**Malware Threat to an Energy Sector**



**Muhammad Abdullah**

#### Roll no: 10548559 MSC Cyber Security

Subject: Applied Research Project

Department of Computer Science Dublin Business Schoool

Ireland

## Certificate of Approval

This is to certify that research work presented in this thesis titled "Malware Thread on anEnergy System" was conducted by Dublin Business School under the supervision of Obinna Izima and cco-supervisor null.

No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to **Andy Fitzgerald** (Department of Computer science) in partial fulfilment of the requirements for the degree of Master of Science (MS) in the field of Computer Science.

A picture containing logo  Description automatically generated

Student Name: Muhammad Abdullah Signature: —————

###### Examination Committee:

|  |  |  |
| --- | --- | --- |
| **Examiners** | **Name, Designation & Address** | **Signature** |
| External Examiner 1 |  |  |
| External Examiner 2 |  |  |
| Supervisor |  |  |
| Co-Supervisor |  |  |
| Department Head |  |  |
| Director Post-Graduate Studies |  |  |

## Thesis Submission Approval

This is to certify that the work contained in this thesis entitled “**Malware Thread on an energy System**”, was carried out by **Muhammad Abdullah**, and in my opinion, it is fully adequate, in scope and quality, for the degree of **MS**. Furthermore, it is hereby approved for submission for review and thesis defense.

Supervisor: ———————————

###### Name: [----name of supervisor---]

Place: DBS, Dublin, Ireland

Co Supervisor: ———————————

###### Name: [------name of co supervisor---]

Place: DBS, Dublin, Ireland

Head, Department of Computer Science: —————————–

###### Name: [---HOD of Computer Science ]

Place: DBS, Dublin, Ireland

**Malware Threat to an Energy Sector**



**Muhammad Abdullah**

Submitted in partial fulfillment of the requirement for the degree of Master of Science (MS). 2022

Department of Computer Science Dublin Business School

Dublin, Ireland

**Dedications**

All glory and honour belongs to Allah Almighty, "Who is Most Generous and Most Merciful." The people who have been my continual sources of inspiration are my parents and all of my friends. Without them, this would not have been possible. They have given me the motivation and self- control to approach any activity with a curb to let go of my zeal and resolve. This study would not have been feasible without the support, direction, help, and suggestions of my research supervisor and co supervisor . I also want to express my gratitude to my other instructors who helped me greatly by contributing their time and expertise. I also want to thank the head of the computer science department for giving us the assistance we needed to complete this task.

**Author Declaration**

I Muhammad Abdullah hereby declare that my MS Thesis titled "**Malware Thread on an Energy System**" is my own work and has not been submitted previously by me or anybody else for taking any degree from **Dublin Business School, Dublin, Ireland** or any other university / institute in the country / world. At any time if my statement is found to be incorrect (even after my graduation), the university has the right to withdraw my MS degree.

———————————————

###### (Muhammad Abdullah)

DBS, Ierland

## Plagiarism Undertaking

I, *Muhammad* Abdullah, I humbly affirm that the research I've done for the postulation "Malware Thread on an Energy System" is entirely original and that no other person had a significant role in it. Although I came up with the entire premise, very little has been committed to or offered anywhere, or even hinted at.

I understand the HEC's and Dublin Business School's (DBS) zero-resilience approach to counterfeiting. Since I am the author of the above-mentioned postulation, I hereby declare that no part of it has been copied, and all sources cited are duly acknowledged.

———————————————

###### (Muhammd Abdullah)

DBS, Ireland

**Malware Threat to an Energy Sector**

Contents

[Malware Threat to Energy Sector 1](#_bookmark0)

[Certificate of Approval 2](#_bookmark1)

[Thesis Submission Approval 3](#_bookmark2)

[Malware Threat to Energy Sector 4](#_bookmark3)

[Dedications 5](#_bookmark4)

[Author Declaration 6](#_bookmark5)

[Plagiarism Undertaking 7](#_bookmark6)

[Malware Threat to Energy Sector 8](#_bookmark7)

[Copyrights Statement 12](#_bookmark8)

[Abstract 13](#_bookmark9)

[List of Abbreviations 14](#_bookmark10)

1. [Introduction 15](#_bookmark11)
   1. [Problem Statement 15](#_bookmark12)
   2. [Business Problem 15](#_bookmark13)
   3. [Research Problem 15](#_bookmark14)
   4. [Characteristics that make the sector especially vulnerable 16](#_bookmark15)
   5. [Research Question 16](#_bookmark16)
   6. [Aim 16](#_bookmark17)
   7. [Objective 16](#_bookmark18)
   8. [Hypothesis 16](#_bookmark19)
   9. [Conclusion 16](#_bookmark20)
   10. [Scope 16](#_bookmark21)
   11. [Limitations 16](#_bookmark22)
   12. [Dissertation Roadmap 17](#_bookmark23)
   13. [What is malware? 17](#_bookmark24)
       1. [History and detail of Malware 17](#_bookmark25)
   14. [Types of malware 18](#_bookmark26)
       1. [Virus 18](#_bookmark27)
       2. [Worm 18](#_bookmark28)
       3. [Trojan horse 18](#_bookmark29)
       4. [Rootkit 19](#_bookmark30)
       5. [Spyware 19](#_bookmark31)
       6. [Adware 19](#_bookmark32)
       7. [Bot 19](#_bookmark33)
   15. [Malware attack vector 19](#_bookmark34)
       1. [Using weaknesses 19](#_bookmark35)
       2. [Roadside downloads 20](#_bookmark36)
       3. [Social engineering 20](#_bookmark37)
2. [Literature Review 21](#_bookmark38)
   1. [Cyberattacks on the Greek, Kazakh, Taiwanese Energy Sector 21](#_bookmark39)
   2. [Cyberattacks on Saudi Arab Energy Sector 21](#_bookmark40)
   3. [Phishing emails with malicious PDFs attached 22](#_bookmark41)
   4. [Iranian cyber activities in critical infrastructure 22](#_bookmark42)
   5. [Cyber-attack types can be categorized 23](#_bookmark43)
      1. [Non-targeted attacks 23](#_bookmark44)
      2. [Targeted attacks 23](#_bookmark45)
   6. [Motivation for research question 23](#_bookmark46)
3. [Materials & Methods 24](#_bookmark47)
   1. [Research Methodology 24](#_bookmark48)
   2. [Research Objective 26](#_bookmark51)

[3.2 Sub Question 26](#_bookmark52)

[Q1) 26](#_bookmark53)

[Q2) 26](#_bookmark54)

[Q3) 26](#_bookmark55)

[Q4) 26](#_bookmark56)

[Q5) 26](#_bookmark57)

[Q6) 26](#_bookmark58)

[Q7) 27](#_bookmark59)

* 1. [Search Scheme 28](#_bookmark60)
  2. [Selection Process 28](#_bookmark61)
  3. [Quality Assessment 30](#_bookmark62)
     1. [Understand the Topic 30](#_bookmark63)
     2. [Outline 30](#_bookmark64)
  4. [Why Wazuh 30](#_bookmark65)
     1. [Endpoint Security 30](#_bookmark66)
     2. [Threat Intelligence 31](#_bookmark67)
     3. [Security Operations 31](#_bookmark68)
     4. [Cloud Security 31](#_bookmark69)

1. [Implementation 32](#_bookmark70)
   1. [Scenario 32](#_bookmark71)
   2. [Scenario # 1 32](#_bookmark72)
   3. [Scenario # 2 45](#_bookmark79)
2. [Results 51](#_bookmark87)
   1. [Configuration Assessment 51](#_bookmark88)
   2. [Containers Security 51](#_bookmark90)
   3. [Anomalies-detection 53](#_bookmark92)
   4. [File-Integrity-Monitoring 53](#_bookmark94)
   5. [Intrusion-detection 54](#_bookmark95)
   6. [Log-data-Analysis 55](#_bookmark98)
   7. [regulatory-compliance 56](#_bookmark100)
   8. [Security-Events 57](#_bookmark102)
   9. [Vulnerabilities Assetment 58](#_bookmark104)
3. [References 60](#_bookmark105)
   1. [Wazuh Refrence 62](#_bookmark106)

[Figure 1 24](#_bookmark49)

[Figure 2 25](#_bookmark50)

Figure 3 27

[Figure 4 33](#_bookmark73)

[Figure 5 33](#_bookmark74)

[Figure 6 34](#_bookmark75)

[Figure 7 35](#_bookmark76)

Figure 8 36

Figure 9 37

Figure 10 37

Figure 11 38

Figure 12 39

Figure 13 39

Figure 14 40

Figure 15 41

Figure 16 41

Figure 17 42

Figure 18 43

Figure 19 43

[Figure 20 44](#_bookmark77)

[Figure 21 44](#_bookmark78)

Figure 22 45

Figure 23 ...................................................................................... **Error! Bookmark not defined.**47 [Figure 24 46](#_bookmark80)

[Figure 25 47](#_bookmark81)

[Figure 26 47](#_bookmark82)

[Figure 27 48](#_bookmark83)

[Figure 28 48](#_bookmark84)

[Figure 29 49](#_bookmark85)

[Figure 30 49](#_bookmark86)

Figure 31 50

[Figure 32 51](#_bookmark89)

[Figure 33 52](#_bookmark91)

[Figure 34 53](#_bookmark93)

[Figure 35 54](#_bookmark96)

[Figure 36 55](#_bookmark97)

[Figure 37 56](#_bookmark99)

[Figure 38 57](#_bookmark101)

[Figure 39 58](#_bookmark103)

Figure 40 59

**Copyrights Statement**

No part of *Muhammad Abdullah's* thesis, "Malware Thread on an Energy System," may be used without the express consent of Dublin Business School. The complete thesis is the intellectual property of DBS Institute of Business School.

—

###### (Muhammd Abdullah)

DBS, Ireland

**Abstract**

The advent of the digital age has brought rapid changes in key organizational management areas such as business network integration and supply chain management. Indeed, a core concern for most business executives today remains securing critical data. Among the sectors of the global economy that faces unprecedented cybersecurity challenges is energy. That is because energy delivery systems comprise both IT infrastructures and physical systems. Thus, tackling cybercrimes and threats in this industry remains an issue of grave concern, given the importance of energy to national and regional security interests. Although the threats in the energy sector cannot be eliminated, they can be mitigated. So, this paper aims to highlight various malware attacks witnessed in the global energy sector and their economic consequences. This also includes an undetectable virus designed by us that gives a complete backdoor to the system.

**List of Abbreviations**

**IDS** Intrusion detection system **IPS** Intrusion prevention system **NDR** Network Detection Response **EC** exclusion criteria

**SE** social engineering

**CR** Crime Group

**SCADA** Supervisory Control and Data Acquisition **ICT** Information and Communication Technology **IC** inclusion criteria

**IoE** Internet of Everything

**PCI DSS** Payment Card Industry Data Security Standard

**IOT** Internet of Things **IoV** Internet of Vehicle **IPF** Interplanetary File

**ISSC** Information Sharing Smart Contract

**PKI** Public Key Infrastructure

**SIEM** security information and event management **SEIMS** security information and event management system **NSIR** Nuclear security and incident response

# Introduction

## Problem Statement

As already mentioned, the energy sector has proven incredibly vulnerable to cybersecurity threats in recent years. At the same time, most of these energy organizations have decentralized cybersecurity leadership structures, making it challenging to coordinate effective security strategies.

## Business Problem

We depend on energy every day to get to work, run our businesses, keep our offices warm and cool, and power the internet. Without it, we wouldn't be able to support ourselves. The United States' energy sector, which includes nuclear energy, oil and gas exploration, research into and distribution of renewable energy sources, and more, is essential to the country's economic prosperity. Revenues from the sector reached $238 billion in 2018, an increase of $25 billion from 2017. Lobbyists have already spent $85.3 million in 2019 because to the industry's financial ties to the legislative system and lucrative nature, which makes it highly divisive and a target for both terrorists and criminals.

The energy sector is very vulnerable to attack due to its highly automated and inadequately secured processes, networks, and organizations. Targeted assaults against the energy sector are conducted by a variety of threat actors, each of whom has a different agenda. One of the top 16 essential infrastructures in the US is at great risk when these two factors are combined with insufficient investments in digital risk management.

## Research Problem

A summary of the issues in the energy industry that need to be resolved served as the analysis's starting point. High-level goals that are anticipated to be shared aims by all energy sector stakeholders have been agreed upon to identify the difficulties facing the industry.

These high-level goals have been compared to the energy infrastructure and market of today, and problems have been determined as a result. The difficulties listed are operational in nature i.e., they are difficulties encountered in day-to-day operations. However, this does not indicate that government backing is always necessary to address these difficulties; some difficulties may be resolved by other methods.

## Characteristics that make the sector especially vulnerable

* First, there are more threats and actors aimed at disrupting utilities, including nation-state actors looking to disrupt economic stability and security, cybercriminals who recognize the economic value of this industry, and hackers looking to publicly voice their opposition to utility projects or broad agendas.
* Due to their geographical spread and organizational complexity, particularly the decentralized nature of many firms' cyber security leadership, utilities have a vast and growing attack surface.

## Research Question

* + Vulnerabilities in energy sector and threats
  + Spread of undetectable virus attack spreads to energy

## Aim

To make an undetectable virus that hackers employ to access sensitive data on a device, rendering the files and systems that utilize the data inaccessible to the user or organization until they pay a ransom to unlock it. If the ransom is not paid, these hostile actors threaten to sell or disclose the data. Any firm can experience an undetectable virus attack.

## Objective

To conduct research on the energy sector regarding the malware attacks and threats as well as making an undetectable virus.

* 1. **Hypothesis**

In the energy industry, the attackers have sent their malicious emails to businesses across the energy, oil and gas, IT, manufacturing, and media industries than it is a malware attack. Energy industry suppliers have also been singled out, which would mean that these attacks are only the beginning of a wider campaign.

## Conclusion

I would like to finish up saying that I have clearly explained questions, research destinations, speculation to be tried and the purpose behind choosing the relevant topic.

## Scope

The goal of the study is to support this strategic body by offering recommendations for helping the Energy sector against malware threats and attacks, cybersecurity and critical infrastructure protection capabilities.

## Limitations

Simply put, the goal of this research is to develop methods for defending networks, programs, and energy industry systems against cyberattacks. These cyber-attacks wreak havoc on the energy sector by disrupting regular business operations, extorting money from users, and accessing, altering, or destroying sensitive information.

## Dissertation Roadmap

Roadmap is necessary to plan strategically to achieve a goal and desired outcome.

The aim of this investigation is to improve the current state of malware grouping craftsmanship using the dated framework for the Security of malware social features. It also aims to assess the viability and effectiveness of such a feature combination. In order to accomplish the objective of this investigation, or at the very least to propose and approve a novel technique for malware grouping and to focus on it from various angles to assess its viability for practical use, this paper describes a number of experiments that were conducted. This section lays the groundwork for the study that is later presented by giving a thorough introduction to the subject of malware investigation, recognition, and characterization, followed by a brief description of writing.

The section closes with the approach embraced for leading this examination. In this proposal I proposed my malware thread security policy after reading the Framework Policy of the [NIST](http://dx.doi.org/10.6028/NIST.SP.800-83r1)[[1]](#_bookmark105) and [Energy.gov](https://www.energy.gov/sites/default/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf)[[2]](#_bookmark105) Framework Policy for the “ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE”

I also build my own lab for the making demonstration how to save energy system.

This section lays the foundation for the research that comes next by offering a thorough introduction to the field of malware investigation, location, and order. A brief summary of writing and malware threads on the energy sectors follows this. A problem statement is established in light of the perceptions brought about by the writing, and the motivation behind the examination is then described. The commitments to logical information made by the introduced examination are immediately highlighted. The system that served as the direction for this investigation is praised at the end of this section.

## What is malware?

Malware, which can cause significant harm and disruption and requires significant recovery efforts inside most organizations, is the most well-known external danger to the majority of people. This package provides advice on how to make a group's malware episode response strategies better. Furthermore, it provides broad suggestions for enhancing a business's ability to react to incidents so that it is better prepared to address malware attacks, especially those with a significant impact.[[3]](#_bookmark105)

### History and detail of Malware

As was already mentioned, the purpose of malware's author is what sets it apart from other applications. Malware is designed to carry out operations on a PC framework against the client's will and without their knowledge. Infection, worm, spyware, and other names for computer programming are all grouped under the umbrella term "malware."

is distinguished by disease and is the subject of in-depth discussion immediately. Through several channels, referred to as the assault vectors and discussed in more detail later, the harmful programming infiltrates an objective structure.[[4]](#_bookmark105)

The initial malware may have been created as a single act of mischief3 or to establish a competitive advantage (Egele et al., 2012), but the criminal imagination quickly anticipated its benefits. The use of PCs rapidly expanded to meet a variety of requirements, malware researchers looked at ways to gain unauthorized access to and control over computer systems in order to accomplish harmful ends. Gains from these activities may include financial (getting money through fictitious bank exchanges), commercial (gaining access to competitors' commercial information to learn about their strategies), or strategic (destroying a nation's atomic arrangement by issuing disastrous orders to the control framework; Langner, 2011), to name a few. According to the Symantec 2016 Web Security Danger Report4, $575 billion is lost annually due to malware, according to BofA Merrill Lynch Worldwide Exploration. Similar research estimates that there were over 430 million new malware variants created in 2015, a 36 percent increase from 2014. This results in a daily average of more than 1,000,000 malware tests. Malware has undoubtedly become a very challenging subject. [[5]](#_bookmark105)

This has led to an ongoing conflict between malware developers, who are constantly attempting to target PC organizations and frameworks for their malicious purposes, and the PC security community, which is working to offer PC framework users a complete security solution through research and development.. [[6]](#_bookmark105)

## Types of malware

### Virus

A thing that mimics the aspect of its natural counterpart that spreads in order to grow is called an infection. A copy of the infection is linked by the underlying sickness to an executable software known as the host application. Every time the host program is executed, the infection is also launched .

The infection spreads as soon as it is launched by making duplicates of itself and joining with another application. The infection may perform additional functions in addition to reproduction, such as deleting data from the infected structure. The contamination spreads to further PCs via shared media, including network connections, USB drives, and other items.[[7]](#_bookmark105)

### Worm

The worm spreads like a virus by making copies of itself, but it does not need a host program to function. It operates on its own, replicates not only on the infected machine but also spreads to other computers via the network.[[8]](#_bookmark105)

### Trojan horse

Malware that downloads into a computer and poses as a trustworthy program is known as a Trojan Horse Virus. The distribution technique frequently involves an attacker using social engineering to conceal

harmful code to try to access consumers' systems using their program within legitimate software[.[9]](#_bookmark105)

### Rootkit

A rootkit is a group of computer program, usually malicious, that are created to grant unauthorized users access to a computer's software or other areas that are not normally accessible. They frequently conceal their own existence as well as the existence of other programs.[[10]](#_bookmark105)

### Spyware

Spyware, as the name implies, spies on the system that has been attacked by obtaining private and sensitive information from the system and passing it over the network to the spyware controller. The type of information gathered from the system depends on the spyware's goals; for example, it may look for username-password combinations to access online bank accounts, collect web browsing data for commercial purposes, or retrieve private information like emails or private data for any nefarious purposes[.[11]](#_bookmark105)

### Adware

This type of malware exposes users to unwanted and unsolicited advertisements. The advertising open in a pop-up window or a new browser tab, both of which may be challenging to close. While these malwares annoy and upset people, they also have a marketing and promotion function. [.[12]](#_bookmark105)

### Bot

Software that functions similarly to spyware by connecting to a distant master via the network is known as a bot, sometimes known as an Internet bot or web bot. A bot's duties include not only spying but also operating the target system at the master's command. To carry out malicious activities on a big scale, a single master can connect to and govern a huge number of Bots dispersed around the network, known as a Botnet.

## Malware attack vector

The means through which an attacker gains access to the objective framework and inserts malware are known as assault vectors. The following diagram illustrates the three major groups of attack vectors that Egele et al. (2012) found.

