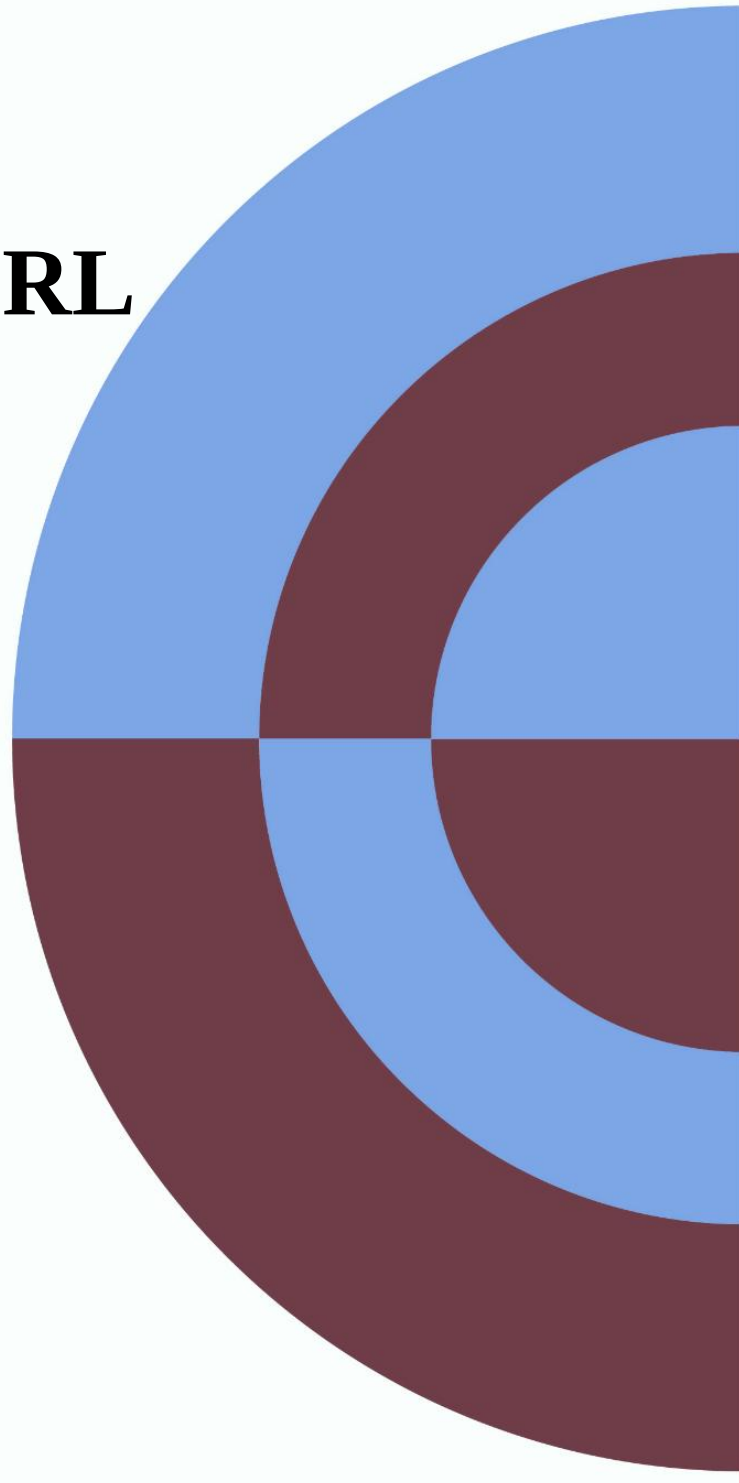
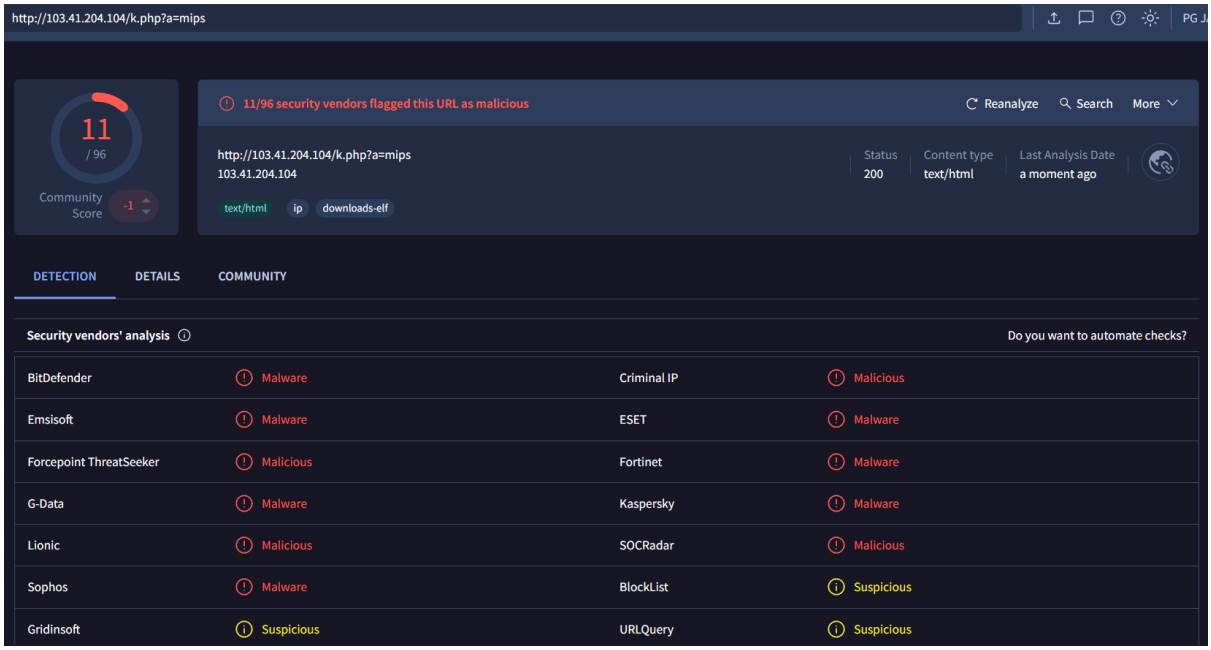


