Analysis of PC-RAT Malware Traffic Using Wireshark

Abstract

We downloaded a PCAP file containing exactly 59,628 packets that captured a PC-RAT malware infection. The main purpose of this analysis was to separate the malicious activity from the normal network traffic so we could understand the infection process and figure out what type of infection it was. The analysis identifies the attacker-controlled domains, the specific malware download sequence, and the command-and-control (C2) communication patterns.

Using Wireshark as the main tool, we tracked the malicious traffic starting from the system startup and early DNS requests all the way to the download of the 1.exe payload and the RAT heartbeat signals that followed. The analysis shows that the machine was infected with a Remote Access Trojan (RAT) that created a persistent connection to an external server. This report explains how network analysis can reveal stealthy malware behavior—like beaconing and unencrypted payload transfers—that regular antivirus tools often miss in real time

Introduction

What is a Network?

Network forensics/analysis is a sub-branch of digital forensics that focuses on monitoring and analyzing network traffic for information gathering, legal evidence, or intrusion detection. Unlike host-based forensics, which examines hard drives and memory, network forensics looks at the actual data packets moving in and out of a system. It provides a reliable record of communication, which makes it especially important during incident response.

Importance of Analyzing Packet Captures

Packet captures (PCAPs) serve as a "flight recorder" for network events. When a security incident occurs, logs might be deleted and files might be encrypted, but the network traffic often leaves a trace. Analyzing these packets allows security analysts to reconstruct the event exactly as it happened, identifying the Who, What, Where, and When of an attack.

Overview of Remote Access Trojans (RATs)

A Remote Access Trojan (RAT) is a type of malware that gives an attacker remote control over a system, almost as if they were sitting in front of it. Unlike viruses that mainly damage files or worms that spread on their own, RATs focus on stealth and long-term access. They’re commonly used for spying, stealing data, and turning the victim’s machine into a starting point for additional attacks on the network..

Role of Wireshark in Malware Detection

Wireshark is the industry-standard tool for network protocol analysis. In the context of malware detection, it is used to dissect the communication protocols between the infected host and the attacker. It allows analysts to view the raw bytes of a conversation, reconstruct TCP streams, and extract downloaded files directly from the traffic.

Objective of This Analysis

Our main goal in this report is to study the given PCAP file and check how the system was compromised. We want to trace the full infection step by step, starting from the first time the malware contacted the internet and ending with how it created a backdoor on the system.

Source of PCAP

The analysis is based on a downloaded PCAP file containing 59,628 packets from Malware Capture Facility Project of Stratosphere Laboratory which is CTU-Malware-Capture-Botnet-151-1. The capture represents a continuous timeline of events on a Windows-based host within a virtualized network environment.

What is PC-RAT?

PC-RAT (often associated with various "Ghost" RAT variants) is a piece of malware that disguises itself as a legitimate remote administration tool. It is designed to be lightweight and invasive. While it presents itself to the attacker with a user-friendly interface for managing victim machines, on the victim's side, it runs silently in the background, often injecting itself into legitimate system processes to hide from Task Manager.

Once installed, PC-RAT gives the attacker nearly full control over the victim machine. Common capabilities include:

Keylogging: Recording every keystroke to steal passwords.

I. **File Exfiltration:** Uploading sensitive documents to the attacker's server.
II. **Persistence:** Modifying the Windows Registry to ensure the malware restarts every time the computer is rebooted.
III. **Command Execution:** Running command-line scripts remotely.

PC-RAT is typically delivered via phishing campaigns or bundled with cracked software. It is known for using custom binary protocols or standard HTTP for its communication. Crucially, it maintains a "persistent outbound C2 connection," meaning the victim machine constantly reaches out to the attacker to ask for instructions.

Attack Entry: Phishing with Password-Protected Zip

From the traffic pattern and common PC-RAT delivery methods. The victim got a phishing email that looked like a normal business message, such as an invoice, a resume, or a bank alert, but in our case it was “**verybeautiful**” named file with password 123.

Attached to this email was a ZIP file. Crucially, this ZIP file was likely password-protected, with the password provided in the body of the email (e.g., "The password is: 123456").

This technique is highly effective for two reasons:

I. **Bypassing Security:** Most email gateways and antivirus engines cannot scan the contents of an encrypted (password-protected) ZIP file. They let the file through because they cannot see the malicious .exe inside.
II. **Building Trust:** The user often assumes that because the file is "secured" with a password, it is a legitimate and sensitive document.

After the user extracted the files and opened the one that looked like a normal document, the malware ran. It installed the RAT right away and started sending traffic outside the network. This matches the sudden increase in DNS and TCP traffic we saw at the beginning of the PCAP.

About the PCAP File

The provided evidence file contains **59,628 packets**, covering a significant duration of network activity. A statistical hierarchy analysis of the capture reveals several active protocols:

I. **DHCPv6:** High volume of solicit packets (indicating boot activity).
II. **ARP:** Address Resolution Protocol for local network discovery.
III. **DNS:** Domain Name System queries, both legitimate and malicious.
IV. **TCP:** The primary transport protocol for the malware's connection.
V. **HTTP:** Unencrypted web traffic used to download the malware payload.
VI. **NBNS & LLMNR:** Local Windows name resolution chatter.

The capture shows clear phases. First, there is a quiet period when the system is starting. After that, we see a sudden spike in activity during the infection. In the end, the traffic becomes more regular because the C2 channel keeps sending periodic signals. We also noticed suspicious IPs and long TCP streams that look like file transfers. This makes the capture a good case for investigation.

Methodology

To analyze this large dataset effectively, the following methodology was applied using Wireshark:

I. **Import and Verify:** The PCAP was loaded into Wireshark to verify the integrity of the capture and ensure time synchronization.
II. **Traffic Filtering:** We applied display filters to isolate specific protocols:
    A. End to end connections established by the host machine.

