CYBER THREAT

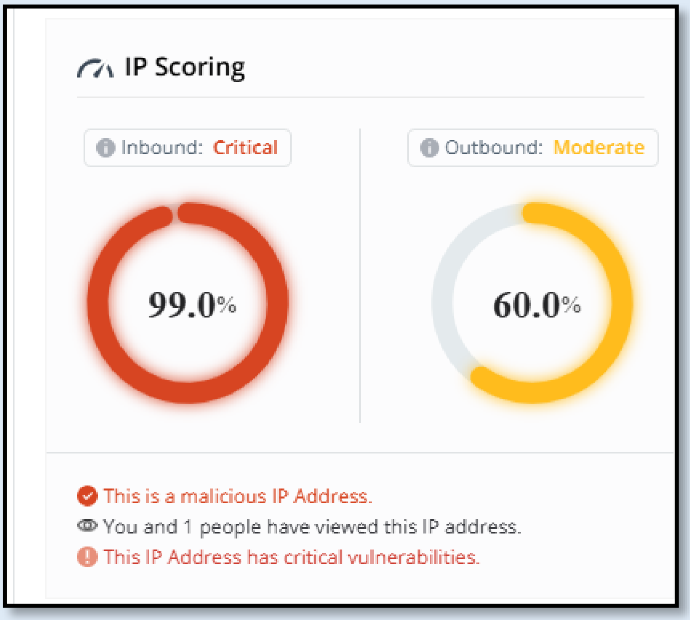
INTELLIGENCE REPORT

DATE OF REPORT: DECEMBER 24, 2024
PREPARED BY: RUSHIRAJ SOLANKI ,
CYBERSECURITY ANALYST

Table of Contents

1. Executive Summary

This report investigates the suspicious activity associated with IP address 80.241.214.92. Analysis indicates potential malicious behavior, including phishing attempts, malware distribution, and possible reconnaissance activities. Multiple security vendors have flagged this IP address and associated files as malicious. This report outlines the findings, threat categories, detection methods, behavior analysis, and recommends immediate actions, detection and response measures, and long-term strategies to mitigate the risks posed by this activity.


IP Scoring

Inbound: Critical

99.0%

Outbound: Moderate

60.0%

This is a malicious IP Address.

You and 1 people have viewed this IP address.

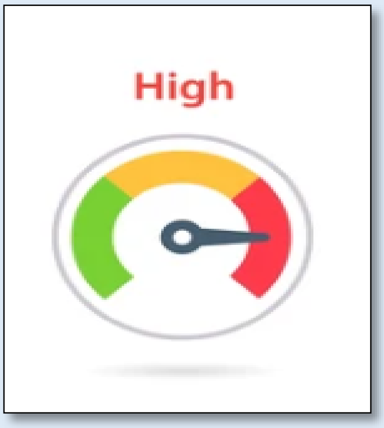
This IP Address has critical vulnerabilities.

2. IOC Analysis

2.1 Identified IP Address: 80.241.214.92

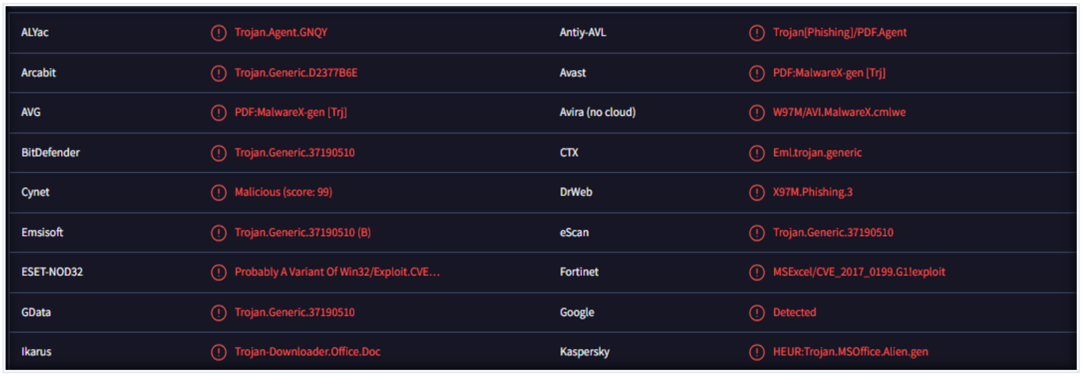
2.2 Threat Categories:

- **High:** Phishing
- **High:** Malware Distribution
- **Medium:** Reconnaissance



2.3 Malware Family Labels:

- **High:** Trojan.Generic
- **Medium:** PDF:MalwareX-gen
- **Medium:** Trojan.Agent
- **Medium:** Eml.trojan.generic
- **High:** Worm/Linux.Mirai.SE276
- **High:** Trojan/Phishing.PDF.Agent



ALYac	Trojan.Agent.GNQY	Antiy-AVL	Trojan[Phishing]/PDF.Agent
Arcabit	Trojan.Generic.D2377B6E	Avast	PDF:MalwareX-gen [Trj]
AVG	PDF:MalwareX-gen [Trj]	Avira (no cloud)	W97M/AVI.MalwareX.cmlwe
BitDefender	Trojan.Generic.37190510	CTX	Eml.trojan.generic
Cynet	Malicious (score: 99)	DrWeb	X97M.Phishing.3
Emsisoft	Trojan.Generic.37190510 (B)	eScan	Trojan.Generic.37190510
ESET-NOD32	Probably A Variant Of Win32/Exploit.CVE...	Fortinet	MSExcel/CVE_2017_0199.G1!exploit
GData	Trojan.Generic.37190510	Google	Detected
Ikarus	Trojan-Downloader.Office.Doc	Kaspersky	HEUR:Trojan.MSOffice.Alien.gen

3. Detection Methods

3.1 YARA Rules Findings:

- **Rule Name:** Base64_Encoded_URL
- **Severity:** Medium
- **Description:** This rule triggered on the presence of Base64-encoded URLs, which can be used to obfuscate malicious links. While not inherently malicious, it warrants further investigation as it can be used to deliver malware or phishing content.
- **Mitigation:** Implement security measures to detect and block suspicious URLs, such as URL filtering and sandboxing.

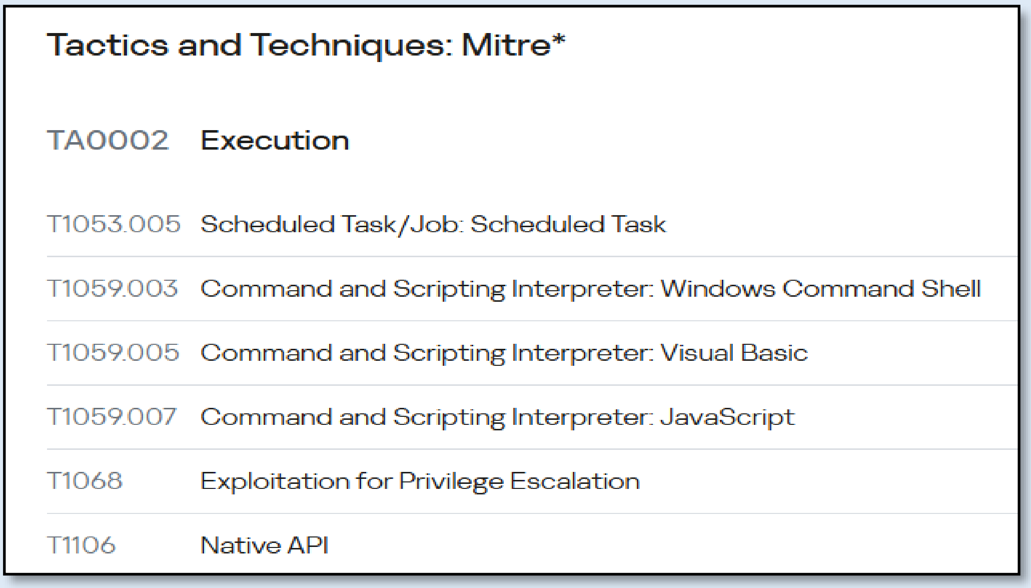
3.2 Sigma Rules Findings:

- **Rule Name:** Office Application Initiated Network Connection To Non-Local IP
- **Severity:** High
- **Description:** This Sigma rule detected an Office application initiating a network connection to a non-private IP address (80.241.214.92), which can be indicative of malicious activity, such as command-and-control communication, data exfiltration, or lateral movement.
- **Mitigation:** Implement security measures to monitor and block suspicious network connections from Office applications. Consider deploying endpoint detection and response (EDR) solutions to monitor application behavior and detect malicious activity.

