Building a Comprehensive Cybersecurity Incident Response Framework

Table of Contents

Week 1: Foundation and Awareness

Report on Cybersecurity Concepts and Network Discovery Techniques

1. Introduction

Cybersecurity involves practices, techniques, and tools designed to protect data, systems, and networks from cyber-attacks, unauthorized access, and other forms of harm. As the digital landscape evolves, threats become more sophisticated, and the need for secure networks is paramount. This report provides an overview of fundamental cybersecurity concepts, common threats faced by networks, and techniques used for network discovery and security testing.

2 Cybersecurity Concepts

2.1. CIA Triad

The CIA Triad is the foundation of cybersecurity and consists of three primary components:

- Confidentiality: Ensures that sensitive data is only accessible to authorized individuals. Methods like encryption, access control, and authentication mechanisms (passwords, biometric verification) are commonly used to maintain confidentiality.
- Integrity: Protects data from being altered by unauthorized entities. This involves checksums, hashing, and version control to ensure data accuracy and consistency during transit and storage.
- Availability: Ensures that systems, networks, and data are accessible when needed. Techniques like load balancing, redundancy, and regular maintenance help maintain availability, especially during attacks like DDoS.

2.2. Authentication and Authorization

- Authentication: The process of verifying the identity of a user. This can be done using passwords, biometrics, or multi-factor authentication (MFA).
- Authorization: Once authenticated, authorization ensures that users have access to the resources they are permitted to use. This is done through roles and permissions.

2.3. Encryption

Encryption is a critical security practice where data is converted into a code to prevent unauthorized access. Common encryption algorithms include:

- AES (Advanced Encryption Standard): Widely used for secure data transmission.
- RSA (Rivest–Shamir–Adleman): Often used for secure data exchanges over the internet.

2.4. Firewalls

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between trusted internal networks and untrusted external networks (like the internet).

2.5. Intrusion Detection and Prevention Systems (IDS/IPS)

- IDS (Intrusion Detection System): Monitors network traffic for suspicious activities and alerts administrators of potential threats.
- IPS (Intrusion Prevention System): Not only detects but also blocks detected threats.

3.Common Cybersecurity Threats

3.1. Malware

Malware is any software intentionally designed to cause harm to a computer, network, or user. Common types of malware include:

- Viruses: Programs that replicate themselves by modifying other software and inserting malicious code.
- Worms: Standalone malware that replicates itself to spread to other computers.
- Ransomware: Encrypts data and demands a ransom for decryption.
- Spyware: Collects data from an infected machine without the user's knowledge.

3.2. Phishing

Phishing is a form of social engineering where attackers impersonate legitimate entities to steal sensitive information such as usernames, passwords, and credit card numbers. Phishing typically occurs through fraudulent emails or websites.

3.3. Distributed Denial of Service (DDoS) Attacks

In a DDoS attack, a network is overwhelmed with a flood of internet traffic, rendering the target system unavailable to legitimate users. DDoS attacks are commonly carried out using botnets.

3.4. Man-in-the-Middle (MITM) Attacks

MITM attacks occur when an attacker intercepts communications between two parties, allowing them to listen, alter, or impersonate one of the parties involved. These attacks can occur in various forms, such as intercepting emails or unsecured Wi-Fi communications.

3.5. Insider Threats

Insider threats occur when individuals within an organization misuse their authorized access to steal, modify, or destroy data. These individuals may be employees, contractors, or other parties with internal access.

3.6. Zero-Day Exploits

Zero-day vulnerabilities refer to security flaws that are unknown to the software vendor. Cybercriminals exploit these vulnerabilities before the vendor has a chance to release a fix or patch.

4.Network Discovery Techniques

4.1. Port Scanning

Port scanning involves sending packets to specific ports on a host to identify which services are available and vulnerable. Commonly used tools include:

- Nmap: One of the most popular tools for network scanning. It helps map out network topology, open ports, and services running on those ports.
- Netcat: Used to read or write data over network connections. It's often used for troubleshooting and network exploration.

4.2. Packet Sniffing

Packet sniffing is a method used to capture and analyze network traffic. It allows the user to see data packets as they pass through the network. A popular tool for this purpose is:

• Wireshark: A network protocol analyzer used for network troubleshooting and analysis.

4.3. Network Mapping

Network mapping refers to creating a visual or logical diagram of a network's structure. It helps identify relationships between various devices and services. Tools like SolarWinds Network Performance Monitor are widely used for network mapping and monitoring.

4.4. Banner Grabbing

Banner grabbing is the process of gathering information about the services running on open ports. Attackers use this technique to identify potential vulnerabilities in software versions. Banner grabbing tools include Telnet and Netcat.

4.5. Traceroute

Traceroute is a diagnostic tool used to track the path that data packets take from the source to the destination. This technique helps in identifying network delays and failures at specific points.

5. Conclusion

Understanding fundamental cybersecurity concepts, common threats, and network discovery techniques is crucial for maintaining a secure network infrastructure. With constant advancements in technology, it is essential to stay informed and deploy updated security practices. Organizations must ensure proper implementation of firewalls, IDS/IPS, encryption, and other security measures to minimize risks from both external and internal threats. Network discovery tools like Nmap, Wireshark, and others play an important role in identifying vulnerabilities and securing network infrastructures.

Week 2: Incident Response Planning

1. Introduction

The following is an example of a Target company full incident response plan. It is intended to be a living document that grows and changes over time at a pace that is tied to evolving threats and best practices. Since attack patterns are known, this plan provides solutions for key elements related to system hardening, secure architecture, access control measures, and coordinated and effective response to the incident of any kind.

2. Scope

Target company has all systems, networks, and data assets under 3 plans, in its ownership and management. This includes both physical and digital assets of all departments and partners.

3. Roles and Responsibilities

With an efficient response, a clearly defined chain of command is necessary. The following roles and responsibilities are established:

- Incident Response Team (IRT): A group of employees with required skills in cybersecurity and coordinating and executing incident response activities.
- Incident Commander: It has responsibility for the IRT and its critical decisions in an incident.
- Security Analysts: Monitor systems, analyze possible threats, and report technical expertise.
- Forensic Investigators: Provides evidence gathering and analyzing, incidental compliance and reconstruction.
- Communication Team: Communicates with stakeholders – internal and external – and updates and advises.
- Legal Counsel: It advises on legal implications of incidents and it guarantees compliance with regulations.
- Management: We provide overall guidance and support to IRT so as to provide resources and also authority of making decisions.