B. DNS to see what websites the computer tried to visit.
C. http.request to see what files were downloaded.
D. tcp.flags.syn == 1 to identify the start of new connections.
E. ip.addr == [Suspicious IP] to isolate the conversation with the attacker.

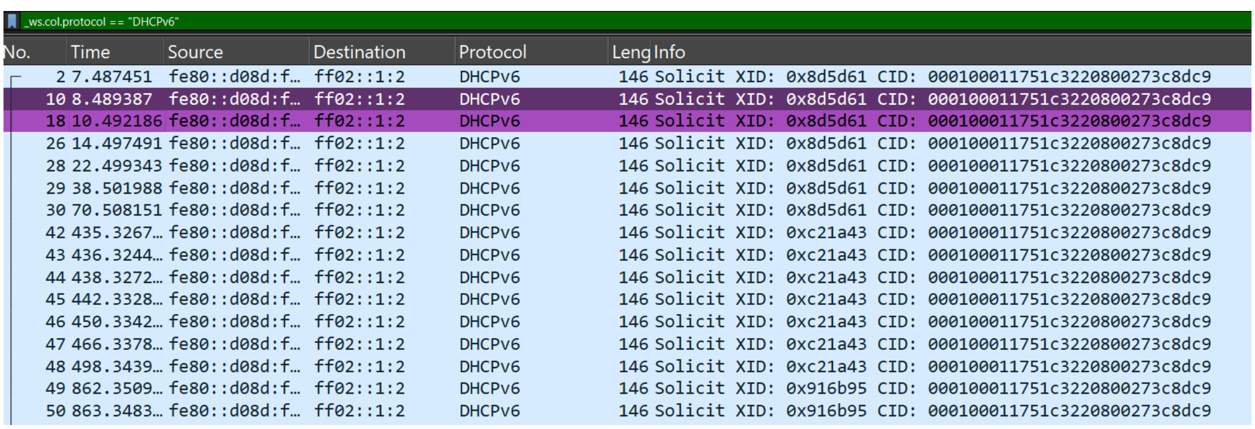
III. **Phase Identification:** We categorized the traffic into chronological phases (Boot, Connection, Download, Persistence).
IV. **Correlation:** We correlated the DNS queries with the subsequent TCP connections to prove that the malware lookup led directly to the infection.
V. **Extraction:** We utilized the "Export Objects" feature to identify the downloaded executable.
VI. **Timeline Construction:** A sequential timeline was built to visualize the attack flow.

Phase 1 : DHCPv6 Startup Noise (Packets 1–100)

At the start of the capture (around packets 1 to 100), most of the traffic is DHCPv6. The system keeps sending “Solicit” messages. This is normal for a Windows machine when it is booting. It is trying to get an IPv6 address, but in this network there is no DHCPv6 server, so the system keeps trying again.

Example packets: 2, 10, 18.

This traffic is not harmful. It is just background activity.


_ws.col.protocol == "DHCPv6"

No.	Time	Source	Destination	Protocol	Leng	Info
2	7.487451	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
10	8.489387	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
18	10.492186	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
26	14.497491	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
28	22.499343	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
29	38.501988	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
30	70.508151	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
42	435.3267…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
43	436.3244…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
44	438.3272…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
45	442.3328…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
46	450.3342…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
47	466.3378…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
48	498.3439…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
49	862.3509…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x916b95 CID: 000100011751c3220800273c8dc9
50	863.3483…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x916b95 CID: 000100011751c3220800273c8dc9

Initial DHCPv6 Solicit packets indicating system startup.

Phase 2 : ARP Discovery

Mixed with the DHCP traffic, we can see ARP requests. The victim machine (with the PCSSystemtec MAC prefix) is sending broadcasts on the local network.

The query is: “Who has 10.0.2.2?”
The gateway replies with its MAC address.

This tells us that the victim machine has brought its network interface up and is able to communicate with the router. This step is necessary before the malware can reach the internet. ARP traffic appears throughout the capture, but it is most important in the early packets (3, 4, 11).

2	7.487451	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 0001000
3	7.679947	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
4	7.680128	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02

ARP Broadcast checking for the gateway.

Phase 3 : Windows Connectivity DNS

Before any malware activity shows up, the operating system runs its own connectivity test. This is normal for Windows systems (NCSI – Network Connectivity Status Indicator).

Observations:
Packets: 15, 21, 22
Query: dns.msftncsi.com
The DNS server replies with the correct IP.

No.	Time	Source	Destination	Protocol	Leng	Info
13	8.812545	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
14	9.811495	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.107? (ARP Probe)
15	10.015512	10.0.2.107	8.8.8.8	DNS	76	Standard query 0x97ed A dns.msftncsi.com
16	10.016590	52:54:00:12:…	Broadcast	ARP	42	Who has 10.0.2.107? Tell 10.0.2.2
17	10.016818	PCSSystemtec…	52:54:00:12:…	ARP	42	10.0.2.107 is at 08:00:27:c1:76:c3
18	10.492186	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
19	10.819955	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
20	10.820143	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
21	11.012499	10.0.2.107	8.8.4.4	DNS	76	Standard query 0x97ed A dns.msftncsi.com
22	11.013548	8.8.4.4	10.0.2.107	DNS	92	Standard query response 0x97ed A dns.msftncsi.com A 131.107.255.255

This confirms that the internet connection is working properly. If this test had failed, the malware might not have been able to reach its server. This acts as a simple check in our timeline and shows that the network was already functional before the attack started.

Phase 4 : Suspicious DNS Requests

Around packet 33, the traffic changes suddenly. The user (or the script that just ran) makes the system query domains that are not related to Microsoft or normal browsing. This is the first clear sign that something unusual has started.