### Using weaknesses

Weaknesses are design faults or coding mistakes that make it possible for attackers to attack the framework. Programmers are equally as likely as programming merchants to look for weaknesses in their products are (both framework programming and applications). In the unlikely occasion that the first party finds a fault, a fix is offered. On the other side, if some programmers find the flaw before the others, they use it as a springboard for their malware to infect the systems running the shoddy code (susceptible software/programs) and spread it to additional systems.[[13]](#_bookmark105)

### Roadside downloads

Spam messages may persuade a victim to visit a few explicit websites that contain a feature that allows malicious code to be executed or downloaded onto the client's computer system using a browser escape clause. The client doesn't aware that code is being downloaded or, alternatively, executed, thus the attacker can contaminate the framework with their malware. [[14]](#_bookmark105)

### Social engineering

The most common method of gaining someone's trust in order to utilise them for bad activities is known as "social engineering." For instance, an aggressor could send a demand through email asking the victim to confirm one of their online accounts while posing as a representative of a bank. Additionally, customers might be enticed to visit specific websites that have hazardous content.[15]

# Literature Review

Various studies have been conducted to assess the reasons behind the energy sector's vulnerability to malware attacks. According to Venkatachary, Prasad, and Samikannu (2018), malware attacks against power plants and clean-energy generators, especially in the developed world, are because legacy generation systems adopted within the aforementioned clean-energy infrastructure are often not designed with cybersecurity in mind. A study by Sullivan and Kamensky (2017) takes a similar position, opining that the existing physical security weaknesses witnessed in power transmission allow malicious actors to access grid control systems. Moreover, Sullivan and Kamensky (2017) mention that the energy sector has, over the past few days, integrated most of its processes with the Internet of Things (IoT) technologies, subsequently increasing cyber-attack surfaces. In this precarious environment, Onyeji, Bazilian, and Bronk (2014) note that the threat landscape has expanded significantly in recent years and today includes new players like nation-state actors who have demonstrated their willingness to target and disrupt daily life in the pursuit of nationalist goals and other nefarious agendas. Apart from nation-state actors in the cybersecurity landscape, individuals and activist groups still possess the capacity to disrupt various functions in the energy sector, including gas operations and electric- power transmission. Another key point worth mentioning is that these threats are increasing when inconsistencies still exist in the capacity of utility companies to secure the appropriate funding and deploy the necessary personnel needed to build security systems that can stand the test of time and serve both present and future needs.

## Cyberattacks on the Greek, Kazakh, Taiwanese Energy Sector

McAfee released a white paper on cyberattacks on the Greek, Kazakh, Taiwanese, and US energy industries (McAfee, 2011). Attacks were launched with the goal of gaining access to extremely sensitive data beginning in late 2009 using methods such as social engineering, spear phishing, Windows OS flaws, and remote administration tools. They first broke into the extranet web servers using SQL injection. Through the compromised web server, they were able to access internal workstations and servers. Then, to get more access, they used a VPN connection to carry out spear phishing attacks on the PCs and password-stealing software. They also released the malware itself as well as tools for remote administration. Finally, they identified the executives' computers and stole their data and emails from those machines. According to reports, "Night Dragon," the group thought to be behind the attacks, has been active at least since 2009 and possibly much earlier. Based on the hacking tools and locations used in the attack, they have a strong suspicion that the attackers were Chinese.

## Cyberattacks on Saudi Arab Energy Sector

Symantec discovered the Shamoon, or W32.Disttrack, virus, which was targeted at the Saudi Arabian oil industry, in August 2012. (Symantec Security Response, 2012a). The consists of three parts malware: Reporter, Wiper, and Dropper. The primary component, called Dropper, is in charge of infecting the target and releasing the additional modules. The Wiper module, which is also responsible for erasing the data, overwrites the master boot record (MBR) of the infected machine. The Reporter module is in charge of reporting to the attacker. When Shamoon joins the network, it uses the network shares to spread throughout every machine in the LAN (Symantec Security Response, 2012b). In November 2016, Shamoon returned to the location. Symantec Security Response for 2016 According to FireEye, the Shamoon assaults were carried out by an Iranian group called "Cutting Sword of Justice" (FireEye, 2016b). Paganini (2012) based his assertion that Iran was responsible for the attacks on a dispute the country had with Saudi Aramco, the company that was the target of the attacks.

## Phishing emails with malicious PDFs attached

A white paper on a cyber espionage campaign against the energy sector was published by Symantec in July 2014 (Symantec Security Response, 2014). To enter the targeted firms, the attackers utilized spear phishing emails with malicious PDF attachments and watering hole assaults. After that, they released the Lights-out (later renamed Hello) exploit kit, which made use of Java and browser exploits to distribute Trojan, one of the main malware tools. Karagany Oldrea or the back entrance. The decision was reached in light of the information at hand. Backdoor. This attack's Oldrea, commonly known as Havex or the Energetic Bear RAT, was made especially for it. To map out the ICS devices, it used the OPC protocol (Nelson, 2016). Although some call the group that carried out the attack "Energetic Bear," Symantec called it "Dragonfly." The company has been active at least since 2011, but it has concentrated on the US and European energy industries since 2013. According to Symantec, the attacks are sophisticated and show a high level of technological proficiency on the part of the gang, making them look to be state-sponsored. Based on malware analysis, they also conjectured that the attackers' base of operations might be in Eastern Europe. time stamps taken from the transcripts of the 13th International Conference on Cyber Warfare and Security. The second initiative, "Dragonfly 2.0," which began operations at the end of 2015, at least had the US, Swiss, and Turkish energy industries in mind. (2017) Symantec Security Response Although it made use of a more modern Trojan, it had much of the same features as its predecessor. Trojan. Karagany. Karagany, B. According to Symantec, the virus in the second wave of attacks contained both Russian and French code, but that they might have been introduced for confusion.

## Iranian cyber activities in critical infrastructure

In 2014, the security firm Cylance investigated Iranian activities in key infrastructure systems. 2014's Cylance. Their Operation Cleaver report covered activities from 2012 till the publication of the study. Both Canada and the United States have reported attacks on energy companies. The aerospace industry and academia are among the targets. Attacks on the oil and gas industry have been reported in a number of nations, including Canada, France, Kuwait, Mexico, Qatar, Saudi Arabia, and Turkey. The main goal was to steal information from crucial infrastructure systems that might be used to launch more attacks. Reuters was successful in locating some of the targets (Finkle, 2014). Calpine Corp., Patrollers Mexicans, and state-owned oil company Saudi Aramco were some of them. Operation Cleaver is ascribed to Iranian players as a result of name conventions, infrastructure registered in Iran, and technologies designed to alert if IP addresses track back to Iran. Cylance also believes Iran was involved because of how crucial the exploited infrastructure was.

.

## Cyber-attack types can be categorized

### Non-targeted attacks

Cyberattacks that are not specifically targeted occasionally harm people who work in the energy sector as well as other sectors. Ransomware operations and non-targeted malware outbreaks are two examples of these attacks. A campaign of attacks requires resources like time and expertise, and targeted assaults are focused on a specific target. A typical moniker for this form of threat is Advanced Persistent Danger, or APT. Non-targeted attacks might include port scanning activities, ransomware outbreaks, and other malware attacks. The information made public regarding these incidents isn't always accurate. Because they don't want their brand to be associated with cyber risks, the worried firms frequently reject questions. On the other hand, it is difficult to isolate information concerning the energy industry because cyber security companies only offer white papers from larger-scale incidents. The only remaining option is to rely on media accounts, which regretfully frequently omit to discuss the technical details and frequently omit to cite their sources. Even though non-targeted attacks may not specifically target a particular company, the disruption they cause can be just as deadly as in targeted attacks. Although underreported, non-targeted threats are probably more common than targeted assaults. Sound cyber security practices, such as teaching personnel about phishing emails and segmenting networks to prevent it from spreading, are the best method to tackle this attack type.

### Targeted attacks

Targeted attacks have only ever resulted in espionage or sabotage up until now, with no infrastructure harm. As evidenced by improvements in attack tactics, attacks are evolving and achieving the refinement found in attacks against traditional IT networks. Because the attacker has the time and knowledge to go past them, conventional security measures are ineffective against these attacks. Strong and diverse defenses lengthen the time it takes to launch an attack and increase the chance that it will be detected before the enemy succeeds in achieving their goal. For instance, the security procedures suggested in the SANS study (Obregon, 2015) would have prevented the use of password theft as an attack vector if two factor authentication had been implemented on the ICS network.

The bulk of targeted attacks lack a clear ICS system target and are instead driven by espionage. The assault cycle can eventually be lessened, though, thanks to the information and knowledge obtained through espionage. The likelihood that the defenders will notice the operation in progress and put a halt to it is thus decreased. Another justification for espionage is to get a competitive edge in business. The rise of a sabotage motive in Ukraine is the condition that raises the greatest red flags. Due to the fact that the energy infrastructure was unharmed, activities could be resumed quite quickly. If it happens in the midst of another crisis, even a momentary outage might have severe consequences. If the attack destroys the intended infrastructure, as it did with the Stuxnet attack, restoration may be quite difficult (Brunner et al., 2010).

## Motivation for research question

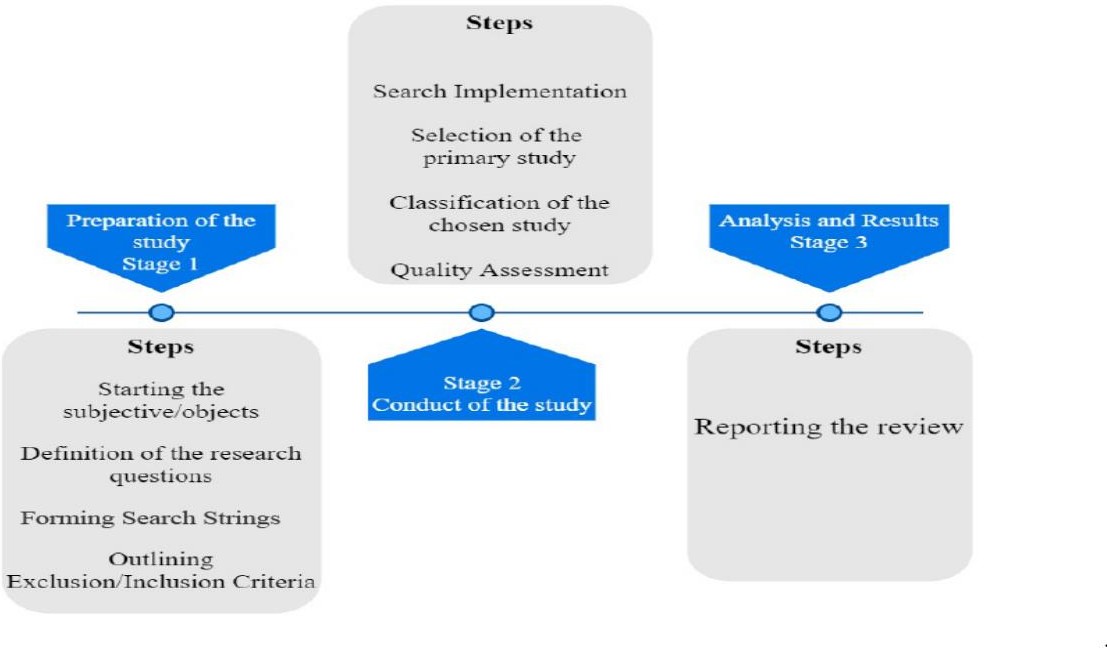
The globe is provided with daily services by the energy sector. They are the most significant aspect of our lives, and as malware threats and attacks have grown in this area, it is vital to offer security against them.

# Materials & Methods

## Research Methodology

The analysis methodology utilized for this study is called Siem. Figure 1.1 outlines the mapping stages taken before writing this article. These three distinct steps are:

1. Planning
2. Carrying out the mapping study
3. Conclusions and reviews.

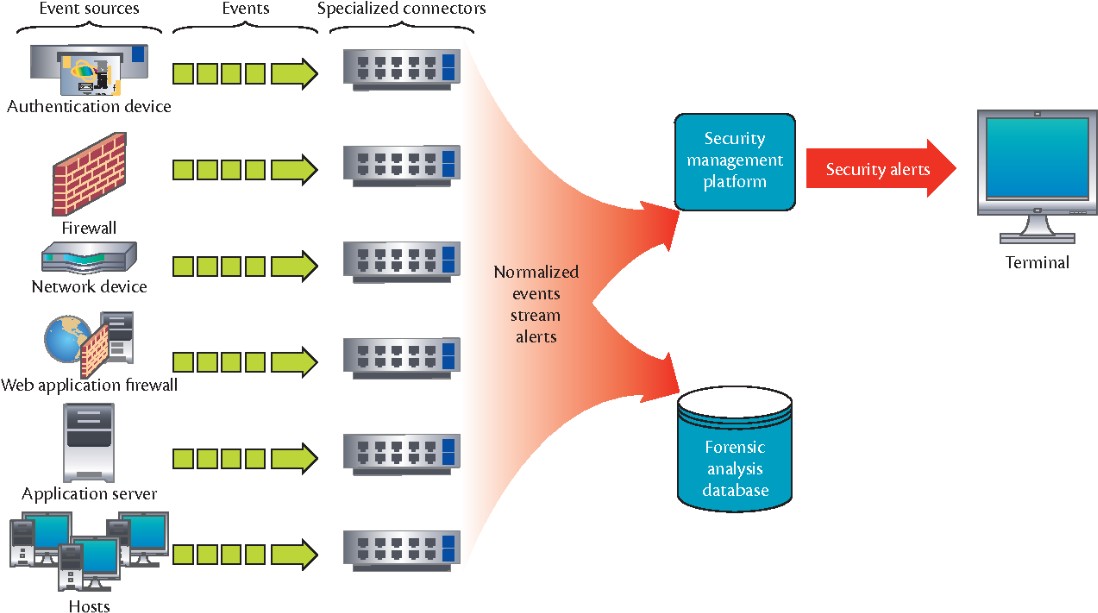


###### Figure 1 Systematic Mapping Study

Critical infrastructure protection (CIP) is a significant problem for both industrialized and

developing nations. Just a few of the infrastructure areas where nations have implemented critical systems include oil and gas, transportation, water treatment and distribution, emergency services, dams, electric power generation, and nuclear power plants[[25].](#_bookmark105) These crucial infrastructures carry out fundamental operational tasks, such as planning and making decisions, monitoring and enforcing rules, and managing information. A properly constructed infrastructure should be flexible, independent, effective, dependable, safe, and useable.

To increase the security of crucial infrastructures, several research and initiatives have been made. Many securities operation centers (SOCs) have been built as part of attempts to defend against cyberattacks. Unfortunately, there are many security events to analyses and reply to, making it impossible to guard against cyberattacks. To increase the effectiveness of incidents response, security event reduction is crucial. By analyzing IPS and FW raw data, we examined four years' worth of cyber threats against an Energy Sectors and electric power firm in this research. This investigation led us to the conclusion that 85% of all cyberattacks originated from other countries. We should simply ban unnecessary foreign IP ranges if an IT system is not connected to international commerce. Therefore, in order to enhance daily incident response actions for critical infrastructures, we recommend the Enhanced Security Control (ESC) [[28]](#_bookmark105) model with Blocking Prioritization (BP) [[29]](#_bookmark105) procedure. When choosing which IT systems should be stopped from foreign IP ranges, this ESC model includes a BP process with six elements to take into account: foreign relation, genuine login, blocking complexity, stop tolerance, outer relation, and stop impact. The Blocking Impact Degree (BID) of IT systems may be prioritized using these six parameters, and the ESC model can assist in deciding which needless foreign IP ranges to block. By lowering security incidents, this ESC approach will improve the environment for focus on the few remaining unblocked and vital IT systems.



###### Figure 2

## Research Objective

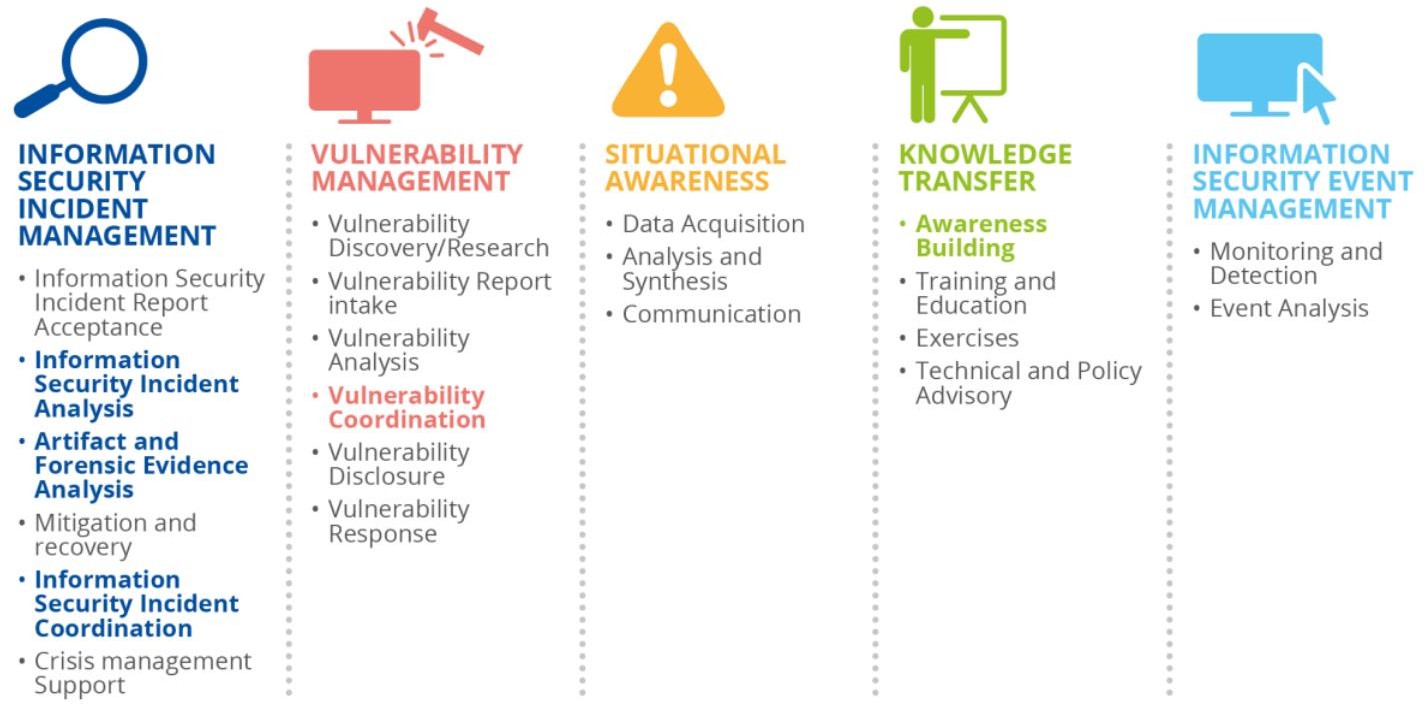
The purpose of a SIEM is to protect businesses from such public reputational harm as well as the costs, downtime, and other logistical effects of a breach. Compliance is a significant concern for many bigger firms as well as those in highly regulated sectors. The following lab that shows us how SEIM actually works and why it is necessary for every organization over the usage of Precious and Price worthy firewalls.

## 3.2 Sub Question

`

|  |  |
| --- | --- |
| **Q1)**  WHY is SIEM significant to businesses? | SIEM is essential for assisting firms in managing security since it filters massive volumes of security data and prioritizes the security warnings the software generates. Thanks to SIEM software, organizations may spot problems that could otherwise go unnoticed. |
| **Q2)**  What benefits come with utilizing a SIEM? | The main benefit of a SIEM is its capacity for precise, timely detection and identification of security incidents. For added advantages, SIEM and Security Orchestration Automation and Response (SOAR) can be coupled. |
| **Q3)**  What is the SIEM system's primary goal? | Real-time event monitoring and analysis, as well as tracking and logging of security data for compliance or auditing requirements, are provided by security information and event management (SIEM), which unites security information management (SIM) and security event management (SEM). |
| **Q4)**  A vulnerability scanner is a SIEM, right? | A vulnerability scanner deals with what's lacking from the environment and what may occur as a result of those items being absent on the most fundamental level. A SIEM focuses on what has really occurred and is occurring. |
| **Q5)**  In very Simply way, what is SIEM? | SIEM stands for security, information, and event management. SIEM technology combines log data, security alerts, and events into one platform to provide real-time analysis for security monitoring. |
| **Q6)**  Is SIEM a tool for monitoring? | SIEM works by combining two technologies. Security information management (SIM), which collects data from log files for analysis and reports on security risks and events, and security event management (SEM), which performs real-time system monitoring and notifies network managers about key concerns. |

|  |  |
| --- | --- |
|  |  |
| **Q7)**  What is a server for SIEM? | Security Information and Event Management, or SIEM, is a piece of software that gathers and analyses activity from a variety of sources throughout your whole IT infrastructure. SIEM gathers security data from network devices, servers, domain controllers, and other sources. |



###### Figure 3 ISIM

## Search Scheme

To find the nearly relevant publications for the chosen acquisition, the following scientific databases/sources were employed: IEEE Digital Library, Springer, ACM, Google Scholar, Elsevier, and MDPI, which was also used for practical research. Google Scholar has been effectively employed for the construction of solid studies.