MALICIOUS URL

PREPARED BY : VIJAYKUMAR

❖ SUMMARY



The URL http://103.41.204.104/k.php?a=mips Out of 96 security vendors, 11 flagged the URL as malicious, with companies like BitDefender, Kaspersky, and Sophos identifying it as malware. Additionally, vendors such as Gridinsoft and URLQuery marked it as suspicious. The community score is -1, indicating a negative reputation. The URL has a status code of 200, meaning it is active and accessible, with a content type of text/html, suggesting a potential web-based threat. Given these detections, the URL could be involved in malware distribution or phishing attacks. It is strongly advised to avoid accessing this URL to prevent security risks.

General Info

URL:	http://103.41.204.104/k.php?a=mips
Full analysis:	https://app.any.run/tasks/7c8171e9-065a-4338-b1b8-4ddd5d759342
Verdict:	Suspicious activity
Analysis date:	February 25, 2025 at 11:30:56
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MD5:	A926B16FB63BCCB6D762C395ED14CE2D
SHA1:	57145AFD8D80A888B42F1111EA483C46900C190D
SHA256:	803F70B1C759FD3FC3B730C08B414599446E3B4774DA8326DF17DE249F6F4BBD
SSDEEP:	3:N1KtM97Vxa4n:CC9XNn

