World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Analysis of Ukraine power grid cyber-attack 2015

Afra Ansaria *

SIGMOID LLC, San Francisco, California.

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(01), 410–412

Publication history: Received on 05 January 2024; revised on 04 February 2024; accepted on 07 February 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.1.0024

Abstract

In December 2015, a regional electricity distribution company in Ukraine reported service outages to its customers. The outages were due to a cyber-attack on the company's computers systems and SCADA systems. Seven 110 kV and 23,335 kV substations were disconnected for many hours. Later reports suggested that additional portions of the electricity distribution grid were impacted and forced the operators to switch to manual mode.

The Ukraine power grid attack of 2015 is perhaps one of the most notable cyberattacks in the ICS industry. Over a period of six months, the attackers were successfully able to launch a series of sophisticated attacks that completely disabled the power system of Ukrainian power companies. The paper discusses the sequence of attacks that led to the final failure of the Ukraine power grid. Further it will highlight the details of each attack steps taken by the attacker. This attack vector can serve as the footprint of the potential threats an organisation might face in the event of a similar attack to the organisation.

Keywords: Cyberattack; Network Attack; Cyber Security; Ukraine; SCADA systems

1. Introduction

1.1. The Ukraine power grid attack

The Ukraine power grid attack of 2015 is perhaps one of the most notable cyberattacks in the ICS industry. Over a period of six months, the attackers were successfully able to launch a series of sophisticated attacks that completely disabled the power system of Ukrainian power companies [1].

The attack vector corresponding to the kill chain of such a cyber-attack will studied in this paper. This attack vector can serve as the footprint of the potential threats an organisation might face in the event of a similar attack to the organisation. Taking a closer look into the details of the attack will show the potential way the attackers can compromise the system, thus giving better insight into the feasible security measures that should be placed in order to strengthen its defences.

In December 2015, a regional electricity distribution company in Ukraine reported service outages to its customers. The outages were due to a cyber-attack on the company's computers systems and SCADA systems. Seven 110 kV and 23,335 kV substations were disconnected for many hours. Later reports suggested that additional portions of the electricity distribution grid were impacted and forced the operators to switch to manual mode. Three different distribution companies were compromised as part of the cyber-attack. The attacks on each of these companies were executed within 30 minutes of each other, impacting more than 225,000 customers spread across the region. The companies were reported to be able to restore the services soon after the outage window that lasted for several hours. While the

* Corresponding author: Afra Ansaria

electrical service was restored, the impacted companies continued to operate their distribution system in an operationally restricted mode.

The attackers used a variety of attack tactics in order to compromise the distribution network of the company. The tactics included using spear-phishing emails, manipulations of Microsoft Office documents, usage of malware such as the BlackEnergy 3 malware to gain a foothold into the IT network of the companies. The attackers were able to gain a foothold and sniff out the credentials to gain access into the ICS (Industrial Control Systems) network of the company. The attacker also interrupted the UPS (Uninterruptible Power Supplies) that would disable the backup power supplies along with taking control of the SCADA systems that control most of the operators and switches of the ICS network.

The cyber-attack was extremely sophisticated and well planned. The attack lasted for more than six months, from March 2015 to December 2015, during which time the attacker carefully planted itself in the IT network of the systems and monitored the activities of the network before it finally launched its attack interrupting the operations of the companies. The initial intrusion into the network was initiated by sending spear-phishing emails, which contained malicious Microsoft Office attachments, to the internal staff members of the companies. The spear- phishing emails took the form of benign marketing/PR emails that prompted the staff personnel to click on the document. When opened, the document would show a pop up asking the users to enable the macros in order to read the document. Once the user allowed the macros, the Black energy 3 malware [1] was installed onto the victim's computer. The vulnerabilities in the Microsoft Office code allowed the attacker to take advantage and plant itself on the local foothold machines. The Blackenergy 3 malware created communication channels to the attacker.

With the use of this communication channel, the attacker was able to collect information from the remaining information systems. The attacker was allegedly in the system for 6 months, performing reconnaissance, collecting the credentials of user accounts, escalating the user privileges and more laterally throughout the environment. The attacker was able to gain access to the user accounts information of the Windows Domain Controllers. With this information, the attacker was able to identify the VPN connections and various entry points that would enable it to enter the ICS network. With the stolen credentials, the attacker was able to pivot into the networks where SCADA workstations and servers existed. Although the SCADA networks were segregated with a firewall, the attacker was able to override it by using the stolen user credentials Upon entry into the network, the attacker tactics were consistent in theme but different in the technical implementation between the three impacted companies. In at least one of the companies, the attacker discovered a network connected to a UPS and reconfigured it so that in the event of the power outage, the power in the energy company's building or data centres would also be impacted.

During the reconnaissance phase, the attacker also studied the distribution management systems (DMS) of the power grid. They learnt about the three distinct DMS environments using the native control present in the system and operator screens. Additionally, they developed malicious firmware for the serial to the ethernet devices. The malicious uploads of firmware were developed before the launch of the attack and had predictable execution. In the final steps for the attack, the attacker installed the malicious software identified as a customised KillDisk across the entire environment. The final act of the attacker was to take control of the operators' workstations and lock them out of the systems. Lastly, to execute the ICS attack, the attacker used the HMIs in the SCADA systems to open the breakers, thus causing at least 27 substations within the three companies to go offline, impacting roughly 225,000 customers. During the same time, the attacker uploaded malicious firmware to the serial to ethernet connections, ensuring that the remote commands could not be used to bring the substations back online.