4. Incident Response Phases

The incident response plan is structured around four key phases:

4.1 Preparation:

- Establish policies and procedures: It is important that Incidnet Response protocols, escalation procedres as well as the communication channels are defined clearly.
- Develop incident response plan: Make the document write, with the details steps of the phase of response, roles, responsibilities and the tools.
- Training and awareness: Train all employees on their incident response procedures, phishing awareness ect on a regular basis.
- System hardening: The following action will strengthen systems but securing will be done to minimize vulnerability with the system.
    - Vulnerability scanning and patching: Keep scan systems on 'high alert', trying to find any new vulnerabilities and patching as soon as possible once discovered.
    - Password complexity and rotation: Enforce strong password policies and enforce password rotation (time).
    - Multi-factor authentication (MFA): MFA should protect every major system and account.
    - Data encryption: Keep sensitive data both in flight and at rest.
    - Secure configurations: Ensure that required security best practices operating systems, applications, and network devices are applied….
    - Logging and monitoring: You can implement a complete logging and monitoring solution to find out unusual activity.
- Secure architecture: Build the secure core that needs least attack surface and least risk:
    - Network segmentation: Keep critical systems and data separate from public networks.
    - Demilitarized zone (DMZ): Host your public facing services in a DMZ.
    - Firewall rules: Also, try to put up enough fire wall rules that prevent any unauthorized access.
    - Intrusion detection and prevention systems (IDS/IPS): Detection and blocking of malicious activity are achieved by install IDS/IPS.
- Access control measures: Implementing robust access control mechanisms to restrict access to systems and data for unnecessary people.

- Least privilege principle: Degrade as low privileges as possible.
- Role-based access control (RBAC): Based on roles assign permissions.
- Access control lists (ACLs): We then use ACLs to control network resources access.

- Incident Response Team (IRT) formation and training: You build your IRT with required skills and take frequency training to enlarge your capability in response procedures.

4.2 Detection:

- Monitoring systems: In confidential information system logs, network traffic, security alerts, and otherwise closely monitor systems for unusual activity.
- Threat intelligence: Just like threat feeds, stay ahead of emerging threats and vulnerabilities by threat intelligence feeds.
- Incident reporting mechanisms: Proper procedures for reporting potential incidents are what you want to do.
- Alerting and escalation: Set trigger alerts that can take a predetermined action triggered off an incident threshold met and escalate an incident to the right level.

4.3 Containment:

- Isolate infected systems: There, you then immediately isolate from the compromise of compromised systems so as to break the vertiginous chain of spread.
- Disrupt attacker activity: Take out the action of the individual who is blocking the attacker's access to the network and systems.
- Secure evidence: To retain evidence of the incident for investigation and subsequent legal proceedings.

4.4 Eradication:

- Remove malware: It does that by removing malicious software and associated files from infected systems.
- Restore systems: Back things up or perform some type of recovery to get them to a clean state.
- Remediate vulnerabilities: During the time of incident, they found out patch vulnerabilities.
- Implement corrective actions: Prevent future occurrences of this by making change to security policies, procedures and systems.

4.5 Recovery:

- Restore critical systems: Besides that, they should restore the basic systems and services.
- Test and validate recovery: Thoroughly restore systems and test them out while they work properly and are secure.
- Communication and reporting: Instead, report out on the incident, communicate on progress toward recovery to stakeholders.

4.6 Post-Incident Activities:

- Review and analysis: 2. Agree on a post incident review and landing on outcome – lessons learned and areas for improvement.
- Documentation and reporting: Document (record) attack and incident response action, reflect on, and what you learned.
- Continuous improvement: And then continuously evaluate and update the incident response plan based on what we learned and what threat endures.

5. Communication Plan

- Internal Communication: Forward this to the people who will send an email regarding the incident or for the people who will include this in the company's intranet so people will be aware.
- External Communication: Deal with media, police or any other outside agencies when necessary and doing so in accordance with legal and privacy requirements.

6. Lea & Legal Compliance

- Incident reporting: Log and report security incidents that meet reportable threshold of the law.
- Data protection: You would like to ensure you meet the GDPR and CCPA requirements properly.
- Forensics: If there is a lawsuit you would have to produce proof of the occurrence of that particular event.

7. Training and Exercises

- Regular training: Teach your employees on what to do and what not to do in the event of an incident, security issues and precautions.
- Tabletop exercises: Use simulation of incidents to enhance on the element, strength, and weakness of an incident handling team.
- Simulations: Select simulated scenarios in order to practice how to ‘live’ in response to such real life situations.

8. Documentation

- Incident Response Plan: And it is a detailed incident response plan this is dynamic document.
- System hardening report: Explain various activities that have been taken to improve the strength with which the system can withstand certain susceptibilities.
- Secure architecture report: To reduce attack surface and overall organisational risk levels where necessary, the security architecture architecture who will design and implement the security architecture.
- Incident reports: Each event described in the attack details, response action, and lessons learned at the end of the questionnaire.

9. Review and Updates

- Regular review: Incident response plan must be at least annually reviewed and updated if changes were made in technology, threats or regulations.
- Post-incident analysis: Make use of post incident analysis to see where things can go wrong.
- Continuous improvement: Review and refine the plan, to see how it further progresses and to learn its capacity and strength to become more of relevant to the changing threats

10. Appendix

- Contact list: List of key people involved in incident response and their resume.
- Relevant policies and procedures: Its links to the other related security policies and procedures.
- Tools and resources: Tools actionable for an incident and resources for it.

Week 3: Simulated Incident and Response

Ransomware Report using Splunk

1. Introduction

In this lab, a ransomware attack was explored and how data analytics tools like Splunk were used to investigate the activities related to this attack. The objective of the report is to document the steps taken during the lab, including detection, containment, removal, and recovery.

2. Objectives

- Attack detection: Using Splunk to detect ransomware activities.
- Data analysis: Analyzing logs and data to determine the nature and extent of the attack.
- Documentation: Documenting the steps taken and how the incident response plan was implemented.

3. Tools used

- Splunk: A tool for data analysis and extracting information from logs.

4. Scenario

A customer sent an email asking for an analyst to investigate the events that occurred on Keegan's machine on **Monday, May 16th, 2022**. The client noted that **the machine** is operational, but some files have a weird file extension. The client is worried that there was a ransomware attempt on Keegan's device.

