Incident Report: Network Traffic Analysis - 2025-06-13

Incident ID: 20250613-NA-001
Date of Report: September 2, 2025

---

1. Executive Summary

On June 13, 2025, a system within the internal network was compromised, leading to the establishment of a command and control (C2) channel and attempted data exfiltration. The initial access vector was a malicious script executed on the victim host, evidenced by a PowerShell-related User-Agent in subsequent web requests. The attacker utilized a sophisticated, likely fileless, method to evade detection by traditional file-based security controls. The C2 traffic was routed to multiple domains designed to impersonate legitimate services, with data being exfiltrated via HTTP URI strings.

---

2. Incident Timeline

- 15:33:55 UTC: First packet captured from the victim host 10[.]6[.]13[.]133.
- 15:34:00 UTC: Normal, benign traffic to Microsoft services observed.
- 15:35:48 UTC: First suspicious HTTP request observed from 10[.]6[.]13[.]133 to event-time-microsoft[.]org. This is the new, definitive start time for the malicious activity.
- 15:35:58 - 15:36:25 UTC: Initial C2 communications observed to various malicious domains, including event-datamicrosoft[.]live and windows-msgas[.]com.
- 15:38:55 UTC: First C2 request containing what appears to be encoded data in the URI is sent to varying-rentals-calgary-predict[.]trycloudflare[.]com, indicating the start of data exfiltration.
- 16:08:03 UTC: The last malicious packet in the PCAP is captured, concluding the documented incident window.

---

3. Technical Analysis

Victim Host: 10[.]6[.]13[.]133 (DESKTOP-5AVE44C[.]massfriction[.]com)

- **Initial Access:** The initial access vector was not a traditional file download. Analysis of the network traffic revealed the first malicious request was initiated with a User-Agent string of WindowsPowerShell/5.1.26100.4202. This strongly suggests that a malicious script was executed on the host, which subsequently initiated network communication without the need for a separate executable binary.
- **Execution & Persistence:** No malicious files were identified or extracted from the PCAP using file-carving tools such as foremost. This indicates the attacker utilized a "fileless" attack method, where the payload was executed in memory, or that the file was delivered over an encrypted channel that was not visible in the PCAP. This tactic is designed to bypass security controls that rely on file hashes and signatures.
- **C2 Communication:** The compromised host communicated with several external hosts via standard HTTP, likely on port 80. The C2 channel was designed to blend in with legitimate traffic by using domains that closely resemble Microsoft services (e.g., event-datamicrosoft[.]live, windows-msgas[.]com). The C2 communication was characterized by:
  - **Unusual Domains:** Typosquatting of legitimate domains to evade detection.
  - **Non-Standard URIs:** The URIs were a mix of random-looking characters and strings (e.g., /NV4RgNEu, /bmvLMt6UaBCc/22jMpHiZLgaCY4). This is a common C2 behavior for transmitting commands and receiving data.
- **Data Exfiltration:** Based on the analysis of TCP streams and HTTP requests, data exfiltration appears to have occurred. Requests to varying-rentals-calgary-predict[.]trycloudflare[.]com contained long, randomized strings within the URI (e.g., &354f9148f3b439a1433a5327275539f4). This pattern is a strong indicator of encoded data being uploaded to the attacker's server. The volume of traffic between the victim and the primary C2 server also supports this finding.

---

4. Indicators of Compromise (IOCs)

This list contains technical artifacts identified during the analysis that can be used for detection and prevention.

- **Malicious IP Addresses:**
  - 104[.]21[.]24[.]186
  - 104[.]21[.]112[.]1
  - 104[.]21[.]16[.]1
  - 104[.]16[.]230[.]132

- **Malicious Domains:**
  - event-time-microsoft[.]org
  - event-datamicrosoft[.]live
  - windows-msgas[.]com
  - varying-rentals-calgary-predict[.]trycloudflare[.]com
- **File Hashes:**
  - **No malicious file hashes were identified.** This is a key finding that suggests the attack employed a fileless execution method or delivered its payload over an encrypted channel.
- **Suspicious User Agents:**
  - WindowsPowerShell/5.1.26100.4202

---

5. Recommendations

Based on the findings of this analysis, the following actions are recommended:

- **Immediate Network Hardening:**
  - **Firewall Rules:** Create and deploy firewall rules to block all inbound and outbound traffic to and from the identified malicious IP addresses.
  - **DNS Filtering:** Immediately add the malicious domains to the corporate DNS filtering blacklists and threat intelligence feeds.
- **Endpoint Security:**
  - **EDR Rules:** Create and deploy new EDR (Endpoint Detection and Response) rules to detect and prevent PowerShell scripts initiating network connections with suspicious User-Agents.
  - **Monitoring:** Enhance monitoring for unusual PowerShell activity, especially its network connections.
- **Future Prevention:**
  - **User Training:** Conduct mandatory security awareness training for all employees on identifying and avoiding malicious downloads and phishing attempts.
  - **Threat Hunting:** Conduct a proactive threat hunt across the network for any signs of communication with the identified IOCs to determine if the attack spread to other systems.