## Selection Process

|  |  |
| --- | --- |
| **Inclusion criteria** | **Exclusion criteria** |
| IC1- Papers published in journals and conferences. | EC1- Duplicated articles. |
| IC2- Studies published between 2016 to 2020 | EC2- Articles does not address Events and SEIM computing |
| IC3- Articles presenting Configuration + events management in any Industry or Energy Sector | EC3- Books, thesis and published abstracts. |
| IC4- Studies from any geographical location. | EC4- Articles that are published pre-2018. |

Table 3: Including and Excluding Standards for the chosen study

The research studies that are most pertinent to the topic of this study are distinguished using a few specific criteria. The identical articles from various sources should not be repeated. In order to determine whether an article will be accepted or rejected, its keywords, abstract, and title are carefully examined. After the articles were initially observed, similar names were disregarded since, evidently, they were not appropriate for a review.

In the energy industry, the goal of cyber security is to maintain reliability and resilience even in the face of a cyberattacks. In contrast to IT systems, a control system in the energy sector that is under attack cannot simply be removed from the network due to potential safety implications. Either brownouts or blackouts. There are three widely recognized protective objectives in cyber security: Integrity and confidentiality& Accessibility (CIA). The most important goal in the energy sector depends on the sector particular uses. For instance, availability and integrity in generating and transmission are the most crucial. Potentially affect how reliable a system is. Data that has been altered or delayed may cause a device to be misconfigured, which may eventually affect system reliability. The security of customer personal data is of utmost importance for the advanced metering infrastructure. Cybersecurity, sometimes known as computer security, is a component of nuclear security. Computer security strives to prevent online activity that might, either directly or indirectly, result in the illegal removal of nuclear or other radioactive material, sabotage of nuclear facilities or nuclear material, or theft of nuclear sensitive data.

It is worth pointing out that the complexities characterizing the energy sector make researching the field incredibly challenging. According to Wiese, Hilpert, Kaldemeyer, and Pleßmann (2018), these challenges exist not only at the technical level but are also linked to societal dynamics. Against this backdrop, they argue that energy system analysis tools should be examined within qualitative contexts that are more suitable for tackling the abovementioned challenges. It is worth mentioning that one of the most important qualitative data collection methods is interviews.

Qualitative researchers

They have long regarded the information collected from interpretive methods such as interviews as reliable and objective. However, Wiese, Hilpert, Kaldemeyer, and Pleßmann (2018) do not shy away from asserting that conducting qualitative research interviews is not a trivial process. Indeed, collecting interview data useful for research purposes requires the researcher to possess skills such as intensive listening, note taking, and careful planning. At the same time, the researcher must have as much expertise as possible in their area of research to allow them to ask informed questions. Suffice to say that although interviews offer an opportunity for researchers to learn about others' worldviews, sometimes this goal may be elusive even in circumstances where the interviewer and interviewee appear to be speaking the same language. For that matter, an interview approach can only provide a rich set of data if well-planned and carefully executed.

As already mentioned, this study will employ interviews as the primary data-collection approach. First, the researcher will identify key stakeholders in the energy sector as those capable of providing insights on behalf of their peers. The study will categorize the stakeholders into five groups: vendors, utility companies, cybersecurity companies, research facilities, and government agencies. Vendors are the businesses that create the software used to run the cyber-physical aspects of the energy industry. On the other hand, utility companies are the stakeholders involved in generating, transmitting, and distributing energy. Moving on, cybersecurity companies will be identified as those organizations that supply cyber-resilience and response products to utility companies. Additionally, the researchers will name research institutions as the bodies creating the frameworks that enhance cyber-resilience in the energy industry. Suffice to say that government agencies represent the stakeholder group that makes policies regulating the energy sector. Pointedly, the researcher will identify potential interviewees by leveraging relationships built in the energy industry.

In total, 28 interviews will be conducted, with the anonymity and confidentiality of participants guaranteed in each case. Moreover, each interview will generally last 40-60 minutes, with the researcher focusing on the respondents' perspectives of limited topics, including the malware attacks that have produced widespread consequences in the energy sector, the current cyber- response mechanisms employed by the energy industry, and the potential solutions to existing cybersecurity gaps. A point worth highlighting is that this study will not assert in any way that the stakeholder analysis is representative of the entire energy sector. Indeed, a complete picture of the stakeholders' perspectives and value propositions can only be formed if tens of thousands of respondents are interviewed. For that matter, the employed design will only seek to identify trends in the sector indicative of the impacts of malware attacks on energy delivery systems. Against this backdrop, future studies could validate this study's conclusion by conducting additional interviews and analyzing multi-stakeholder events.

Cyber Response Framework

Different threat actors, from nation states to non-state actors, can launch cyberattacks. When their systems are attacked, operators are often preoccupied with restoring an appropriate degree of protection, keeping them working, or bringing them back to life. Support from Member States or coordinated efforts amongst Member States (federal or regional approach) may be needed in the event of large coordinated assaults. This might involve groups like NATO or the OSCE. Already, each unit's cyber reaction is covered under the NATO accords. However, due to a mismatch between NATO Nation States and EU Member States, certain EU Member States are not included in the NATO cyber defense system. The EU must take into account nations who are not members of the NATO alliance but are yet connected to the European energy system, such as Austria. The Joint Framework to tackle hybrid threats has begun to address this issue, which has already been identified. A Cyber response framework that includes a classification of attacks, definition of responsibilities and capabilities needed to respond adequately on different levels of sophistication of cyber-attacks.

1. Support from Member States or tighter coordination across Member States.
2. Seek for support from diplomacy (e.g., OSCE) and/or military (e.g., NATO). 4. All EU Member States to be included (as these do not correspond to NATO Nation States). 5. International alliances.
3. Coordination and information exchange between the attacked organization, Member States, Nation States, EU, OSCE, NATO and international alliances and coordinated response mechanisms.

Protecting against cybersecurity threats

For organizations that are planning to adopt a strategic threat intelligence program should do the following:

Identify loopholes and potential indicators of compromise based on current threat intelligence. Based on threat intelligence, create awareness among staff, employees, third-party vendors, or anyone directly or indirectly associated with the organization.

The threat intelligence program should be robust and effective, including identification, strategic threat intelligence, operational and tactical procedures.

Incident response plans should be clearly defined and aligned with the organization’s goals and objectives for dealing with various sophisticated and complex threats.

Organizations should train their critical stakeholders on product development and information sharing best practices.

For the energy sector and worry about your cybersecurity posture, we suggest you opt for VAPT (Vulnerability Assessment and Penetration Testing) services. VAPT is a strenuous task that requires a lot of critical thinking and resources.

## Quality Assessment

### Understand the Topic

Wazuh SEIM

### Outline

###### A comprehensive SIEM solution

The Wazuh Security Information and Event Management (SIEM) solution provides monitoring, detection, and alerting of security events and incidents

## Why Wazuh

### Endpoint Security

* + Configuration Assessment
  + Extended Detection and Response
  + File Integrity Monitoring

### Threat Intelligence

* + Threat Hunting
  + IT Hygiene
  + Vulnerability Detection

### Security Operations

* + Log Data Analysis
  + Malware Detection
  + Audit and Compliance

### Cloud Security

* + Posture Management
  + Workload Protection
  + Container Security

# Implementation

## Scenario

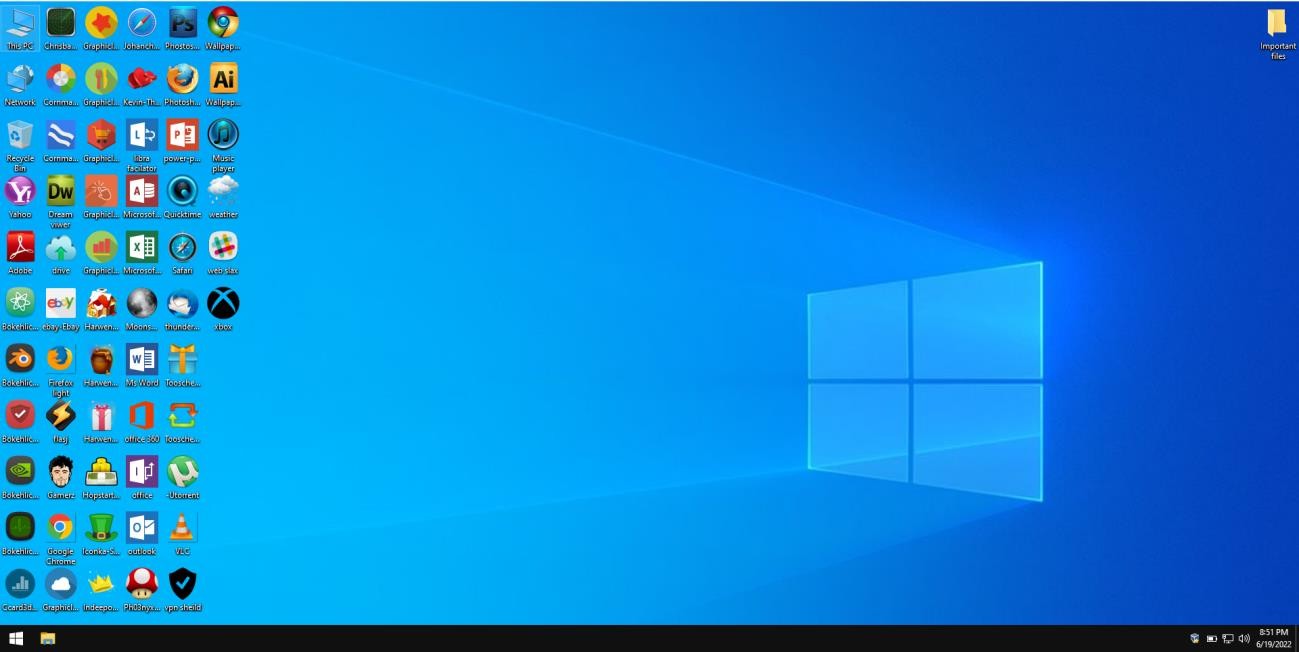
In this lab, we will learn how much SIEM configuration is important in any Energy Sector or industry. Basically, I use wazuh for it and wazuh is the best open-source event management or Integrity handler Manager.

This lab scenario has two interfaces.

The first interface defines the attack vector side without using any SIEM configuration. Second Scenario define the real-time monitoring of event to handle the Malware to harm any component of the Digital Integrated Machinery of any Industrial Machinery or Energy Sector also we have found a vulnerability in windows 10 that we have deigned an undetectable virus which is not detected by windows 10 and we can have its reverse shell over the internet.

## Scenario # 1

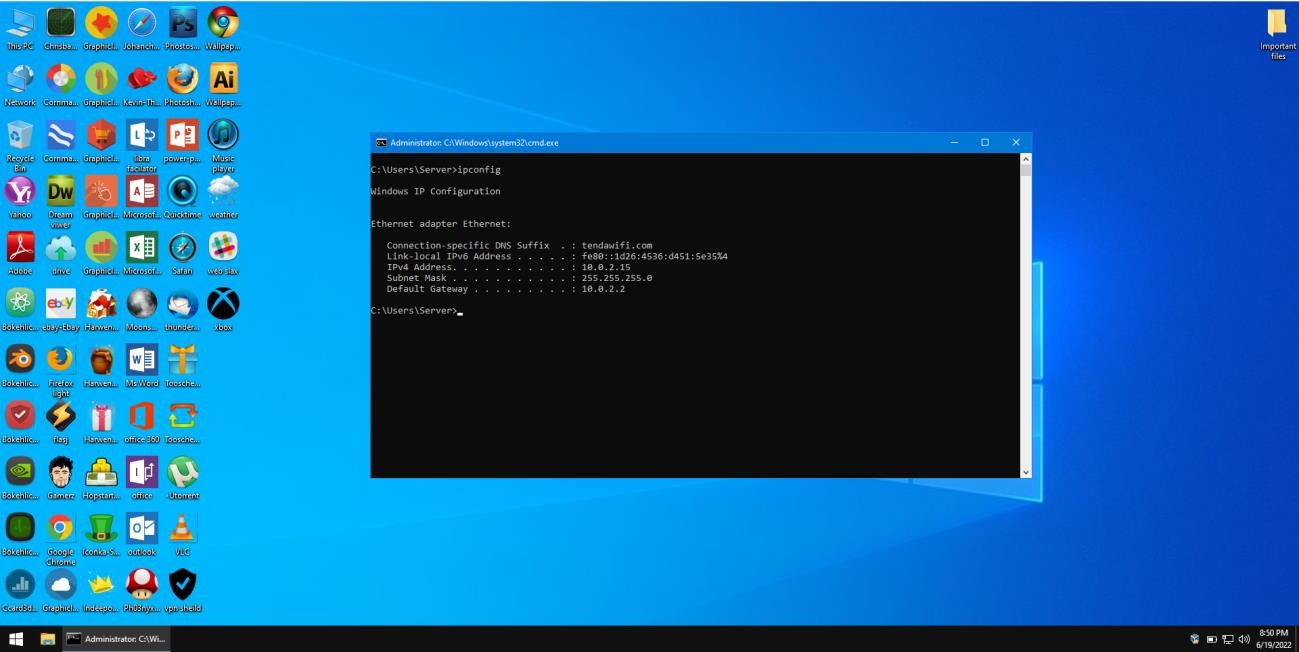
This is the snap of the Server machine that run in the energy sector unfortunately Energy sector security export does not configure any SIEM solution in their entire industry. The FUD malware attacks the Energy Sector and Exploit the Main server machine of the Energy Sector. The malware main function is that to high up the resource usage of the machine in such a way that machinery to make overloaded and make them unusable by high their level to their entire Working capacity.



Snap # 1

*Figure 4*

This shows the Server machine working in an energy sector.



Checking the network of that Server machine

*Figure 5*

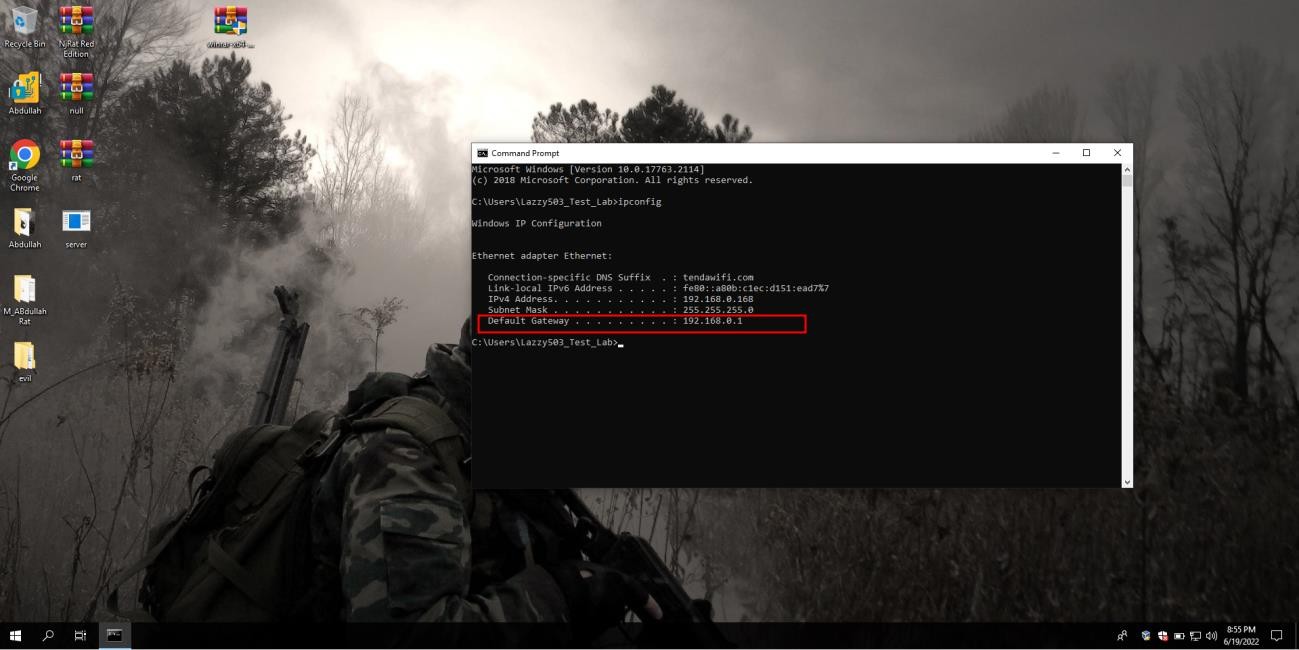
Yes, it’s a private Network of IP series -- > 10.0.2.15

###### On the other Hand, Attacker Side is:



*Figure 6*

This is an attacker Machine Interface and below to this picture demonstrate the Network Address

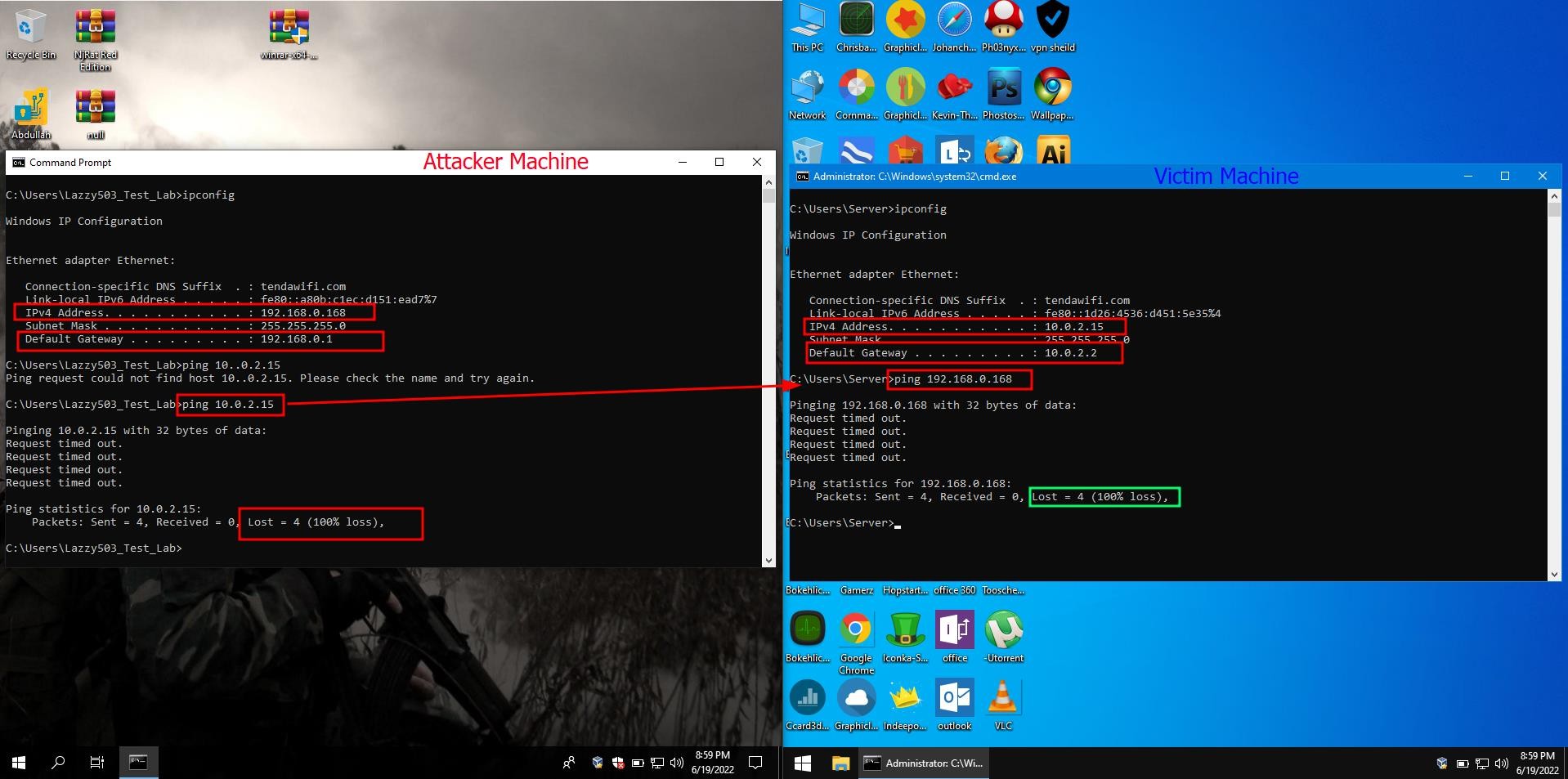


*Figure 7*

Ip address of attacker machine is 192.168.0.168 with the network of 0

Now we check that they are not in the same network and different to each other.

