indeed indicate that the attack originated from Russia. Nonetheless, the different stages of the attack indicate that actors from different levels have been working on the different stages of the attack. This means that there is a possibility that this attack was done in cooperation between cybercriminals and nation-state actors - it anyway had to be done by extremely capable and well-funded group of actors. Given the political tensions between the two countries since the annexation of Crimea in 2014, the scenario is a possible explanation. In case the attack had been a political act by Russia and its government, the aim of the TDoS would also to shake the Ukrainians' trust on the Ukrainian power companies and government. [3]

After the annexation of Crimea, Ukrainian energy companies there were nationalized by Crimean authorities which obviously antagonized the owners. As revenge, pro-Ukrainian activists physically attacked substations that feed power to Crimea. This led to large power outage in the Russian annexed parts and left two million Crimeans and one Russian naval base without power. As this incident happened right before the Ukrainian power grid attack and thus, some speculate that the latter incident was a mere revenge for the former. [3, 9] However, the planning of the attack in Ukraine had been stated at least six months before but it would seem that the attack in Crimea rushed the attack to Ukraine. Rushing with the plans was necessarily not a good idea as the attackers would have benefitted about having more time to plan the attack, according to data. [3]

Yet another speculation reckon that if the attackers were indeed from Russia, the reason would have to do with Ukraine's recent plans to nationalize Ukraine's privately owned power companies. The owner of some of the companies is a Russian oligarch close to Putin and the attack might thus have been an objection to nationalization. [3]

An interesting notion that has been made is that the attackers could have done much more damage by physically destroying substation equipment in the process. This would have been extremely easy to do. Whatever the cause of the attack, experts have come to the conclusion that the aim was to send some kind of message to Ukraine. [3]

The attack was first of its kind and no serious damage was done due to the nature of the attack and the prompt actions at the power stations. It remains to be seen if this kind of attack will be redone and what are the consequences then - there is potential to a much bigger catastrophe. [3, 5]

The attack to the Ukrainian power companies has been analyzed in tight cooperation with the United States and as much learnings as possible for has been tried to derive from it to be better reserved for similar attacks in the future [8].

How can these electric utilities protect themselves?

In December 2014, ICS-CERT reported that BlackEnergy was detected on the control system networks of US too. As these utilities rely on same technologies across the geographical locations as in ukraine , following practices are recommended:[7]

- **Review SCADA/ICS security architecture:**

Experienced and qualified ICS security professionals should regularly review ICS network architecture including VPN configuration, firewall placement and rules, and router access control lists.

- **Enhance Network security monitoring capability:**

Robust log collection and network traffic monitoring are the initial components of a defensible ICS network. Failure to perform these essential security functions prevents timely detection, pre-emptive response, and accurate incident investigation which are very important for network security.

- **Search for Indicators of Compromise:**

Capability to monitor the network security should be in place, automated tools that can alert security experts and process operators when abnormal , strange behavior or ICS-oriented malware such as BlackEnergy 3, is identified/observed in the environment.

- **Review Incident Response Plans**

As of today , the electric utilities are capable to respond frequently to outages caused by weather or equipment failure, similarly they must also provide response plans for cyber attack. The plans should cover response protocols for realistic scenarios such as the wiper malware seen during the Ukraine attack.

Lessons Learned

Slovakia-based security firm, ESET provided the common cybersecurity advice as to keep the system software up to date, secured and recruit competent employees. Form technical perspective, the report said that the systems running on Windows XP were widespread, not all workstations were running with antivirus software, lots of systems and software hadn't been patched and critical systems were also remotely accessible, poorly defended and ran on networks that weren't segmented.[10]

Writer says that the mistakes made by the attackers related with BlackEnergy and Killdisk has given them an opportunity to study the attacker's tools and techniques. For instance, researchers have recovered the full source code of various pieces of attack code, including malware and command-and-control infrastructure code to understand as how the attackers were able to penetrate in the system. Network security monitoring tools could have helped to spot the attackers before they shut off the power. The report recommends using multi-factor authentication for any remote access communications.

Sources

[1] FireEye: Sandworm Team and the Ukrainian Power Authority Attacks (Jan, 2016)
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

[2] Booz, Allen, Hamilton report "When the lights went out" (2016)
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

[3] Wired: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid (March, 2016)
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] F-Secure whitepaper "BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks"
https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

[5] SANS-ICS Electricy Information Sharing and Analysis Center whitepaper "Analysis of the Cyber Attack on the Ukrainian Power Grid" (March, 2016)
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[6] Wired: Everything We Know About Ukraine's Power Plant Hack (Jan, 2016)
https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[7] NATO Cooperative Cyber Defence Center of Excellence Tallinn, Estonia (CCDCOE): Cyber War in Perspective: Russian Aggression against Ukraine
https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html

[8] US Dept. of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure (Feb, 2016) https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[9] Foreign Policy: Did Russia Knock Out Ukraine's Power Grid? (Jan, 2016)
http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

[10] Ukrainian Power Grid Blackout Alert: Potential Hack Attack (Dec 2016)
http://www.bankinfosecurity.com/ukrainian-power-grid-attacks-lessons-learned-a-9604