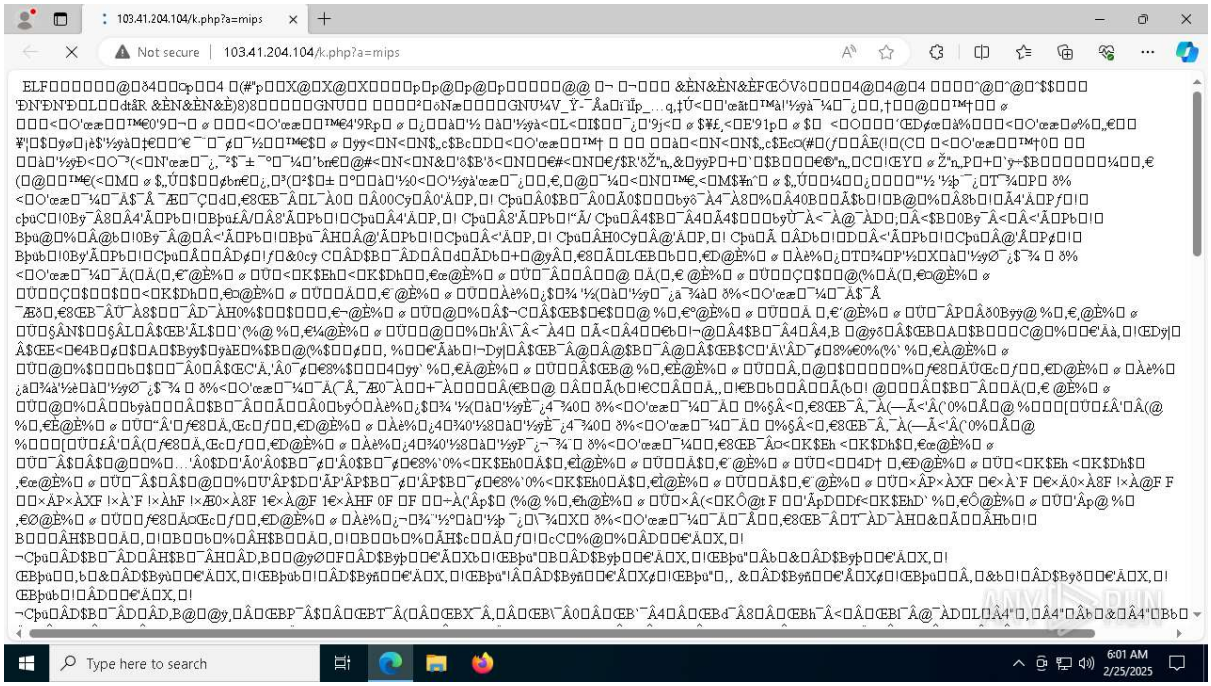
❖ URL ANALYSIS:

1.Malicious Content: The URL has been flagged as malicious by multiple security vendors (as seen in the previous VirusTotal analysis). It is likely distributing malware targeting MIPS architecture systems.

2.Binary ELF File: The text displayed resembles a corrupted or improperly rendered ELF (Executable and Linkable Format) binary file, often associated with Linux-based systems.

3.Potential Malware Distribution: Given the unreadable format and presence of ELF indicators, the URL may be serving a malicious executable, possibly for IoT botnets, remote access trojans, or exploits.

4.Security Risk: Accessing or downloading files from this URL poses a serious security threat. It is strongly advised to avoid interaction with this URL and ensure antivirus protection is in place.



IP Information

Field	Value
IP Address	103.41.204.104
ASN	AS2914
City	Englewood
Country	United States (US)
ISP	NTT America, Inc.
Organization	AS2914 NTT America, Inc.