Now you can that on the left side ip is 192.168.0.168 and on the right side ip is 10.0.2.15 they are not in the same network that’s why are not able to do ping to each other because they have no single or bridged network.

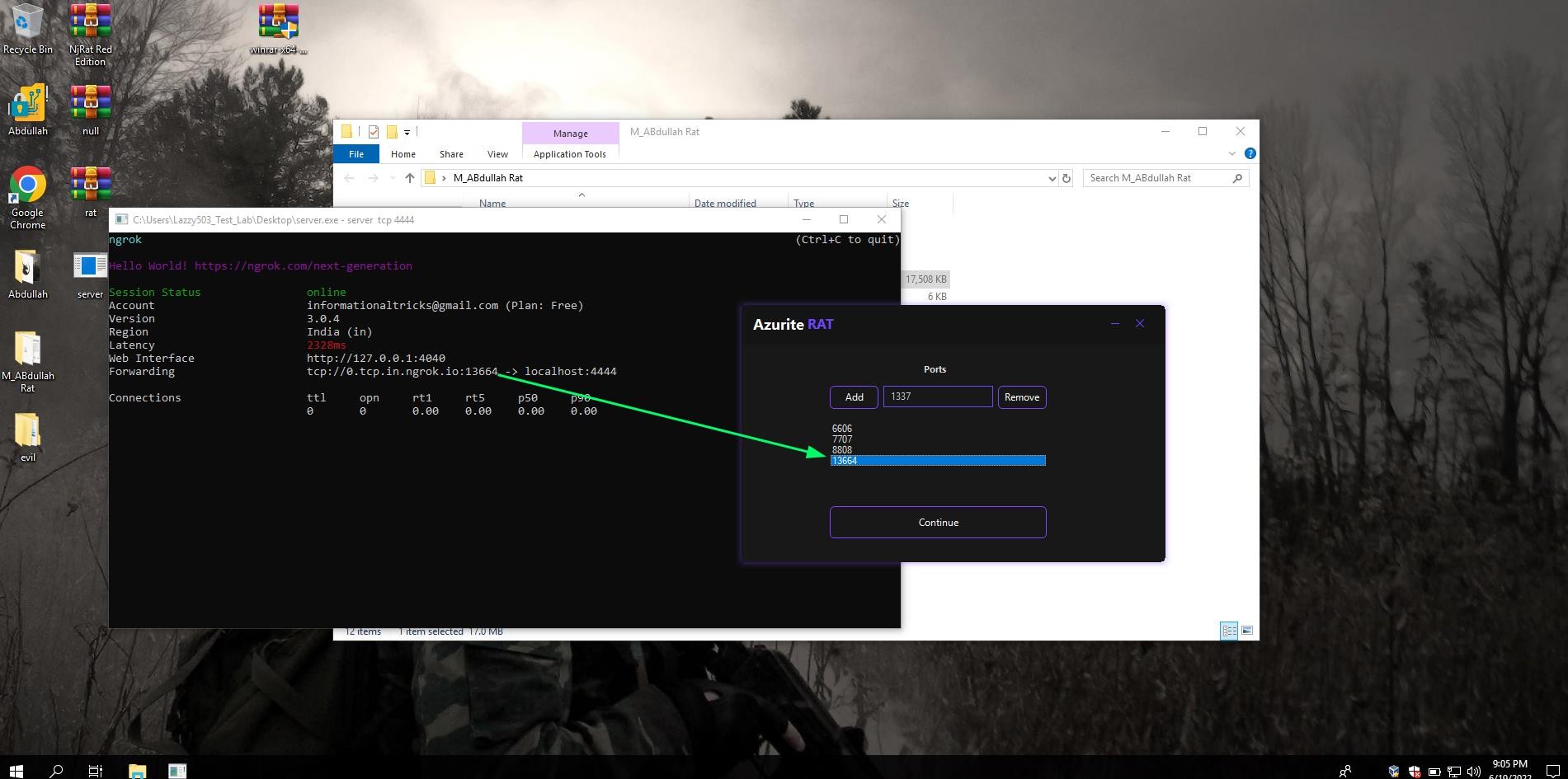


*Figure 8*

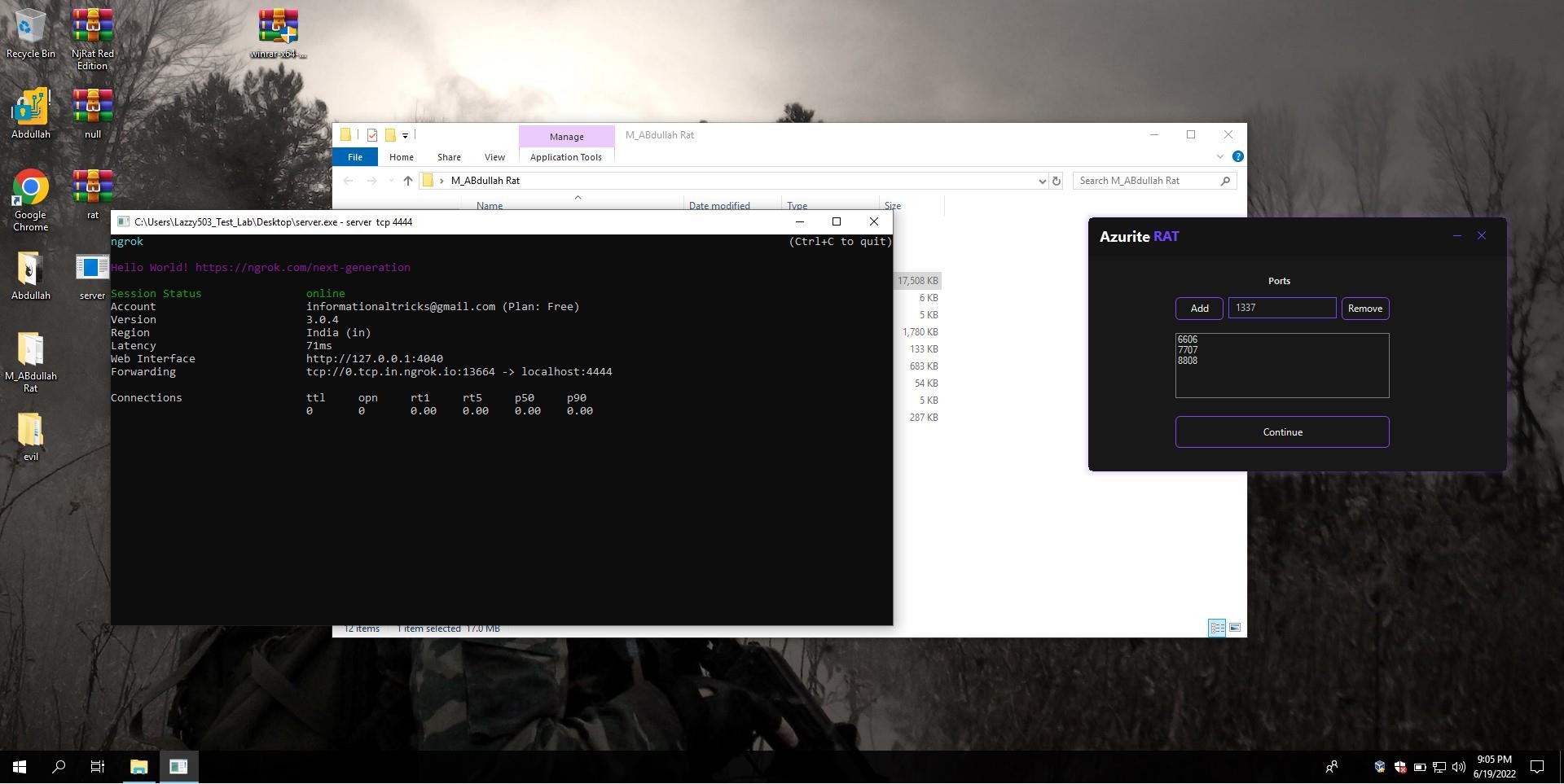
##### Now attacker use the rat to hack the server machine of the energy sector

Now attacker use the ngrok to forward the port to connect with the victim server machine, because attack is from another country and victim is from another country.

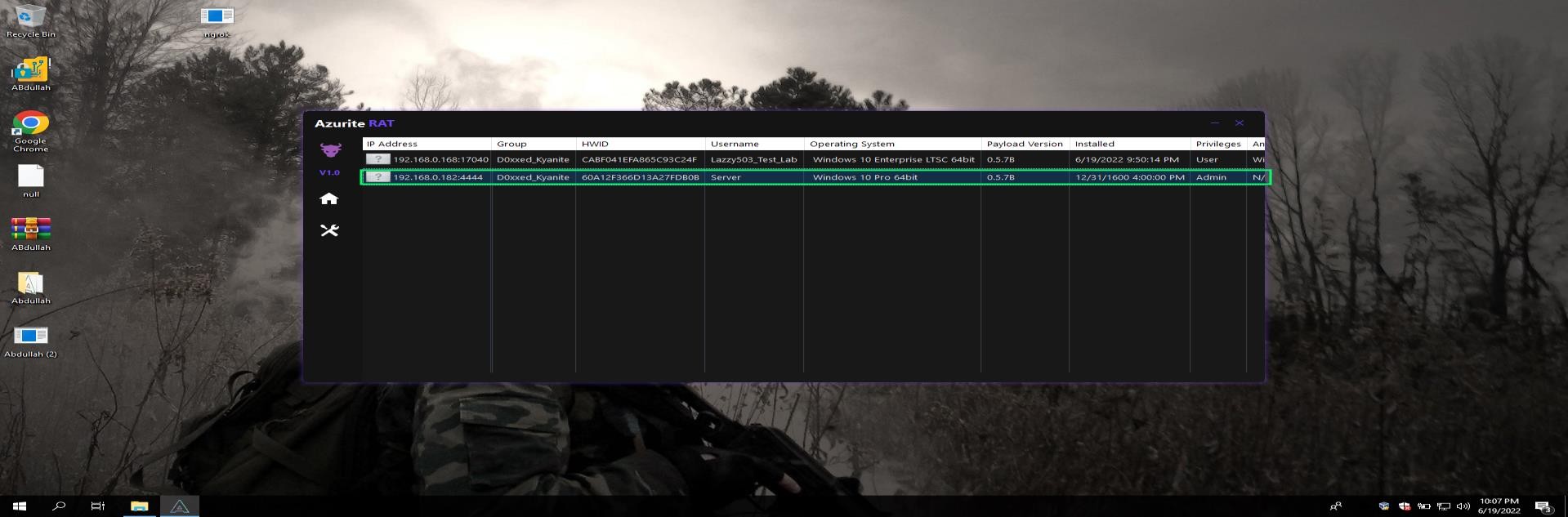
*Figure 9*

Now configuring the rat according to the server that will used to forward the port over all the Internet. Attacker add the port number of the ngrok server because he/she use it for the port forwarding now.

*Figure 10*

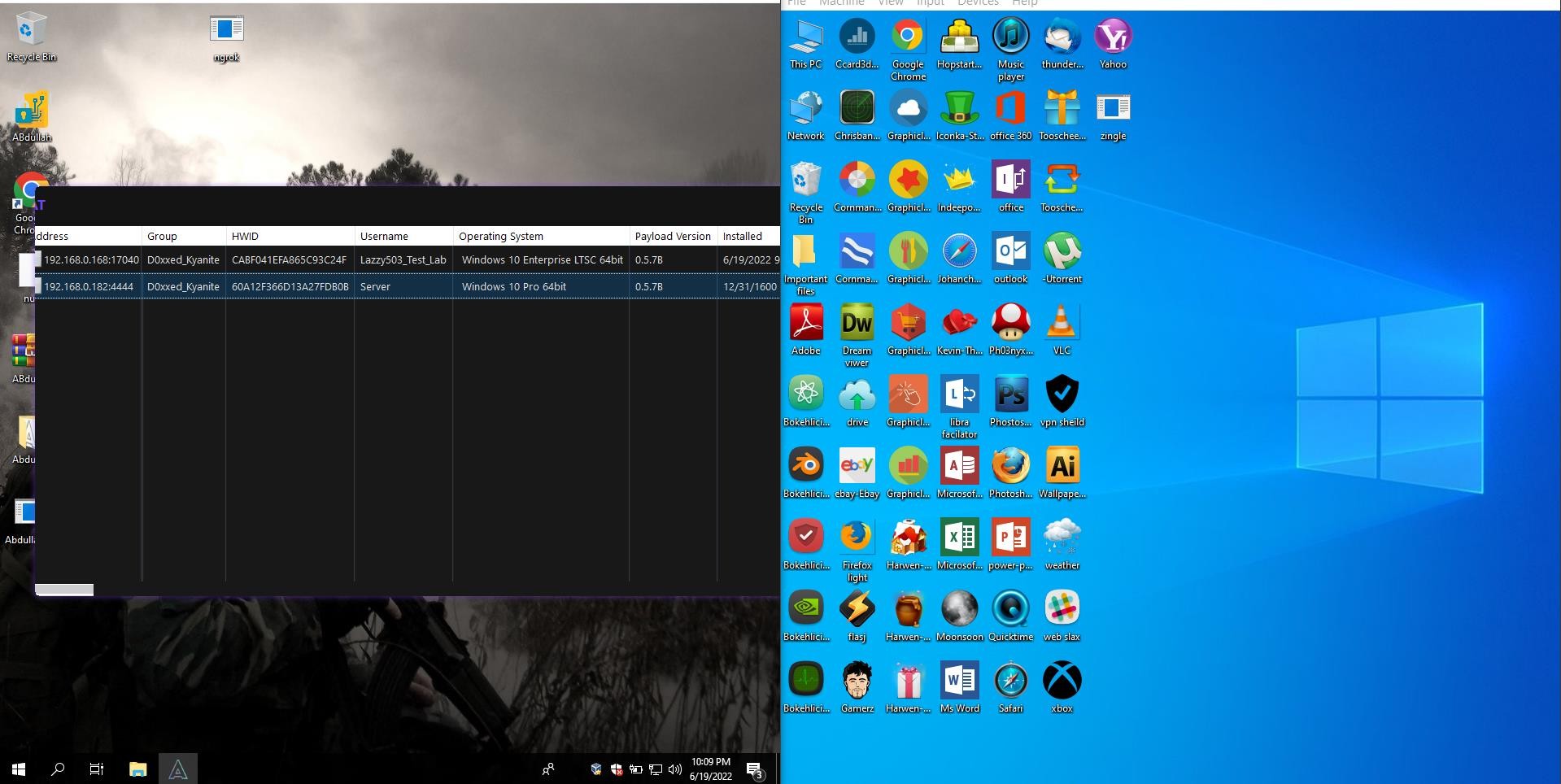


*Figure 11*



*Figure 13*

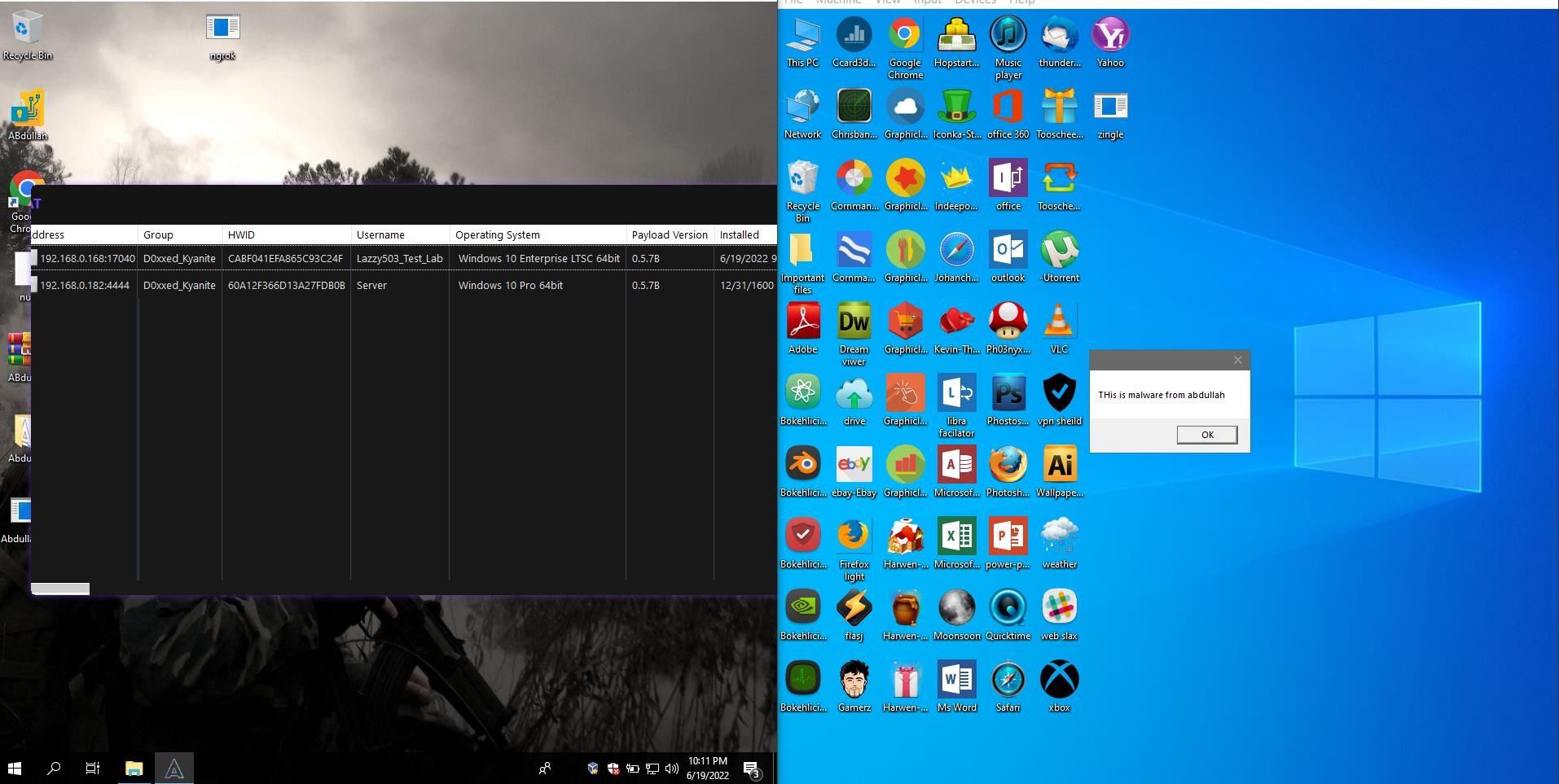
now after sending the virus to the server machine through social engineering technique of USB dropping in form of the employee of the energy sector. The greedy employee carries up the usb and pugged it its own personal computer of the Energy sector. Malware gained access to its pc first and then move to other system or machinery of connected through Network.