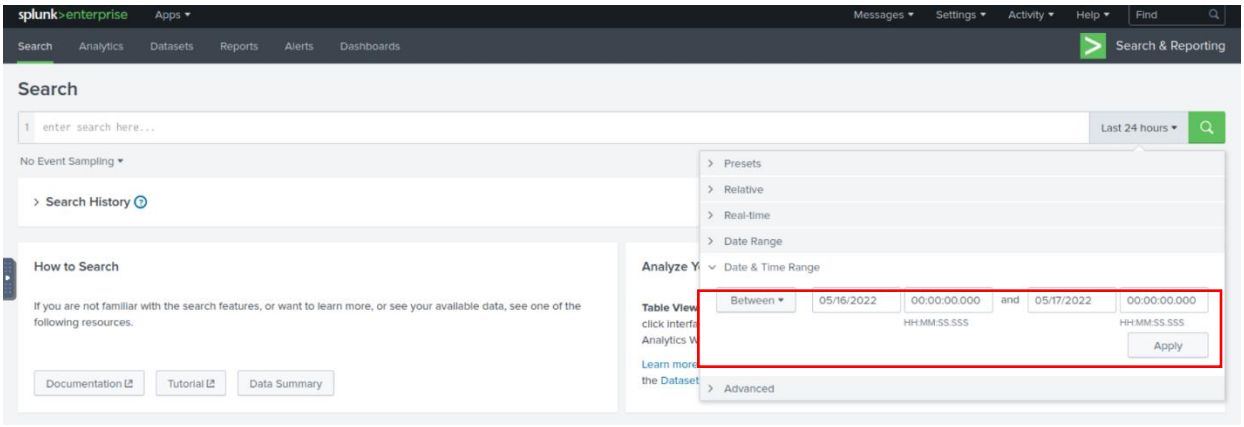
5. Steps followed

5.1. Attack detection

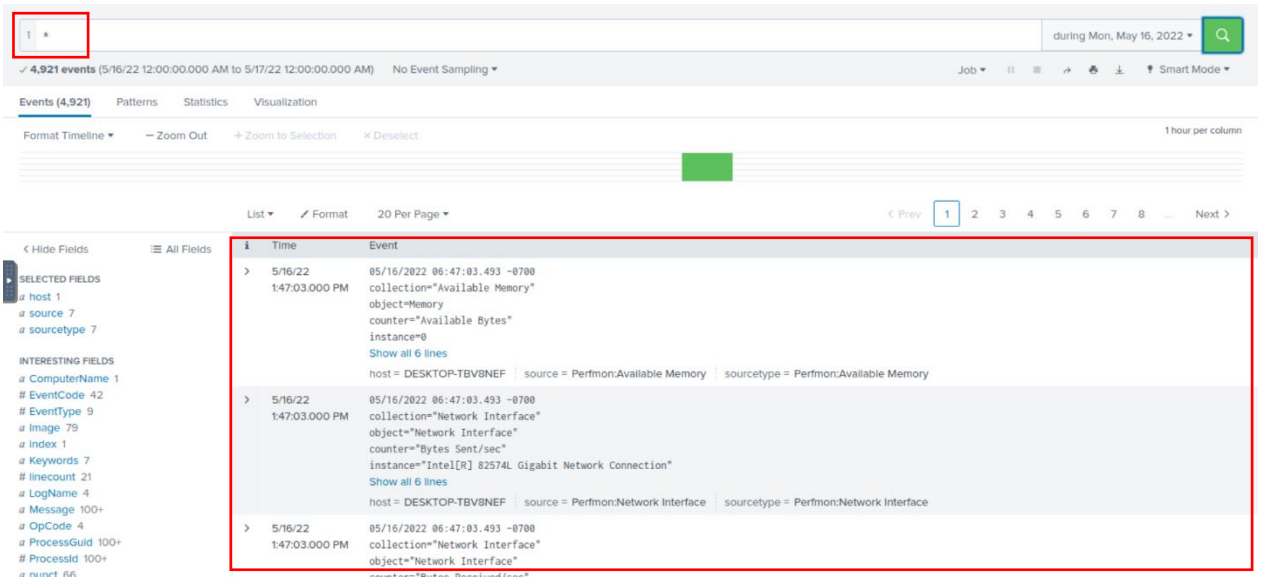
Splunk login: Logged into Splunk platform to access logs.

Search: Splunk search queries were used to identify suspicious activities related to the ransomware attack.

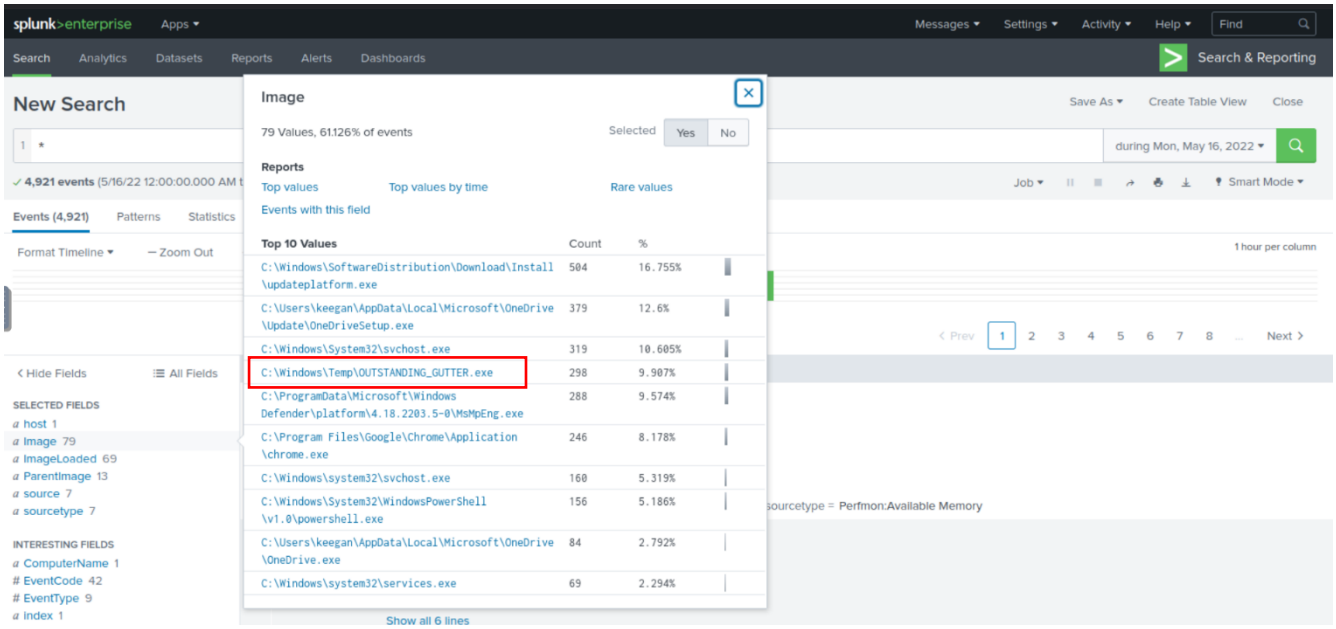
1. Determine the time the incident occurred.