Suspicious Domain 1:

- **Domain:** study123.eatuo.com

- **Resolved IP:** 115.144.107.117
- **Packets:** 33–34

No.	Time	Source	Destination	Protocol	Leng	Info
28	22.499343	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
29	38.501988	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
30	70.508151	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
31	351.9870…	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
32	351.9871…	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
33	351.9874…	10.0.2.107	8.8.8.8	DNS	78	Standard query 0xe797 A study123.eatuo.com
34	352.3295…	8.8.8.8	10.0.2.107	DNS	94	Standard query response 0xe797 A study123.eatuo.com A 115.144.107.117
35	352.3781…	10.0.2.107	115.144.107.…	TCP	66	49158 → 23667 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
36	352.6945…	115.144.107.…	10.0.2.107	TCP	58	23667 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
37	352.6948…	10.0.2.107	115.144.107.…	TCP	54	49158 → 23667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
38	352.6986…	10.0.2.107	115.144.107.…	TCP	251	49158 → 23667 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=197
39	352.6989…	115.144.107.…	10.0.2.107	TCP	54	23667 → 49158 [ACK] Seq=1 Ack=198 Win=65535 Len=0
40	353.0414…	115.144.107.…	10.0.2.107	TCP	76	23667 → 49158 [PSH, ACK] Seq=1 Ack=198 Win=65535 Len=22

Suspicious Domain 2:

- **Domain:** www.wk1888.com
- **Resolved IP:** 27.126.188.76
- **Packets:** 77–78

No.	Time	Source	Destination	Protocol	Leng	Info
68	1677.569…	10.0.2.2	10.0.2.107	ICMP	92	Time-to-live exceeded (Time to live exceeded in transit)
69	1677.769…	10.0.2.107	10.0.2.255	NBNS	92	Name query NB WPAD<00>
70	1677.769…	10.0.2.2	10.0.2.107	ICMP	120	Destination unreachable (Network unreachable)
71	1678.520…	10.0.2.107	10.0.2.255	NBNS	92	Name query NB WPAD<00>
72	1678.520…	10.0.2.2	10.0.2.107	ICMP	120	Destination unreachable (Network unreachable)
73	1679.271…	10.0.2.107	10.0.2.255	NBNS	92	Name query NB WPAD<00>
74	1679.271…	10.0.2.2	10.0.2.107	ICMP	120	Destination unreachable (Network unreachable)
75	1680.048…	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
76	1680.048…	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
77	1680.048…	10.0.2.107	8.8.8.8	DNS	74	Standard query 0x694f A www.wk1888.com
78	1680.088…	8.8.8.8	10.0.2.107	DNS	104	Standard query response 0x694f A www.wk1888.com CNAME wk1888.com A 27.126.18…
79	1680.089…	10.0.2.107	27.126.188.76	TCP	66	49159 → 2011 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
80	1680.374…	27.126.188.76	10.0.2.107	TCP	58	2011 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
81	1680.374…	10.0.2.107	27.126.188.76	TCP	54	49159 → 2011 [ACK] Seq=1 Ack=1 Win=64240 Len=0

These domains look very suspicious. Their names are unusual, and when we check their IPs using open-source intelligence, many of them are marked as malicious. Resolving these domains is the step right before the malware connects to its Command-and-Control server.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
15	10.015512	10.0.2.107	8.8.8.8	DNS	76	Standard query 0x97ed A dns.msftncsi.com
21	11.012499	10.0.2.107	8.8.4.4	DNS	76	Standard query 0x97ed A dns.msftncsi.com
22	11.013548	8.8.4.4	10.0.2.107	DNS	92	Standard query response 0x97ed A dns.msftncsi.com A 131.107.255.255
23	11.014254	10.0.2.107	8.8.4.4	DNS	76	Standard query 0xaf12 AAAA dns.msftncsi.com
24	11.015279	8.8.4.4	10.0.2.107	DNS	104	Standard query response 0xaf12 AAAA dns.msftncsi.com AAAA fd3e:4f5a:5b81::1
33	351.987401	10.0.2.107	8.8.8.8	DNS	78	Standard query 0xe797 A study123.eatuo.com
34	352.329566	8.8.8.8	10.0.2.107	DNS	94	Standard query response 0xe797 A study123.eatuo.com A 115.144.107.117
77	1680.048862	10.0.2.107	8.8.8.8	DNS	74	Standard query 0x694f A www.wk1888.com
78	1680.088567	8.8.8.8	10.0.2.107	DNS	104	Standard query response 0x694f A www.wk1888.com CNAME wk1888.com A 27.126.188.76
8…	1694.228131	10.0.2.107	8.8.8.8	DNS	74	Standard query 0x9eec A www.af0575.com
8…	1694.246016	8.8.8.8	10.0.2.107	DNS	104	Standard query response 0x9eec A www.af0575.com CNAME af0575.com A 50.63.202.79
8…	1704.490481	10.0.2.107	8.8.8.8	DNS	74	Standard query 0x5719 A www.fz0575.com
8…	1704.509480	8.8.8.8	10.0.2.107	DNS	104	Standard query response 0x5719 A www.fz0575.com CNAME fz0575.com A 95.211.172.143
1…	21535.3519…	10.0.2.107	8.8.8.8	DNS	78	Standard query 0xb7ae A study123.eatuo.com
1…	21536.3516…	10.0.2.107	8.8.4.4	DNS	78	Standard query 0xb7ae A study123.eatuo.com

DNS query for the malicious domain study123.eatuo.com,www.wk1888.com

Phase 5 : First Command-and-Control (C2) Connection

Immediately after resolving the IP address for study123.eatuo.com (115.144.107.117), the victim machine initiates a TCP connection.