*Figure 12*

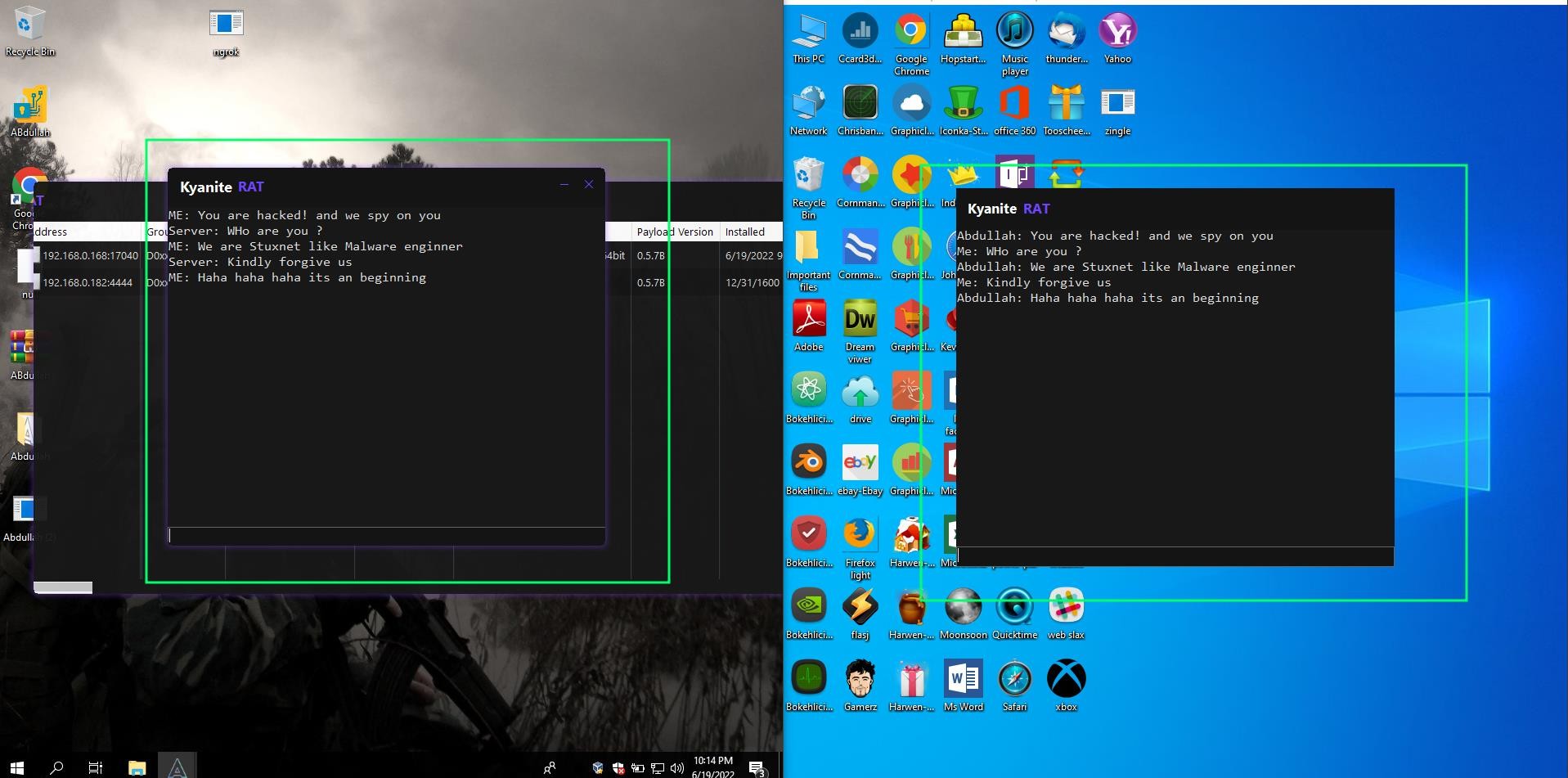
After gaining access to the network attacker would misuse the Energy sector according to its own once.

Now in this case attacker first warn the employees of the Energy sector and then give them malicious message just for their own fun.

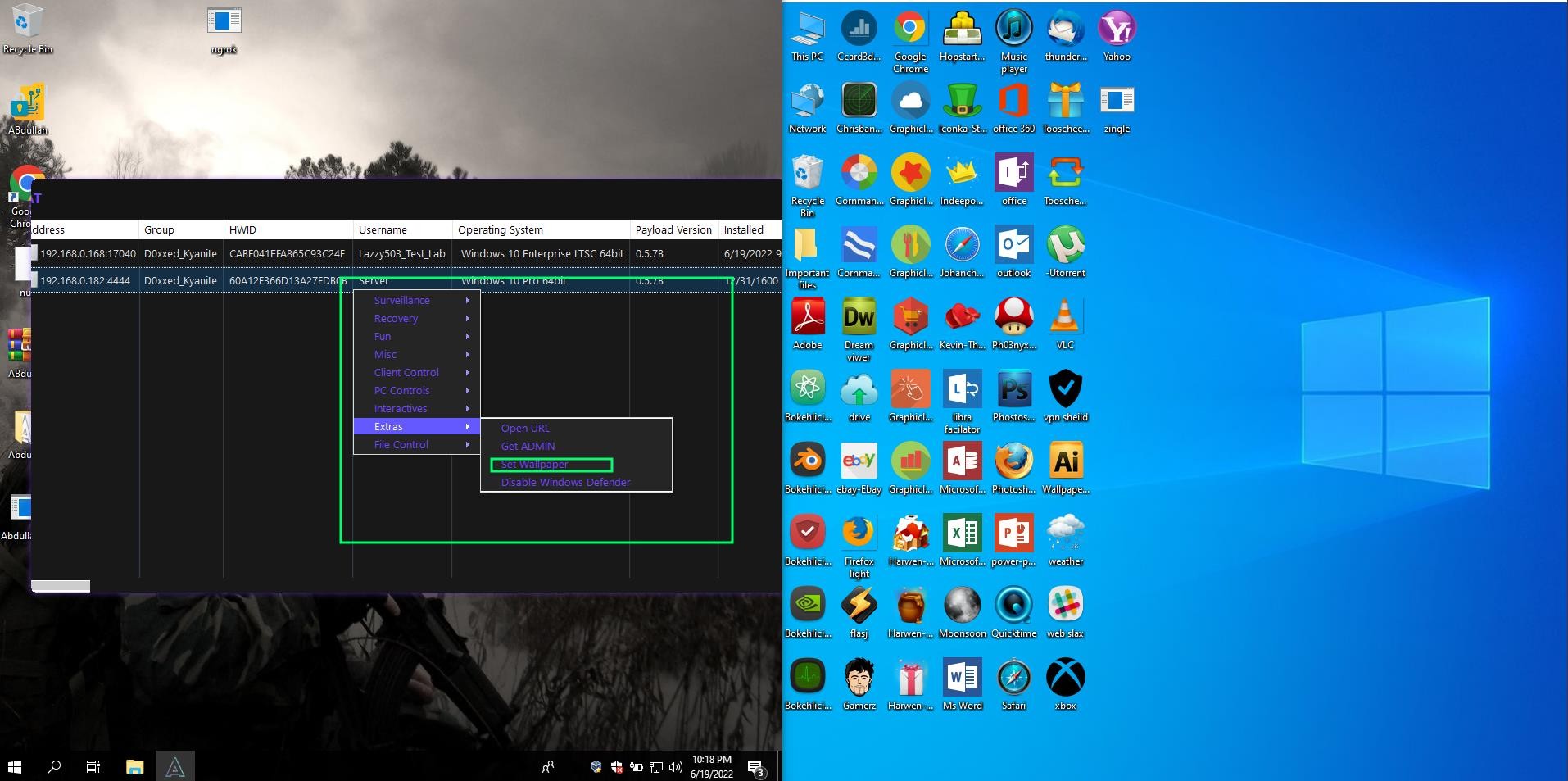


*Figure 14*

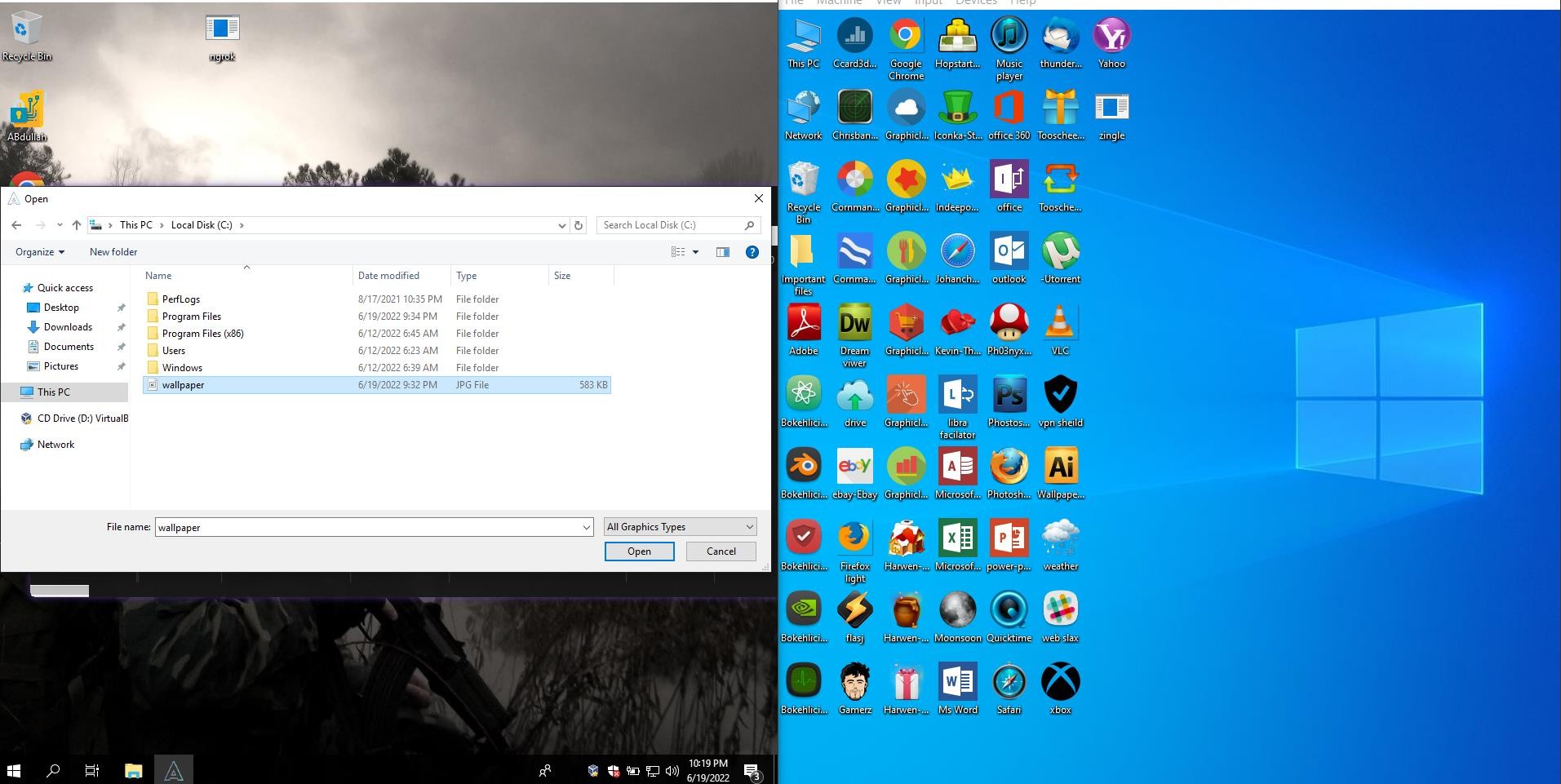
##### Now this is the message that attacker sends to the victim’s machine.



*Figure 16*



*Figure 15*



*Figure 17*

Attacker is also able to change the wallpaper of the victim.

Now you can see that wallpaper has been changed.

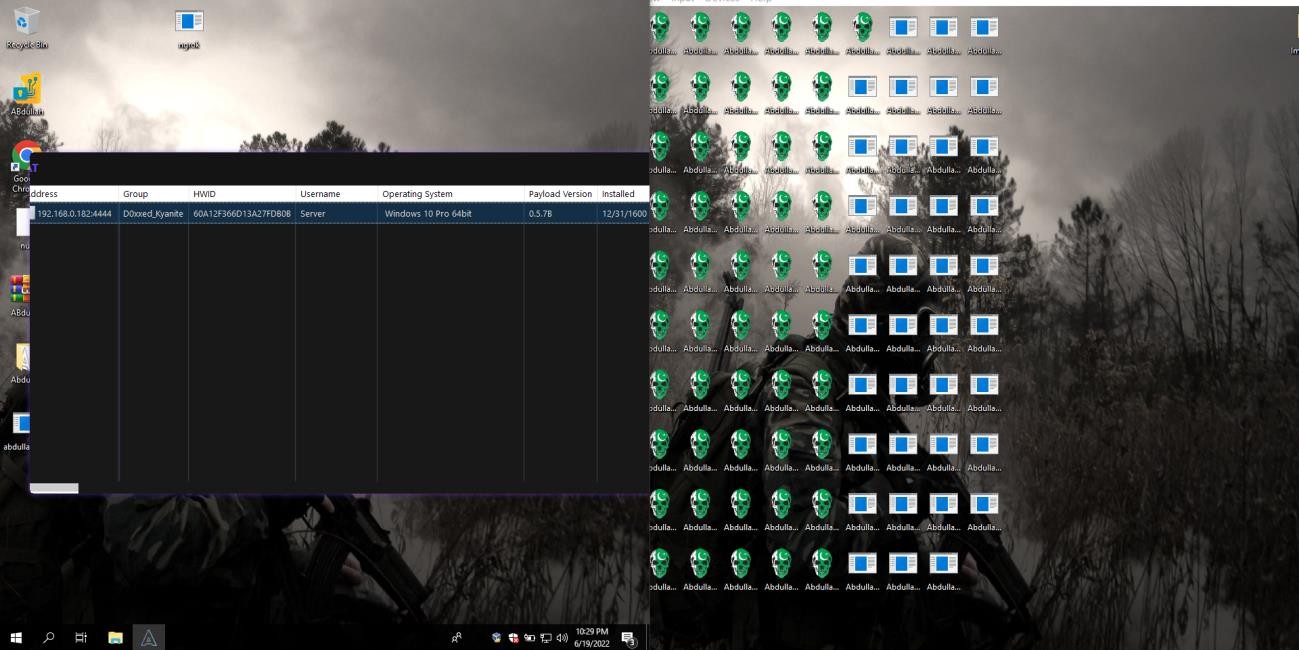


*Figure 19*



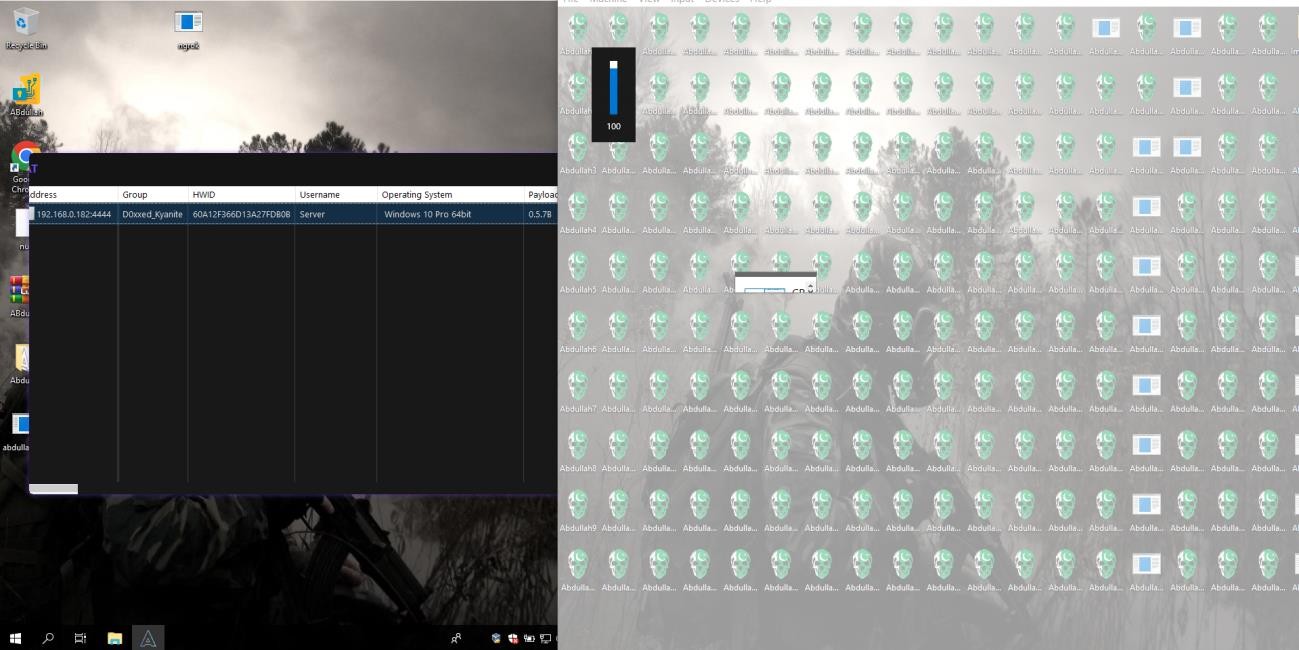
*Figure 18*

After this attacker send the malware to make a worm in server.



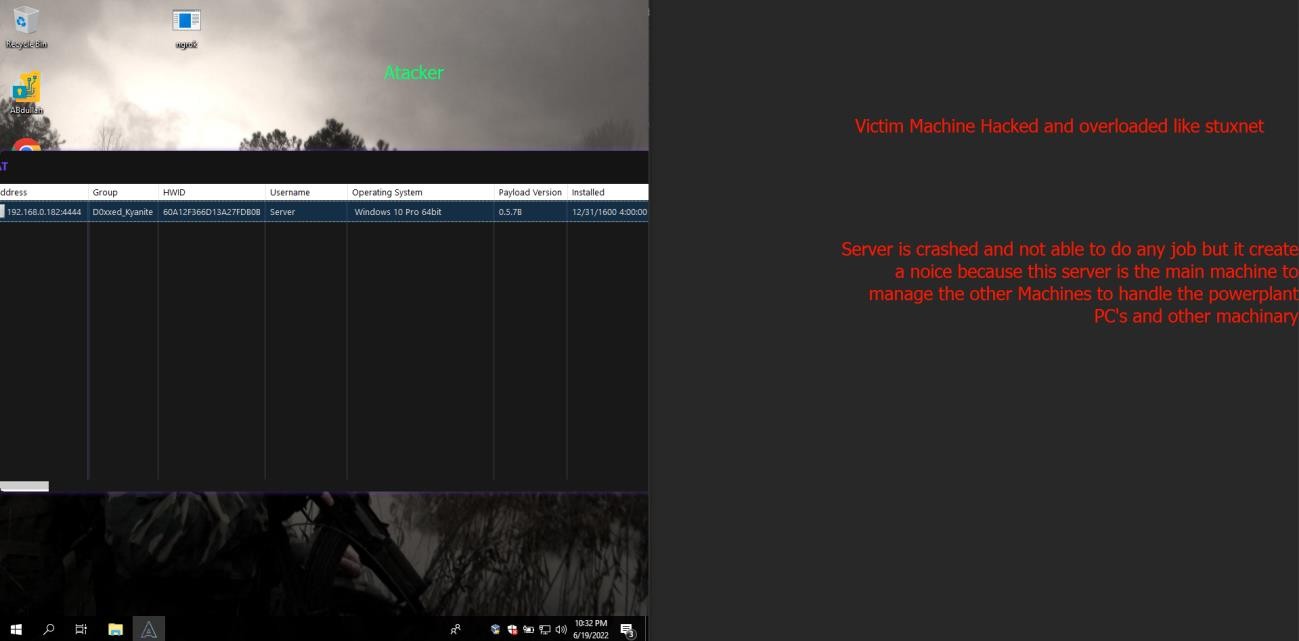
*Figure 20*

Now you can see that worm also replicating itself with the name of Abdullah.exe and also do the volume server as at full level.



*Figure 21*

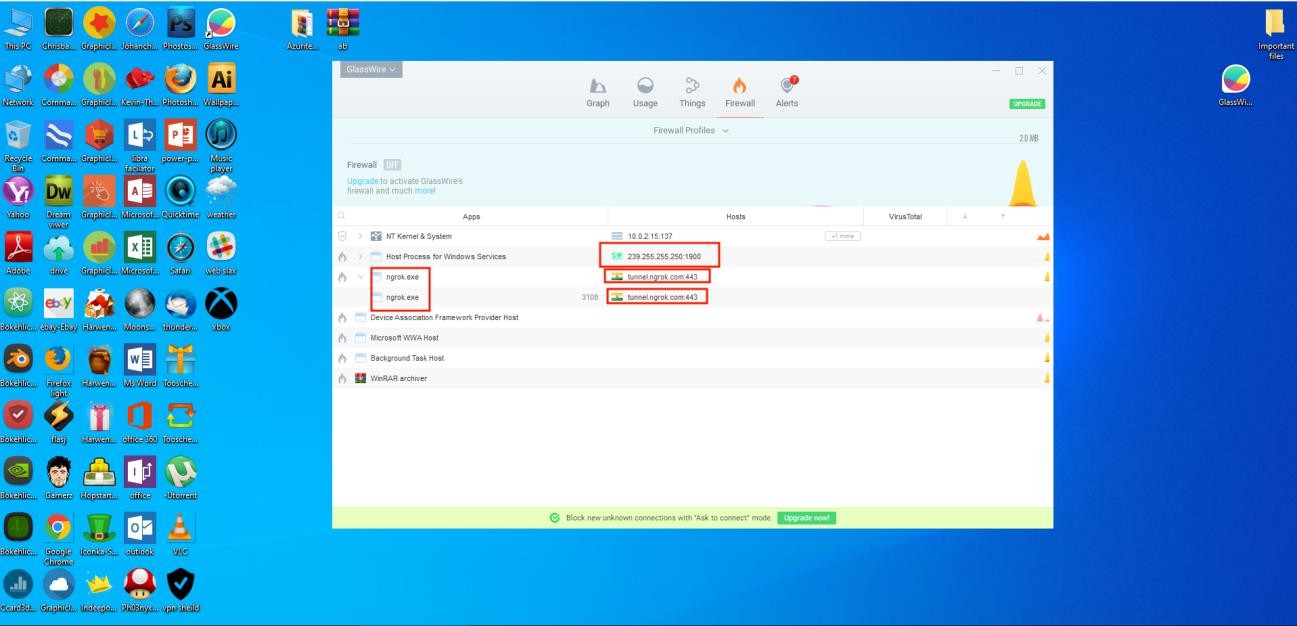
After this server machine is enable to do any response back and high up the machinery working that result in the crash of that Energy sector.



