CRIMINAL IP ADDRESS

- **87.98.225.65**

JANUARY 13, 2025

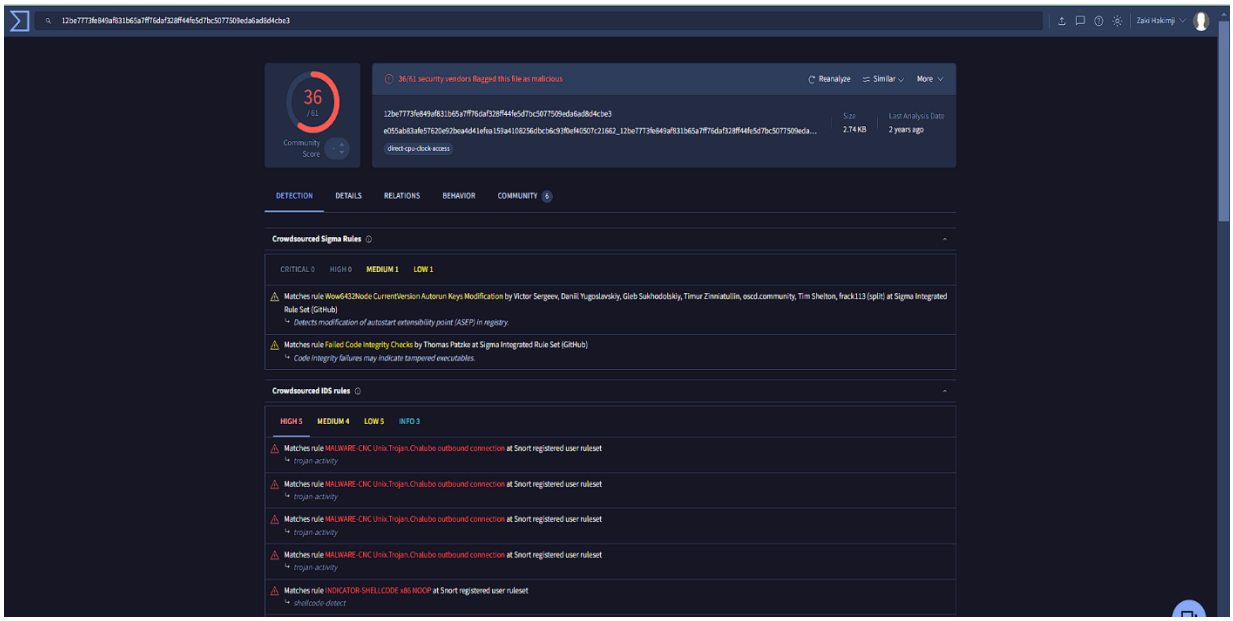
PREPARED BY: ZAKI HAKIMJI

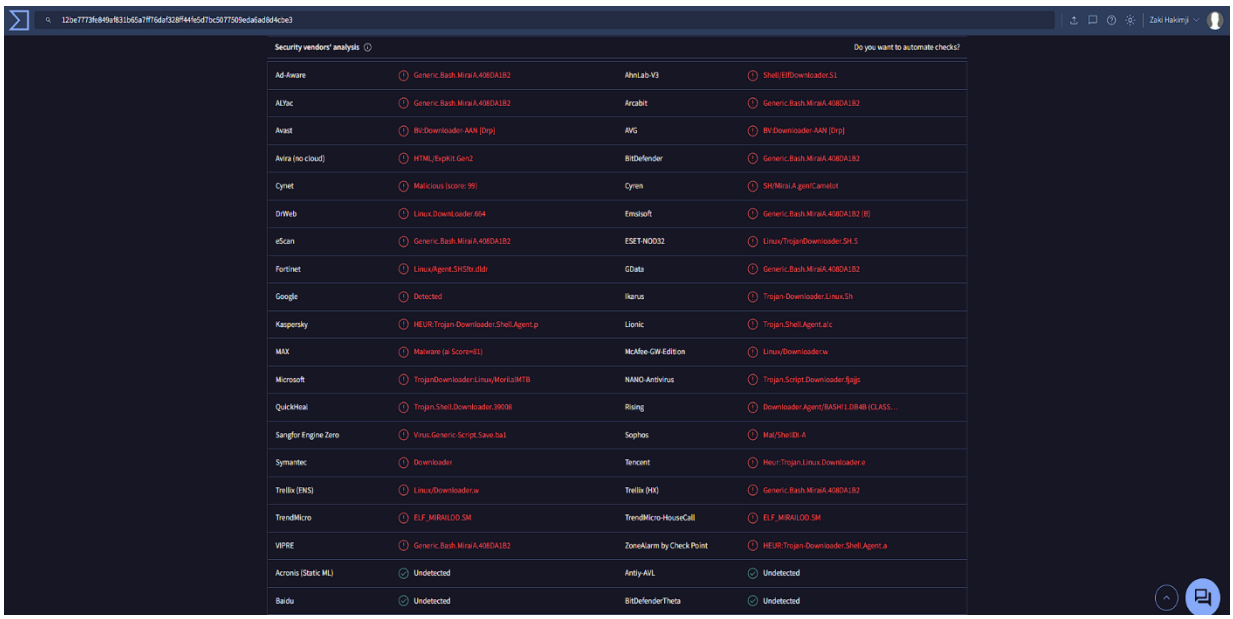
Table of Contents:

1.Incident Summary

Hash file: (12be77f3fe49af831b65a7ff7cdaf32ff44fe5d7bc5077509eda6ad8d4cbeb3), has been flagged as potentially malicious by 36 out of 61 security vendors. The report includes details on matched Sigma and IDS rules, suggesting suspicious behaviours such as modifications to autorun registry keys and code integrity violations. Additionally, IDS rules highlight trojan-related activity and possible outbound connections to command-and-control (CNC) servers, indicative of malware or shellcode activity.

Highlighting detection results from various security vendors. Out of the listed vendors, many flagged the file as malicious with identifiers such as "**Generic. Bash. Mirai.A408DAB2**," "Trojan-Downloader," and "Linux/Agent.SHStr.dldr." These names suggest the file exhibits characteristics of malware, including behaviour commonly associated with trojans, shell agents, and downloaders. A few vendors, such as Acronis and Baidu, reported the file as "Undetected," indicating they did not recognize it as malicious. The high level of consensus among prominent antivirus engines reinforces the likelihood of the file being a security threat.





2. Threat Assessment

- **Sigma Rules:**

1. **Autorun Keys Modification:** A registry change in the Wow6432Node CurrentVersion suggests an attempt to establish persistence through an autostart extensibility point (ASEP).
2. **Code Integrity Failures:** Matched rules indicate potential tampering with executable files, which is a common tactic to evade detection or escalate privileges.

- **IDS Rules:**

1. **Shellcode Detected:** A match to INDICATOR-SHELLCODE x86 NOOP suggests the presence of malicious shellcode, often used in exploits.
2. **Malware Command-and-Control (CNC):** Several matches for Unix.Trojan.Chalubo outbound connections, which indicates the file may attempt to communicate with a remote CNC server, a key component of trojans or botnets.
3. **Suspicious Network Indicators:**

3.1 Matches for IPs with poor reputations and known hostile traffic groups point to connections to potentially malicious hosts.

3.2 A match for a compromised curl User-Agent outbound attempt indicates potential data exfiltration or reconnaissance.

Unix.Trojan.Chalubo

Contacted URLs (18)

Scanned	Detections	Status	URL
?	?	-	http://192.168.1.15:51793/UD/?9
2024-11-02	13 / 96	-	http://46.19.141.122/bins/mips
2024-11-02	12 / 96	-	http://46.19.141.122/bins/x86
2024-12-23	0 / 96	200	http://init-p01st.push.apple.com/bag
2023-03-20	12 / 92	200	http://46.19.141.122/bins/sh4
2023-03-20	13 / 92	404	http://46.19.141.122/bins/x86_64
2023-03-20	13 / 92	200	http://46.19.141.122/bins/i486
2023-03-20	12 / 92	404	http://46.19.141.122/bins/m68k
?	?	-	http://192.168.1.15:51794/UD/?9
2022-11-01	22 / 90	200	http://46.19.141.122/bins/mpsl

3.Attack Analysis

- **Identify Relevant TTPs**:

1. Cross-reference the observed behaviours from the incident (e.g., malware activity, lateral movement, data exfiltration) with the MITRE ATT&CK matrix categories.
2. Match the detected activities to the tactics (Reconnaissance, Initial Access, Execution, etc.) and techniques in the matrix.

- **Document the Incident Timeline**: Include when each phase of the attack occurred, based on logs and alerts (e.g., initial compromise, privilege escalation, etc.).
- **Include Indicators of Compromise (IOCs)**: Highlight IOCs such as IP addresses, file hashes, domains, or specific malware signatures that were used.
- **Analyse Adversary Goals**: Discuss what the attacker might have intended to achieve based on the data accessed or systems targeted (e.g., financial gain, espionage, disruption).
- **Mitigation Recommendations**: List countermeasures for each identified technique (e.g., enabling multi-factor authentication for "Valid Accounts" under Initial Access).

