Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 04 Issue 02
2023

Research Article
https://doi.org/10.56979/402/2023

Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids

Faiza Babar Khan[1,*], Ali Asad[1], Hanif Durad[1], Syed Muhammad Mohsin[2,3,] , and Sadia Nishat Kazmi[4]

[1]Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad 45650, Pakistan.

[2]Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan.

[3]College of Intellectual Novitiates (COIN), Virtual University of Pakistan, Lahore 55150, Pakistan.

[4]Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, Gliwice, 44-100, Poland.

[*]Corresponding Authors: Faiza Babar Khan Email: faiza_19@pieas.edu.pk.

Received: December 08, 2022 **Accepted:** March 12, 2023 **Published:** March 29, 2023.

Abstract: The Energetic Bear group, also known as Dragonfly, is a collection of cyber attackers that have successfully infiltrated the critical infrastructure of American and European governments. They have been identified as the primary suspects in one of the most severe instances of cyber espionage in the history of the United States, utilizing Advanced Persistent Threat (APT) tactics for their operations. Through a variety of techniques, such as social engineering, Trojanized software, and watering hole attacks, the group has targeted its victims. This paper uses the group's attack scenario as a case study for cyber-attacks on power grids, presenting the methods used by the group. The paper also includes an analysis of the malware samples used by the group and provides forensic findings.

Keywords: Dragonfly; Critical Infrastructure; Industrial Control System; SCADA; Malware Attacks

1. Introduction

Targeted cyber-attacks are a type of cyber-attack that focus on a specific organization, individual, or system. These attacks are carefully planned and executed by skilled cybercriminals who use a range of techniques to gain unauthorized access to a particular target [1]. Targeted cyber-attacks can take many forms, including spear-phishing attacks, watering hole attacks, and Advanced Persistent Threats (APTs) [2]. Criminal groups, hacktivists, or nation-state actors with specific goals in mind, such as stealing intellectual property, disrupting critical infrastructure, or conducting espionage, often conduct these attacks. These attacks can be particularly devastating, as they are specifically tailored to the target, and often go undetected for long periods.

Targeted cyber-attacks against Industrial Control Systems (ICS) are emerging cyber threats to governments and industries. These are designed to exploit vulnerabilities in the computerized control systems that manage critical infrastructure, such as power plants, water treatment facilities, and manufacturing plants [3]. In an ICS, computers, and networks are used to monitor and control physical processes, such as the temperature and pressure of machinery [4]. Targeted cyber-attacks against ICS are usually carried out by APTs, which are well-funded, highly skilled groups that have the resources and expertise to develop sophisticated attack methods. These attacks are often stealthy and difficult to detect.

For example, in September 2010, the Stuxnet worm, designed to specifically target its uranium enrichment plant attacked Iran [5].

Supervisory Control and Data Acquisition (SCADA) systems are used in many critical infrastructure systems, such as power grids and water treatment plants. These systems are designed to provide real-time data and control over the various components of a power grid, such as generators, transformers, and transmission lines. SCADA systems play a critical role in maintaining the reliability and efficiency of power grids. They allow operators to monitor the flow of electricity through the grid, detect any anomalies or issues that may arise, and take corrective action as needed. For example, if a transmission line becomes overloaded, a SCADA system can detect the issue and alert operators to take action to prevent a potential blackout or other outages.

Malware attacks on power grids can have devastating consequences, as they can cause widespread power outages, disrupt critical infrastructure, and affect public safety [6]. Malware is a type of malicious software that is designed to infiltrate computer systems and cause harm, such as stealing sensitive data, corrupting files, or taking control of a system. In the case of power grids, a malware attack could potentially allow an attacker to take control of key systems and cause power outages or other disruptions. This could have serious implications for public safety and could even result in loss of life. To mitigate the risk of malware attacks on power grids, it is important to have strong cybersecurity measures in place, such as firewalls, intrusion detection systems, and regular system updates and patches. Additionally, it is important to educate power grid employees about the risks of malware and how to identify and prevent attacks.

The insight of the analysis is that cyber attackers have gained a very high level of attack capabilities, especially on critical infrastructure. As can be seen in the campaign of the Dragonfly group how they used different types of attack vectors according to the situation and used next-level obfuscation techniques. So it has become very much important to pay attention to cyber security. As it may seem apparent that it has no effect preemptive measures can save from great loss. The purpose of the analysis presented in this thesis was to highlight exploitation techniques and defenses against them. Previous studies [7-9] have revealed the existence of vulnerabilities in communication protocols utilized in Supervisory Control and Data Acquisition (SCADA) architecture. However, none of the cited literature has provided concrete evidence of malware specifically created for the power sector.

The main contributions of this study are mentioned below.

1. We have provided concrete evidence of malware specifically created for the power sector.
2. The techniques utilized by the Energetic Bear group are outlined.
3. An analysis of the malware artifacts utilized by the Energetic Bear group is provided, including a discussion of the vulnerabilities that were exploited.
4. A case study of a dragonfly attack on the power grid is presented.

The remainder of the paper is organized as follows: Section 2 presents the previous work done to explore malware attacks on SCADA systems. Section 3 describes the preliminaries and background of ICS components. Section 4 gives a brief case study of a dragonfly attack. Finally, Section 5 summarizes the paper with upcoming research directions.