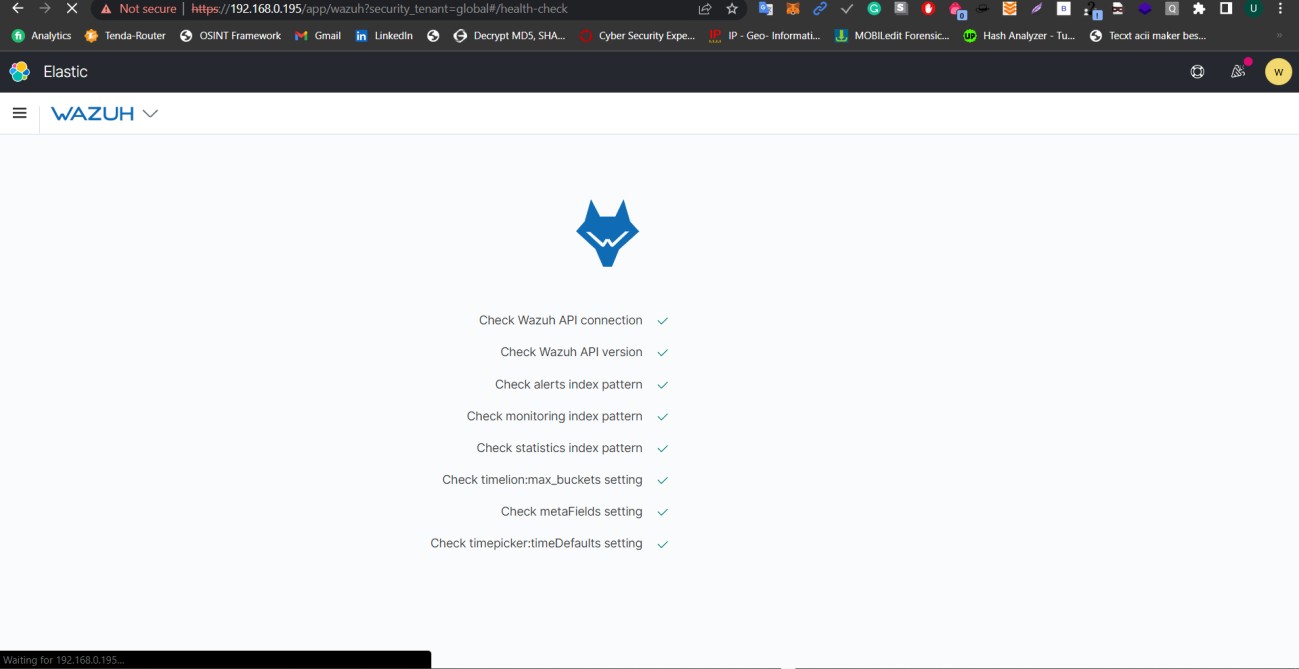
*Figure 22*

## Scenario # 2

Installing host-based firewall for more security. In this snap shot Glass wire is Installed on the server machine to monitor the traffic of tcp/udp over the gui interface.

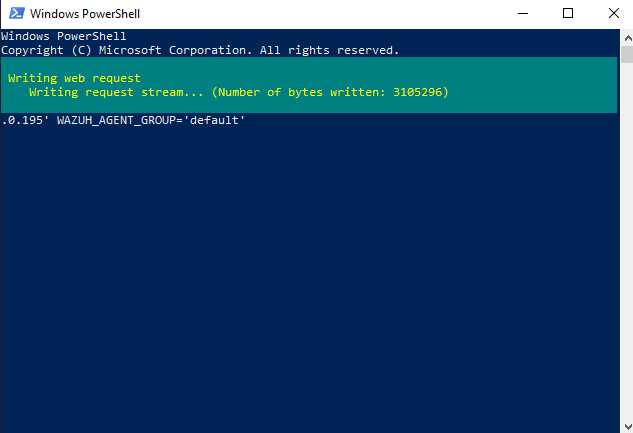


*Figure 23*



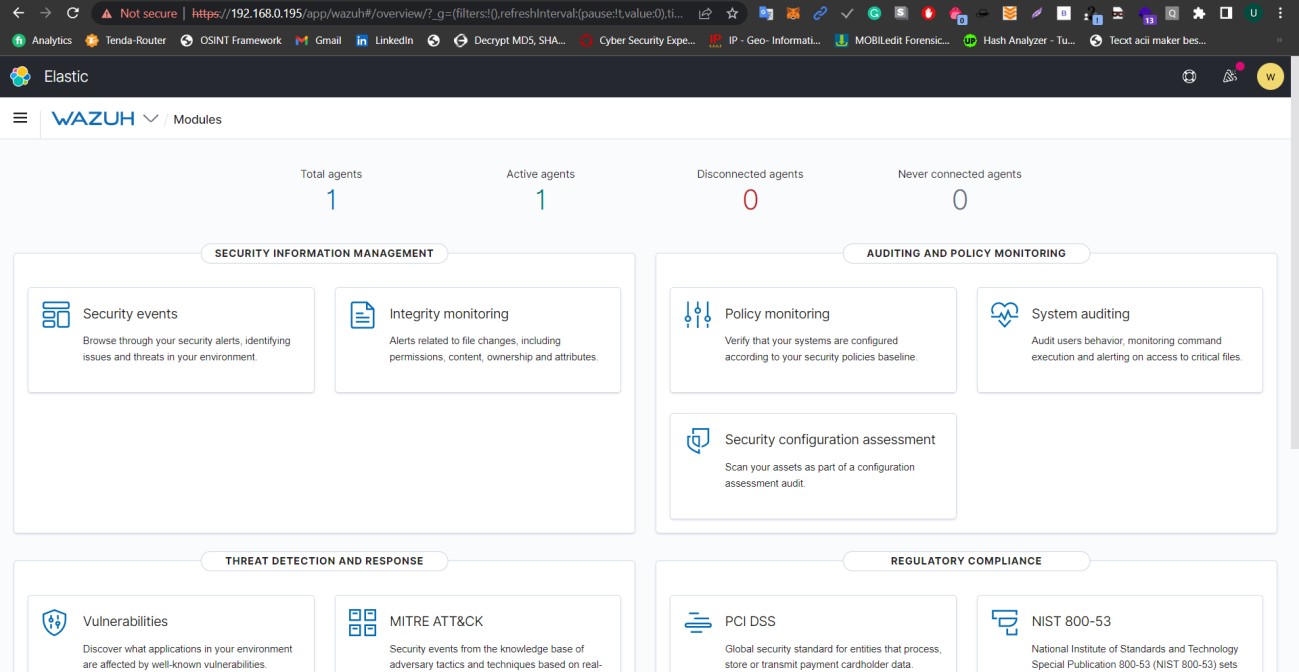
*Figure 24*

Now installing wazuh to monitor the event to detect the suspicious activity



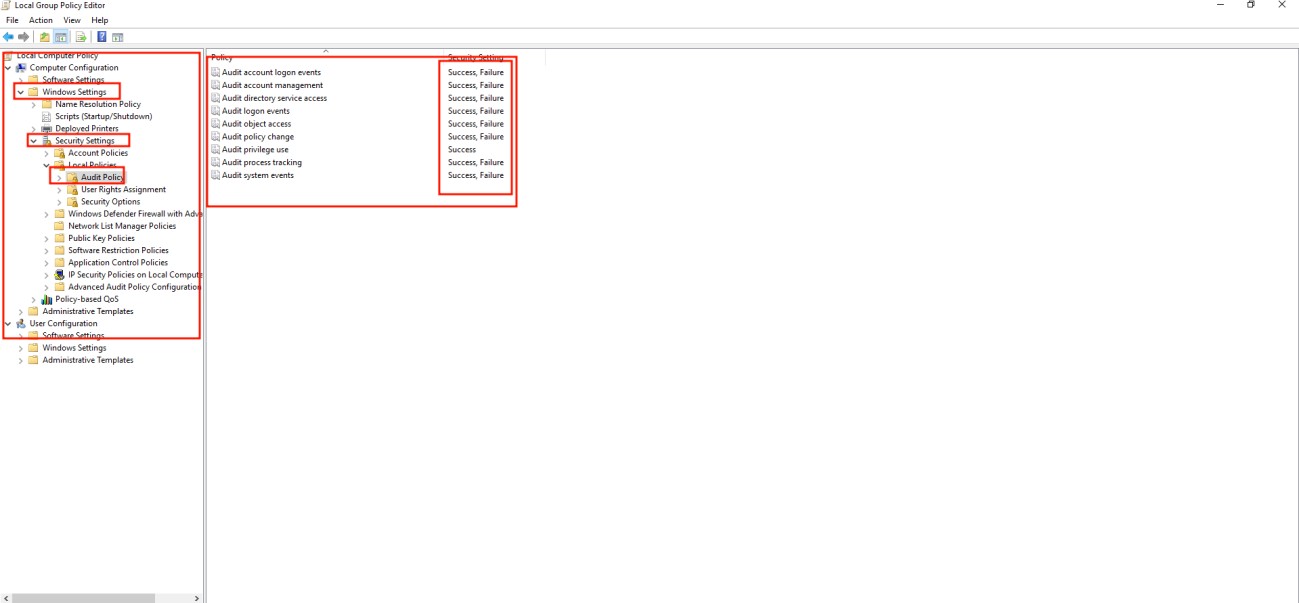
*Figure 25*

This snap shot shows us the installation of the wazuh agent on the client machine.



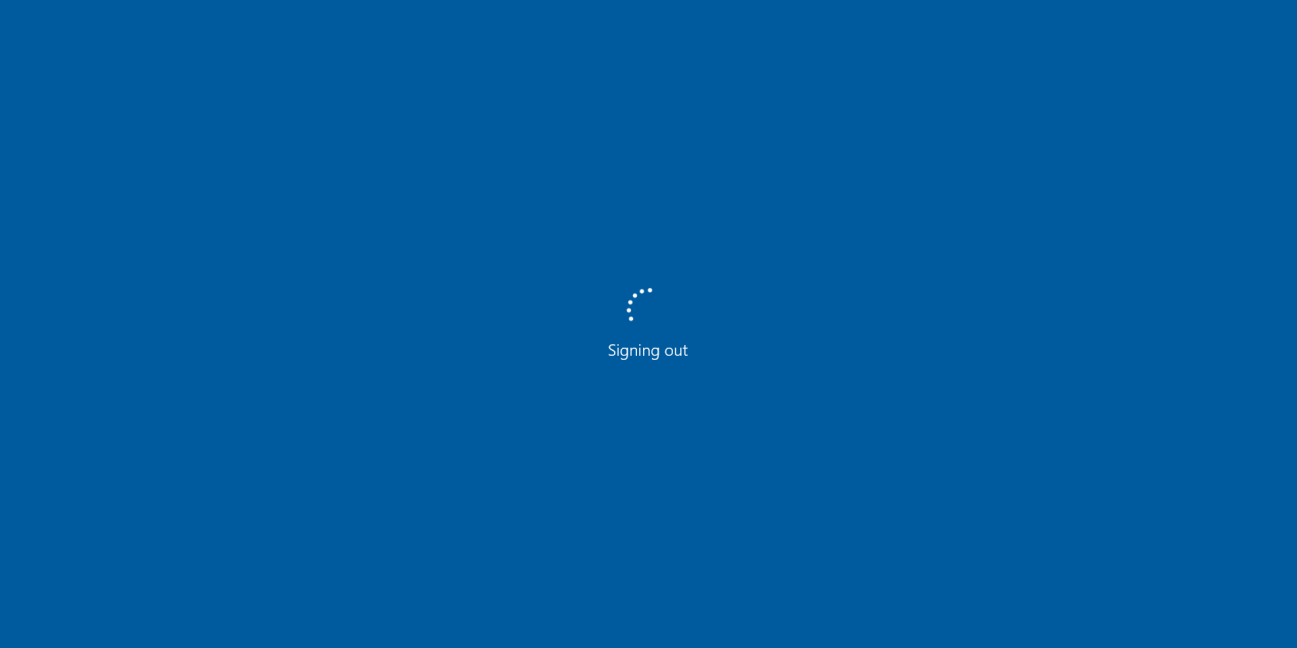
*Figure 26*

After installing and configuring the wazuh agent on the client machine wazuh manager is able to get response from the client machine.



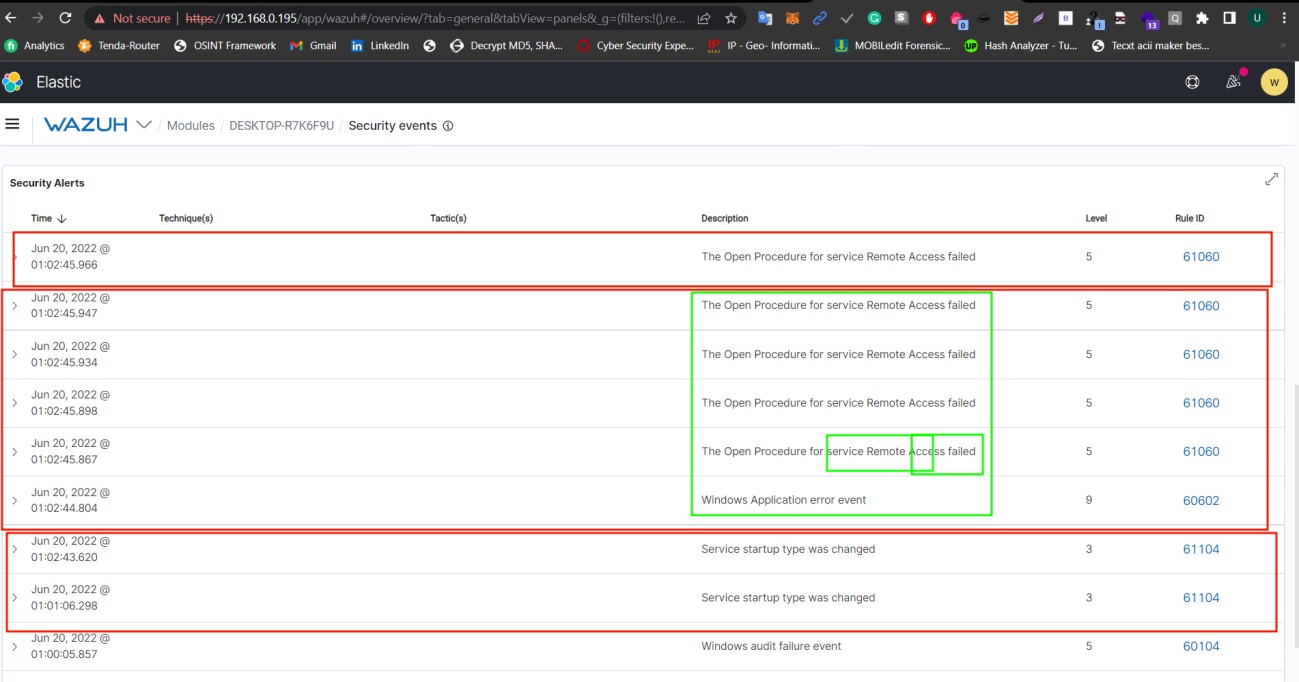
*Figure 27*

After this configure the client machine to send response to the wazuh siem. Wazuh mainly works on the response of the events now turn on the windows events for the wazuh manager.



*Figure 28*

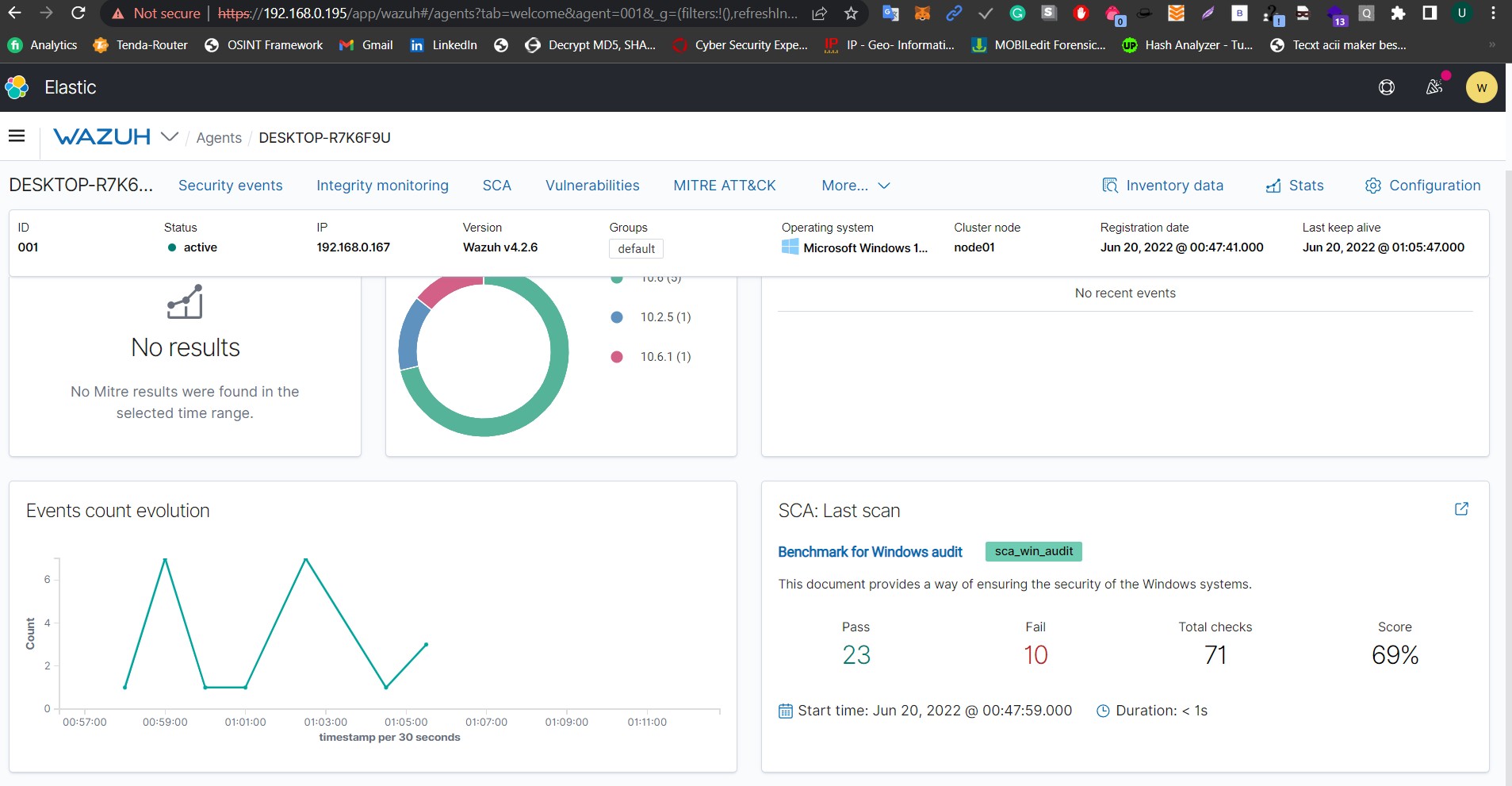
After this restart the machine to check the response on the wazuh manager to check our lab setup is Okay or not.



*Figure 29*

Here we got the result wazuh manager give the result that when and how windows sign our or restart, shutdown etc.

The main thing is that wazuh auto detect and stop the malicious activity in the system. In the above picture you can cleary see that.