Mitre Att&ck Matrix

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Gather Victim Identity Information	Scripting	Valid Accounts	Windows Management Instrumentation	Scripting	DLL Side-Loading	Disable or Modify Tools	OS Credential Dumping	File and Directory Discovery	Remote Services	Archive Collected Data	Ingress Tool Transfer
Credentials	Domains	Default Accounts	Command and Scripting Interpreter	DLL Side-Loading	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	LSASS Memory	System Information Discovery	Remote Desktop Protocol	Data from Local System	Encrypted Channel
Email Addresses	DNS Server	Domain Accounts	Scheduled Task/Job	Scheduled Task/Job	Process Injection	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Screen Capture	Non-Standard Port
Employee Names	Virtual Private Server	Local Accounts	PowerShell	Registry Run Keys / Startup Folder	Scheduled Task/Job	Software Packing	NTDS	Security Software Discovery	Distributed Component Object Model	Clipboard Data	Remote Access Software
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Registry Run Keys / Startup Folder	Timestomp	LSA Secrets	Process Discovery	SSH	Keylogging	Multi-hop Proxy
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	DLL Side-Loading	Cached Domain Credentials	Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Non-Application Layer Protocol
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	Extra Window Memory Injection	DCSync	Application Window Discovery	Windows Remote Management	Web Portal Capture	Application Layer Protocol
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Masquerading	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Proxy
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	Process Injection	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols

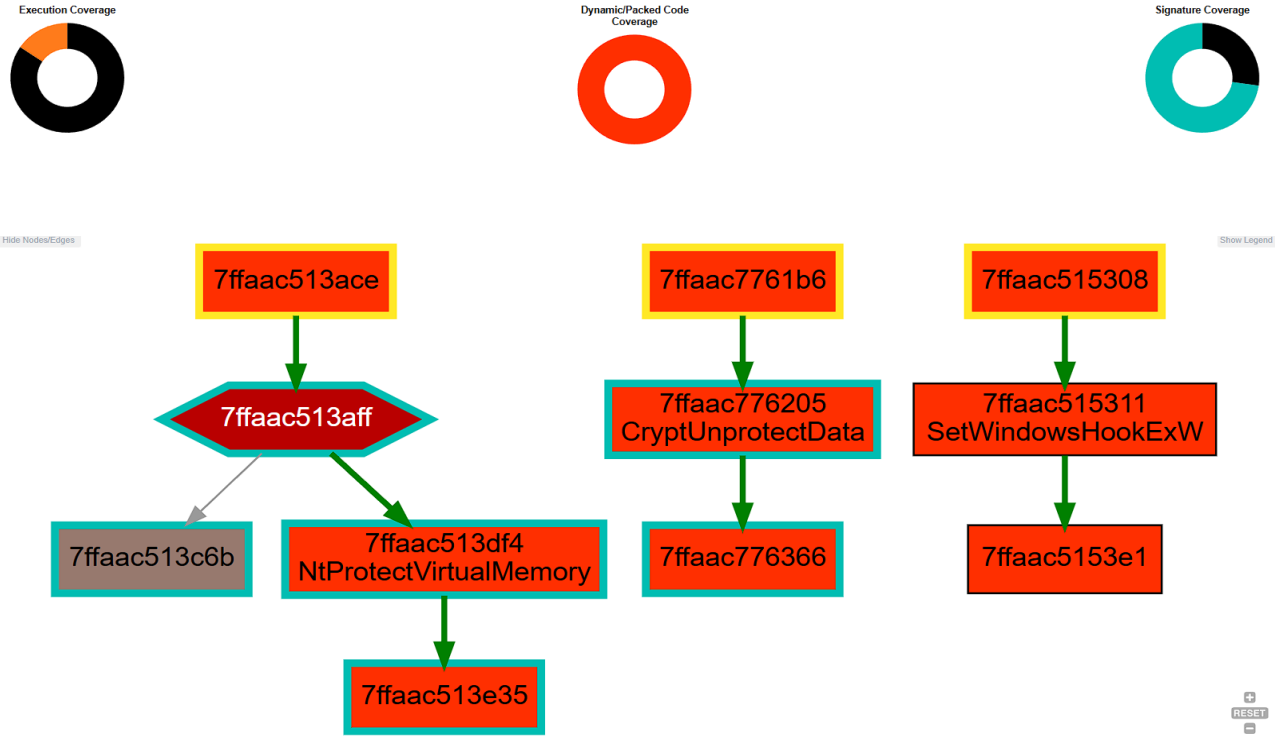
Signatures

- Antivirus / Scanner detection for submitted sam...
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Attempt to bypass Chrome Application-Bound E...
- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE hea...
- Found malware configuration
- Malicious sample detected (through community ...
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Suricata IDS alerts for network traffic
- Yara detected Amadey
- Yara detected Amadeys stealer DLL
- Yara detected Babadeda
- Yara detected BrowserPasswordDump
- Yara detected DanaBot stealer dll
- Yara detected Keylogger Generic