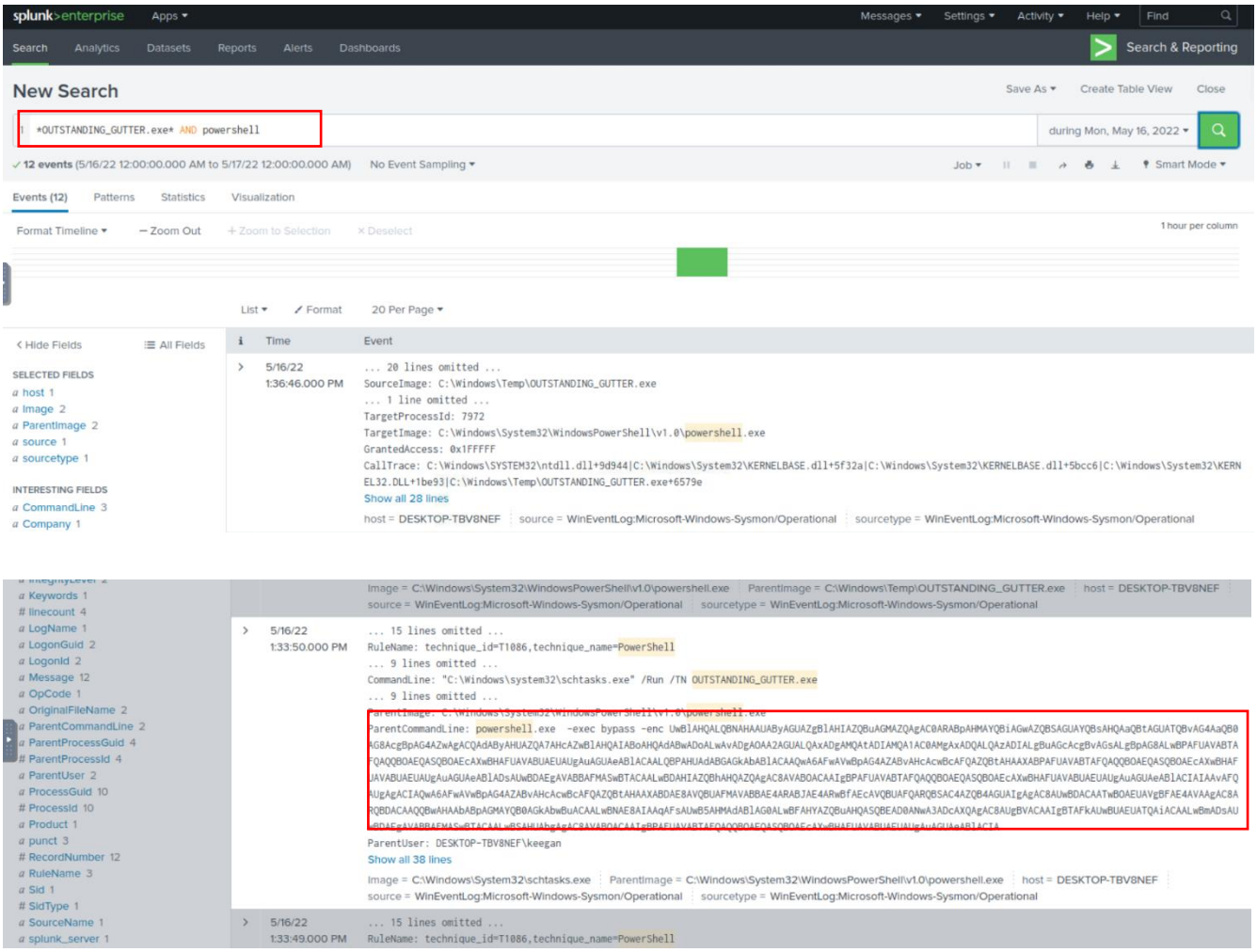
2. Find all events on that day



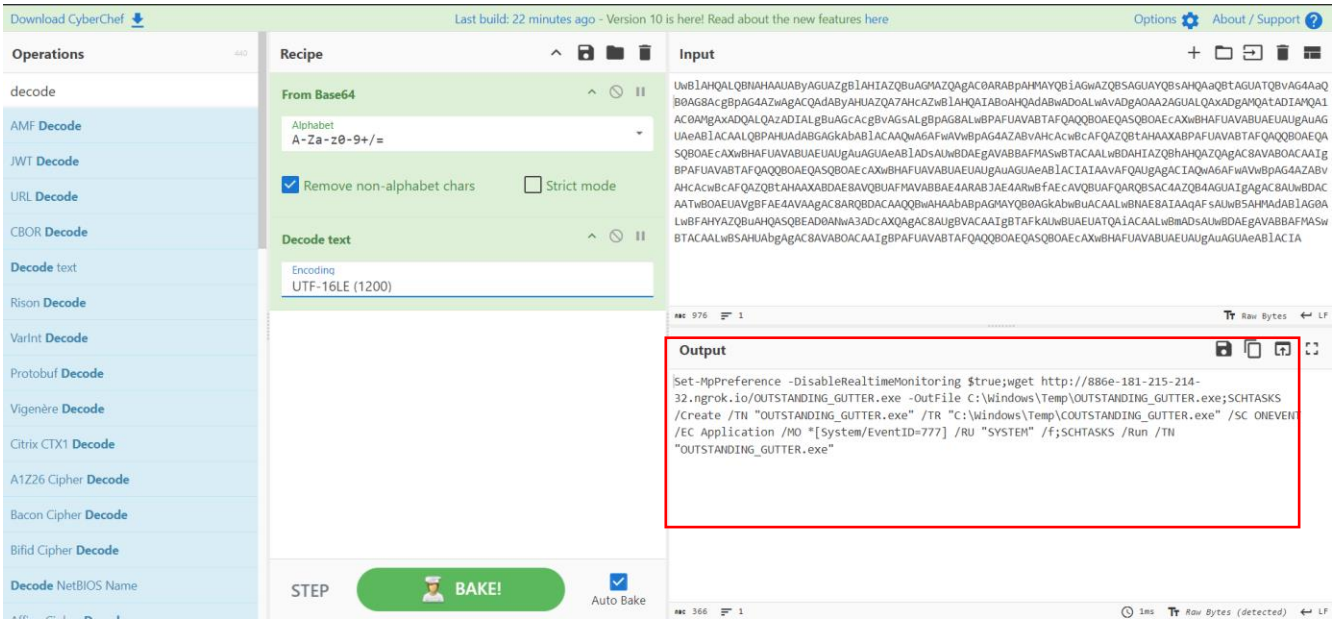
3. Search for suspicious binary file



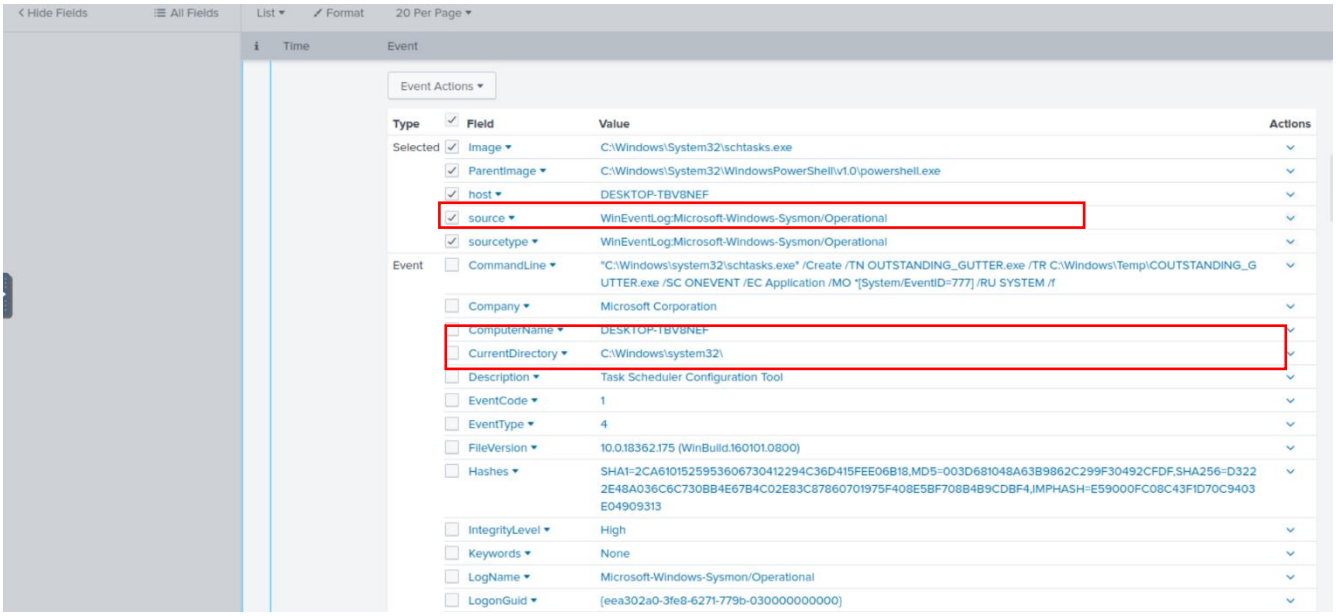
4. The address where the file was downloaded



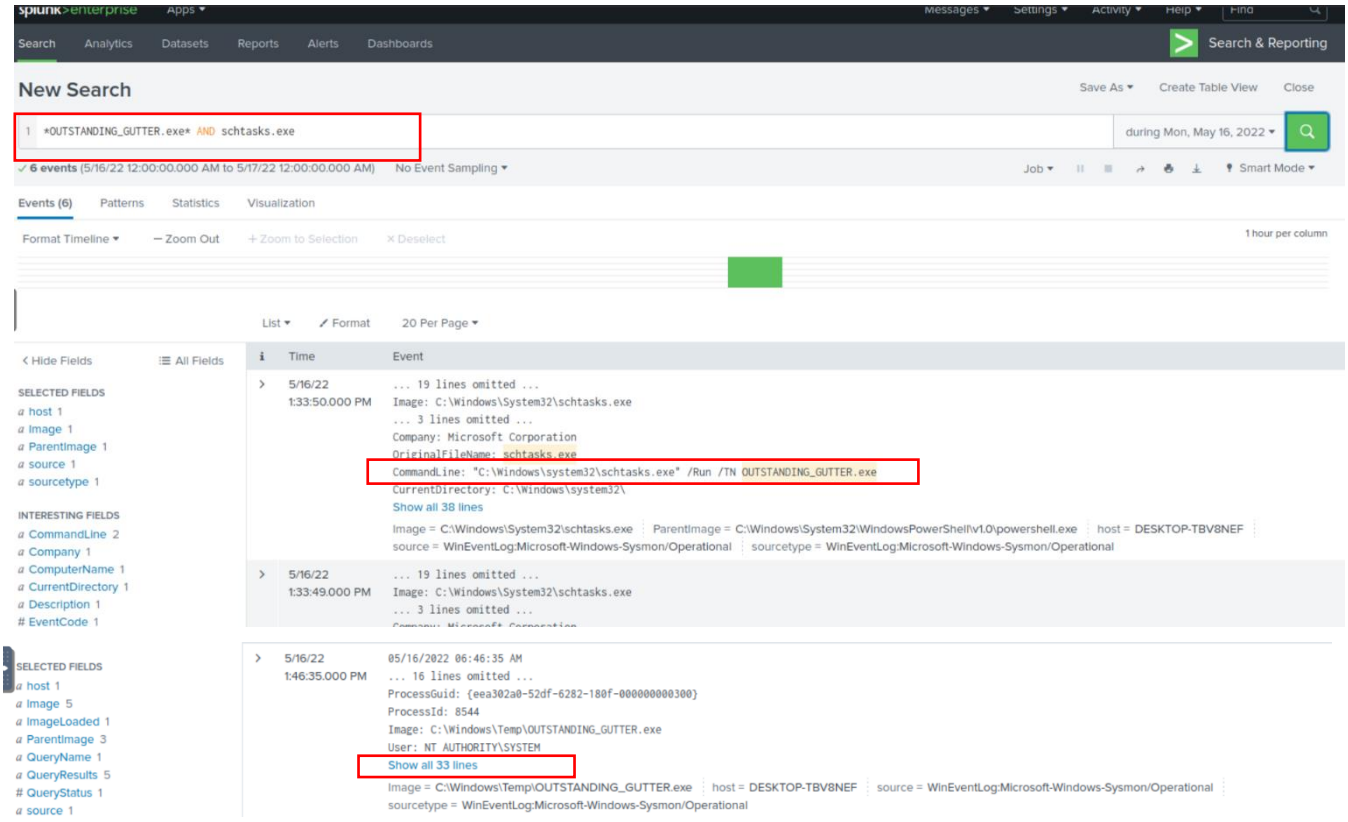