Table 1. List of Abbreviations

Acronym	Description
APT	Advanced Persistent Threat
SCADA	Supervisory Control and Data Acquisition
ICS	Industrial Control Systems
MAlSim	Mobile Agent Malware Simulator

IDS	Intrusion Detection System
PLCs	Programmable Logic Controllers
MITM	Man-in-the-Middle
DoS	Denial of Service
HMI	Human Machine Interface
MTU	Master Terminal Unit
RTU	Remote Terminal Unit
C&C	Command and Control
OPC	OLE for Process Control
XDP	XML Data Package
SWF	Shockwave Flash

2. Literature Review

SCADA network and architecture are based on ad-hoc components. So attack vectors deployed by attackers are engineered to attack a specific setup. Fovino , et al. [10] have demonstrated malware attacks on power-related SCADA. They used Mobile Agent Malware Simulator (MAlSim) as a toolkit for the simulation of attacks. They showed that malware can take control of the SCADA system in their experiments. B. Zhu, et al. [14] focused on a systematic approach to identify and classify expected cyber attacks counting cyber-generated cyber-physical attacks on SCADA systems. In [15], the researchers analyzed a multitude of cyber-security incidents related to critical infrastructure and SCADA systems, and organized them based on the sectors involved in the incident (i.e., Source and Target), the method used to carry out the attack, and the resulting impact. .In [16] J. Ibarra et. al. focused on the fact that ransomware injection is the most predominant offensive trajectory as it denies the obtainability of vital documents and structures unless attackers collect the required payment. So authors analyzed the risk effect of ransomware injection into SCADA and recommended some remedies to protect the components.

In [22], authors scrutinized different attacks to gain a deeper understanding into the advancement of upcoming cybersecurity techniques for ICSs. As a concluding step, they put forth a few suggestions for implementing the most effective measures to safeguard ICSs. In [23], Deval et al. focused on the transition of ICSs from self-contained systems to cloud-based settings. The authors explored prominent research efforts by both industry and academia, specifically regarding the use of machine learning techniques to enhance ICS cybersecurity. In [24], authors explored the range of attack vectors utilized by APTs against conventional and novel components of an industrial ecosystem. Following this, an examination of the progression and suitability of Intrusion Detection Systems (IDS) proposed by both industry and academia is presented. In [25], introduced an innovative approach to implement network monitoring in cybersecurity, which has shown remarkable effectiveness in safeguarding Critical Infrastructure sectors such as Oil and Gas, Power Generation, and Energy Distribution. SecurityMatters provided an impartial perspective on the effectiveness of network monitoring techniques, including both successful and unsuccessful strategies, and explained the underlying reasons behind their effectiveness or shortcomings.

In [26], the authors categorized security measures into three groups - compliance with prevailing standards, attack detection, and prevention - and examined the potential future obstacles that SCADA networks may encounter, particularly from quantum-based attacks. In addition, it outlined potential research directions for the advancement of this field. The authors in [27] presented the fundamental principle of PLC. Subsequently, an analysis of several security aspects, including PLC code security, firmware security, network security, and Modbus communication protocol, is carried out. The discussion in [28] encompassed all the security and privacy concerns that are currently known pertaining to Power

Line Communication systems, and their analysis was focused on evaluating these issues based on their respective levels of security.

In [29], a method is presented for detecting cyber-attacks in smart grid systems. The suggested method monitors ICS traffic and identifies abnormal data flows using unlabeled data. For intrusion detection in ICS traffic, two semi-supervised deep learning-based anomaly detection algorithms, AE-GRU and GAN-RNN, are developed. GRU and RNN are used in these models to improve their ability to learn temporal connections in multivariate data. For identifying cyber-attacks in power systems, the models are utilized for feature extraction and applying several anomaly detection approaches such as Isolation forest, Local outlier factor, One-Class SVM, and Elliptical Envelope. The authors in [30] presented a systematic review to perform a thorough analysis of various methodologies, advanced techniques, and prospective strategies to address cyber-security in Smart Grids.

Authors in [31] focused on examining the various methods employed in phishing attacks. The ultimate goal was to encourage expert discourse on the subject of phishing, raise public consciousness about the tactics used in these attacks, and enhance education surrounding the matter. In [32], threat-modeling approaches have been explored. The authors highlighted the drawbacks of some of these models and proposed ways to enhance their effectiveness in describing cyber-attacks on energy infrastructure with greater accuracy. Authors in [33] offered a fundamental offensive approach that focuses on modifying registers in a systematic manner and utilized a standard industrial setting to display its susceptibilities to cyber-attacks through widely available open-source tools. In [34], the authors focus on the attacks on SCADA systems. A mathematical model is introduced to describe the propagation of industrial viruses in SCADA systems. The equilibrium point of the model is analyzed to determine its existence and stability. To manage the spread of the virus more efficiently when resources are limited, an optimal control system was developed for the model.

3. Preliminaries and Background

The analysis reveals that cyber attackers, particularly on critical infrastructure, have gained a significant level of attack capabilities. This is evident in the Dragonfly group's campaigns, where they employed various attack vectors and advanced obfuscation techniques. Therefore, it is crucial to prioritize cybersecurity as it may not appear to have an immediate impact, but taking preventive measures can prevent significant losses. The goal of this thesis is to shed light on the exploitation techniques used by the Dragonfly group and propose defenses against them.The objective of this case-study is to examine the malware samples utilized by the Dragonfly group. Through a comprehensive analysis, this research identified the attack vectors and payloads used by the group. Attack vectors refer to the methods used by attackers to gain access to computer systems, while payloads are the actual programs used to perform various functions on the victim's computer. Additionally, this study recommends attack prevention techniques based on the Dragonfly group's experience.