4. Behavior Analysis

4.1 Suspicious Executables:

- **ELF File:** The analysis identified an ELF file associated with the IP address, which was flagged as malicious by multiple security vendors. This file exhibited characteristics of known malware families, including Trojan.Generic and Worm/Linux.Mirai.SE276.
- **Potential Behavior:**
  - **Trojan.Generic:** This label indicates that the file may exhibit a wide range of malicious behaviors, such as downloading and executing other malware, stealing credentials, or performing data exfiltration.
  - **Worm/Linux.Mirai.SE276:** This label suggests the file may be related to the Mirai botnet, known for its ability to infect IoT devices and recruit them into a botnet for DDoS attacks.



Tactics and Techniques: Mitre*

TA0002	Execution
T1053.005	Scheduled Task/Job: Scheduled Task
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1059.007	Command and Scripting Interpreter: JavaScript
T1068	Exploitation for Privilege Escalation
T1106	Native API

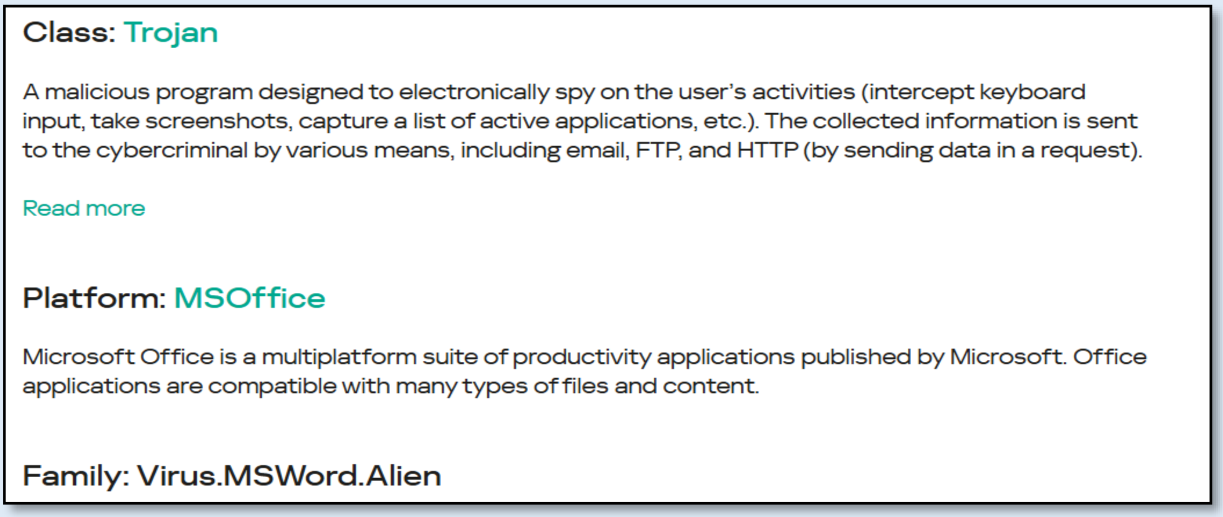
4.2 Malware Persistence:

- **Potential Mechanisms:**
    - **Registry Entries:** Malware may create persistent registry entries to ensure it runs automatically on system startup.
    - **Scheduled Tasks:** Malware may create scheduled tasks to execute malicious code at specific intervals.
    - **System Services:** Malware may install itself as a system service to maintain persistence.

4.3 Malware Family Indicators:

- **Trojan.Generic:** This broad label indicates that the malware may exhibit a wide range of behaviors and should be investigated further.
- **PDF:MalwareX-gen:** This label suggests the malware may be delivered through malicious PDF documents, potentially exploiting vulnerabilities in PDF readers.
- **Trojan.Agent:** This label indicates that the malware may act as an agent for a larger botnet or command-and-control infrastructure.
- **Eml.trojan.generic:** This label suggests that the malware may be delivered through email attachments.
- **Worm/Linux.Mirai.SE276:** This label indicates that the malware may be related to the Mirai botnet, known for infecting IoT devices.

- **Trojan/Phishing.PDF.Agent:** This label suggests that the malware may be delivered through phishing emails containing malicious PDF attachments.