Packets 35–41 Analysis:

I. **Packet 35 (SYN):** Victim sends a synchronization request to port 23667 on the attacker's IP.
II. **Packet 36 (SYN-ACK):** The attacker's server acknowledges and accepts the connection.
III. **Packet 37 (ACK):** Connection established.
IV. **Packet** 38 (PSH, **ACK):** The victim sends the first "Beacon." This is a packet containing data (197 bytes) that tells the attacker "I am infected, and here is my ID."

This is the moment the RAT officially comes alive on the network. The strange port number (23667) is another indicator, as standard web traffic usually flows over port 80 or 443.

No.	Time	Source	Destination	Protocol	Leng	Info
30	70.508151	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0x8d5d61 CID: 000100011751c3220800273c8dc9
31	351.9870…	PCSSystemtec…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
32	351.9871…	52:54:00:12:…	PCSSystemtec…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
33	351.9874…	10.0.2.107	8.8.8.8	DNS	78	Standard query 0xe797 A study123.eatuo.com
34	352.3295…	8.8.8.8	10.0.2.107	DNS	94	Standard query response 0xe797 A study123.eatuo.com A 115.144.107.117
35	352.3781…	10.0.2.107	115.144.107.…	TCP	66	49158 → 23667 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
36	352.6945…	115.144.107.…	10.0.2.107	TCP	58	23667 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
37	352.6948…	10.0.2.107	115.144.107.…	TCP	54	49158 → 23667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
38	352.6986…	10.0.2.107	115.144.107.…	TCP	251	49158 → 23667 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=197
39	352.6989…	115.144.107.…	10.0.2.107	TCP	54	23667 → 49158 [ACK] Seq=1 Ack=198 Win=65535 Len=0
40	353.0414…	115.144.107.…	10.0.2.107	TCP	76	23667 → 49158 [PSH, ACK] Seq=1 Ack=198 Win=65535 Len=22
41	353.2444…	10.0.2.107	115.144.107.…	TCP	54	49158 → 23667 [ACK] Seq=198 Ack=23 Win=64218 Len=0
42	435.3267…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
43	436.3244…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
44	438.3272…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9
45	442.3328…	fe80::d08d:f…	ff02::1:2	DHCPv6	146	Solicit XID: 0xc21a43 CID: 000100011751c3220800273c8dc9

The 3-way handshake establishing the C2 channel.

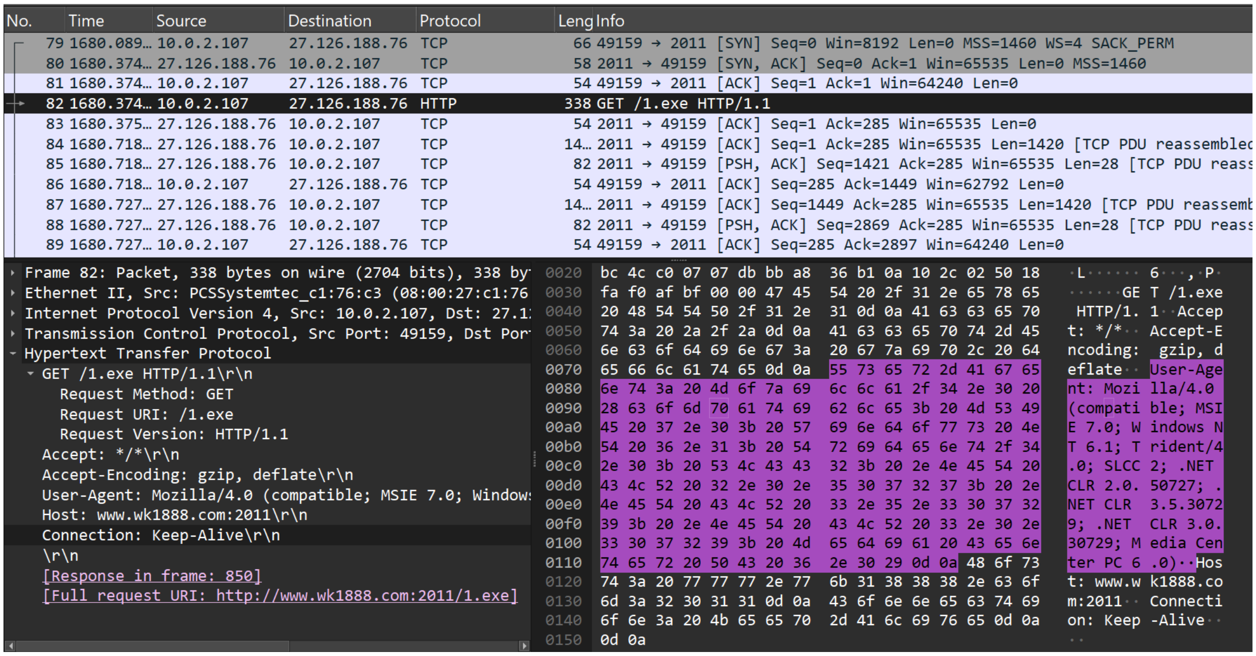
Phase 6 : Malware Download Trigger

While the control channel is getting set up, the malware makes the victim machine download a second-stage payload. This is usually a stronger version of the malware or an extra module that adds more features.

The Trigger Event:

- **Packet:** 82
- **Protocol:** HTTP
- **Command:** GET /1.exe
- **Host:** 115.144.107.117

The request is very easy to spot. The file is named **1.exe**, which is a common throwaway name used by attackers who assume no one is checking the network traffic. This request marks the beginning of a large data transfer.