This section will provide a thorough investigation of malware used by the Dragonfly / Energeticbear group to attack power-related critical infrastructure.

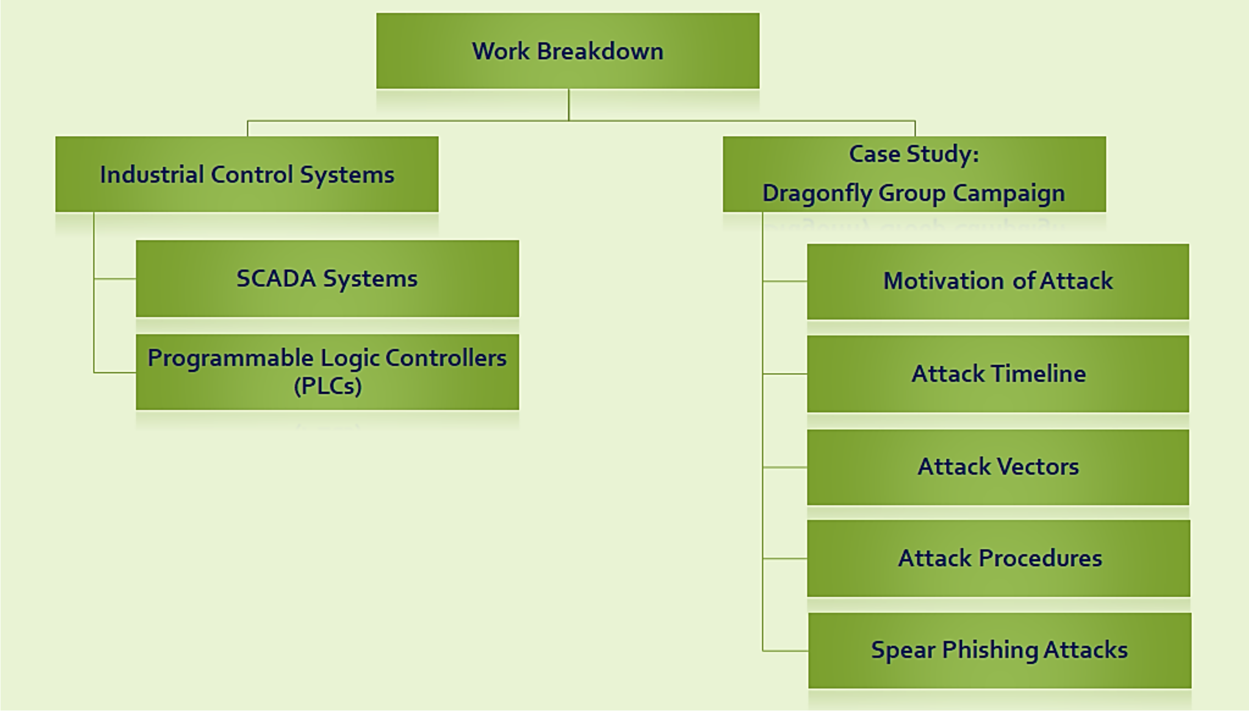


Figure 1. Paper Layout

The composition of the case study is shown in Figure 1.

3.1. Industrial Control Systems (ICS)

Industrial Control Systems are used to control automation processes in the industry. Supervisory Control and Data Acquisition (SCADA) Systems and Programmable Logic Controllers (PLCs) both come under the category of Industrial Control Systems. These are highly distrusted systems spread physically and using different communication mediums for connecting devices. A description of the components of the ICS is provided below.

3.1.1. SCADA Systems

SCADA systems are used to manage the various power generation sources that contribute to a power grid. This includes both traditional fossil fuel-based power plants as well as renewable energy sources such as solar and wind power. SCADA systems help to balance the output of these different power sources to ensure that the power grid is operating efficiently and reliably. Communication protocols are essential components of these systems, and any vulnerabilities in these protocols can have severe consequences. Several vulnerabilities that exist in communication protocols used in SCADA architecture include Lack of Encryption, Weak Authentication, Lack of Authorization, Buffer Overflow, etc. Various attacks like Protocol Spoofing, Man-in-the-Middle (MITM) Attacks, and Denial-of-Service (DoS) are very dangerous for SCADA systems [18].

SCADA systems provide consistent centralized monitoring of the whole process [19]. The finest use of SCADA is in the power sector where power generation, distribution, and transmission are scattered but working coherently. SCADA is used in the power sector to control entities involved in all three systems. SCADA systems also provide a centralized user-based or automatic command issuing system using which commands can be sent to remote devices. Due to the critical infrastructure that SCADA systems manage and monitor, any security breaches in these systems can result in severe consequences [20].

SCADA systems are used when centralized control of geographically distributed objects is required, and when central data acquisition is important for making changes in a system based on the collected information, as compared to PLCs [18]. For example, SCADA systems are commonly used in the power sector, public transportation, oil and gas, and wastewater management industries. These systems aggregate data coming from remote locations and present it to the operator through the use of a Human Machine Interface (HMI), which can display data in the form of text or graphs. The operator can then send remote commands through the transmission system. Depending on the requirements, tasks at individual locations can be automated or controlled by the operator.

