CYBER THREAT INTELLIGENCE

SUSPECTED IP: 62.60.148.85

Prepared by: Vazir Faiz

19/12/2024

Table of Contents

1 Executive Summary (Detailed Explanation)

This section provides a comprehensive overview of the suspicious activity surrounding the IP address **62.60.148.85**, identified during the analysis. The IP has raised concerns due to its association with potential malicious activities, as flagged by multiple threat intelligence sources.

2. IOC Analysis

2.1 Identified IP Address

- **IP Address**: 62.60.148.85
  The specific IP under investigation. It has been flagged as suspicious due to its association with malware and its connections to questionable domains.

- **CIDR Range**: 62.60.148.0/22
  This range indicates that the IP is part of a larger subnet. The CIDR (Classless Inter-Domain Routing) range defines a block of IPs (from 62.60.148.0 to 62.60.151.255) that are managed together. The entire range might require monitoring as other IPs in the same block could potentially exhibit similar malicious behaviour.

- **ASN (Autonomous System Number)**: 210644
  This ASN is registered to **Aeza International Ltd**, an organization that provides hosting services. Malicious actors often exploit such hosting providers for their activities, setting up domains and IPs to evade detection.

- **Geolocation**: France (FR)
  The IP is physically or virtually routed through France. While the location does not inherently imply maliciousness, it helps analysts understand the infrastructure used by threat actors. Cybercriminals frequently use specific geolocations to mask their operations.

- **Last Analysis Date**: **20 days ago**
  The IP was last scanned for threats 20 days prior. This delay might indicate changes to its behaviour or new associations since then, requiring reanalysis.

2.2 Threat Categories

- **Category**: **Malware**
  The primary detection flags the IP as a source or host of malicious activity. Malware-related IPs are often used to:
  - Host command-and-control (C2) servers.
  - Deliver malicious payloads such as ransomware, trojans, or spyware.
  - Redirect users to phishing or malicious websites.
- **Detection**:
  The IP was flagged as malicious by:

MalwareURL: A vendor known for identifying URLs and IPs hosting malicious content.

SOCRadar: A vendor that specializes in threat intelligence and identifies risks based on traffic patterns and malicious activities.

The detections from these trusted vendors suggest that the IP has been associated with confirmed malware-related activities.

2.3 Malware Family Labels

- **Malware Family**: Not explicitly identified.
  The IP is flagged generically as being involved in malware-related activities. This lack of specificity may occur if:
  - The malware is custom-built or uncommon.
  - It serves as an intermediary (e.g., redirect or proxy) in larger campaigns.
  - Analysis data is insufficient to associate the IP with a specific malware strain.

While no specific malware family has been named, the generic categorization is significant as it highlights the risk associated with this IP.

2.4 Associated Domains

The IP is linked to three domains that were resolved via Passive DNS (Domain Name System). Each domain's activity and detection status are detailed below:

1. **vps.fourdjeem.shop**
    - **Resolution Date**: **2024-12-17**
    - **Detection Status**: 0/94 detections
      This domain shows no detections by security vendors. However, its association with the flagged IP and the naming pattern (vps) suggests it may be part of a virtual private server (VPS) infrastructure, commonly used to host malicious or phishing websites.
2. **sloto.fourdjeem.shop**
    - **Resolution Date**: **2024-12-11**
    - **Detection Status**: 0/94 detections
      Similar to the first domain, this has not been flagged as malicious. However, the term sloto could hint at potential associations with gambling or fraud-related campaigns, often used as fronts for malicious activities.
3. **fourdjeem.shop**
    - **Resolution Date**: **2024-12-11**
    - **Detection Status**: 1/94 detections
      This domain has been flagged by one security vendor, suggesting potential malicious activity. The generic. shop TLD (top-level domain) is frequently used in malicious campaigns due to its affordability and ease of registration.
    - **Pattern Analysis**:
      All three domains share the same root (fourdjeem.shop), indicating they belong to a single infrastructure. This clustering strongly suggests the IP is part of a coordinated setup to host malicious content or conduct phishing campaigns.