Response Headers Details

Field	Value
Date	Tue, 25 Feb 2025 05:58:58 GMT
Server	Apache/2.2.8 (Win32), mod_ssl/2.2.8, OpenSSL/0.9.8g
X-Powered-By	PHP/5.2.6
Keep Alive	timeout=5, max=100
Connection	Keep-Alive
Transfer Encoding	Chunked
Content Type	text/html
X-Pad	Avoid browser bug

❖ Description of Network Analysis:

1.HTTP Requests Analysis:

- The first image displays a table of HTTP requests, including details like Process ID (PID), process name, request method (GET), HTTP response code, IP address, URL, and reputation (malicious/whitelisted).
- Notably, requests to http://103.41.204.104/k.php?a=mips http://103.41.204.104/favicon.ico were marked as malicious.
- Other requests to Microsoft and DigiCert-related domains were marked whitelisted, indicating trusted sources**.**

2.Packet Capture Analysis (Wireshark):

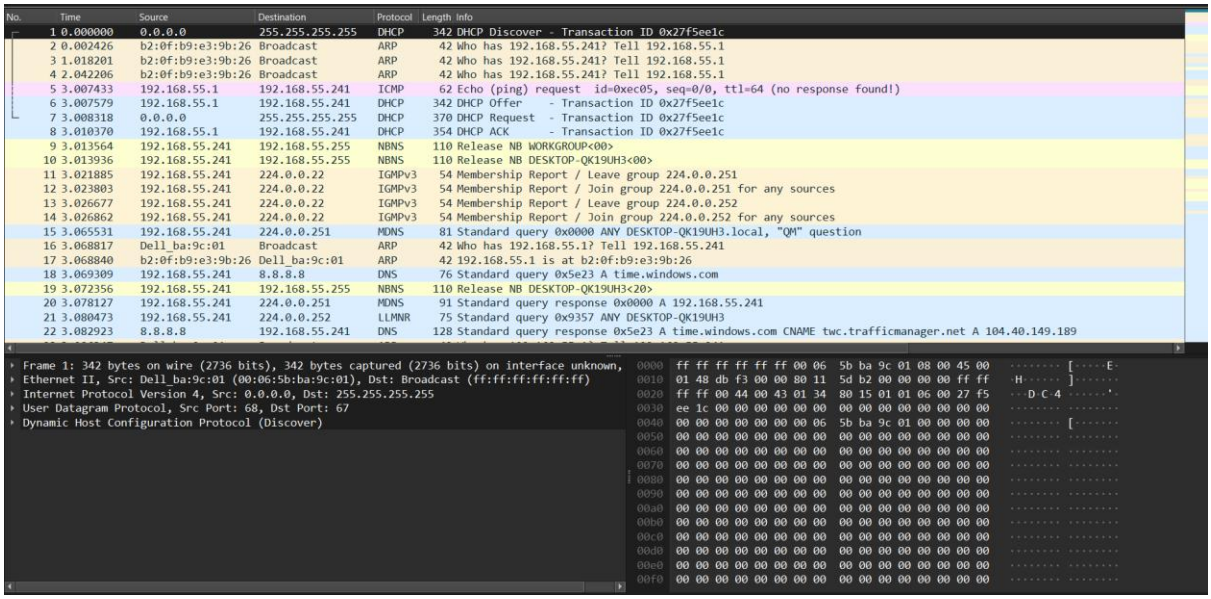
- The second image is a Wireshark capture showing network traffic.
- The data includes DHCP (Dynamic Host Configuration Protocol) transactions, ARP (Address Resolution Protocol) queries, ICMP (ping) requests, and DNS (Domain Name System) lookups.

3.Key observations:

- DHCP discover and offer messages indicate a device requesting an IP from a DHCP server.
- ARP requests are resolving local network addresses.
- An ICMP Echo (ping) request was sent to 192.168.55.241, but there was no response.DNS queries include a request to time.windows.com, a Microsoft time synchronization service.
- Some multicast queries (IGMP, MDNS, LLMNR) show local network communication.

4.Security Implications:

- The presence of malicious URLs suggests potential malware activity or an attempt to access a command-and-control (C2) server.
- The ICMP request with no response might indicate network filtering or a disabled host.
- Frequent DNS and multicast queries could be normal but should be monitored for unusual patterns.



HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6976	msedge.exe	GET	404	103.41.204.104:80	http://103.41.204.104/favicon.ico	unknown	–	–	malicious
6976	msedge.exe	GET	200	103.41.204.104:80	http://103.41.204.104/k.php?a=mips	unknown	–	–	malicious
6112	BackgroundTransferHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	whitelisted
6700	SIHClient.exe	GET	200	23.219.150.101:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
6700	SIHClient.exe	GET	200	23.219.150.101:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted

6976	msedge.exe	103.41.204.104:80	–	PT Infinys System Indonesia	ID	malicious
6976	msedge.exe	13.107.42.16:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6976	msedge.exe	103.41.204.104:443	–	PT Infinys System Indonesia	ID	malicious

HTTP Response ⓘ

Final URL

http://103.41.204.104/k.php?a=mips

Serving IP Address

103.41.204.104

Status Code

200

Body Length

898.99 KB

Body SHA-256

70bb9306edd99627e855a3fa10520809f8e1953b31e9f4b77b5a31770b7fba76 | Analyse

Headers

Date	Tue, 25 Feb 2025 06:01:15 GMT
Server	Apache/2.2.8 (Win32) mod_ssl/2.2.8 OpenSSL/0.9.8g PHP/5.2.6
X-Powered-By	PHP/5.2.6
Keep-Alive	timeout=5, max=100
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html
X-Pad	avoid browser bug

❖ YARA RULES ANALYSIS

The provided image contains YARA rules, which are used for malware detection and threat hunting. Here's a breakdown of the YARA rule in the image:

Rule Name:

autoyar_unknown_8d896997aa37

This suggests an automatically generated rule with a unique identifier.

Metadata:

Description: - 8d896997aa37e9126ebfd5151b31d2e304066e831951735462d9716d1a5b6c51"

Author: "ThreatZone"

Reference: "Default reference"

Date: "2025-02-25"

Hash1: Identifies a specific hash, likely corresponding to a malware sample.

Strings (Suspicious Indicators in the Code):

The rule contains several suspicious strings, each assigned a detection score. :

"After=multi-user.target" (Common in systemd service files)

"unplugply", "if_data_ptr <= (char *) &ifas[newlink + newaddr]" (Possibly related to network configuration manipulation)

"error while loading shared libraries" (Indicates possible library loading issues, often seen in exploits)

"dmidecode --type baseboard" (Might be gathering system hardware information)

"/etc/host.conf" (Possible tampering with system configuration)

IOC Patterns:

$ioc1 = "keld@akuug.dk" (Potentially a malicious email identifier)

$ioc2 = "8.8.8.8" (Google DNS, might indicate network traffic redirection)

Detection Conditions:

ELF File Format:

The rule checks if the first 16 bits of the file match 0x457f, which corresponds to an ELF (Executable and Linkable Format) file.

File Size Restriction:

Only files between 808KB and 988KB are considered.

Indicators of Compromise (IOCs):

At least 2 IOC patterns must match.

Suspicious Strings:

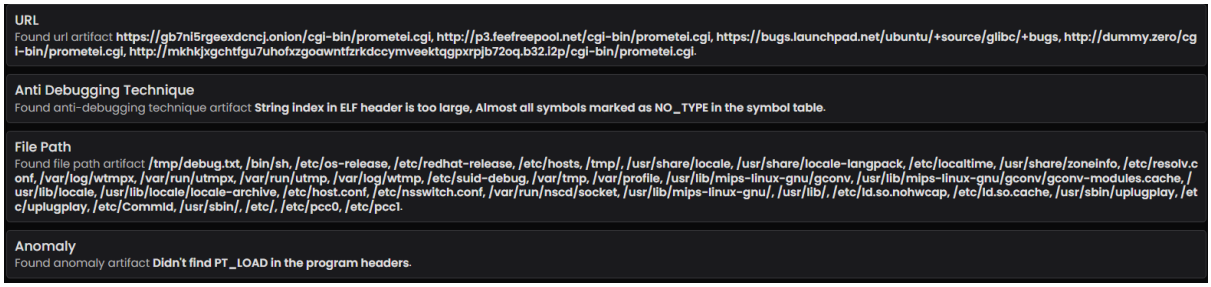
All strings from $s* must be present.