5. Cyberchef was used for encryption



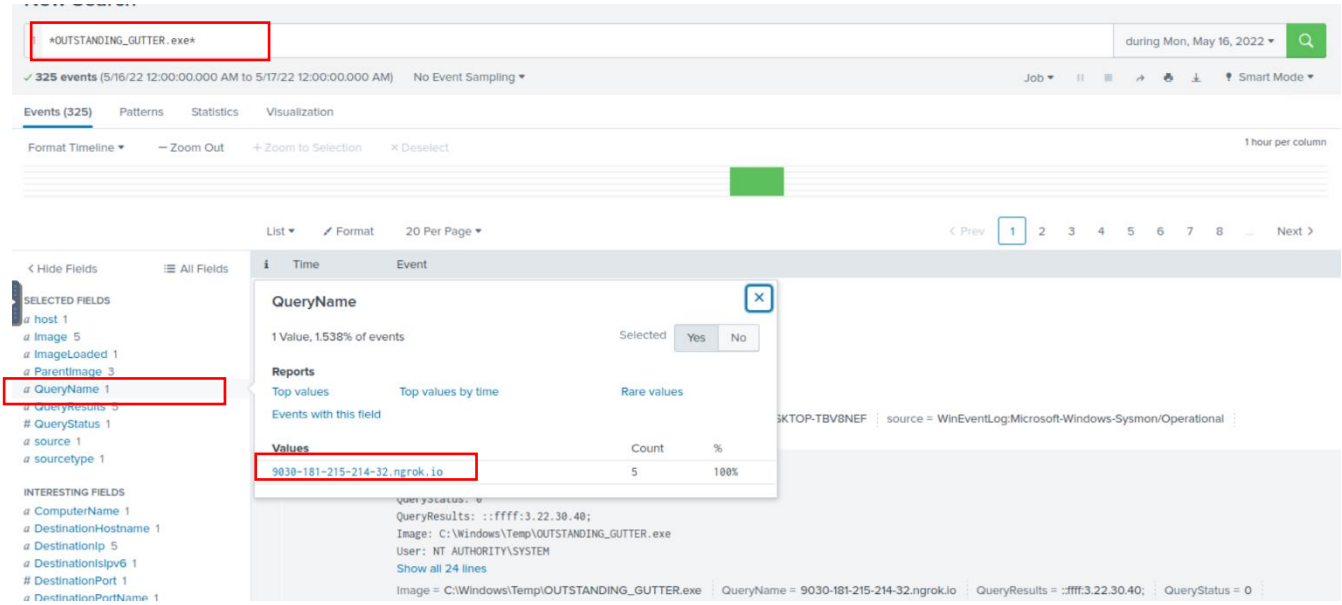
6. Find the Windows executable file that was used to download the file. And What command was executed to configure the suspicious binary to run with elevated privileges?