4.Security Analysis and Detection

➢ Highlighted Nodes

1. **Each node represents a memory address or function, such as:**
   - **NtProtectVirtualMemory**: Often used to modify memory protection in processes, which can be a sign of injection or exploitation techniques.
   - **CryptUnprotectData**: Decrypts data protected by the Windows Data Protection API, which could indicate access to sensitive data like credentials.
   - **SetWindowsHookExW**: Can set a global hook to intercept system events, often misused for keylogging or spying activities.
2. **Colour Coding and Shapes:**
   - The colours (red, orange, and others) likely indicate the severity or categorization of nodes (e.g., suspicious, benign, or unknown).
   - Arrow directions show the flow or dependencies, where one call leads to another.
3. **Purpose for Report:**
   - This graph can provide insight into a malicious chain of events or functions.
   - Highlight connections between functions that could indicate malicious intent (e.g., decrypting sensitive data and injecting memory).
   - Document the sequence for Incident Response or Threat Intelligence.



5.Malware

Malware often uses malicious files and suspicious IP addresses to carry out its activities. Malicious files typically include executable files, scripts, or documents embedded with harmful code. These files are designed to exploit vulnerabilities, execute unauthorized actions, or provide backdoor access to the attacker. For instance, malware may use obfuscated code or packers to evade detection by security software. Files containing exploits may inject malicious payloads into legitimate processes, as seen in the use of APIs like NtProtectVirtualMemory for altering memory protections or SetWindowsHookExW for intercepting user inputs.

- **AV Detection**

  1. Multiple antivirus engines detected the file as malicious.

  2. The file contains identifiable malware configuration, confirming its malicious intent.

  3. Yara rules flagged the file as associated with Remcos RAT, a Remote Access Trojan often used for espionage, credential theft, and e-banking fraud.

  4. AI and machine learning systems identified the sample as suspicious.

- **Networking:** Suricata Intrusion Detection System (IDS) flagged suspicious network traffic generated by the file.
- **Remote Access Functionality:** This indicates the device might be compromised, allowing remote access to an attacker.
- **Phishing:** This means that the system has detected a potential phishing attempt. Phishing attacks try to trick you into revealing sensitive information like passwords or credit card numbers
- **Stealing of Sensitive Information:**
  1. Yara: This refers to a tool used to identify malware based on specific patterns.
  2. Bdaejec and RisePro Stealer**:** These are likely the names of the detected malware strains
- **Key, Mouse, Clipboard, Microphone and Screen Capturing**: This indicates that the detected malware might be capable of recording your keystrokes, mouse movements, clipboard content, microphone input, and screen activity.
- **HIPS/PFW/Operating System Protection Evasion:** This category refers to malware or techniques that try to avoid detection by security software or the operating system itself