Class: Trojan

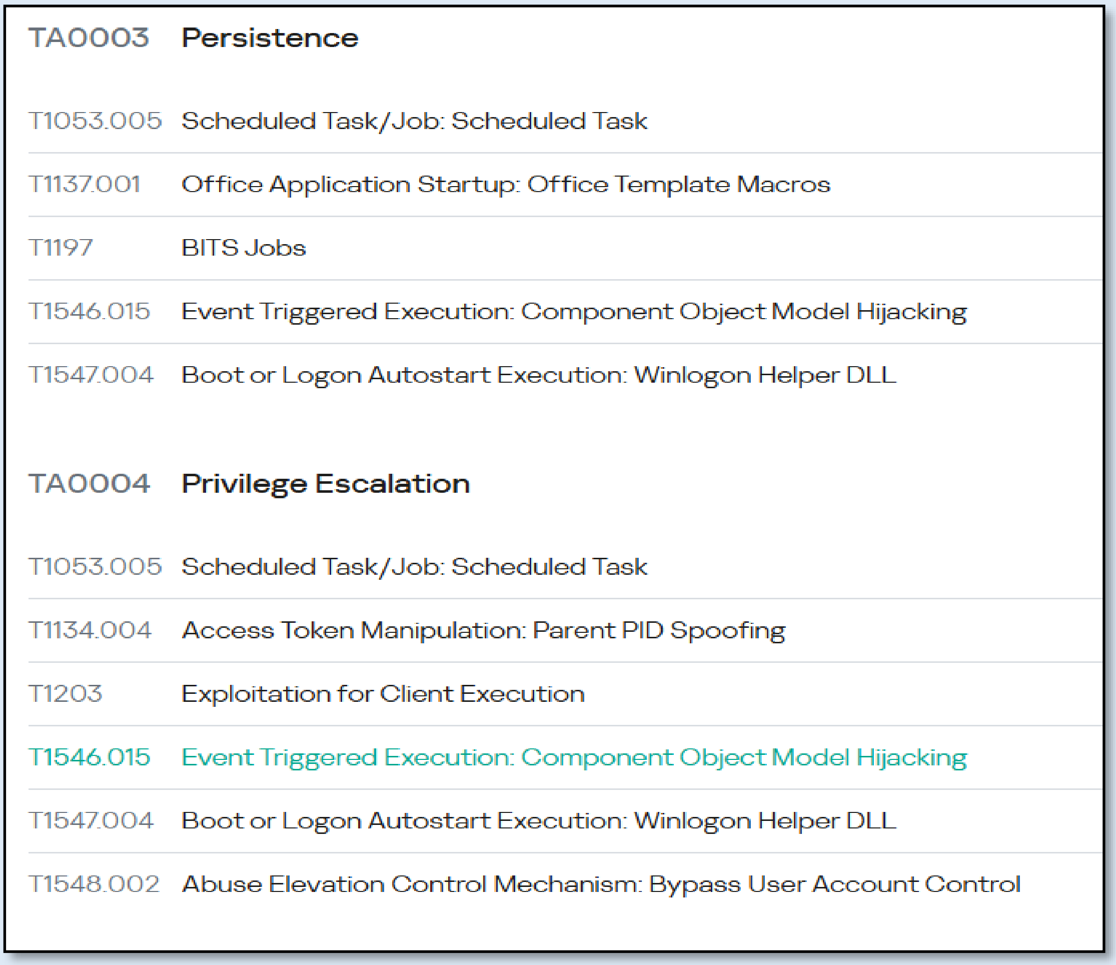
A malicious program designed to electronically spy on the user’s activities (intercept keyboard input, take screenshots, capture a list of active applications, etc.). The collected information is sent to the cybercriminal by various means, including email, FTP, and HTTP (by sending data in a request).

Read more

Platform: MSOffice

Microsoft Office is a multiplatform suite of productivity applications published by Microsoft. Office applications are compatible with many types of files and content.