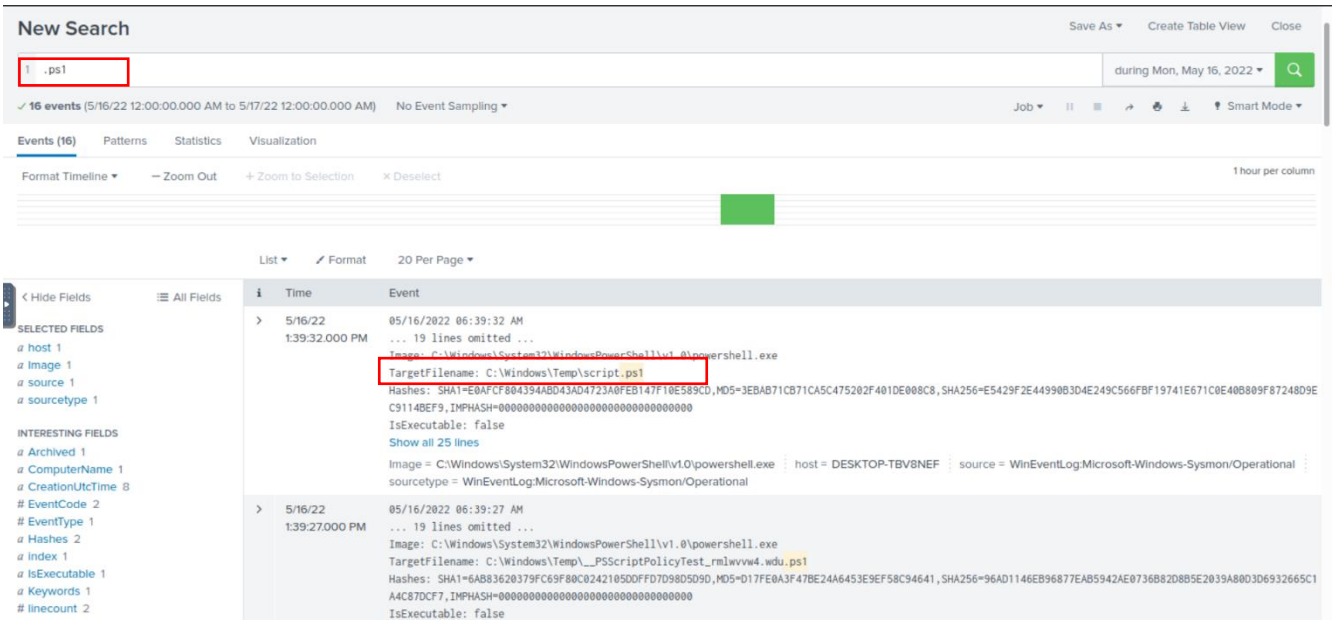
7. The permissions under which the suspicious binary will be run and the command to run the binary with elevated privileges.



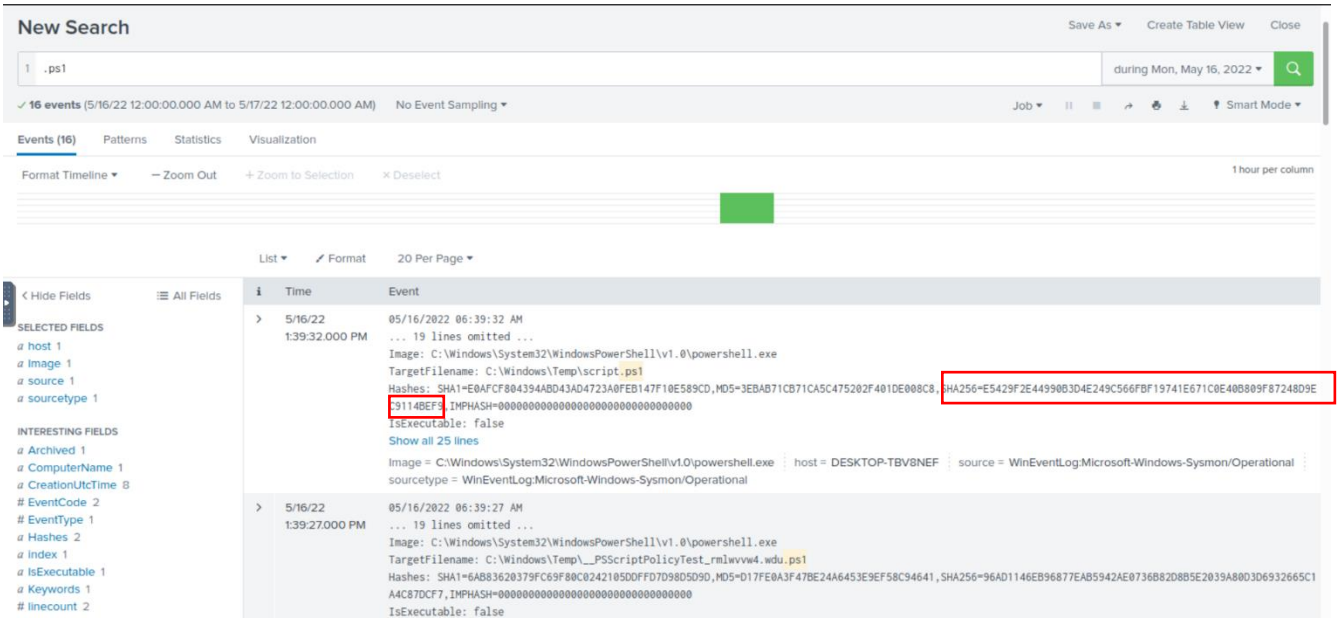
8. The address where the file was connected to the remote server.