Stealing of Sensitive Information

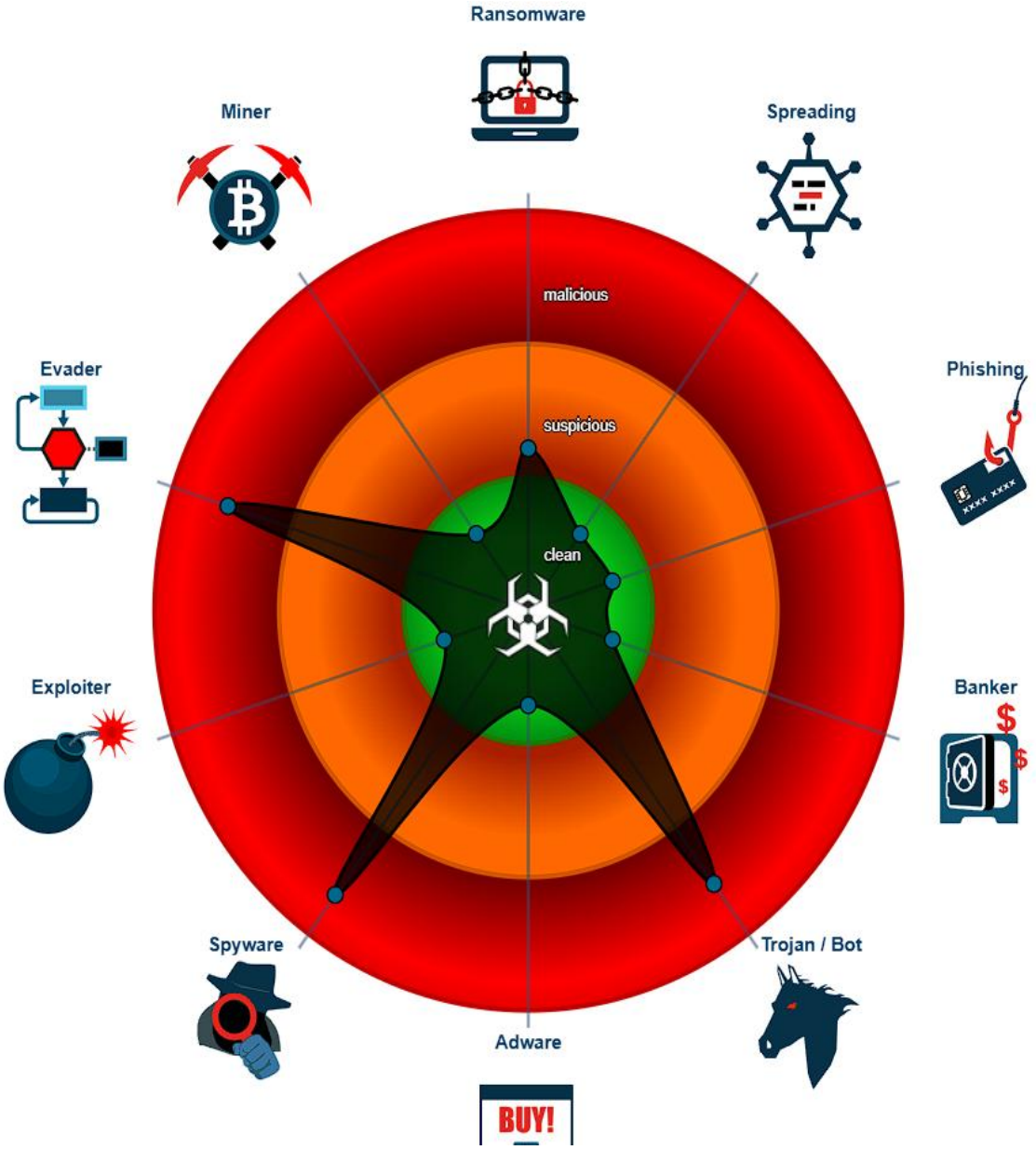
- Yara detected Amadey
- Yara detected Amadeys stealer DLL
- Yara detected BrowserPasswordDump
- Yara detected DanaBot stealer dll
- Yara detected LummaC Stealer
- Yara detected Poverty Stealer
- Yara detected PureLog Stealer
- Yara detected StormKitty Stealer
- Yara detected Vidar stealer

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Yara detected Keylogger Generic
- Yara detected VenomRAT

HIPS / PFW / Operating System Protection Evasion

- Sigma detected: Drops fake system file at system root drive



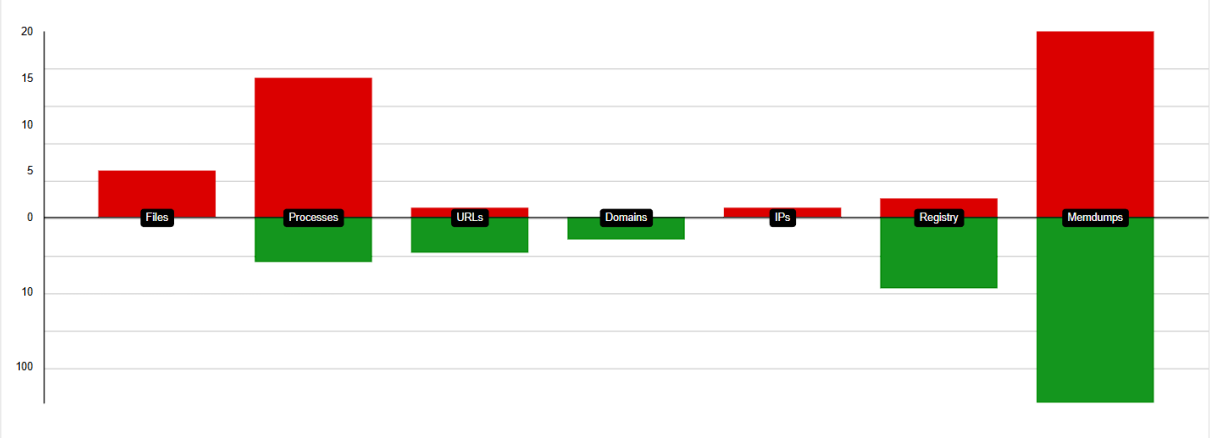
6. Indicators of Compromise (IOCs)

The report appears to be a visual representation of Indicators of Compromise (IOCs) related to a specific file, **DB5rQYsfd6.exe**. IOCs are artifacts or data points that can be used to detect the presence of malicious activity on a system or network.