SCADA systems consist of both hardware and software components. Below is a list of the primary hardware components.

- Master Terminal Unit (MTU) at Control Center
- Communications Tools
- Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) at remote sites

The data gathered from RTUs is processed and stored in MTUs. Local processes and communication hardware managed by RTUs and PLCs facilitate connections between MTUs, RTUs, and PLCs. Communication hardware, which includes a radio, telephone link, cable, and satellite link, enables this connectivity. Additionally, the software is programmed to identify abnormal parameter values and determine appropriate actions. It also specifies which parameters to monitor and when to monitor them. Automatic responses based on inputs are also programmed into the software.

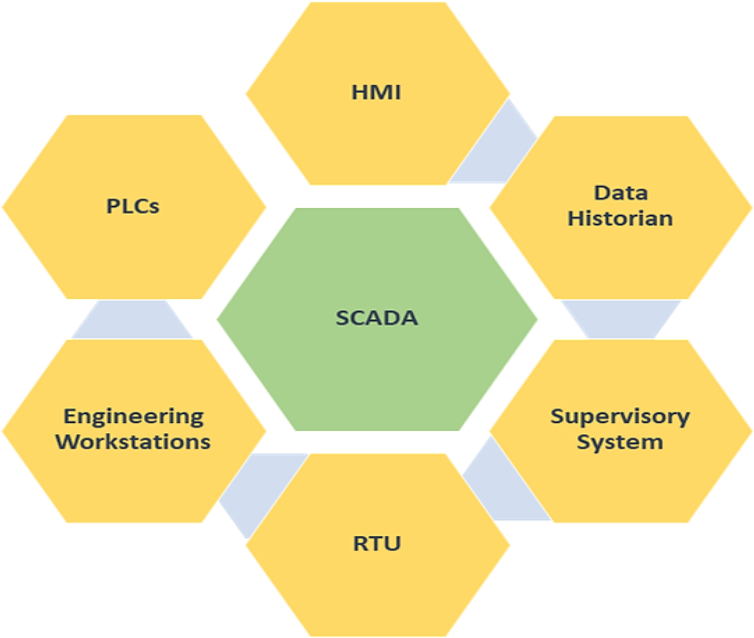


Figure 2. Basics of SCADA

Figure 2 depicts the various components of a standard SCADA system. The Control Center is composed of a Human Machine Interface (HMI), Data Historian, Engineering Workstations, Control Servers (MTUs), and communication routers. The HMI is used to present information to the operator. Engineering workstations run an engineering application program that collects data from the control server. Data historian records historical data, while communication routers maintain a link to remote locations. All of these Control Center components are linked through a Local Area Network (LAN). Communication channels form a wide area network and technologies used, are telephones lines, Cellular technology, Microwave link, and finally satellite connectivity. WAN connects the Control center with field sites. Field sites contain communication equipment that interacts with WAN and uses standard or proprietary communication protocols. Field sites also contain RTU or PLCs which look after the local process. Field sites send parameter values to the control center and receive remote commands from the control center.

3.1.2. Programmable Logic Controllers (PLCs)

Programmable Logic Controllers (PLCs), are computer-based devices that operate independently from SCADA systems. Although they can be integrated into SCADA as a sub-component, their primary purpose is to automate a specific task. As a result, they are often deployed as stand-alone units in industry for automation processes [7]. PLCs have both analog and digital inputs and outputs, and their programming dictates the output in response to the inputs and the present state. Additionally, PLCs are designed to operate in real-time mode, with sensor outputs serving as inputs and the output from the PLC used to effect changes in the environment through actuators.

PLCs are extensively used in industry to connect equipment to a computer for monitoring consumer devices due to their ease of installation and adaptability [21]. They interface with the external world through input and output mechanisms. With the development of motion control technology for chain drives, the use of PLCs in conjunction with power electronics for electric machine applications has been gradually adopted in factory automation.

PLCs act as units in SCADA setup and can also act as individual industrial automation devices. PLC is a control device that can be programmed locally to process inputs and generate responses. PLCs have user-programmable memory which can be programmed to take care of the following tasks:

- Input / Output Management
- Logic
- Timing
- Counters
- Communications
- Data and File processing

4. Dragonfly: A Case Study

This section provides a thorough investigation of malware used by the Dragonfly / Energeticbear group to attack power-related critical infrastructure. Dragonfly, Energetic Bear, and Crouching Yeti is the name given by different antivirus vendors to a group of people who have launched cyber-attacks against critical infrastructure of European and American governments. The group is believed to be backed by the Russian government [17]. Symantec an American technology company recognizes the group as Dragonfly while Kaspersky Lab, an international software security group with headquarters in Russia recognizes the group as Energetic Bear or Crouching Yeti.