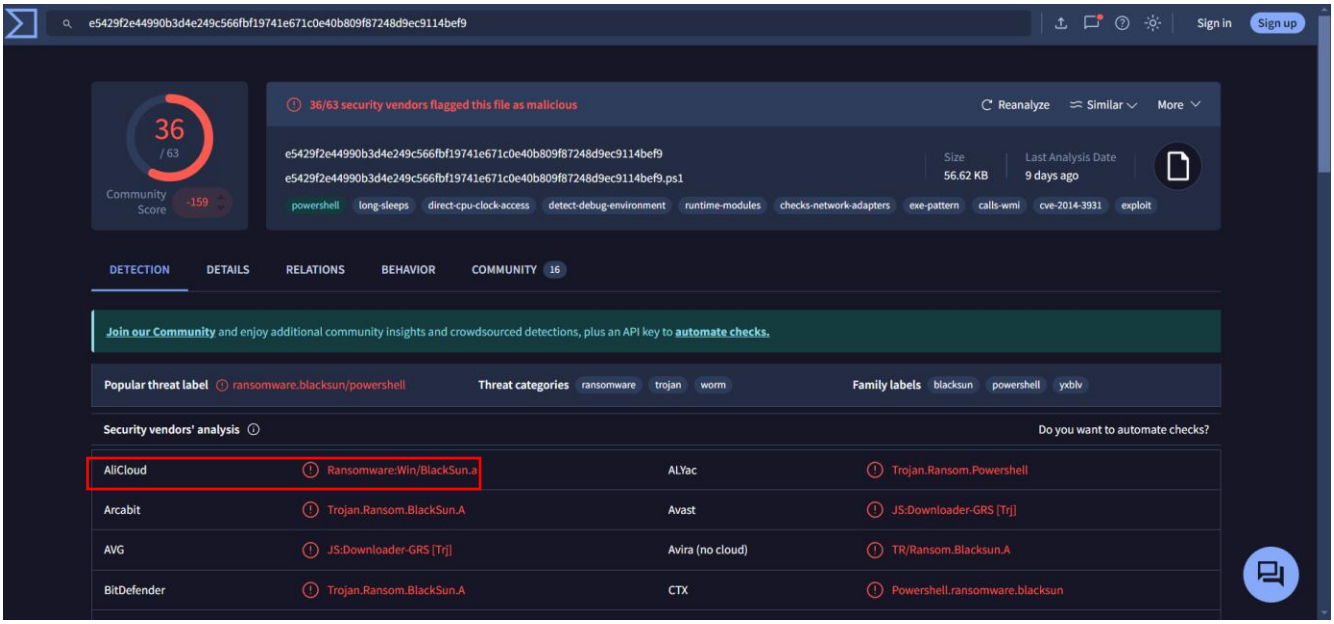


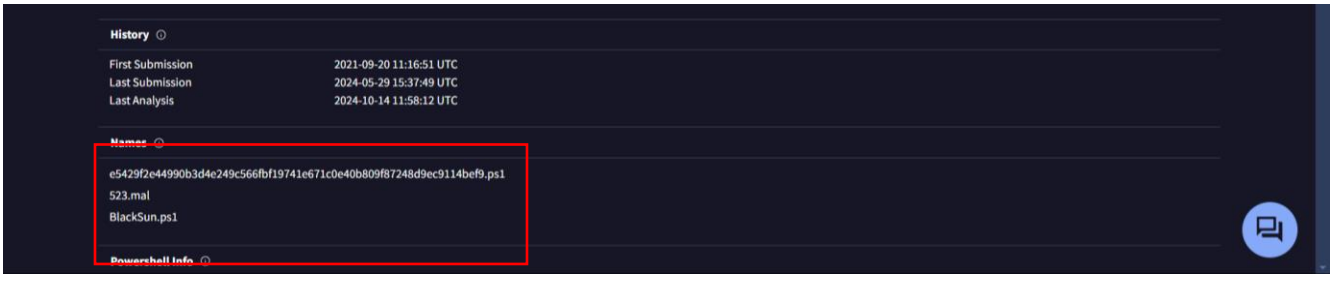
9. The file that the PowerShell script is downloaded to is the same location as the file.



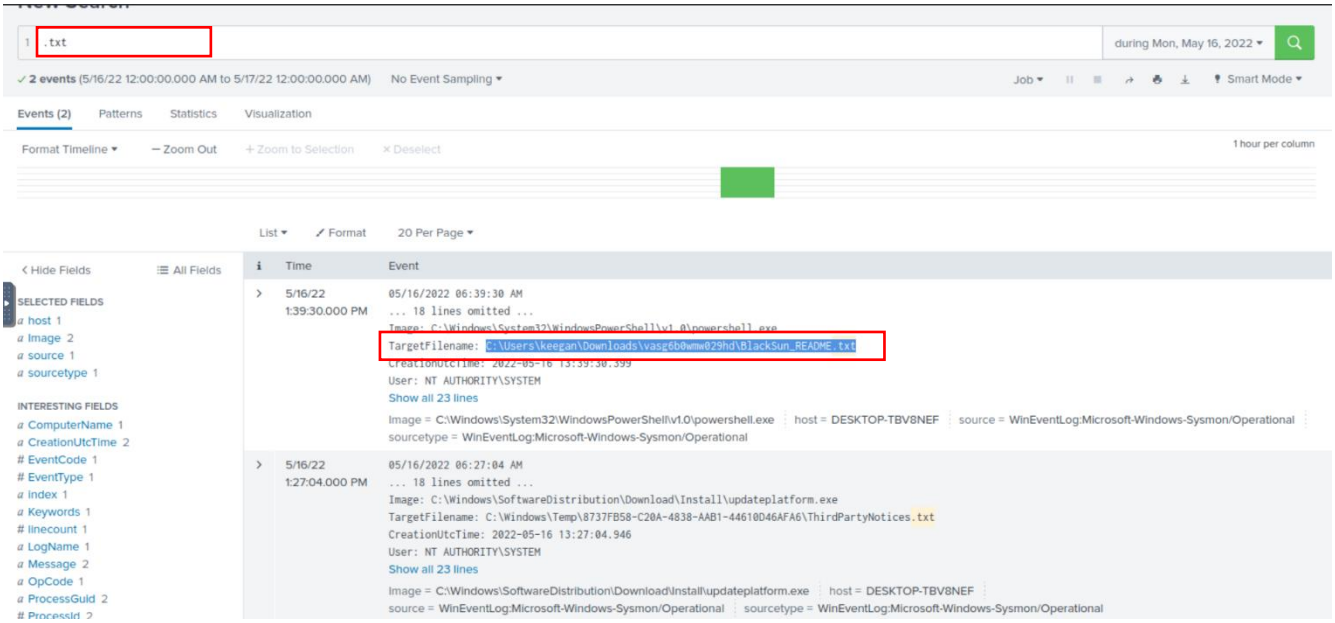
10. The real name of the malicious script was searched for by SHA256 searching on VirusTotal.