- **File:** The report shows a significant number of IOCs associated with the file itself (represented by the red bar). This suggests that the file is likely malicious or has been compromised.
- **Processes:** There are a moderate number of IOCs related to processes. This could indicate that the file is actively executing or interacting with other processes on the system.
- **URLs and Domains:** The number of IOCs associated with URLs and domains is relatively low. This might suggest that the file is not actively communicating with external servers or downloading additional components.
- **Registry:** The number of IOCs related to the registry is also low. This suggests that the file may not be making extensive modifications to system settings.
- **Memory Dumps:** There are a significant number of IOCs related to memory dumps. This could indicate that the file is actively loading malicious code into memory or attempting to evade detection by security tools.

IOC Report

DB5rQYsfd6.exe



Files

File Path	Type	Category	Malicious	Download
DB5rQYsfd6.exe	PE32 executable (GUI) Intel 80386, for MS Windows	initial sample		
C:\ProgramData\GoogleDat\GoogleUpdate.exe	PE32 executable (GUI) Intel 80386, for MS Windows	dropped		
C:\ProgramData\GoogleDat\GoogleUpdate.exe:Zo…	ASCII text, with CRLF line terminators	dropped		
C:\ProgramData\bootdata\logs.dat	data	dropped		
C:\Users\user\AppData\Local\Temp\install.vbs	data	modified		

Processes

Path	Cmdline	Malicious
C:\Users\user\Desktop\DB5rQYsfd6.exe	"C:\Users\user\Desktop\DB5rQYsfd6.exe"	
C:\Windows\SysWOW64\cmd.exe	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\S…	
C:\Windows\SysWOW64\reg.exe	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\S…	
C:\Windows\SysWOW64\wscript.exe	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\install.vbs"	
C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c "C:\ProgramData\GoogleDat\GoogleUpdate.exe"	
C:\ProgramData\GoogleDat\GoogleUpdate.exe	C:\ProgramData\GoogleDat\GoogleUpdate.exe	
C:\Windows\SysWOW64\cmd.exe	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\S…	
C:\Windows\SysWOW64\svchost.exe	svchost.exe	
C:\Windows\SysWOW64\reg.exe	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\S…	
C:\ProgramData\GoogleDat\GoogleUpdate.exe	"C:\ProgramData\GoogleDat\GoogleUpdate.exe"	

URLs

Name	IP	Malicious
apleegodfivem.ddns.net		
http://geoplugin.net/json.gp	unknown	
http://geoplugin.net/json.gp/C	unknown	

IPs

IP	Domain	Country	Malicious
198.50.242.157	unknown	Canada	

Registry

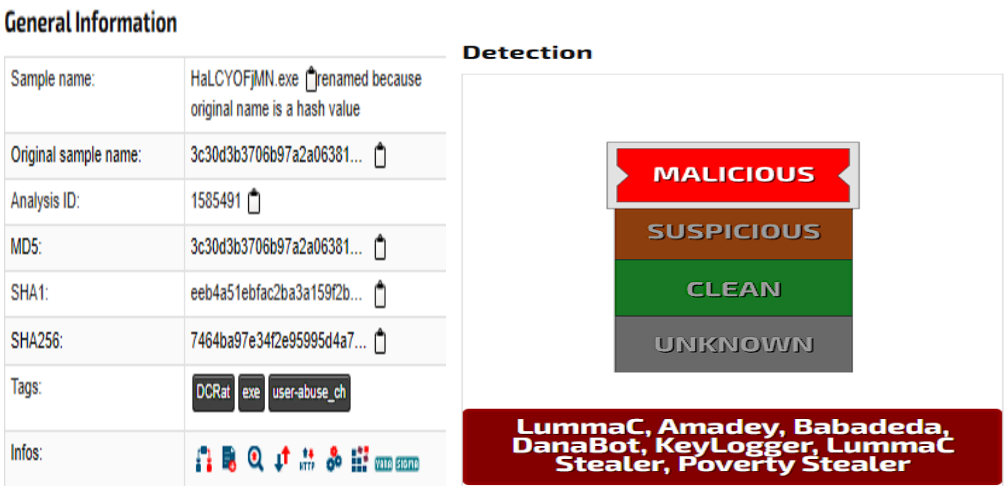
Path	Value	Malicious
HKEY_LOCAL_MACHINE\SOFTWARE\Microsof…	ChromeUpdater	
HKEY_LOCAL_MACHINE\SOFTWARE\Microsof…	EnableLUA	
HKEY_CURRENT_USER\SOFTWARE\Microsoft…	ChromeUpdater	