The Dragonfly group has been operational since 2011 according to Symantec. The group has been conducting espionage using Advanced Persistent Threat (APT). The main targets of the group are defense contractors and government organizations. Dragonfly has been launching Stuxnet-type attacks against petroleum pipeline operators, grid operators, electricity generation firms, and other critical energy companies coming under the umbrella of industrial control systems. Dragonfly group has been using spam emails and watering hole attacks to infect the pointed organizations. The Dragonfly APT group (also known as APT29) has been known to target a variety of sectors, but they have a particular focus on the energy sector. In 2014, Symantec published a report on Dragonfly that identified over 1,000 organizations that had been targeted by the group, with 84% of those organizations being in the energy sector. The report stated that the majority of the organizations targeted were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

In 2017, Dragonfly resurfaced and targeted energy companies in Europe and North America. In a report published by Symantec in September 2017, the company identified at least 20 organizations that had been compromised by Dragonfly, with a focus on the energy sector. The report did not provide a percentage breakdown of the victim organizations but noted that the majority of the targets were in the United States, Switzerland, and Turkey.

In 2018, the US Department of Homeland Security (DHS) issued a warning about a new Dragonfly campaign that was targeting US critical infrastructure organizations. The warning stated that Dragonfly had targeted multiple organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors, with a focus on the United States.

Table 2. Percentage Distribution of the sector-wise victims since 2011

Organization	Percentage of Victims
Govt Sector	7%
Defence, Aviation & Healthcare	9%
Energy and Power Sector	84%

Table 2. shows a breakdown of the identified victims of Dragonfly per sector, based on Symantec report 2014 [12]. Two key malware gears have been used by the group which include Karagany (Trojan) and Oldrea (Backdoor). Backdoor. Oldrea is custom-written Remote Access Trojan. [13]. Different aspects of attack launch are discussed in detail in the next subsection.

4.1. Motivation of Attack

According to Symantec Corporation, Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability [10]. The main motivation of the group was espionage. Espionage is the practice of spying to get information that can be used for military and business purposes. Based on information collected from espionage real-world damage can be caused to target courtiers' critical infrastructure. So the campaign launched by the Dragonfly group can be an effort to access the vulnerabilities in critical infrastructures of target countries. So these vulnerabilities can be exploited when needed.

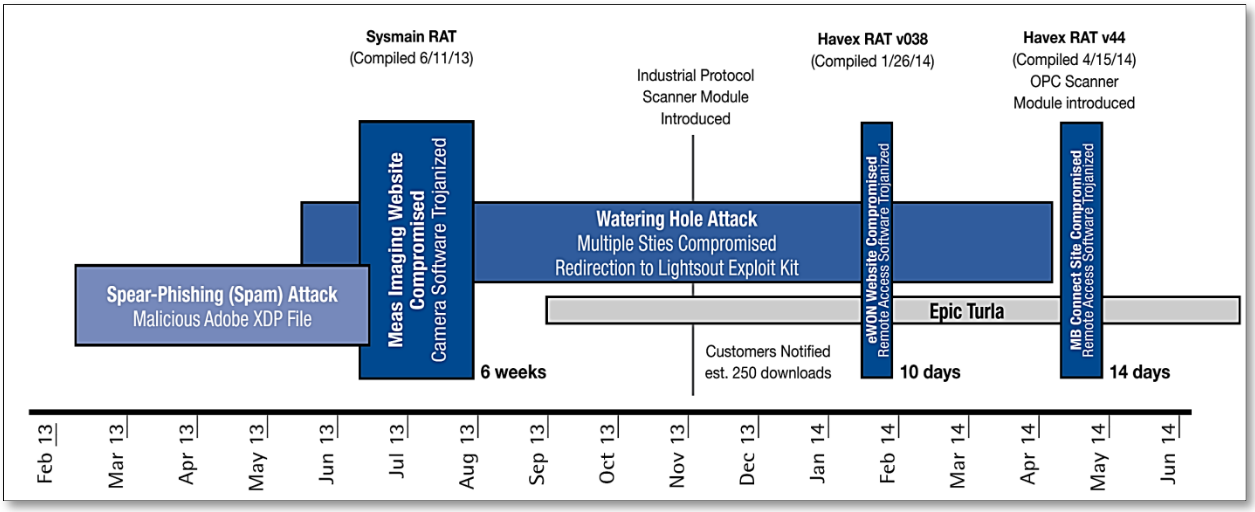


Figure 3. Attack Timeline

4.2. Attack Timeline

According to Symantec reports the first observation of spear phishing attempts, its span was from Feb 2013 to June 2013 as shown in Figure 3. It is email spoofing fraud targeting specific organizations and finding illegal ingress to secret data.In May 2013, a technique, watering hole, was used to make the trusted websites compromised which eventually allure the website visitors to get directed towards malicious sites. This remained until April 2014.

Therefore due to this attacking technique, several ICS vendors made legitimate software available for download from their websites equipped with malicious content. This Trojan replacement of real ICS software continued for almost one year, beginning in June 2013 and ending in May 2014. [11].

4.3. Attack Vectors

Two malware codes were used by the Dragonfly group both of which were Remote Access Tools (RATs) intended to perform espionage maneuvers. These codes were dispersed and touched the targets using three attack vectors:

4.3.1. Email Operation

Some of the chosen executives and high-ranking employees of specific companies received emails with a PDF attachment containing malicious RAT. Symantec identified the different targetted organizations in this movement; almost 1 -84 emails were sent per organization.

4.3.2. Watering Hole Attacks

Attackers that were to be approached by people employed in the energy sector targeted legitimate websites. When a visitor would reach to some infected websites, he would be immediately forwarded to other infected but genuine Web site introducing an exploit kit. This exploit kit then launched RAT his machine.