3. Detection Methods

3.1 YARA Rules Findings

- No YARA rule matches were triggered during the analysis of this IP and associated domains.

3.2 Sigma Rules Findings

- No Sigma rules were matched in this analysis.

4. Behaviour Analysis

4.1 Suspicious Executables

- No specific executables were identified during the URL and IP analysis.

4.2 Malware Persistence

- No evidence of persistence mechanisms detected.

4.3 Malware Family Indicators

- While no specific malware family indicators were identified, the flagged domains suggest potentially malicious activities. explain in details

5. Recommendations

5.1 Immediate Actions

1. Block IP

- **Action**: Immediately block the IP address **62.60.148.85** at firewalls, intrusion prevention systems (IPS), and other security tools.
- **Reasoning**:
    - This IP has been flagged by security vendors as malicious, indicating its potential use in phishing, malware distribution, or Command and Control (C2) operations.
    - Blocking the IP ensures that no further connections can be established with it, eliminating an immediate threat vector.
- **Implementation**:
    - Update firewall and security appliance rules to deny inbound and outbound traffic to **62.60.148.85**.
    - Ensure that block lists are propagated across all network segments and geographic locations to avoid gaps in protection.

2. Monitor Traffic

- **Action**: Monitor network traffic for any connections to the associated domains:
    - fourdjeem.shop
    - sloto.fourdjeem.shop
    - vps.fourdjeem.shop
- **Reasoning**:
    - These domains are linked to the flagged IP and may serve as part of a malicious infrastructure.
    - Monitoring for DNS queries or HTTP/HTTPS traffic to these domains can help identify compromised systems within the network.

- **Implementation**:
  - Use network monitoring tools (e.g., SIEM, IDS/IPS) to log and analyze traffic for interactions with these domains.
  - Configure alerts for anomalous activity or unexpected connections to these domains.

5.2 Detection and Response

1. Cross-Reference Flagged Domains

- **Action**: Cross-reference the flagged domains (fourdjeem.shop, sloto.fourdjeem.shop, vps.fourdjeem.shop) with internal logs to identify previous or ongoing access attempts.
- **Reasoning**:
  - If any internal systems have communicated with these domains, it may indicate a compromise or ongoing malicious activity.
  - Identifying compromised systems allows for containment and remediation efforts.
- **Implementation**:
  - Query DNS and HTTP logs in your SIEM or log management system to find any instances of these domains.
  - Perform forensic analysis on any systems that show signs of communication with the flagged domains.

2. Integrate IP Reputation Monitoring

- **Action**: Deploy IP reputation monitoring tools to automatically flag suspicious IPs.
- **Reasoning**:
  - Threat intelligence feeds and reputation-based tools can provide real-time updates on malicious IPs, enabling proactive detection and response.
  - This reduces reliance on manual analysis and improves the efficiency of threat detection efforts.

- **Implementation**:
    - Use platforms like VirusTotal, AlienVault OTX, or Palo Alto AutoFocus to receive threat intelligence updates.
    - Configure security appliances to automatically block or quarantine traffic associated with flagged IPs and domains.

5.3 Long-Term Strategies

1. Regular Traffic Analysis

- **Action**: Regularly analyze traffic to and from high-risk regions or ASNs.
- **Reasoning**:
    - Certain regions or Autonomous System Numbers (ASNs), such as **ASN 210644 (Aeza International Ltd)**, are more frequently associated with malicious activities.
    - Regular analysis can uncover patterns of abuse and help preemptively block risky infrastructure.
- **Implementation**:
    - Develop a list of high-risk ASNs based on threat intelligence data and audit traffic logs for communication with these networks.
    - Utilize geolocation filtering to restrict traffic to or from regions associated with high volumes of malicious activity.

2. Leverage Threat Intelligence Feeds

- **Action**: Subscribe to and actively use threat intelligence feeds to stay updated on emerging threats.
- **Reasoning**:
    - Threat intelligence feeds provide timely information about newly identified malicious IPs, domains, and malware families.
    - Leveraging this data enhances situational awareness and helps preemptively block new threats.