Memdumps

Base Address	Regiontype	Protect	Malicious
456000	unkown	page readonly	
456000	unkown	page readonly	
456000	unkown	page readonly	
3230000	heap	page read and write	
456000	unkown	page readonly	
68D000	heap	page read and write	
456000	unkown	page readonly	
456000	unkown	page readonly	
456000	unkown	page readonly	
456000	unkown	page readonly	

7. Impact Assessment

- **Data Theft**: If the file is a data stealer, it could potentially steal sensitive information such as:
  - Credentials: Login credentials for various accounts (e.g., email, social media, banking, etc.)
  - Financial Data: Credit card numbers, bank account details, cryptocurrency wallets, etc.
  - Personal Information: Personally Identifiable Information (PII) like names, addresses, phone numbers, etc.
- **System Compromise**: The file could compromise the system's integrity by:
  - Installing Backdoors: Creating entry points for attackers to gain remote access and control over the system.
  - Disabling Security Features: Disabling antivirus, firewall, and other security mechanisms.
  - Modifying System Settings: Changing critical system settings to facilitate malicious activity.
- **Data Destruction**: The file might be designed to:
  - Delete or Encrypt Data: Wiping critical files or encrypting data and demanding a ransom (ransomware).
  - Disrupt System Operations: Causing system crashes, slowdowns, or instability.
- **Data Exfiltration**: The file could exfiltrate sensitive data from the system to a remote location controlled by the attacker. This could include:
  - Sending data over the network: Exfiltrating data through various channels like email, file transfer protocols, etc.
  - Storing data on external storage: Copying data to removable drives or cloud storage.



Process Tree

- System is w10x64
- 2evua791WH.exe (PID: 6240 cmdline: "C:\Users\user\Desktop\2evua791WH.exe" MD5: 3F390F2A4F32D4EC988F79A6A4A3B97B)
  - svchost.exe (PID: 4460 cmdline: "C:\Users\user\AppData\Local\Temp\svchost.exe" MD5: 3F390F2A4F32D4EC988F79A6A4A3B97B)
    - netsh.exe (PID: 5164 cmdline: netsh firewall add allowedprogram "C:\Users\user\AppData\Local\Temp\svchost.exe" "svchost.exe" ENABLE MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
      - conhost.exe (PID: 2520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - taskkill.exe (PID: 5324 cmdline: taskkill /F /IM Exsample.exe MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
      - conhost.exe (PID: 5224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- svchost.exe (PID: 2656 cmdline: "C:\Users\user\AppData\Local\Temp\svchost.exe" .. MD5: 3F390F2A4F32D4EC988F79A6A4A3B97B)
- svchost.exe (PID: 4048 cmdline: "C:\Users\user\AppData\Local\Temp\svchost.exe" .. MD5: 3F390F2A4F32D4EC988F79A6A4A3B97B)
- svchost.exe (PID: 2676 cmdline: "C:\Users\user\AppData\Local\Temp\svchost.exe" .. MD5: 3F390F2A4F32D4EC988F79A6A4A3B97B)
- cleanup

8.Response and Recommendations

1. Immediate Response:

- Isolate the System: Isolate the infected system from the network immediately. This is crucial to prevent the malware from spreading to other systems on the network and to block any communication channels used by the attackers.
- Document the Incident: Start documenting the incident response process. Record all actions taken, observations made, and any relevant information. This documentation will be valuable for future analysis, reporting, and legal investigations.

2. Investigation and Analysis:

- **Conduct a Thorough Investigation:**
  - Analyse the IOCs in detail to understand the malware's behaviour and capabilities.
  - Examine system logs, network traffic, and any other relevant data for clues about the infection and potential damage.
  - **Identify any other compromised systems or accounts.**

3. Remediation and Cleanup:

- **System Cleanup:**
  - Perform a thorough system cleanup, including removing any suspicious files, registry entries, and services.
  - Consider reinstalling the operating system if the infection is severe or difficult to remove.
- **Password Changes:**
  - Change passwords for all accounts that might have been compromised, including email, social media, banking, and any other accounts that used credentials stored on the infected system.
  - Enable multi-factor authentication (MFA) wherever possible to enhance account security.

4. Data Recovery and Restoration:

- Restore from Backups: If available, restore critical data from recent backups.
- Data Recovery Tools: If data loss has occurred, consider using data recovery tools to recover lost files. However, exercise caution to avoid further compromising the system.