This YARA rule is designed to detect ELF malware targeting Linux systems, potentially modifying system configurations, gathering hardware information, and containing suspicious email/network indicators. It seems to focus on a specific malware variant based on the hash reference.

```
rule autoyar_unknown_8d896997aa37 {
  meta:
    description = "k.php - 8d896997aa37e9126ebfd5151b31d2e304066e831951735462d9716d1a5b6c51"
    author = "ThreatZone"
    reference = "Default reference"
    date = "2025-02-25"
    hash1 = "8d896997aa37e9126ebfd5151b31d2e304066e831951735462d9716d1a5b6c51"
  strings:
    $s1 = "After=multi-user.target" fullword ascii /* score: '17.00'*/
    $s2 = "((size + offset) & (GLRO (dl_pagesize) - 1)) == 0" fullword ascii /* score: '12.00'*/
    $s3 = "uplugplay" fullword ascii /* score: '8.00'*/
    $s4 = "ifa_data_ptr <= (char *) &ifas[newlink + newaddr] + ifa_data_size" fullword ascii /* score: '8.00'*/
    $s5 = "upnpsetup" fullword ascii /* score: '8.00'*/
    $s6 = "error while loading shared libraries" fullword ascii /* score: '12.00'*/
    $s7 = "Unexpected netlink response of size %zd on descriptor %d" fullword ascii /* score: '10.00'*/
    $s8 = "dmidecode --type baseboard" fullword ascii /* score: '10.00'*/
    $s9 = "ELF load command address/offset not properly aligned" fullword ascii /* score: '15.00'*/
    $s10 = "/etc/host.conf" fullword ascii /* score: '9.00'*/
    //IOC patterns
    $ioc1 = "keld@dkuug.dk"
    $ioc2 = "8.8.8.8"
  condition:
    uint16(0) == 0x457f and filesize < 988KB and filesize > 808KB and
    2 of ($ioc*) and
    all of ($s*)
}
```

❖ YARA Rule for Threat Detection:

- The image shows a YARA rule used to detect a specific malicious binary.
- **Key Elements:**
- **Meta Information:** Includes a description, author ("ThreatZone"), reference, date, and hash value of the detected sample.
- **String Indicators:** Defines specific patterns (ASCII strings) that are commonly found in the malicious sample.
- **IOC (Indicators of Compromise):** Includes hardcoded IOC patterns such as email (keld@akuug.dk) and IP address (8.8.8.8).
- **Detection Condition:** The rule triggers if:
- The file size is between 808KB and 988KB.
- The magic bytes match (uint16(0) == 0x457f).
- At least 2 IOC patterns and all string patterns are found.



❖ Suspicious URL, Anti-Debugging, and Anomalies:

- The image lists various forensic artifacts identified in a malware sample.
- **Key Observations:**
- **Malicious URLs:** Includes .onion links (Tor-based C2 servers), suspicious .cgi scripts, and compromised websites.
- **Anti-Debugging Techniques:** The binary employs string obfuscation in the ELF header to hinder analysis.
- **File Path Artifacts:** Lists critical system files the malware attempts to access, such as /tmp/debug.txt, /etc/hosts.conf, and /usr/lib/locale/locale-archive.
- **Anomalies:** Mentions missing PT_LOAD in ELF headers, suggesting a non-standard binary format or packed executable.

