19-Dec-2024

Incident Analysis Report

Suspicious Network Activity from IP 62.60.148.85

Prepared by :

Patel Vasu

Table of Contents

1. Executive Summary

On **2024-12-17**, an investigation revealed unusual network activity originating from the IP address **62.60.148.85**, linked to Aeza International Ltd.

The IP is flagged for suspicious behavior, particularly its association with domains known for hosting phishing content **(vps.fourdjecem.shop, sloto.fourdjecem.shop)**.

Despite a low detection rate among security vendors **(2 out of 94),** the domains are tied to active phishing campaigns. This detailed report provides a thorough analysis of the identified indicators of compromise (IOCs), potential threat behaviors, and actionable recommendations to mitigate associated risks.

2. IOC Analysis

2.1 Identified IP Address

- **IP Address:** 62.60.148.85
- **ASN:** AS 210644 (Aeza International Ltd)
- **Subnet:** 62.60.148.0/22
- **Geolocation:** Predominantly Eastern Europe and Russia.
- **Traffic Patterns:** Analysis indicates frequent connections to known malicious domains, along with automated scanning patterns.

2.2 Associated Domains

- **Primary Domains:**
  - vps.fourdjecem.shop
  - slot0.fourdjecem.shop
- **Root Domain:** fourdjecem.shop
- **Role:** These domains are hosted on the same IP and are utilized for phishing campaigns. The root domain fourdjecem.shop serves as a redirect for compromised sites.
- **Analysis:** Both domains show high traffic volumes during specific periods, correlating with spikes in reported phishing incidents.

2.3 Threat Categories

- **Phishing Infrastructure:** Domains are used to host phishing kits designed to capture sensitive user information, such as login credentials and credit card details.
- **Malware Hosting:** The IP serves as a repository for malicious files, typically masked as legitimate updates or utilities.
- **Reconnaissance Activities:** Indicators suggest potential use for scanning and lateral movement within networks, making it a command-and-control (C2) hub.

3. Detection Methods

3.1 Passive DNS Analysis

- **Observation:** Historical DNS resolution logs show multiple queries pointing to the 62.60.148.85 IP from various networks, often associated with new domain registrations.
- **Analysis:** The IP consistently resolves to the fourdjecem.shop domain, supporting its role in active phishing campaigns and indicating persistent use of the compromised infrastructure.

3.2 VirusTotal Findings

- **Flagging Details:**
  - **2024-12-17:** 0/94 detections—Indicates evasion of standard detection methods, possibly due to the use of advanced obfuscation techniques.
  - **2024-12-11:** 1/94 detections—Suggests sporadic usage, potentially indicative of temporary spikes in malicious activity.
  - **2024-12-11:** 0/94 detections—Reiterates the deliberate strategy to avoid detection by security tools.
- **Community Reports:** Despite low detection rates, community-driven reports point to significant phishing activity and suspicious file distributions, underscoring the need for a deeper investigation.

4. Threat Behavior Analysis

4.1 Malicious Use Cases

- **Phishing Campaigns:**
  - **Fake Login Pages:** Domains host fraudulent login portals designed to harvest sensitive information from users. These portals are often secured with HTTPS to bypass security measures.
  - **Credential Harvesting:** Forms on these sites capture login credentials and send them to remote servers.
- **Command-and-Control (C2):**
  - **Data Exfiltration:** The IP acts as a hub for exfiltrating sensitive data from compromised devices, often using encrypted HTTP/HTTPS connections.
  - **Update Mechanism:** The use of domain generation algorithms (DGAs) enables rapid changes to domains, making it more challenging to detect via IP or DNS blocking.
- **Data Exfiltration:**
  - **Persistent Threats:** The IP sends stolen data through HTTP POST requests to predefined servers, a tactic that allows bypassing network-based detection solutions.

4.2 Reputation Analysis

- **Community Insights:** Numerous forums and threat intelligence platforms report similar behaviors from the 62.60.148.85 IP, noting its involvement in hosting phishing domains and malware.
- **Historical Analysis:** WHOIS records and passive DNS data reveal a pattern of frequent changes in domain ownership and registrations, suggesting efforts to evade detection.
- **Indicators of Compromise (IoCs):**
    - Rapid changes in domain registrar information.
    - High DNS record churn, indicating dynamic changes in C2 infrastructure.
    - Specific traffic patterns (e.g., large spikes in HTTP requests during peak hours) hinting at coordinated attacks.

5. Recommendations

5.1 Immediate Actions

- **IP Blocking:** Block the IP address 62.60.148.85 at all network perimeters, including firewalls, IPS, and NGFWs.
- **Domain Blacklisting:** Implement DNS filtering and URL filtering to block fourdjecem.shop and associated subdomains.
- **Network Isolation:** Segment the network to isolate systems that communicate with the compromised IP, including separating key data, high-risk users, and guest networks.

5.2 Detection and Response Strategies

- **Threat Hunting:** Use SIEM tools to search for network traffic patterns matching the compromised IP address. Focus on detecting anomalies, such as unusual traffic spikes or connections to known malicious domains.
- **Enhanced Logging:** Enable detailed logging for DNS queries, HTTP/HTTPS requests, and email traffic to identify potential phishing attempts.
- **Email Analysis:** Inspect email traffic for links to flagged domains, utilizing behavior analytics to detect suspicious email patterns.

5.3 Long-Term Mitigation Strategies

- **Phishing Simulations:** Regularly conduct phishing simulations as part of security awareness training to educate employees on recognizing suspicious links and emails.
- **Network Segmentation:** Implement a zero-trust network architecture with strict access controls to limit lateral movement of threats across the network.
- **Endpoint Detection and Response (EDR):** Deploy EDR solutions to detect and respond to potential threats, especially those establishing communication with known malicious IPs.
- **Regular Patching:** Ensure all systems and software are updated with the latest security patches to minimize vulnerabilities exploited by attackers.

6. Conclusion

The IP address 62.60.148.85, associated with Aeza International Ltd, is not safe. It is linked to **suspicious activities, particularly phishing and malware hosting**. Despite a low detection rate among security vendors, its involvement in distributing malicious content and serving as a command-and-control hub necessitates immediate action. Implementing measures such as IP blocking, domain blacklisting, and network isolation will help mitigate the associated risks and protect organizational networks.