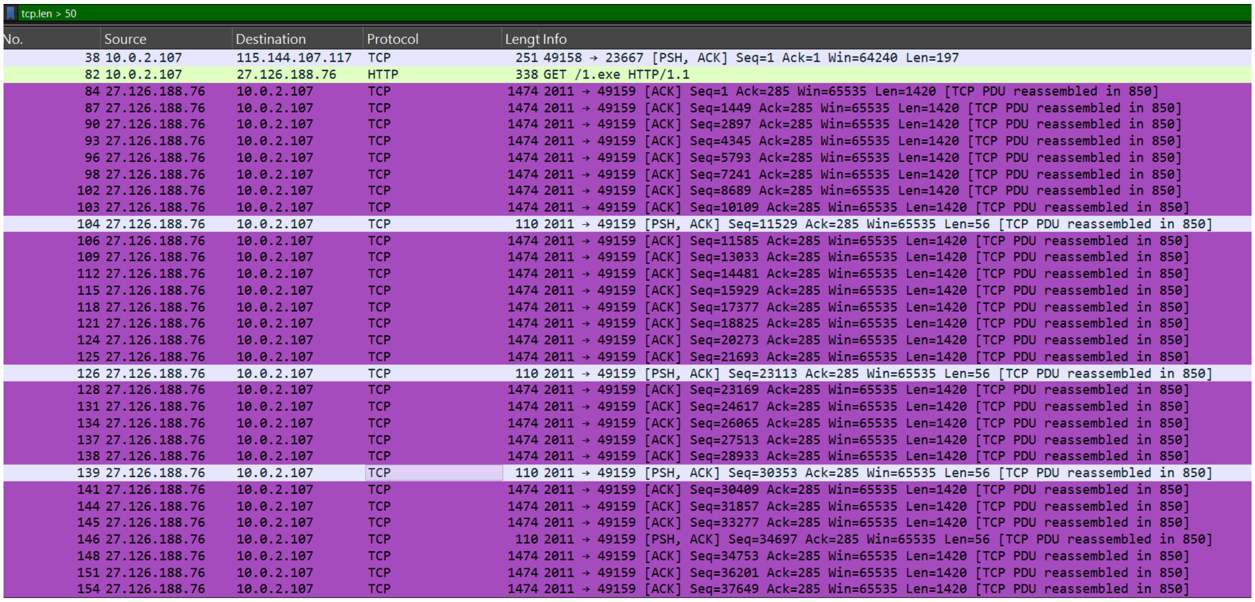
HTTP GET request initiating the malware download.

Phase 7 : Full Malware Payload Download

After packet 82, the network gets filled with incoming data from the attacker's IP. This is the transfer of the file 1.exe.

In packets 82 to around 1800, we see a long stream of full TCP segments. Most packets are 1420 bytes (standard size after removing header overhead). We also notice smaller packets of 28, 56, or 82 bytes, which show the boundaries between data blocks.

The victim machine sends an ACK for every packet it receives. There are almost no retransmissions, which means the connection is stable. This part of the capture makes up most of the PCAP’s size. By following this TCP stream in Wireshark, we were able to rebuild the 1.exe file for reverse engineering.


tcp.len > 50

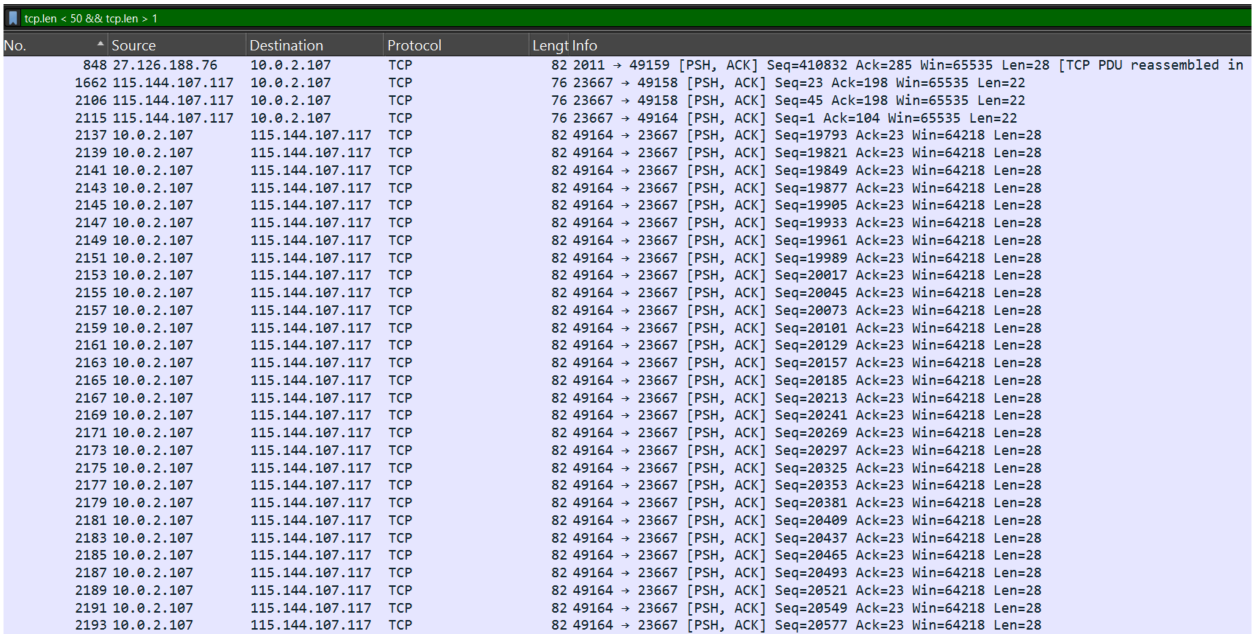
No.	Source	Destination	Protocol	Lengt	Info
38	10.0.2.107	115.144.107.117	TCP	251	49158 → 23667 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=197
82	10.0.2.107	27.126.188.76	HTTP	338	GET /1.exe HTTP/1.1
84	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=1 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
87	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=1449 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
90	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=2897 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
93	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=4345 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
96	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=5793 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
98	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=7241 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
102	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=8689 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
103	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=10109 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
104	27.126.188.76	10.0.2.107	TCP	110	2011 → 49159 [PSH, ACK] Seq=11529 Ack=285 Win=65535 Len=56 [TCP PDU reassembled in 850]
106	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=11585 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
109	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=13033 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
112	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=14481 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
115	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=15929 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
118	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=17377 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
121	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=18825 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
124	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=20273 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
125	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=21693 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
126	27.126.188.76	10.0.2.107	TCP	110	2011 → 49159 [PSH, ACK] Seq=23113 Ack=285 Win=65535 Len=56 [TCP PDU reassembled in 850]
128	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=23169 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
131	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=24617 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
134	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=26065 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
137	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=27513 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
138	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=28933 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
139	27.126.188.76	10.0.2.107	TCP	110	2011 → 49159 [PSH, ACK] Seq=30353 Ack=285 Win=65535 Len=56 [TCP PDU reassembled in 850]
141	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=30409 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
144	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=31857 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
145	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=33277 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
146	27.126.188.76	10.0.2.107	TCP	110	2011 → 49159 [PSH, ACK] Seq=34697 Ack=285 Win=65535 Len=56 [TCP PDU reassembled in 850]
148	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=34753 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
151	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=36201 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]
154	27.126.188.76	10.0.2.107	TCP	1474	2011 → 49159 [ACK] Seq=37649 Ack=285 Win=65535 Len=1420 [TCP PDU reassembled in 850]