❖ System API Calls and Registry Modifications:

- The image showcases low-level system calls related to file and registry access, likely captured from a malware analysis sandbox.
- **Highlighted API Calls:**
- **NtCreateFile / NtOpenFile:** Malware interacting with suspicious file paths (Connect\\Input, Connect\\Output).
- **NtDuplicateObject / NtOpenProcessToken:** Possible privilege escalation or process injection attempts.
- **NtOpenKey / NtQuerySystemInformation:** Modifies Windows Registry settings to alter system behavior (e.g., disabling security policies).
- **NtOpenSection / NtCreateThreadEx:** Likely attempts to allocate memory or spawn new malicious threads.
- **NtQueryVolumeInformationFile:** Could be used for anti-VM checks or fingerprinting the system.

❖ Prevention and Mitigation Measures for Dropped Files & Suspicious Activities

The dropped files shown in the image suggest potential threats, including data tracking, persistence mechanisms, and possible malware activity linked to msedge.exe. Below are steps to prevent and mitigate such security risks:

1. Prevention Measures

✅ **Keep Software & OS Updated**

- Ensure Microsoft Edge, Windows, and security software are up to date.
- Enable automatic updates to patch vulnerabilities.

✅ **Use Endpoint Protection**

- Deploy **Next-Gen Antivirus (NGAV)** and **Endpoint Detection & Response (EDR)** solutions to monitor suspicious processes like msedge.exe.
- Enable real-time protection for **file integrity monitoring**.

✅ **Control File & Process Execution**

- Restrict execution of unknown .TMP and .OLD log files using **AppLocker** or **Group Policy**.
- Monitor for abnormal process behavior and API calls (e.g., NtCreateFile, NtOpenKey).

✅ **Web & Email Filtering**

- Block access to suspicious URLs and domains (e.g., .onion links found in the first screenshot).
- Use **email security gateways** to prevent phishing-based malware drops.

✅ **Implement Least Privilege Access**

- Restrict admin access to prevent unauthorized changes to Edge's user data files.
- Prevent execution of scripts in **AppData, Temp, and User directories**.

2. Mitigation Measures (If Infection is Suspected)

🛑 **Isolate the Affected System**

- Disconnect the compromised system from the network immediately.
- Investigate processes linked to **PID 5136 (msedge.exe)** for unusual activity.

🔍 **Analyze Dropped Files**

- Check hashes (SHA256/MD5) of the dropped files against VirusTotal for known malware indicators.
- Investigate log files (LOG.old, LOG.old~RF1273b1.TMP) for unauthorized modifications.

🔄 **Restore from Backup**

- If critical data is affected, restore system/user data from the latest clean backup.

🚀 **Run Full Security Scans**

- Use **Windows Defender, Malwarebytes, or an EDR solution** to scan and remove threats.
- Look for persistence mechanisms (e.g., registry modifications, scheduled tasks).

🔐 **Enhance Network Security**

- Block suspicious domains (e.g., .onion addresses) at the firewall level.
- Enforce **multi-factor authentication (MFA)** to prevent unauthorized access.

❖ Conclusion

The analysis of the dropped files and suspicious activities associated with msedge.exe indicates a potential security risk, including unauthorized file modifications, persistence mechanisms, and possible malware infiltration. The presence of .TMP and .OLD log files within Microsoft Edge's directories suggests attempts at data tracking, log manipulation, or the establishment of persistence. Additionally, the previous images highlighting API calls (NtCreateFile, NtOpenKey, etc.) and connections to .onion domains reinforce the likelihood of malware involvement.

To mitigate these threats, organizations must enforce endpoint protection, least privilege access, and application control policies. Security teams should also monitor file integrity, restrict execution of unverified processes, and analyze system logs for anomalies. If infection is suspected, immediate isolation, forensic investigation, and remediation steps should be taken, including blocking suspicious domains, scanning dropped files, and restoring from clean backups.

Furthermore, regular security awareness training for employees, along with multi-factor authentication (MFA) and network segmentation, can significantly reduce the risk of such attacks. Continuous monitoring and proactive threat hunting using SIEM solutions and EDR tools will help organizations detect and neutralize potential threats before they cause significant damage. By implementing these best practices, organizations can strengthen their cybersecurity posture and prevent future incidents.