2. Telephone Denial of Service attack

During the last stage of the attack execution, the attacker also performed a remote telephonic denial of service on the company's call center. The attackers sent thousands of calls to the call centre, ensuring that the impacted customers could not report the outages. While this attack was initially assumed to keep the customers away from informing the operators about the outage, it was more likely executed to frustrate the customers should they reach out to the customer support or gain information regarding the power outage.

Below is the consolidated list of the technical tactics used by the attacker throughout the Kill Chain:

- Spear-phishing email to gain access to the local foothold machines of the company.
- Initiation of Black energy 3 malware at each of the impacted companies.
- Credentials sniffing of the internal users on the IT network.
- Gaining access to the VPN network.

- Entering the ICS network through the SCADA controls.
- Using SCADA controls to execute tools or issuing remote commands directly to the HMI operator.
- Installing malicious firmware on the serial to ethernet communication devices.
- Using a modified KillDisk, erase the master boot record of the impacted subsystems within the organisation and targeted deletion of the logs.
- Reconfiguring the UPS systems to impact the load further during the service outage.
- Telephone- based Denial of Service attack at the call center of the companies.

The entire cyber-attack from the period of March 2015- Dec 2015 is depicted in the attack vector shown below:

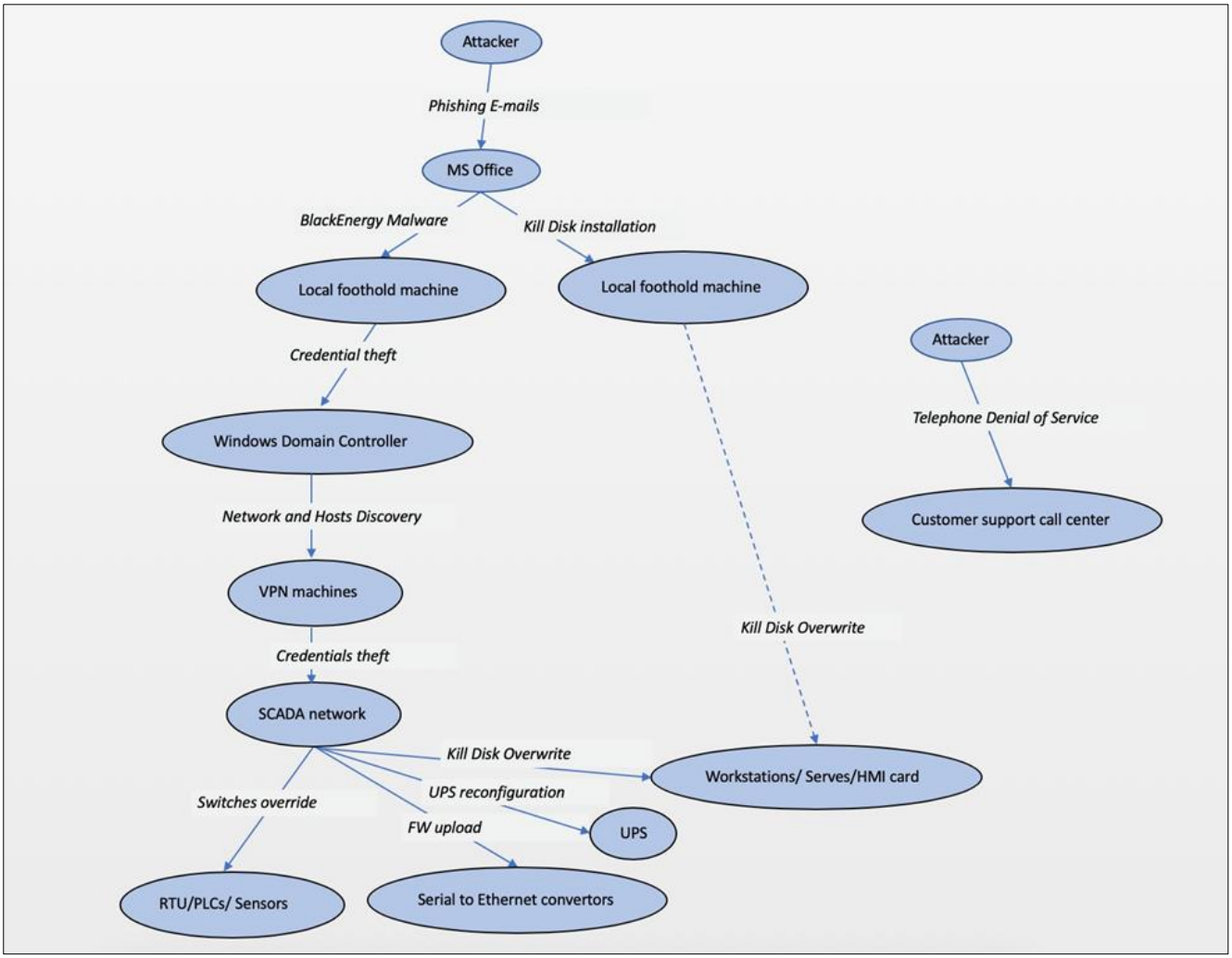

Figure 1 Attack Vector for the Ukraine Power Grid Attack 2015

3. Conclusion

The Ukraine power grid attack of 2015 demonstrated a highly sophisticated cyber-attack targeting industrial control systems, resulting in significant disruptions to the power infrastructure. This paper aims to dissect the attack vector, providing insights into potential threats organizations may face and emphasizing the importance of robust security measures. Through tactics like spear-phishing, malware deployment, and manipulation of SCADA systems, the attackers gained access and executed a coordinated attack, highlighting the critical need for enhanced cybersecurity in critical infrastructure networks.

References

[1] E-SAC, SANS: Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016