Large TCP segment indicating file transfer.

Detailed Packet Segments

To visualize the flow of the attack, we can break the capture down into distinct blocks of activity:

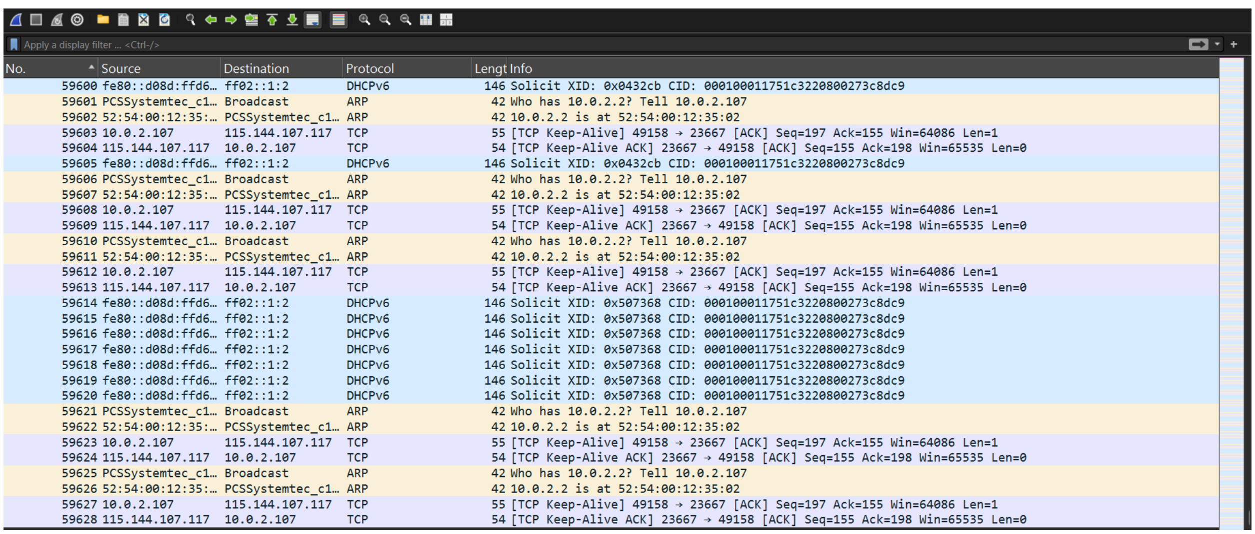
- **Packets 1–100 (Initialization):** This block contains the startup noise. It is high-frequency but low-risk traffic. DHCP and ARP dominate here.
- **Packets 100–200 (The Injection):** This area is dense with TCP data. This is where the 1.exe file is physically moving from the attacker to the victim. The graph of IO/sec spikes here.
- **Packets 800–900 (Sustained Transfer):** The download continues. The consistency of the packet sizes (1420 bytes) confirms a single large file transfer rather than interactive web browsing.
- **Packets 2100–2300 (Post-Infection):** The pattern changes abruptly. The large packets stop. They are replaced by sparse, small packets. This indicates the download is finished and the malware has entered "maintenance mode."