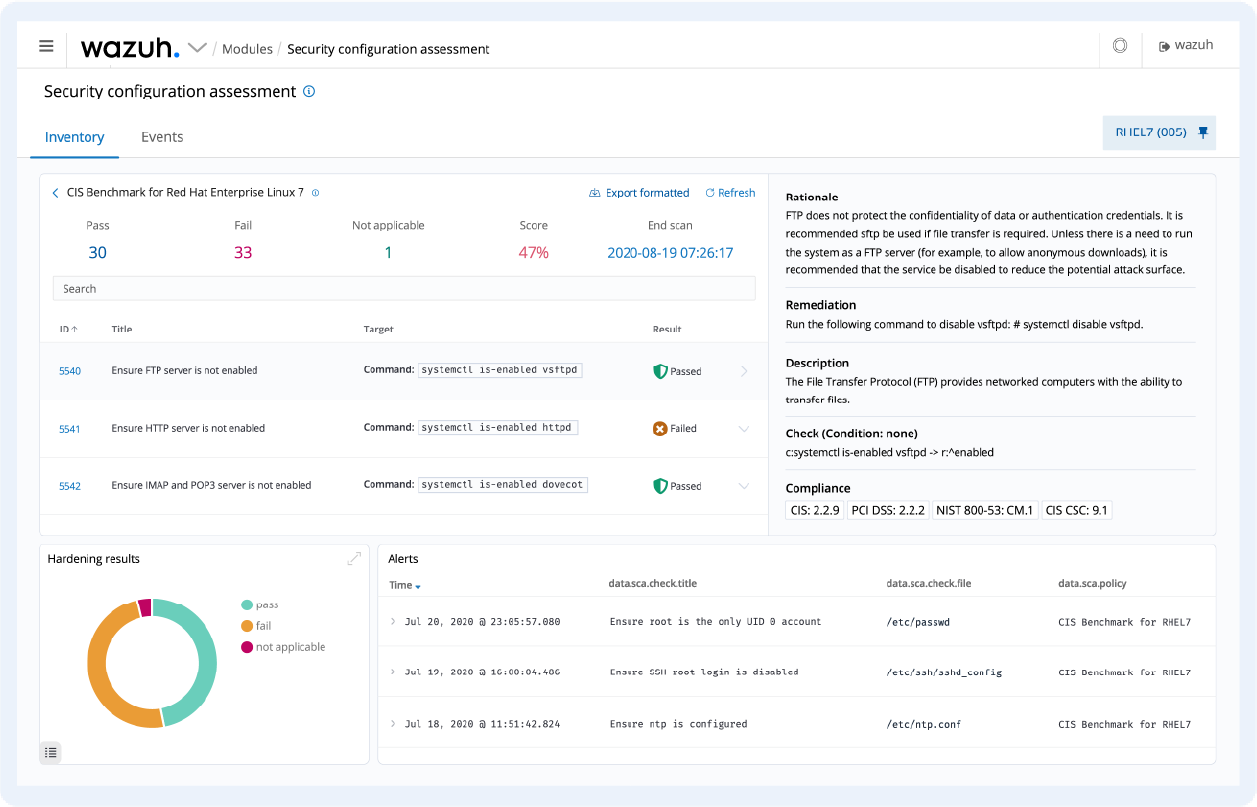
*Figure 30*

Here we can see the final output in dashboard

# Results

## Configuration Assessment

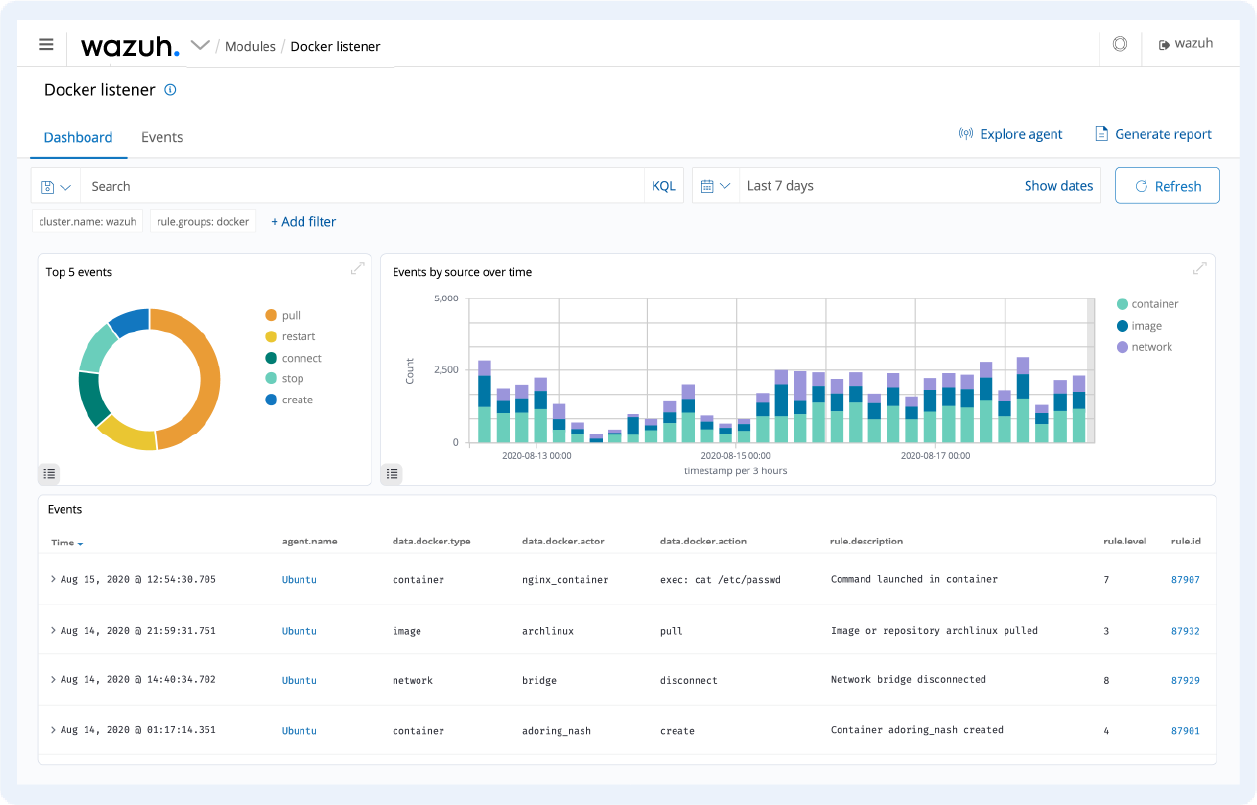
Wazuh keeps track of system and application configuration settings to make sure they adhere to your security standards, rules, and/or hardening instructions. To find apps that are known to be vulnerable, unpatched, or set insecurely, agents do frequent scans.



*Figure 31*

## Containers Security

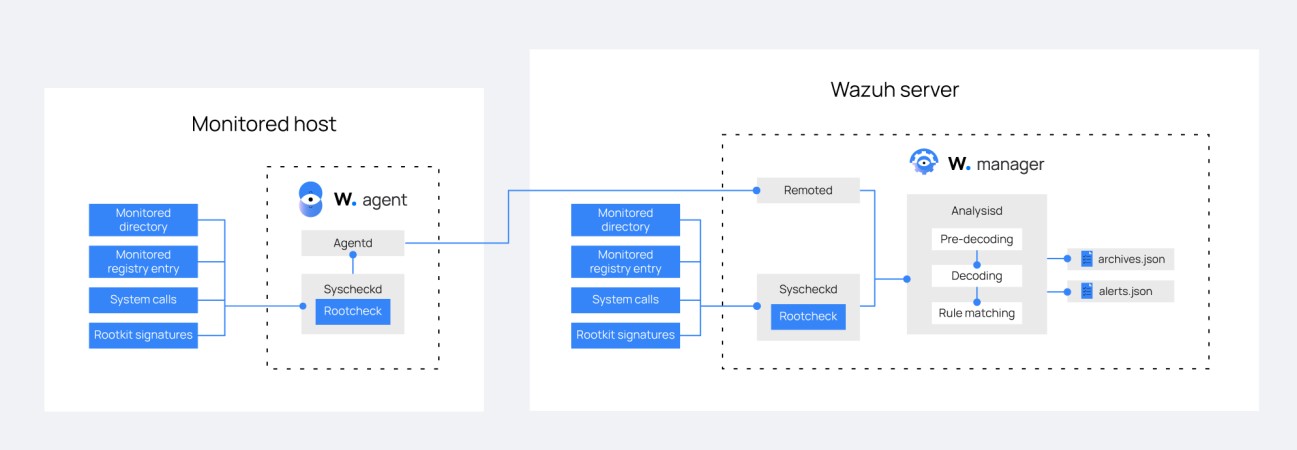
With the ability to monitor the activity of your Docker hosts and containers and identify risks, vulnerabilities, and abnormalities, Wazuh offers security visibility. Users can monitor images, volumes, network configurations, and active containers with the Wazuh agent thanks to its natural interaction with the Docker engine.



*Figure 32*

## Anomalies-detection

This section describes the checks performed by Wazuh to find the anomalies caused by an intruder or malware.

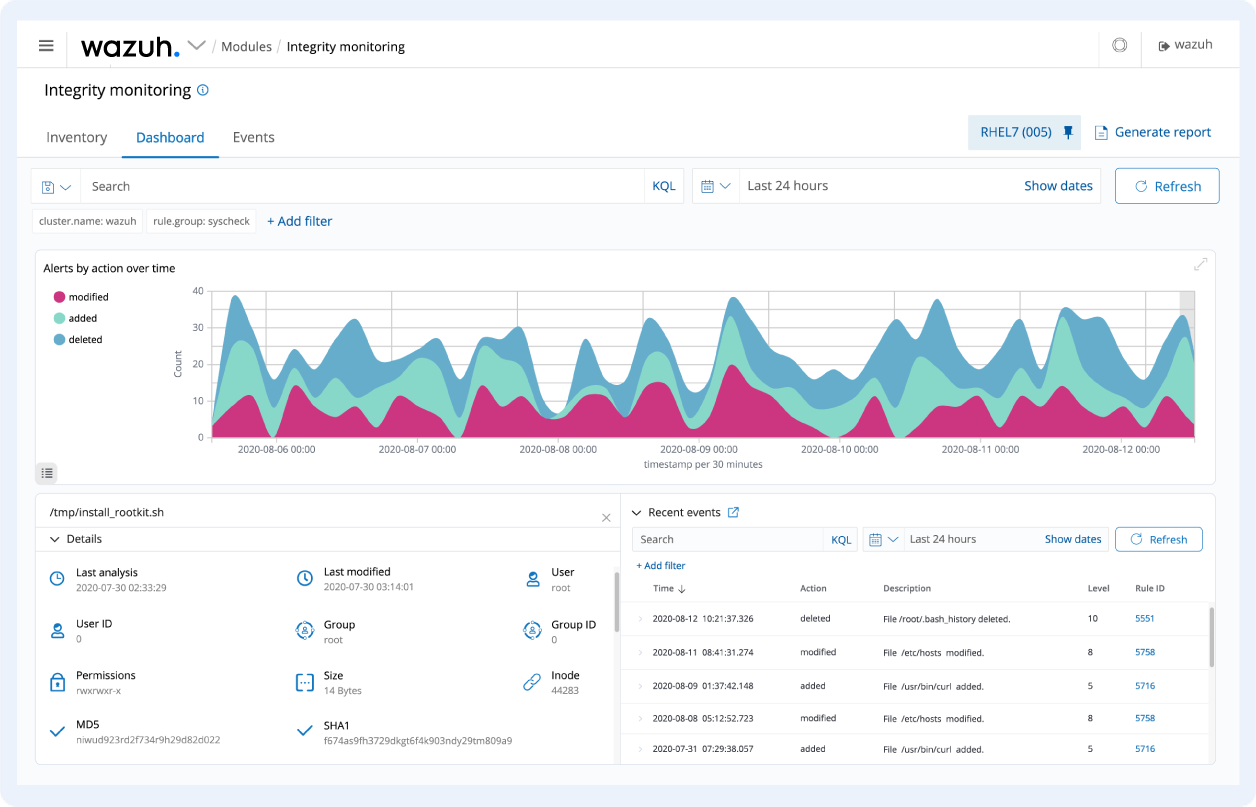


*Figure 33*

## File-Integrity-Monitoring

To find threats or compromised hosts, file integrity monitoring tools can be used in conjunction with threat intelligence. In addition, it is required by a number of regulatory compliance requirements, including PCI DSS.

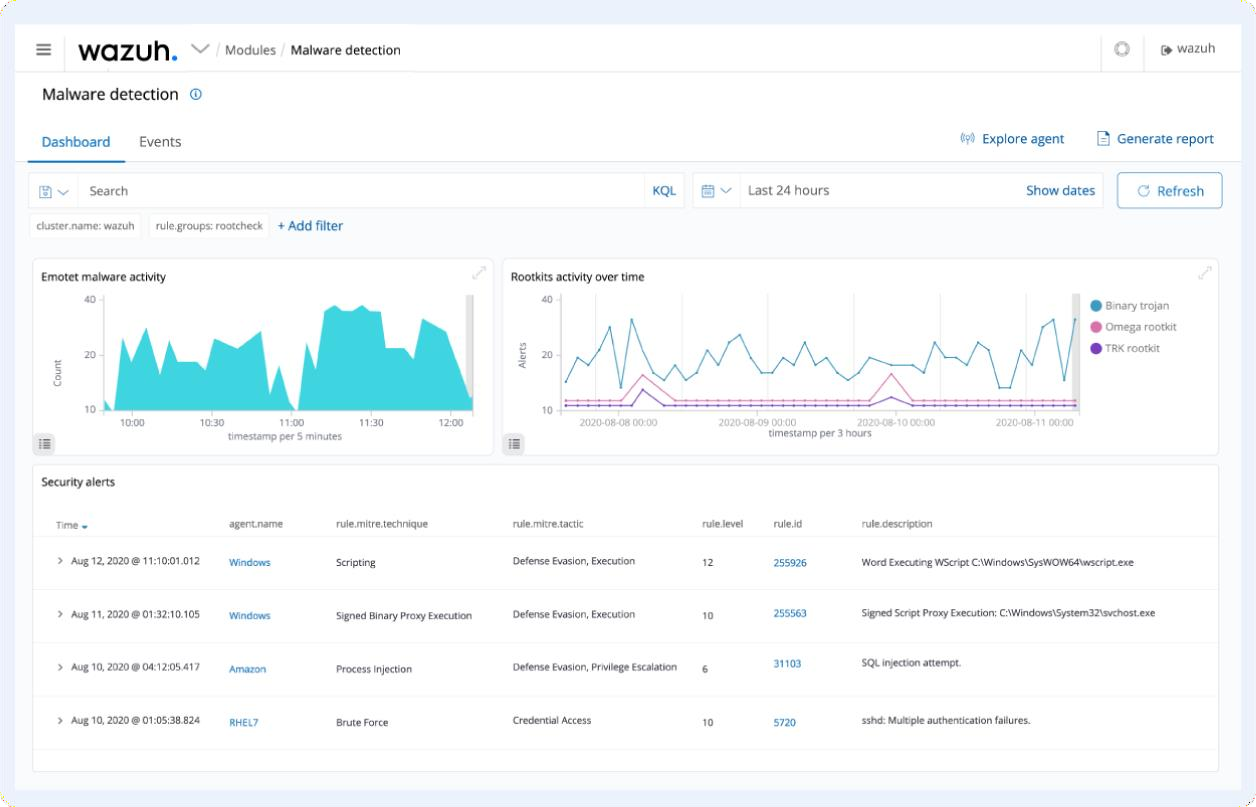
Wazuh keeps track of the file system, alerting you to changes in file properties such as ownership, permissions, and content. Additionally, it automatically recognizes the individuals and programs that have created or modified files.



## Intrusion-detection

*Figure 34*

The monitored systems are scanned by Wazuh agents for malware, rootkits, and suspicious abnormalities. They can identify cloaked processes, hidden files, unregistered network listeners, inconsistent system call replies, and concealed files. In addition to agent capabilities, the server component employs a signature-based approach to intrusion detection, analyzing gathered log data and searching for signs of penetration using its regular expression engine.

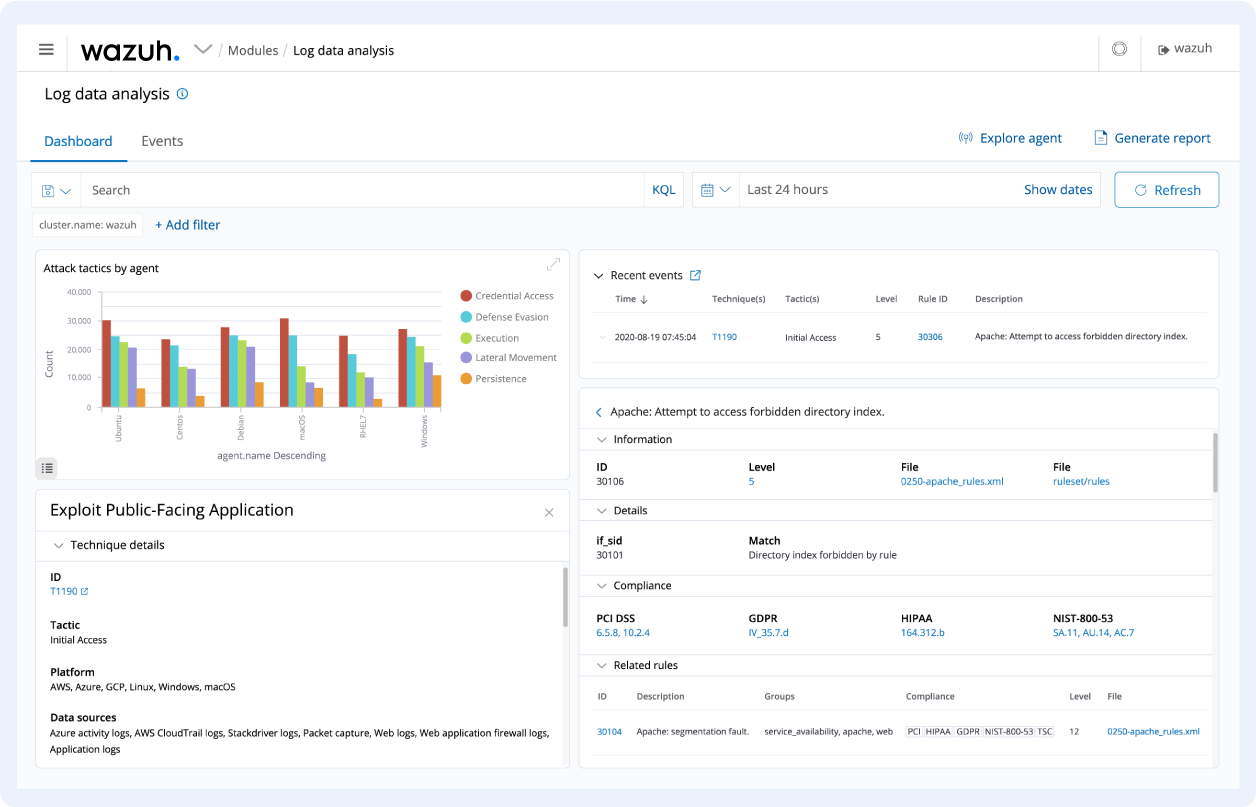


*Figure 35*

* 1. **Log-data-Analysis**

Operating system and application logs are analyzed and sent securely by Wazuh agents to a central manager for rule-based storage and analysis.

The Wazuh rules assist in alerting you to application or system faults, misconfigurations, attempted and/or successful malicious operations, policy violations, as well as a number of other security and operational problems.