5. Continuous Monitoring and Response:

- Monitor System Activity: Continuously monitor system logs and network traffic for any suspicious activity.
- **Conduct Regular Security Audits:** Regularly review security configurations and identify any vulnerabilities.
- **Maintain Incident Response Plan:** Regularly review and update your incident response plan to ensure it is effective and up-to-date.

9.Prevention

1. Strong Security Foundation

- **Antivirus and Anti-malware Software:** Install and maintain up-to-date antivirus and anti-malware software on all devices. Configure them to perform regular scans and updates.

- **Firewall:** Enable and configure a robust firewall (both software and hardware) to monitor and block incoming and outgoing network traffic.
- **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** Consider implementing an IDS/IPS to detect and prevent malicious activity on your network.

2. User Education and Training

- **Security Awareness Training:** Educate users about cybersecurity threats, including phishing attacks, social engineering, and the dangers of clicking on suspicious links or downloading attachments from unknown sources.
- **Safe Browsing Practices:** Encourage users to practice safe browsing habits, such as verifying website authenticity, avoiding suspicious websites, and using strong, unique passwords for each account.

3. Software Updates and Patches

- **Regular Updates:** Keep operating systems, software applications, and firmware updated with the latest security patches and updates. These updates often include critical security fixes that address vulnerabilities exploited by malware.

4. Data Backup and Recovery

- **Regular Backups:** Regularly back up critical data to a secure location (e.g., external hard drive, cloud storage). This will allow you to restore data in case of a malware infection or other data loss incidents.
- **Test Backups:** Regularly test your backup and recovery procedures to ensure they work as expected.

5. Access Control and Least Privilege

- **User Access Controls:** Implement strong access controls to limit user privileges and restrict access to sensitive data and systems.
- **Least Privilege Principle:** Grant users only the necessary privileges to perform their job duties.

6. Network Segmentation:

- **Isolate Critical Systems:** Isolate critical systems and networks to limit the impact of a potential infection.

7. Incident Response Planning:

- **Develop an Incident Response Plan:** Create a comprehensive incident response plan that outlines the steps to be taken in the event of [1] a malware infection or other security incident. This plan should include procedures for containment, investigation, remediation, and recovery.

8. Third-Party Risk Management:

- **Vendor Security Assessments:** Conduct security assessments of third-party vendors and partners to ensure they have adequate security measures in place.

9. Continuous Monitoring and Improvement:

- **Regular Security Audits:** Conduct regular security audits and penetration tests to identify and address vulnerabilities.
- **Security Information and Event Management (SIEM):** Implement a SIEM system to collect and analyse security logs from various sources, allowing you to detect and respond to threats more quickly.
- **Threat Intelligence:** Stay informed about the latest cyber threats and vulnerabilities by monitoring threat intelligence feeds and security advisories.

10.Conclusion

The investigation revealed the presence of a suspicious IP address actively communicating with the infected system, alongside the malicious file "**DB5rQYsfd6.exe**." Analysis of the IOC Report highlighted concerning activity, including the file's interaction with system processes, memory loading behaviour, and potential attempts to establish communication channels.

While a comprehensive analysis would require further investigation, the evidence suggests a potential compromise of the system with potential impacts such as data theft, system disruption, and unauthorized access.

- **Immediate Response:**
  - Isolate the infected system from the network to prevent further spread and data exfiltration.
  - Document all actions taken and observations made during the investigation.
- **Thorough Investigation:**
  - Analyse the suspicious IP address, its communication patterns, and any associated domains or URLs.
  - Deep dive into the malicious file "**DB5rQYsfd6.exe**" to understand its functionality, origins, and potential impact.
  - Examine system logs, network traffic, and other relevant data for evidence of the attack and its scope.
- **Security Enhancements:**
  - Implement and enforce strong password policies, including the use of multi-factor authentication.
  - Educate users on cybersecurity best practices, including recognizing phishing attempts and avoiding suspicious websites.
  - Regularly patch and update operating systems, software, and firmware.
  - Implement and maintain a robust intrusion detection and prevention system (IDS/IPS).
  - Conduct regular security audits and penetration tests to identify and address vulnerabilities.
- **Incident Response Plan:**
  - Review and update the incident response plan based on the lessons learned from this incident.
  - Conduct regular tabletop exercises to test the effectiveness of the incident response plan.
- **Key Takeaways:**
  - Proactive threat hunting and incident response are critical for maintaining a strong security posture.
  - Continuous monitoring and analysis of system activity are essential to detect and respond to threats promptly.
  - Regular security training and awareness programs are crucial to educate users and minimize human error.
  - Collaboration and information sharing within the security community are vital for effective threat intelligence and response.