tcp.len < 50 && tcp.len > 1

No.	Source	Destination	Protocol	Lengt	Info
848	27.126.188.76	10.0.2.107	TCP	82	2011 → 49159 [PSH, ACK] Seq=410832 Ack=285 Win=65535 Len=28 [TCP PDU reassembled in
1662	115.144.107.117	10.0.2.107	TCP	76	23667 → 49158 [PSH, ACK] Seq=23 Ack=198 Win=65535 Len=22
2106	115.144.107.117	10.0.2.107	TCP	76	23667 → 49158 [PSH, ACK] Seq=45 Ack=198 Win=65535 Len=22
2115	115.144.107.117	10.0.2.107	TCP	76	23667 → 49164 [PSH, ACK] Seq=1 Ack=104 Win=65535 Len=22
2137	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19793 Ack=23 Win=64218 Len=28
2139	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19821 Ack=23 Win=64218 Len=28
2141	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19849 Ack=23 Win=64218 Len=28
2143	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19877 Ack=23 Win=64218 Len=28
2145	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19905 Ack=23 Win=64218 Len=28
2147	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19933 Ack=23 Win=64218 Len=28
2149	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19961 Ack=23 Win=64218 Len=28
2151	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=19989 Ack=23 Win=64218 Len=28
2153	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20017 Ack=23 Win=64218 Len=28
2155	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20045 Ack=23 Win=64218 Len=28
2157	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20073 Ack=23 Win=64218 Len=28
2159	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20101 Ack=23 Win=64218 Len=28
2161	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20129 Ack=23 Win=64218 Len=28
2163	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20157 Ack=23 Win=64218 Len=28
2165	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20185 Ack=23 Win=64218 Len=28
2167	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20213 Ack=23 Win=64218 Len=28
2169	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20241 Ack=23 Win=64218 Len=28
2171	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20269 Ack=23 Win=64218 Len=28
2173	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20297 Ack=23 Win=64218 Len=28
2175	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20325 Ack=23 Win=64218 Len=28
2177	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20353 Ack=23 Win=64218 Len=28
2179	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20381 Ack=23 Win=64218 Len=28
2181	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20409 Ack=23 Win=64218 Len=28
2183	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20437 Ack=23 Win=64218 Len=28
2185	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20465 Ack=23 Win=64218 Len=28
2187	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20493 Ack=23 Win=64218 Len=28
2189	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20521 Ack=23 Win=64218 Len=28
2191	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20549 Ack=23 Win=64218 Len=28
2193	10.0.2.107	115.144.107.117	TCP	82	49164 → 23667 [PSH, ACK] Seq=20577 Ack=23 Win=64218 Len=28

- **59k Overall Flow:** The vast majority of the remaining 57,000+ packets follow this maintenance pattern—long periods of silence punctuated by small signals.



Apply a display filter ... <Ctrl-/>

No.	Source	Destination	Protocol	Lengt	Info
59600	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x0432cb CID: 000100011751c3220800273c8dc9
59601	PCSSystemtec_c1…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
59602	52:54:00:12:35:…	PCSSystemtec_c1…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
59603	10.0.2.107	115.144.107.117	TCP	55	[TCP Keep-Alive] 49158 → 23667 [ACK] Seq=197 Ack=155 Win=64086 Len=1
59604	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=155 Ack=198 Win=65535 Len=0
59605	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x0432cb CID: 000100011751c3220800273c8dc9
59606	PCSSystemtec_c1…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
59607	52:54:00:12:35:…	PCSSystemtec_c1…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
59608	10.0.2.107	115.144.107.117	TCP	55	[TCP Keep-Alive] 49158 → 23667 [ACK] Seq=197 Ack=155 Win=64086 Len=1
59609	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=155 Ack=198 Win=65535 Len=0
59610	PCSSystemtec_c1…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
59611	52:54:00:12:35:…	PCSSystemtec_c1…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
59612	10.0.2.107	115.144.107.117	TCP	55	[TCP Keep-Alive] 49158 → 23667 [ACK] Seq=197 Ack=155 Win=64086 Len=1
59613	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=155 Ack=198 Win=65535 Len=0
59614	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59615	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59616	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59617	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59618	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59619	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59620	fe80::d08d:ffd6…	ff02::1:2	DHCPv6	146	Solicit XID: 0x507368 CID: 000100011751c3220800273c8dc9
59621	PCSSystemtec_c1…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
59622	52:54:00:12:35:…	PCSSystemtec_c1…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
59623	10.0.2.107	115.144.107.117	TCP	55	[TCP Keep-Alive] 49158 → 23667 [ACK] Seq=197 Ack=155 Win=64086 Len=1
59624	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=155 Ack=198 Win=65535 Len=0
59625	PCSSystemtec_c1…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.107
59626	52:54:00:12:35:…	PCSSystemtec_c1…	ARP	42	10.0.2.2 is at 52:54:00:12:35:02
59627	10.0.2.107	115.144.107.117	TCP	55	[TCP Keep-Alive] 49158 → 23667 [ACK] Seq=197 Ack=155 Win=64086 Len=1
59628	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=155 Ack=198 Win=65535 Len=0