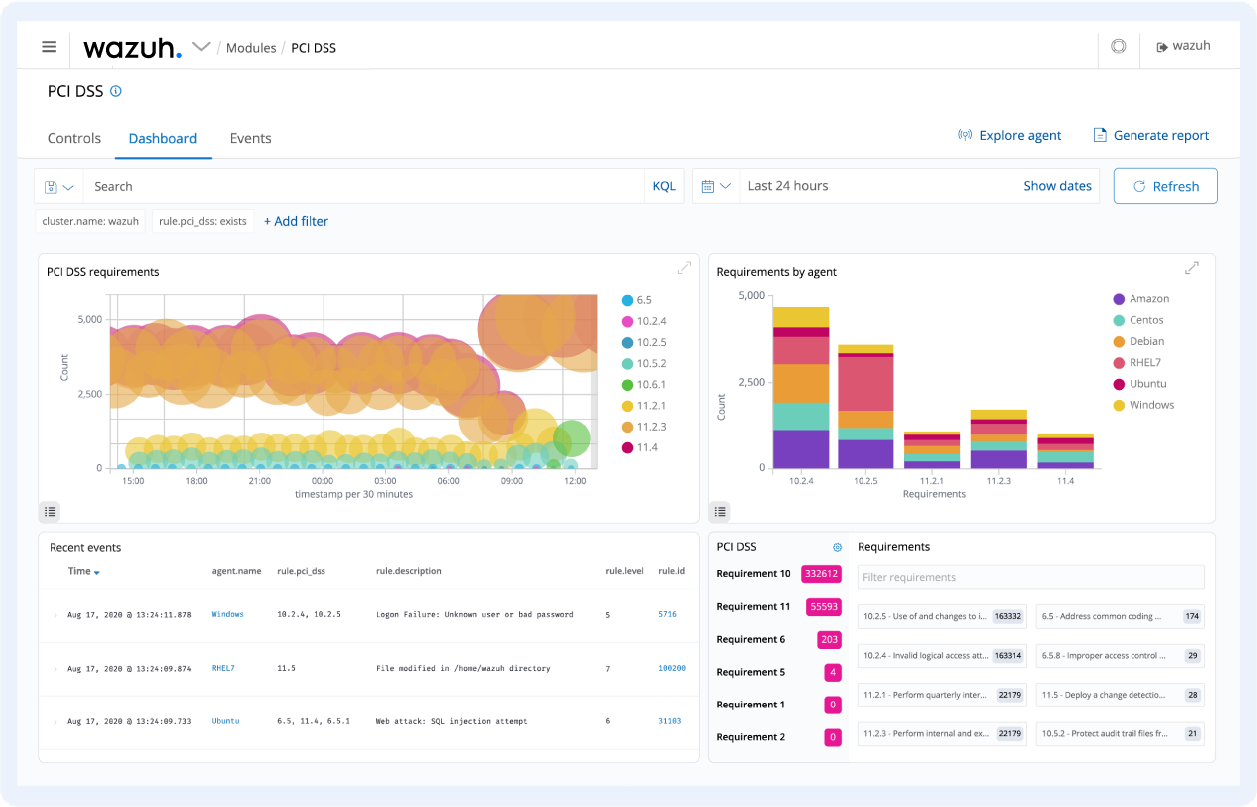


*Figure 36*

* 1. **regulatory-compliance**

Wazuh offers some of the security measures required to adhere to industry requirements and laws. Organizations may achieve technical compliance standards with the aid of these characteristics, along with its scalability and multi-platform compatibility. Financial institutions and payment processing businesses frequently utilise Wazuh to comply with PCI DSS (Payment Card Industry Data Security Standard) regulations. Reports and dashboards are available through

its online user interface, which can help with this and other requirements including GDPR, NIST 800-53, GPG13, TSC SOC2, and HIPAA.

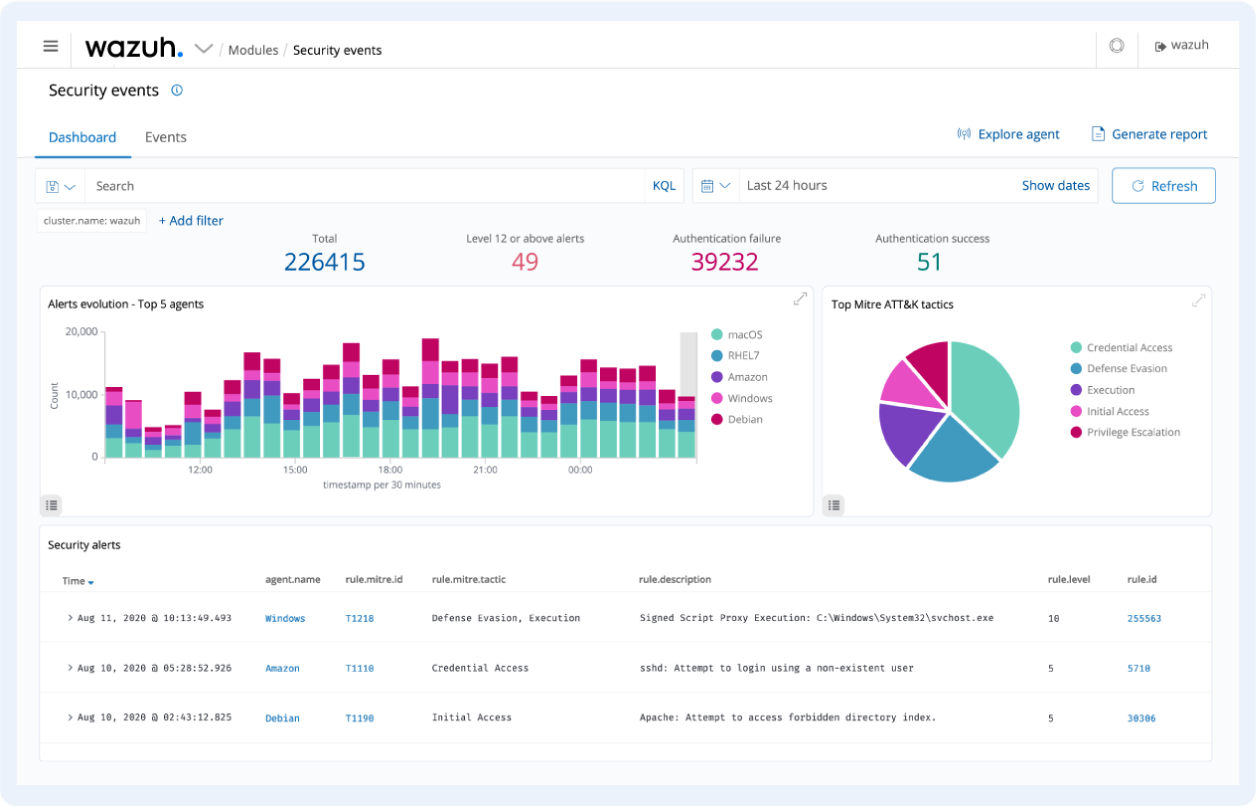


*Figure 37*

* 1. **Security-Events**

Wazuh is used by enterprises to gather, aggregate, index, and analyse security data in order to find threats, intrusions, and behavioural abnormalities. Real-time monitoring and security analysis are necessary for quick threat identification and threat response as cyber attacks become more complex. Because of this, while our server component provides the security intelligence and conducts data analysis, our lightweight agent offers the essential monitoring and reaction

capabilities.

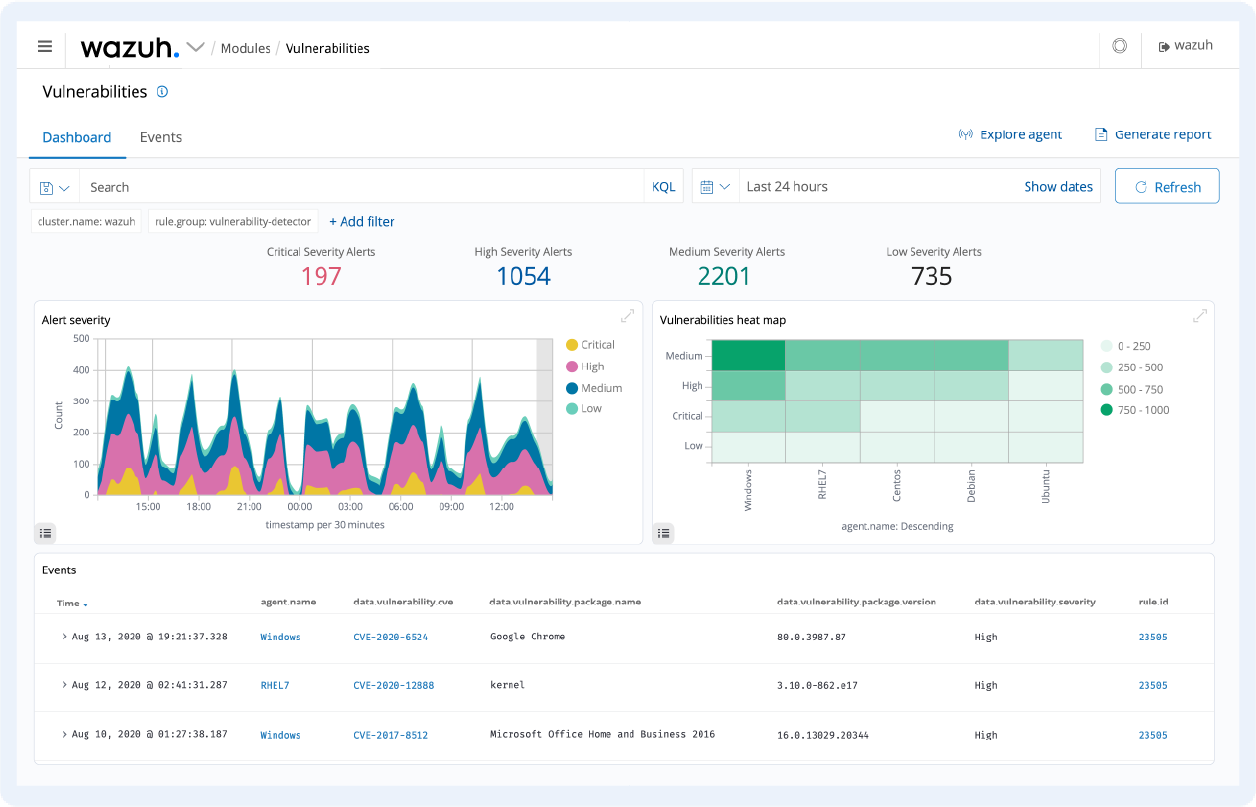


*Figure 38*

* 1. **Vulnerabilities Assetment**

In order to detect well-known susceptible software, Wazuh agents collect software inventory data and transfer it to the server, where it is compared with regularly updated CVE (Common Vulnerabilities and Exposure) databases. Automated vulnerability assessment enables you to identify the areas of vulnerability in your key assets and take action before attackers do to

damage your company or steal sensitive information.



*Figure 39*

1. **References**
2. Murugiah Souppaya Karen Scarfone, `NIST Special Publication 800-83 “Guide to Malware Incident Prevention and Handling for Desktops and Laptops.” *United State 2013* <http://dx.doi.org/10.6028/NIST.SP.800-83r1>
3. National Institute of Standards and Technology. “Framework for Improving Critical Infrastructure Security”. NIST, February 2014. *United State* <http://www.nist.gov/cyberframework/index.cfm>
4. [https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is- malware.html](https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html)
5. Department of Energy. Cybersecurity Capability Maturity Model. DOE, February 2014.

*(DOE 2014a) United States.*

[http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2- program/cybersecurity-](http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-%20program/cybersecurity-capability-maturity-model-c2) [capability-maturity-model-c2](http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-%20program/cybersecurity-capability-maturity-model-c2)

1. <https://download.bitdefender.com/resources/files/Main/file/Malware_History.pdf>
2. [https://www.kaspersky.com/about/press-releases/2005\_viruses-for-mobile-platforms-history- nd-forecasts](https://www.kaspersky.com/about/press-releases/2005_viruses-for-mobile-platforms-history-nd-forecasts)
3. Raza, A., Fatima, U., Rafiq, M., Ahmed, N., Khan, I., Nisar, K. S., & Iqbal, Z. (2021). Mathematical analysis and design of the nonstandard computational method for an epidemic model of computer virus with delay effect: application of mathematical biology in computer science. *Results in Physics*, *21*, 103750. <https://www.degruyter.com/document/doi/10.1515/ijnsns-2019-0063/html>
4. Nedeljkovic, Dusan, and Zivana Jakovljevic. "CNN based method for the development of cyber-attacks detection algorithms in industrial control systems." *Computers & Security* 114 (2022): 102585. <https://www.computer.org/csdl/magazine/co/2021/10/09548104/1x9TEOGAlNe>
5. Cassano, L., Iamundo, M., Lopez, T.A., Nazzari, A. and Di Natale, G., 2022. DETON: DEfeating hardware Trojan horses in microprocessors through software ObfuscatioN. *Journal of Systems Architecture*, p.102592.<https://www.tandfonline.com/doi/abs/10.1080/10643389.2020.1845531>
6. Datta, P.M., 2022. Cybersecurity Threats: Malware in the Code. In *Global Technology Management 4.0* (pp. 155- 170). Palgrave Macmillan, Cham.

<https://link.springer.com/chapter/10.1007/978-3-030-96929-5_10>

1. REISINGER, P.P., THROUGH THE SPYING-GLASS: DATA PRIVACY CONCERNS REGARDING MOBILE SPYWARE APPS.

<https://bciptf.org/wp-content/uploads/2022/04/Reisinger_Through-the-Spying-Glass.pdf>

1. Hernandez-Suarez, Aldo, Gabriel Sanchez-Perez, Linda K. Toscano-Medina, Jesus Olivares-Mercado, Jose

Portillo-Portilo, Juan-Gerardo Avalos, and Luis Javier García Villalba. "Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks." *Applied Sciences* 12, no. 7 (2022): 3234. [https://www.researchgate.net/profile/Jithin-Joy-](https://www.researchgate.net/profile/Jithin-Joy-4/publication/357973796_Implication_of_the_cyber_threats_and_its_issues_in_the_business_process_organization_A_case_study_of_Tesco/links/61e998645779d35951c0d6f1/Implication-of-the-cyber-threats-and-its-issues-in-the-business-process-organization-A-case-study-of-Tesco.pdf) [4/publication/357973796\_Implication\_of\_the\_cyber\_threats\_and\_its\_issues\_in\_the\_business\_process\_organization\_](https://www.researchgate.net/profile/Jithin-Joy-4/publication/357973796_Implication_of_the_cyber_threats_and_its_issues_in_the_business_process_organization_A_case_study_of_Tesco/links/61e998645779d35951c0d6f1/Implication-of-the-cyber-threats-and-its-issues-in-the-business-process-organization-A-case-study-of-Tesco.pdf) [A\_case\_study\_of\_Tesco/links/61e998645779d35951c0d6f1/Implication-of-the-cyber-threats-and-its-issues-in-the-](https://www.researchgate.net/profile/Jithin-Joy-4/publication/357973796_Implication_of_the_cyber_threats_and_its_issues_in_the_business_process_organization_A_case_study_of_Tesco/links/61e998645779d35951c0d6f1/Implication-of-the-cyber-threats-and-its-issues-in-the-business-process-organization-A-case-study-of-Tesco.pdf) [business-process-organization-A-case-study-of-Tesco.pdf](https://www.researchgate.net/profile/Jithin-Joy-4/publication/357973796_Implication_of_the_cyber_threats_and_its_issues_in_the_business_process_organization_A_case_study_of_Tesco/links/61e998645779d35951c0d6f1/Implication-of-the-cyber-threats-and-its-issues-in-the-business-process-organization-A-case-study-of-Tesco.pdf)

1. Roben, Caroline KP, Evan Kipp, Stevie S. Schein, Amanda H. Costello, and Mary Dozier. "Transitioning to telehealth due to COVID‐19: Maintaining model fidelity in a home visiting program for parents of vulnerable infants." *Infant Mental Health Journal* 43, no. 1 (2022): 173-184.<https://onlinelibrary.wiley.com/doi/10.1002/imhj.21963>
2. Sharma, Nikhil, and Ravi Shanker. "Analysis of Ransomware Attack and Their Countermeasures: A Review." In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pp. 1877-1883. IEEE, 2022. <https://ieeexplore.ieee.org/abstract/document/9770351>
3. Siddiqi, Murtaza Ahmed, Wooguil Pak, and Moquddam A. Siddiqi. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures." *Applied Sciences* 12, no. 12 (2022): 6042. <https://www.mdpi.com/2076-3417/12/12/6042/pdf?version=1655208887>
4. Gjesvik, Lars, and Kacper Szulecki. "Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout." *European Security* (2022)

<https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2082838>

1. Kim, D., 2022. *Integrating Human and Machine Intelligence to Secure the Web Browsing, IoT, and Control Plane Safety for the Edge of the Network* (Doctoral dissertation, Indiana University).

(Oladimeji and Kerner, 2021; see par. 5; [https://www.proquest.com/openview/ee0535510dcc08fee9c4a3e4851394b6/1?pq-](https://www.proquest.com/openview/ee0535510dcc08fee9c4a3e4851394b6/1?pq-origsite=gscholar&cbl=18750&diss=y) [origsite=gscholar&cbl=18750&diss=y](https://www.proquest.com/openview/ee0535510dcc08fee9c4a3e4851394b6/1?pq-origsite=gscholar&cbl=18750&diss=y)

1. Watney M. Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. InEuropean Conference on Cyber Warfare and Security 2022 Jun 8 (Vol. 21, No. 1, pp. 319-327). <https://link.springer.com/book/10.1007/978-1-4614-4769-6>

[https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-](https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att) [standards-in-response-to-solarwinds-att](https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att)

1. Kim, D.Y., 2014. Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, *65*, pp.141-143.

<https://ieeexplore.ieee.org/abstract/document/9770351>

1. Chayal, Narendrakumar Mangilal, Ankur Saxena, and Rijwan Khan. "A review on spreading and Forensics Analysis of Windows-Based ransomware." *Annals of Data Science* (2022): 1-22. <https://link.springer.com/article/10.1007/s40745-022-00417-5>
2. Gjesvik, L. and Szulecki, K., 2022. Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security*, pp.1-21. <https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2082838>
3. Tariq, N., Asim, M., & Khan, F. A. (2019). Securing SCADA-based critical infrastructures: Challenges and

open issues. *Procedia computer science*, *155*, 612-617.

<https://www.sciencedirect.com/science/article/pii/S1877050919310002>

1. Ciancamerla, E., Minichino, M. and Palmieri, S., 2013, July. Modeling cyber attacks on a critical infrastructure scenario. In *IISA 2013* (pp. 1-6). IEEE.

<https://ieeexplore.ieee.org/abstract/document/6623699>

1. Wang, Zongjian, and Xiaobo Li. "Intrusion prevention system design." In Proceedings of the International Conference on Information Engineering and Applications *(IEA) 2012, pp. 375-*

*382. Springer, London, 2013.* [*https://link.springer.com/chapter/10.1007/978-1-4471-4847-0\_47*](https://link.springer.com/chapter/10.1007/978-1-4471-4847-0_47)

1. Ellefsen, Ian, and Sebastiaan Von Solms. “Critical Information Infrastructure Protection in the Developing World.” In Critical Infrastructure Protection IV, edited by Tyler Moore and Sujeet Shenoi, 29-40. Berlin, Germany: Springer Berlin Heidelberg, 2010. doi: 10.1007/978-3- 642-16806-2\_3.
2. Dacey, Robert F. Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. (GAO-04-628T). Washington, DC: U.S. Government Accountability Office, 2004. Last accessed July 31, 2016.
3. Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018). [http://www.gao.gov/products/GAO- 04-628T](http://www.gao.gov/products/GAO-04-628T)
4. Han, C. H., Park, S. T., & Lee, S. J. (2019). The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection*, *26*, 100312. [*https://www.sciencedirect.com/science/article/pii/S1874548219300460*](https://www.sciencedirect.com/science/article/pii/S1874548219300460)
5. Han, C.H., Park, S.T. and Lee, S.J., 2019. The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection*, *26*, p.100312.

[*https://www.sciencedirect.com/science/article/pii/S1874548219300460*](https://www.sciencedirect.com/science/article/pii/S1874548219300460)

https://us-cert.cisa.gov/ncas/alerts/aa20-352a], likely carried out by a group affiliated with Russia’s FSB security service

## 6.1 Wazuh Refrence

<https://documentation.wazuh.com/current/deployment-options/splunk/splunk-basic.html>

[https://documentation.wazuh.com/current/deployment-options/splunk/splunk-minimal-](https://documentation.wazuh.com/current/deployment-options/splunk/splunk-minimal-distributed.html) [distributed.html](https://documentation.wazuh.com/current/deployment-options/splunk/splunk-minimal-distributed.html)

<https://documentation.wazuh.com/current/deployment-options/splunk/splunk-distributed.html> <https://documentation.wazuh.com/current/deployment-options/splunk/splunk-app.html> <https://documentation.wazuh.com/current/deployment-options/splunk/splunk-reverse-proxy.html>

<https://documentation.wazuh.com/current/deployment-options/splunk/splunk-polling.html> <https://documentation.wazuh.com/current/deployment-options/splunk/splunk-rbac.html> [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/index.html) [ansible/index.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/index.html)

[https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/installation-guide.html) [ansible/installation-guide.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/installation-guide.html) [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-ansible.html) [ansible/guide/install-ansible.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-ansible.html) [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-indexer-dashboard.html) [ansible/guide/install-indexer-dashboard.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-indexer-dashboard.html) [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-manager.html) [ansible/guide/install-wazuh-manager.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-manager.html) [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-cluster.html) [ansible/guide/install-wazuh-cluster.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-cluster.html) [https://documentation.wazuh.com/current/deployment-options/deploying-with-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-agent.html) [ansible/guide/install-wazuh-agent.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/guide/install-wazuh-agent.html)

[https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/setup-](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/setup-remote-systems.html) [remote-systems.html](https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/setup-remote-systems.html)