4.3.3. Software transferred from ICS-Associated vendors

Dragonfly employees managed to hack the websites of no less than three different vendors related to ICS and inject the malware into real software that could be downloaded by the customers. The malware is then launched on the prey's machine to transfer software or update itself. The first software package identified as Trojanized provides VPN access to the Programmable Logic Controller (PLCs) and similar devices. PLC device-type manufacturing company, e.g. Siemens, Delta etc. the second one, had one Trojanized driver. The third one included in this campaign develops Industrial controlled systems for energy markets, mainly renewable.

4.4. Attack Procedures

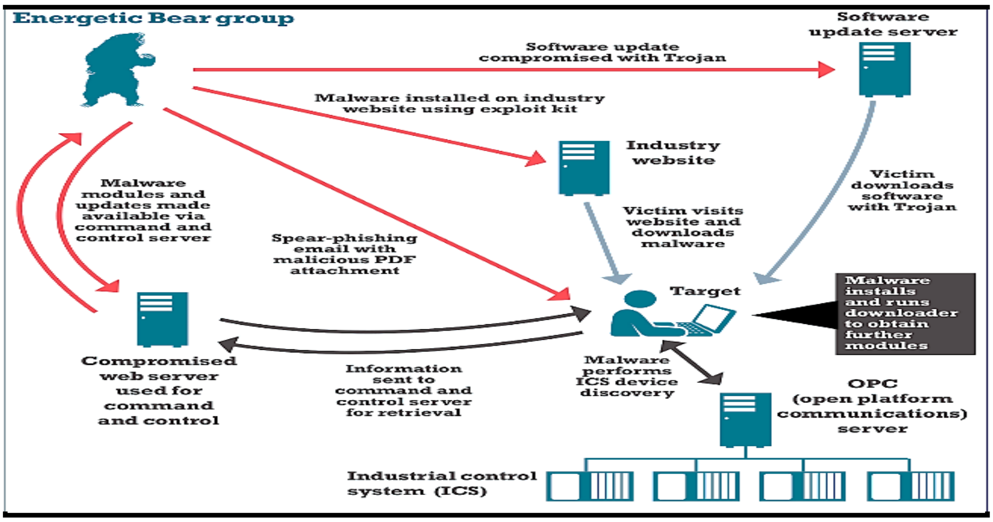

Energetic Bear group
Software update server
Software update compromised with Trojan
Malware installed on industry website using exploit kit
Industry website
Victim downloads software with Trojan
Malware modules and updates made available via command and control server
Victim visits website and downloads malware
Spear-phishing email with malicious PDF attachment
Target
Malware installs and runs downloader to obtain further modules
Compromised web server used for command and control
Information sent to command and control server for retrieval
Malware performs ICS device discovery
OPC (open platform communications) server
Industrial control system (ICS)

Figure 4. Energetic Bear Group Attack Vectors

Methods of attack used by Dragonfly focus on stealing sensitive data and installing further malware on an infected system. In Figure 4, the red arrow represents Energetic Bear activity, the gray arrow represents victim-initiated activities, and the black arrow represents malware activity. The following activities are performed:

1. Spear-phishing emails were sent to seven energy organizations in the UK/US between February and June 2013.

2. The Hello exploit kit was employed to conduct waterhole attacks on users who visited malicious energy sector websites. The website introduces the exploit kit, and Java and browsers are used to download either the Havex downloader or a Trojan called Kargany, which is traded on secretive Russian mediums. Once installed, the malware can collect passwords, screenshots, list documents on the infected machine, and communicate with command and control servers (C&CS).

3. In January 2014, the content management system on www.ewon.biz was compromised, and hyperlinks were redirected to a file containing a Trojan that established a VPN structure. The malware allowed attackers to access the Talk2M cloud infrastructure, which contained encrypted account information. Ewon issued a new version of its software with a malware cleaner and required users to update and connect to its service.

4. The Trojan is transmitted to the infected machine, and it installs a module called Tmproviderxxx.dll, which connects to command and control servers to download additional payload modules. One such module is the ICS sniffer, which uses OPC to explore ICS components on the network.

5. The information gathered by the malware is flattened and encoded before being sent to the command and control servers.

6. The Energetic Bear group obtained the information, and the command and control servers contain updates for the malware to copy to infected computers.

