MALWARE URL ANALYSIS

"THREAT ASSESSMENT & INSIGHTS

BigX TECHNOLOGY

Prepared for: BIGXTechnology | **Report Date:** 26 FEB 2025 | **Analyst:** Tank Mehul

INDEX

INTRODUCTION

PURPOSE OF ANALYSIS

The purpose of this analysis is to investigate a potentially malicious URL using VirusTotal. This report aims to determine whether the URL poses a security threat, assess its characteristics, and provide insights into its potential impact. By analysing the detection rate across multiple security vendors, we can evaluate the likelihood of it being used for malicious activities such as malware distribution, phishing, or exploitation of system vulnerabilities.

FILE OVERVIEW

The analysis is based on the URL:
http://103.41.204.104/k.php?a=mips

- **IP Address:** 103.41.204.104
- **Detection Rate:** 11/96 security vendors flagged the URL as malicious.
- **Content Type:** text/html
- **Status Code:** 200 (OK)
- **Last Analysis Date:** 15 hours ago
- **Additional Tags:** downloads-elf

URL DETAIL

CATEGORIES

alphaMountain.ai	Malicious, Suspicious (alphaMountain.ai)
Sophos	spyware and malware
Forcepoint ThreatSeeker	malicious web sites

The URL http://103.41.204.104/k.php?a=mips has been classified into different threat categories by security vendors. These categories help in understanding the nature of the potential risk.

Category Descriptions:

- Malicious, Suspicious: The URL is considered untrustworthy and may be involved in harmful activities such as malware distribution or phishing.
- Spyware and Malware: The site is linked to software that can secretly gather user information or infect systems with malicious code.
- Malicious Websites: The URL is associated with harmful online activities, possibly used for cyberattacks, fraudulent schemes, or hosting malicious payloads.

These categorizations indicate that the URL should be considered a security risk and should not be accessed without further in-depth analysis.

HISTORY

First Submission	2024-12-07 05:14:45 UTC
Last Submission	2025-02-25 06:01:33 UTC
Last Analysis	2025-02-25 06:01:33 UTC

The URL **http://103.41.204.104/k.php?a=mips** has been previously analyzed on multiple occasions.

Analysis Insights:

- The URL was **first submitted on December 7, 2024**, indicating that it has been under investigation for some time.
- The **latest submission and analysis took place on February 25, 2025**, suggesting that it is still actively being monitored.

- The repeated analysis implies **ongoing suspicious activity** or continued relevance in cybersecurity investigations.

HTTP RESPONSE

The URL http://103.41.204.104/k.php?a=mips returned the following HTTP response details:

Response Overview

Parameter	Value
Final URL	http://103.41.204.104/k.php?a=mips
Serving IP Address	103.41.204.104
Status Code	200 (OK)
Body Length	1.32 MB
Body SHA-256	16da969240a77e0fe319b8a85cdc4ec771d697cf9bceae1d4e63996dd05a3f44

Response Headers

Header	Value
X-Powered-By	PHP/5.2.6
Connection	Keep-Alive
Content-Type	text/html
Date	Tue, 25 Feb 2025 06:01:19 GMT
Keep-Alive	timeout=5, max=100
Server	Apache/2.2.8 (Win32) mod_ssl/2.2.8 OpenSSL/0.9.8g PHP/5.2.6
Transfer-Encoding	chunked
X-Pad	avoid browser bug

Analysis & Observations

1. Outdated Software:
    - The server is running Apache/2.2.8, OpenSSL/0.9.8g, and PHP/5.2.6, all of which are obsolete and contain known vulnerabilities.
    - Attackers often exploit outdated software to host and distribute malware.
2. Large Response Body (1.32 MB):
    - The relatively large response size suggests that the URL may be serving a binary file, possibly malware.
    - The SHA-256 hash (16da969240a77e0fe319b8a85cdc4ec771d697cf9bceae1d4e63996dd05a3f44) should be further analyzed to determine its contents.
3. Keep-Alive & Transfer-Encoding:
    - The Keep-Alive header indicates that the server maintains persistent connections, which could be leveraged for botnet communication or C2 (Command and Control) infrastructure.
    - Chunked Transfer-Encoding can sometimes be used to evade network-based malware detection.

Potential Risks

- The presence of outdated server software and a large payload suggests that the URL may host malware.
- Further investigation of the SHA-256 hash is required to determine if the URL serves a malicious executable.