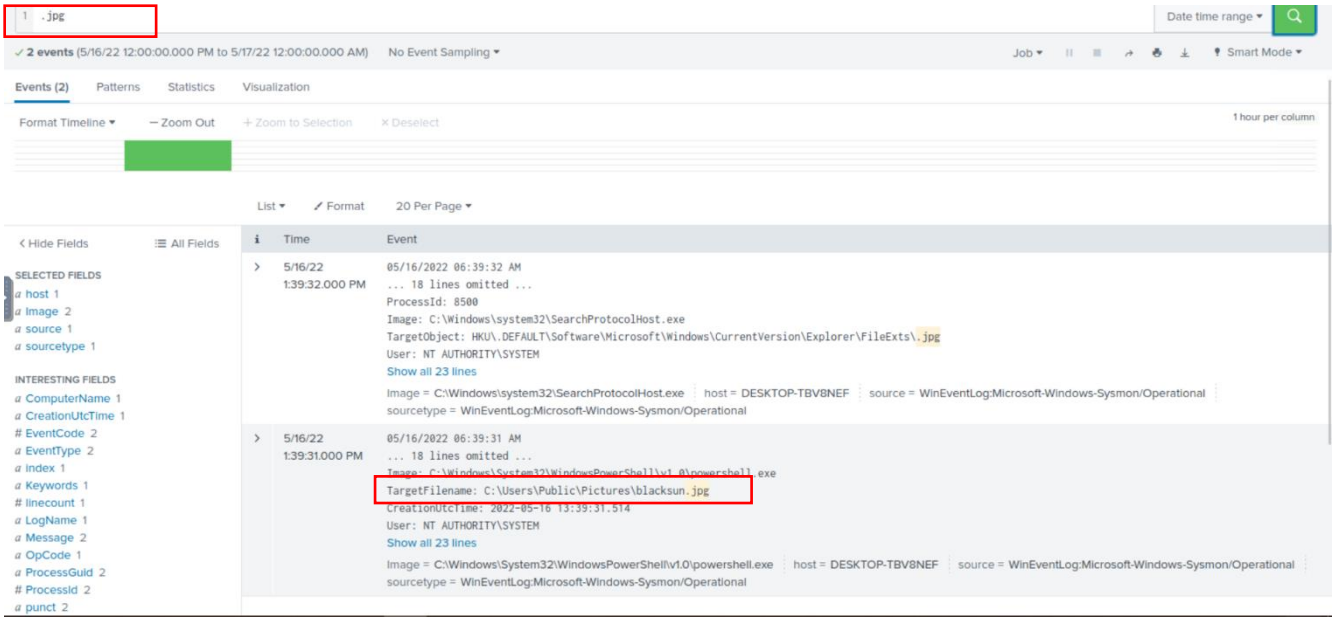




11. Full path to where the ransom note was saved on disk



12. The full path to the image that the attacker would have used to replace the user's desktop wallpaper, which could also serve as an identification card.



6. Containment

6.1. Identifying affected systems

- First, you should identify all systems affected by the attack. Using tools like Splunk, you can examine logs to identify suspicious activity.
- Look for evidence that indicates:
- Files that have started to be encrypted.
- Suspicious processes associated with the encryption.
- Network activity that may indicate communications with the attackers' servers.

6.2. Isolate affected systems

- Once you have identified affected systems, immediately isolate them from the network to prevent the malware from spreading to other systems. This can include:
- Disconnecting the infected systems from the network: Immediately disconnecting any systems connected to the network (Wi-Fi, LAN, etc.).
- Disabling access to shared resources: If the infected systems are accessing shared files or servers, this access should be cut off.

6.3. Stopping suspicious processes

- With Splunk and system analysis tools, you can identify suspicious or malicious processes that are encrypting files or communicating with external servers.
- Use process management tools (such as ProcMon) to stop malicious processes immediately.

6.4. Disable affected accounts

- If the attack targeted specific user accounts or accounts were used to compromise systems, these accounts should be disabled immediately.
- Ensure that passwords are updated and that security protocols such as multi-factor authentication (MFA) are in place to protect accounts.

6.5. Block malicious IP addresses and domains

- Based on the logs analyzed, identify any suspicious IP addresses or domains that the attack is communicating with.
- Using Splunk or a firewall, you can block these addresses and domains to prevent any future communications with the attacker's servers.

6.6. Stop the spread of suspicious software

- If the attack was initiated through internal software or tools (such as suspicious email attachments), ensure that any suspicious software or files are prevented from being downloaded and distributed to other systems.

6.7. Notify relevant teams

- Ensure that all relevant security teams are notified of the attack immediately.
- The SOC and IT teams should be aware of the situation so that they can take action quickly.

6.8. Coordination with external parties (if necessary)

- If the company works with external vendors or technology service providers, it may be necessary to coordinate with them to stop suspicious operations on shared systems or networks.

6.9. Effective internal communication

- It is important to maintain an internal line of communication with all stakeholders in the organization to ensure that everyone is aware of the attack, which systems have been isolated, and what actions have been taken.

6.10. Activate a contingency plan

- You may need to activate contingency plans to ensure business continuity while the attack is contained. These plans may include:
- Using backup copies of affected systems.
- Driving operations to alternate sites or systems.

7. Eradication

7.1. Confirm Ransomware Identification:

- In Splunk, use the analyzed logs to identify the source of the malware such as:
- Suspicious files uploaded or executed.
- Encryption-related activities.
- Malicious IP addresses or domains.

7.2.Isolate the affected systems:

- Ensure that the affected systems are completely isolated from the network to prevent the ransomware from spreading to other devices or files.

7.3.Remove the malware:

- Use antivirus tools or advanced antimalware solutions (such as Malwarebytes or Kaspersky) to completely remove the ransomware.
- If the ransomware is detected by Splunk and has access to the infected systems, you can use local tools on those systems to remove the malicious files.

7.4.Ensure the system is clean:

- Rescan the systems using multiple tools to verify that all malware has been removed.
- Ensure that there are no abnormal processes or suspicious files.
- You can use tools such as ProcMon and TCPView to ensure that there is no hidden activity on the system.

8.Recovery

8.1. Restore files and systems from backups:

- If data is encrypted: Restore uninfected backups from servers or cloud storage devices.
- Make sure that the backups you are restoring from have not been affected by ransomware. It is a good idea to check them first before restoring.

8.2. Reformat infected systems (if necessary):

- If the infected system is beyond repair or if you suspect that the malware is still present, it is best to completely re-format the system and install the software again.

8.3. Fix vulnerabilities:

- Update all software and systems with the latest security updates.
- Make sure that any vulnerabilities exploited by the attacker are closed.
- Implement security policies such as enabling firewalls and access control settings.

8.4. Monitor systems after restoration:

- After restoring systems and data, systems should be carefully monitored to ensure that malicious activity does not recur.
- You can use tools such as Splunk to continue monitoring the network and system logs.
- Implement future security policies:

8.5. Implement strict security protocols such as:

- MFA (Multi-Factor Authentication).
- Encrypt data.
- Update software regularly. Train employees on how to recognize suspicious emails or phishing attempts.