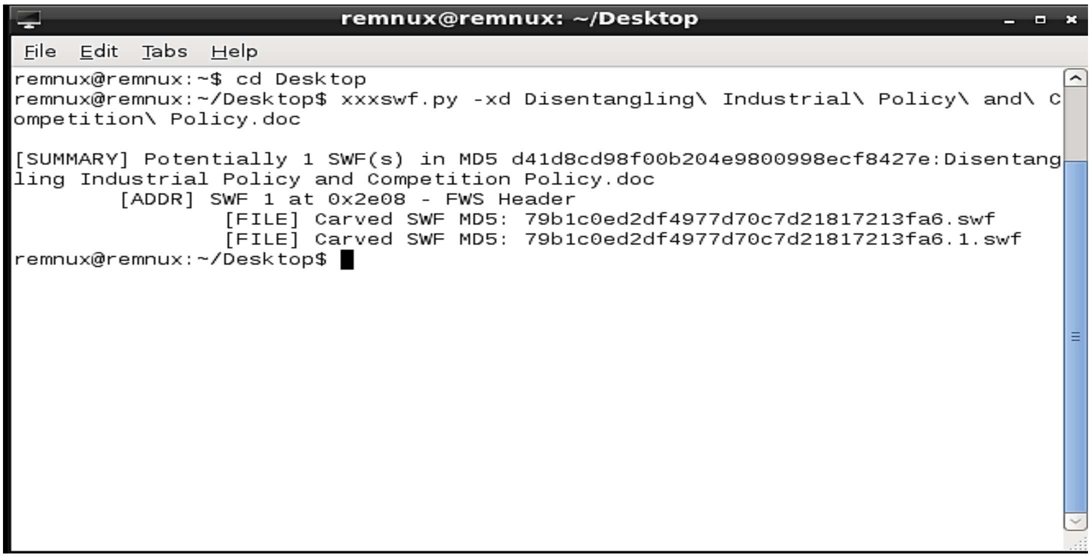
4.5 Spear Phishing Attacks

Spear Phishing attacks used malicious Adobe XML Data Package (XDP) files sent to senior managers and high-ranking employees of target companies. This file manipulated the PDF/SWF exploit CVE-2011-0611 allowing the Decryption, installation, and execution of Havex PE-DLL. The XDP format permits a PDF file to be packed within an XML container, hiding the PDF file and offering some level of discovery elusion from any malware prevention software present in the victim's computers.

CVE-2011-0611 vulnerability surfaced in Adobe Flash Player within the ActionScript Virtual Machine 2 (AVM2), which handles ActionScript 3.0 language. CVE-2011-0611 vulnerability may cause a crash and possibly lets the attack launcher fully capture the affected system. This vulnerability can be exploited against Adobe products and Flash (.swf) files implanted in a Microsoft Word (.doc) or Microsoft Excel (.xls) file which was sent as an email attachment to target the Windows platform.

4.6 Forensics Analysis of the Exploit

The Word document exploiting the above vulnerability is titled "Disentangling Industrial Policy and Competition Policy.doc" and is available for download at the contagio blog [13].



```
remnux@remnux:~$ cd Desktop
remnux@remnux:~/Desktop$ xxxswf.py -xd Disentangling\ Industrial\ Policy\ and\ C
ompetition\ Policy.doc

[SUMMARY] Potentially 1 SWF(s) in MD5 d41d8cd98f00b204e9800998ecf8427e:Disentang
ling Industrial Policy and Competition Policy.doc
        [ADDR] SWF 1 at 0x2e08 - FWS Header
                [FILE] Carved SWF MD5: 79b1c0ed2df4977d70c7d21817213fa6.swf
                [FILE] Carved SWF MD5: 79b1c0ed2df4977d70c7d21817213fa6.1.swf
remnux@remnux:~/Desktop$ 
```

Figure 5. SWF File Extraction from Word Document

To reverse engineer the carved SWF file Sothink SWF decompiler is used which converts the SWF file into action script code. Xxxswf.py utility is already included in the REMnux Linux distribution as shown in Figure 5. To reverse engineer the carved SWF file Sothink SWF decompiler is used which converts the SWF file into action script code. So, think SWF Decompiler is a software program that can convert Adobe Flash SWF files into their corresponding source code formats, such as FLA, FLEX, HTML5, or XML. This tool allows users to extract various assets from SWF files, including images, sounds, videos, shapes, and scripts, and then modify or reuse them in other projects. SWF file is composed of Header, tags, shapes, btimaps, sounds and ActionScripts. ActionScript is a scripting language that is used to add interactivity and logic to SWF files.

The exploit code exploits a vulnerability in Action Script Version 1. To make use of this exposure, the invaders packaged the AVM1 code inside an AVM2-based Flash file. The latter is rooted inside the Word document and assigned to setting up the exploitation environment.

```
function frame1()
{
    this.s = new ByteArray();
    this.s3 = new ByteArray();
    this.a = new Array();
    this.t = "465730ACC0500007800055F00000FA00000180100441100000000F03A70500000960C0005000795;
    this.i = 0;
}
```

The SWF file contains an embedded hex string as this.t data member as shown above. This is an encoded SWF file that is executed by the AVM2-based flash file using the following code as shown below:

```
this.r = this.hexToBin(this.t);
this.ldr = new Loader();
this.ldr.loadBytes(this.r);
```

hexToBin function converts hex string to binary string and loadBytes load that binary and executed that string.

5. Conclusion & Future Work

Cyber warfare encompasses a wide range of activities, from mobile phone attacks to attacks on industrial control systems. In today's world, cyber threats are not just limited to individual attackers with small goals; instead, they are mostly sponsored by nations that target assets of other countries. The energy sector has been a major target of cyber espionage campaigns, where attackers gain access to launch sabotage operations against their victims. In recent years, several attacks have been reported in the energy sector, including those by Dragonfly, a capable group that primarily targets energy and related industries. The group, also known as Energetic Bear, has been operational since 2011 and has evolved over time. Initially, they targeted defense and aviation companies in the US and Canada before shifting focus to European energy firms and the US in early 2013. They have also targeted companies related to industrial control systems. In this study, we analyze the malware used by this group to understand their attack methods in detail and provide mitigation techniques for prevention.

The analysis reveals that cyber attackers have acquired highly advanced attack capabilities, particularly targeting critical infrastructure. This is evident in the Dragonfly group's campaigns, where they employed various attack paths and clever obfuscation techniques. As a result, cybersecurity has become increasingly important, and implementing preemptive measures can save significant money. The goal of this investigation was to promote knowledge of exploitation methods and defenses against them.