Family: Virus.MSWord.Alien



TA0003	Persistence
T1053.005	Scheduled Task/Job: Scheduled Task
T1137.001	Office Application Startup: Office Template Macros
T1197	BITS Jobs
T1546.015	Event Triggered Execution: Component Object Model Hijacking
T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL

TA0004	Privilege Escalation
T1053.005	Scheduled Task/Job: Scheduled Task
T1134.004	Access Token Manipulation: Parent PID Spoofing
T1203	Exploitation for Client Execution
T1546.015	Event Triggered Execution: Component Object Model Hijacking
T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL
T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control

5. Recommendations

5.1 Immediate Actions:

- **Block the IP Address:** Implement measures to block all traffic from and to the IP address 80.241.214.92 on your network perimeter and endpoints using firewalls and intrusion prevention systems (IPS).
- **Quarantine and Analyze Suspicious Files:** Identify and quarantine any files associated with the IP address, particularly the ELF file. Conduct a thorough analysis of these files using sandboxing and malware analysis tools to determine their exact functionality and potential impact.
- **Update Security Controls:** Ensure all security controls, including firewalls, IDS, and endpoint protection solutions, are updated with the latest signatures and threat intelligence.
- **Notify Affected Users:** If any users have interacted with emails or files associated with this IP address, notify them of the potential risks and advise them to take appropriate precautions, such as changing passwords and scanning their devices for malware.

5.2 Detection and Response

- **Implement Advanced Threat Protection:**
  - ➢ Deploy sandboxing solutions to analyze suspicious files and detect malicious behavior before they can execute.
  - ➢ Implement machine learning-based detection to identify and block unknown threats.

    - Consider deploying endpoint detection and response (EDR) solutions to monitor application behavior, detect malicious activity, and respond to incidents in real-time.

- **Conduct Regular Security Audits:**
    - Perform regular security audits and vulnerability assessments to identify and address potential weaknesses in your network and systems.
    - This includes conducting penetration testing, vulnerability scans, and security configuration reviews.
- **Improve Incident Response Capabilities:**
    - Develop and test incident response plans to ensure a rapid and effective response to security incidents.
    - Train your security team on incident response procedures, including threat hunting, containment, eradication, and recovery.

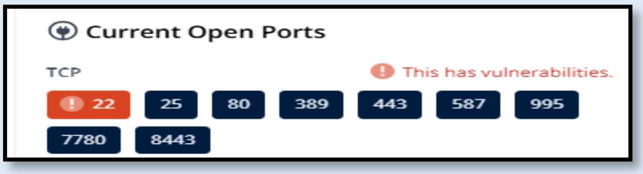
5.3 Long-term Strategies:

- **Employee Security Training:**
    - Conduct regular security awareness training for employees to educate them about phishing attacks, social engineering tactics, and safe browsing practices.
    - Emphasize the importance of verifying the authenticity of emails and attachments before opening them.
    - Train employees to recognize and report suspicious emails and websites.

- **Threat Intelligence Monitoring:**
  - Continuously monitor threat intelligence feeds and security advisories to stay informed about emerging threats and vulnerabilities.
  - Leverage threat intelligence platforms to proactively identify and block malicious actors and their associated infrastructure.
- **Security Posture Review:**
  - Conduct regular reviews of your overall security posture to identify and address any gaps or weaknesses in your defenses.
  - This includes reviewing security policies, access controls, and data protection measures.

6. Harmfulness of the IP Address

- **Malicious Classification:** The IP address is classified as "Malicious" by multiple security vendors, indicating a high probability of involvement in malicious activities.
- **Critical Inbound Traffic:** The IP address exhibits a high volume of inbound traffic, suggesting it may be actively involved in botnet activity, spam campaigns, or exploitation attempts.
- **Expired SSL Certificates:** The presence of expired SSL certificates on services hosted by this IP address poses a security risk, as attackers can exploit vulnerabilities to intercept sensitive information.
- **Open Ports and Vulnerabilities:** The IP address has multiple open ports with known vulnerabilities, increasing the risk of exploitation and unauthorized access.
- **Policy Violation:** The IP address is in violation of network security policies, indicating potential misuse of resources or suspicious activity.

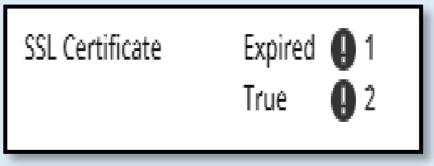


Current Open Ports

TCP

! This has vulnerabilities.

! 22 | 25 | 80 | 389 | 443 | 587 | 995 | 7780 | 8443



SSL Certificate	Expired	! 1
	True	! 2

7. Conclusion

The analysis indicates that the IP address **80.241.214.92** poses a significant security risk. The presence of **malicious files**, potential phishing activities, and indications of reconnaissance warrant **immediate action**. By implementing the recommended measures, organizations can significantly reduce their exposure to threats associated with this IP address and improve their overall security posture.