REDIRECTION CHAIN

The URL http://103.41.204.104/k.php?a=mips does not appear to have any redirections, meaning it directly serves the requested content without forwarding the user to another domain.

Analysis & Implications

1. No Redirection Detected:
    - Since there is no redirection, the URL likely hosts content directly on the server 103.41.204.104 rather than acting as a gateway to another malicious domain.
    - This suggests that the server itself may be compromised or intentionally set up for hosting malware.
2. Direct Hosting of Potentially Malicious Content:
    - As seen in the HTTP Response Analysis, the body size is 1.32 MB, which could indicate that the server is distributing a payload directly rather than redirecting to an external malicious site.
    - The SHA-256 hash should be analyzed to determine if the content is an executable malware sample (such as an ELF binary for Linux systems).
3. Potential Exploit Server:
    - Since the server is running outdated software (Apache/2.2.8, OpenSSL/0.9.8g, PHP/5.2.6), it could be hosting exploits, botnet payloads, or spyware targeting vulnerable systems.
    - The lack of redirection may indicate that the URL is designed for automated attacks rather than phishing campaigns (which typically use multiple redirects to evade detection).

VIRUSTOTAL ANALYSIS

DETECTION ANALYSIS

- **Malicious Classification:**
    - Multiple reputable antivirus and security vendors (e.g., BitDefender, Emsisoft, Sophos, Kaspersky, Fortinet) have classified this URL as Malware or Malicious.
    - Some sources (e.g., Criminal IP, Forcepoint ThreatSeeker, and SOCRadar) flagged it specifically as Malicious, indicating it may be involved in cybercrime-related activities.
- **Suspicious Classification:**
    - Vendors like Gridinsoft, BlockList, and URLQuery marked the URL as Suspicious, meaning it may not yet be confirmed as outright malware but exhibits behavior commonly associated with malicious sites.

Implications & Risk Assessment

1. **High Confidence of Malicious Activity**
    - Since several major vendors classify it as Malware, the risk level is high.
    - The presence of multiple malware detections suggests the URL is actively hosting or distributing harmful content.
2. **Potential Cybercrime Involvement**
    - Criminal IP's classification suggests the IP address 103.41.204.104 may be linked to cybercriminal networks or botnet infrastructure.
    - The presence of spyware-related flags (Sophos) raises concerns about data theft or keylogging activities.
3. **Possible Phishing or Exploit Hosting**
    - The suspicious classification from some vendors could indicate:
        - A new threat that is still being analyzed.
        - A command-and-control (C2) server used by malware.
        - A phishing attempt targeting unsuspecting users.

CONCLUSION & RECOMMENDATIONS

CONCLUSION:

The analysis of the URL **http://103.41.204.104/k.php?a=mips** using VirusTotal reveals that it has been flagged as **malicious** by multiple security vendors, including BitDefender, Emsisoft, Sophos, Kaspersky, and Fortinet. The URL is associated with **malware distribution, spyware, and other malicious activities**. Additionally, the **hosting server (103.41.204.104)** is running outdated software, increasing the likelihood of it being compromised or intentionally set up for cybercriminal activities.

RECOMMENDATIONS:

1. **Immediate Blocking & Mitigation:**
    - Block access to **http://103.41.204.104/k.php?a=mips** and the associated **IP address (103.41.204.104)** at the **firewall, network, and endpoint security levels**.
    - Check network logs for any previous attempts to connect to this IP.
2. **Further Investigation:**
    - Perform a deep analysis of the **SHA-256 hash** to determine the nature of the file hosted on this URL.
    - Identify if any compromised systems have accessed this URL and conduct **forensic investigation** if necessary.
3. **Security Awareness & Prevention:**
    - Educate users about avoiding unknown or suspicious URLs.
    - Ensure **antivirus and endpoint protection solutions** are up to date to detect threats like those associated with this URL.
    - Implement **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** to detect and block similar threats.
4. **Threat Intelligence Sharing:**
    - Report the URL and IP address to **cyber threat intelligence platforms** for broader awareness.

REFERENCES

Below are the sources and tools used for the analysis of the malicious URL **http://103.41.204.104/k.php?a=mips**:

1. **VirusTotal Analysis** – https://www.virustotal.com
    - Used to scan the URL and retrieve threat intelligence from multiple security vendors.
2. **VirusTotal Reports & Detection Engines**
    - Security vendors that flagged the URL as **malicious or suspicious** (BitDefender, Sophos, Kaspersky, Fortinet, etc.).