To protect SCADA systems, specialized antimalware software will be developed to monitor the system for malware attempting to do dangerous SCADA actions such as scanning SCADA devices or delivering commands to them. It will be ensured that antimalware system is compatible with the SCADA sytems and it will have minimal impact on SCADA system performance. Furthermore, an emphasis will be placed on creating intrusion detection and prevention systems for industrial control system communication protocols, which can reduce the risk of intrusion.

References

1. Mousavinejad, E., Yang, F., Han, Q. L., & Vlacic, L. (2018). A novel cyber attack detection method in networked control sytems. *IEEE transactions on cybernetics*, *48*(11), 3254-3264.
2. Khoei, T. T., Slimane, H. O., & Kaabouch, N. (2022). A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. *arXiv preprint arXiv:2207.07738*.
3. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464.
4. Yılmaz, E. N., & Gönen, S. (2018). Attack detection/prevention system against cyber attack in industrial control systems. *Computers & Security*, *77*, 94-105.
5. Jones, W. D. (2012). Declarations of cyberwar. *IEEE Spectrum*, *49*(8), 18-18.
6. Akhtar, T., Gupta, B. B., & Yamaguchi, S. (2018, January). Malware propagation effects on SCADA system and smart power grid. In *2018 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-6). IEEE.
7. Dondossola, G., Szanto, J., Masera, M., & Nai Fovino, I. (2008). Effects of intentional threats to power substation control systems. *International journal of critical infrastructures*, *4*(1-2), 129-143.
8. Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection*, *1*, 37-44.
9. Masera, M., Fovino, I. N., & Leszczyna, R. (2008). Security assessment of a turbo-gas power plant. In *Critical Infrastructure Protection II 2* (pp. 31-40). Springer US.
10. Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A. (2009). An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection*, *2*(4), 139-145.
11. Response, S. S. (2014). Dragonfly: Western energy companies under sabotage threat.
12. Response, S. I. (2014). Dragonfly: Cyberespionage attacks against energy suppliers. *Rapp. tecn*, *7*.
13. Apr. 8 CVE-2011-0611 Flash Player Zero day - SWF in DOC/ XLS http://contagiodump.blogspot.com/2011/04/apr-8-cve-2011-0611-flash-player-zero.html
14. Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 380-388). IEEE.
15. Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56).
16. Ibarra, J., Butt, U. J., Do, A., Jahankhani, H., & Jamal, A. (2019, January). Ransomware impact to SCADA systems and its scope to critical infrastructure. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 1-12). IEEE.
17. Thomson, A., & Rahn, C. (2014). Russian Hackers Threaten Power Companies, Researchers Say. *Bloomberg, July*.
18. Bailey, D., & Wright, E. (2003). *Practical SCADA for industry*. Elsevier.
19. Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials*, *22*(3), 1942-1976.
20. Salvador, L. C. R., Dai, N. H. P., & Zoltán, R. (2023, January). SCADA Systems: Security Concerns and Countermeasures. In *2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI)* (pp. 000251-000254). IEEE.
21. Assiya, B., Ardak, A., Madina, M., Gulshat, A., & Ramzat, A. (2022, September). Intelligent Microclimate Control System Using PLC and SCADA. In *2022 7th International Conference on Computer Science and Engineering (UBMK)* (pp. 188-191). IEEE.
22. Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1-8.
23. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *computers & security*, *89*, 101677.
24. Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, *87*, 101561.
25. Etalle, S. (2019, November). Network monitoring of industrial control systems: The lessons of securitymatters. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy* (pp. 1-1).
26. Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access*, *7*, 135812-135831.
27. Pan, X., Wang, Z., & Sun, Y. (2020). Review of PLC security issues in industrial control system. *Journal of Cybersecurity*, *2*(2), 69.
28. Yaacoub, J. P. A., Fernandez, J. H., Noura, H. N., & Chehab, A. (2021). Security of power line communication systems: issues, limitations and existing solutions. *Computer Science Review*, *39*, 100331.
29. Dairi, A., Harrou, F., Bouyeddou, B., Senouci, S. M., & Sun, Y. (2023). Semi-supervised deep learning-driven anomaly detection schemes for cyber-attack detection in smart grids. In *Power Systems Cybersecurity: Methods, Concepts, and Best Practices* (pp. 265-295). Cham: Springer International Publishing.
30. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975.

31. Alghenaim, M. F., Bakar, N. A. A., & Rahim, F. A. (2023, February). Awareness of Phishing Attacks in the Public Sector: Review Types and Technical Approaches. In *Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems: ICETIS 2022 Volume 1* (pp. 616-629). Cham: Springer International Publishing.
32. Attenberger, A. (2023, February). Modeling Approaches for Cyber Attacks on Energy Infrastructure. In *Computer Aided Systems Theory–EUROCAST 2022: 18th International Conference, Las Palmas de Gran Canaria, Spain, February 20–25, 2022, Revised Selected Papers* (pp. 199-206). Cham: Springer Nature Switzerland.
33. Ramirez, R., Chang, C. K., & Liang, S. H. (2023). PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. *Electronics*, *12*(5), 1195.
34. Zhu, Q., Zhang, G., Luo, X., & Gan, C. (2023). An industrial virus propagation model based on SCADA system. *Information Sciences*, *630*, 546-566.