- **Implementation**:
    - Integrate feeds such as MITRE ATT&CK, MISP, or commercial solutions like Recorded Future into your SIEM or threat detection tools.
    - Create automated workflows to update firewall and IDS/IPS rules based on feed data.

6. Mitigation Strategies

6.1 Regular Patching

- **Action**: Ensure all systems, applications, and firmware are updated regularly to address known vulnerabilities.
- **Reasoning**:
  - Attackers often exploit unpatched vulnerabilities in software or hardware to gain unauthorized access or deploy malware.
  - Timely updates close these vulnerabilities, reducing the risk of exploitation.
- **Implementation**:
  - Automate patch management systems to schedule regular updates across all devices and software.
  - Prioritize critical patches, especially those for vulnerabilities that are actively exploited or associated with the flagged IP's malware activities.
  - Conduct regular vulnerability scans to identify and remediate outdated systems.

6.2 Network Segmentation

- **Action**: Implement robust network segmentation to isolate critical assets from less secure segments.
- **Reasoning**:
  - If an infection occurs, segmentation prevents lateral movement, containing the threat within a specific area of the network.
  - Isolated segments reduce the impact of attacks and make it more difficult for malware to propagate.
- **Implementation**:
  - Separate sensitive networks (e.g., finance, HR, R&D) from general user networks using VLANs or dedicated subnets.

    - Use firewalls and access controls to enforce strict communication rules between segments.
    - Regularly test segmentation configurations to ensure they are effective against real-world attack scenarios.

6.3 Email Filtering

- **Action**: Deploy advanced email filtering solutions to block phishing emails that may link to malicious domains like fourdjeem.shop.
- **Reasoning**:
    - Phishing emails are a common vector for malware delivery and credential theft.
    - Effective filtering prevents malicious emails from reaching users, reducing the chance of accidental infection.
- **Implementation**:
    - Use AI-powered email filtering solutions to detect and block emails with malicious attachments or links.
    - Enable sandboxing for email attachments to analyze potentially malicious files in a secure environment.
    - Continuously update email filters with threat intelligence on newly discovered phishing campaigns and domains.

6.4 Security Awareness

- **Action**: Conduct regular security awareness training to help employees recognize and avoid phishing attempts or malicious links.
- **Reasoning**:
    - Human error is a leading cause of successful cyberattacks. Educating employees reduces the likelihood of them falling victim to phishing or other social engineering tactics.
    - Awareness ensures that employees report suspicious activities promptly, enabling quicker response times.

- **Implementation**:
  - Organize mandatory training sessions on identifying phishing emails, recognizing fake websites, and reporting suspicious links.
  - Conduct simulated phishing campaigns to assess employee awareness and provide targeted training where needed.
  - Provide easy access to reporting tools (e.g., a “Report Phishing” button in email clients).

6.5 Endpoint Protection

- **Action**: Deploy advanced endpoint protection solutions with behavioural analytics capabilities to detect and respond to threats.
- **Reasoning**:
  - Modern endpoint protection tools go beyond traditional antivirus by detecting anomalous behaviours associated with malware, such as those flagged in this analysis.
  - Behavioural analytics allow detection of zero-day attacks and polymorphic malware that traditional signature-based tools may miss.
- **Implementation**:
  - Deploy Endpoint Detection and Response (EDR) tools like CrowdStrike, SentinelOne, or Microsoft Defender for Endpoint.
  - Enable real-time monitoring and automatic containment of suspicious activities.
  - Regularly update endpoint protection tools with the latest threat intelligence and signatures.

7. Conclusion

The IP 62.60.148.85, associated with ASN 210644, has been flagged as malicious by two vendors. The associated domains (fourdjeem.shop, etc.) indicate potential malicious activity, warranting further investigation and continuous monitoring. Implement the outlined mitigation and detection strategies to enhance organizational security and reduce risks from such threats.