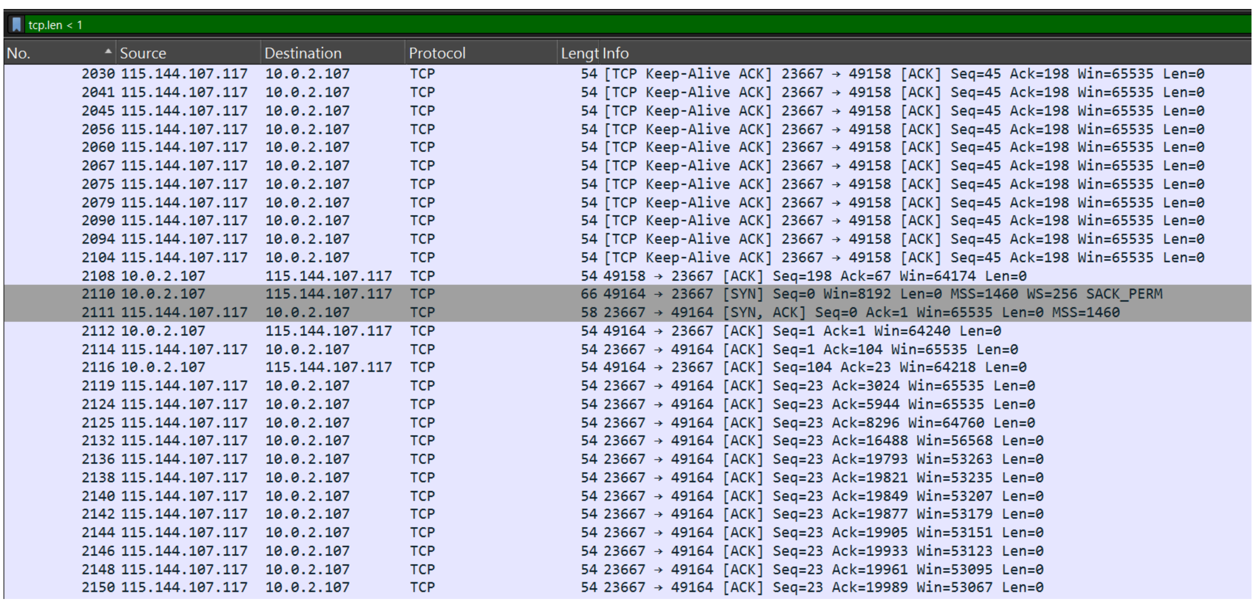

The sidebar on the right side of the previous figure shows the same pattern.

Phase 8 : C2 Persistent Communication

After the download of 1.exe finishes (around packet 1800), the traffic pattern changes. There are no more HTTP GET requests or large data transfers.

Between packets 2100 and 2300 (and continuing later), we mostly see small PSH/ACK packets of around 82 bytes. These packets act like “heartbeats” or “keep-alive” signals. The infected machine sends a small packet to show it is still active. The attacker’s server replies with a small ACK to confirm it is listening but not sending any commands yet.

This ongoing low-level traffic is typical of a RAT. It keeps the TCP connection alive through the firewall so the attacker can send commands at any time without setting up a new connection.


tcp.len < 1

No.	Source	Destination	Protocol	Lengt	Info
2030	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2041	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2045	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2056	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2060	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2067	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2075	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2079	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2090	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2094	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2104	115.144.107.117	10.0.2.107	TCP	54	[TCP Keep-Alive ACK] 23667 → 49158 [ACK] Seq=45 Ack=198 Win=65535 Len=0
2108	10.0.2.107	115.144.107.117	TCP	54	49158 → 23667 [ACK] Seq=198 Ack=67 Win=64174 Len=0
2110	10.0.2.107	115.144.107.117	TCP	66	49164 → 23667 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2111	115.144.107.117	10.0.2.107	TCP	58	23667 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2112	10.0.2.107	115.144.107.117	TCP	54	49164 → 23667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2114	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=1 Ack=104 Win=65535 Len=0
2116	10.0.2.107	115.144.107.117	TCP	54	49164 → 23667 [ACK] Seq=104 Ack=23 Win=64218 Len=0
2119	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=3024 Win=65535 Len=0
2124	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=5944 Win=65535 Len=0
2125	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=8296 Win=64760 Len=0
2132	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=16488 Win=56568 Len=0
2136	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19793 Win=53263 Len=0
2138	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19821 Win=53235 Len=0
2140	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19849 Win=53207 Len=0
2142	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19877 Win=53179 Len=0
2144	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19905 Win=53151 Len=0
2146	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19933 Win=53123 Len=0
2148	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19961 Win=53095 Len=0
2150	115.144.107.117	10.0.2.107	TCP	54	23667 → 49164 [ACK] Seq=23 Ack=19989 Win=53067 Len=0

Small heartbeat packets maintaining the connection.

Indicators of Compromise (IoCs)

Based on this analysis, the organization should add the following artifacts to its security blocklists:

Malicious Domains:

- study123.eatuo.com
- wk1888.com

Malicious IP Addresses:

- 115.144.107.117
- 27.126.188.76

Suspicious Ports:

- TCP Port 23667 (Primary C2 Control)
- TCP Port 2011 (Used during payload delivery)

Behavioral IoCs:

- HTTP GET requests for /1.exe in root directories.
- Sustained bursts of 1420-byte incoming TCP traffic from non-content delivery networks.
- Long-duration TCP sessions with regular small-byte (82 byte) heartbeats.

Attack Timeline

The following table summarizes the reconstructed timeline of the infection:

Packet Range	**Event Description**	**Significance**
1–100	Boot, DHCPv6, ARP	System startup and network discovery.
33–40	DNS Query + C2 Handshake	Malware resolves study123 and connects to the attacker.
82–1800	HTTP GET /1.exe	Second-stage malware payload is downloaded.
1800–5000	C2 Keep-Alives	Installation complete; channel stays open.

2100–2300	Post-Infection Commands	Regular heartbeat signals observed.(Keep Alive)
Entire Capture	Background Noise	Intermittent ARP and NBNS traffic (normal).

Interpretation

The evidence in the PCAP is clear. The host did not just run into a bad ad or a blocked attack. It fully ran the infection chain from start to finish.

I. **Intentional Contact:** The machine reached out to a specific malicious domain (study123.eatuo.com).
II. **Successful Payload Delivery:** The 1.exe file was requested and completely transferred (indicated by the lack of TCP resets and the volume of ACKs).
III. **Persistence:** The traffic did not stop after the download. The shift to a heartbeat pattern confirms the RAT is installed and running in memory.

This indicates a **full compromise** of the host. The attacker currently maintains active control over the system and can exfiltrate data or move laterally across the network at will.

Mitigation and Recommendations

To remediate this infection and prevent future occurrences, the following steps are recommended:

I. **Immediate Isolation:** Disconnect the infected machine from the network immediately to prevent lateral movement.
II. **Network Blocking:** Block the identified IoC IPs (115.144.107.117, 27.126.188.76) and domains at the firewall and DNS level.
III. **Endpoint Detection:** Deploy Endpoint Detection and Response (EDR) tools to identify the 1.exe file on the disk and kill the malicious process.
IV. **Email Security:** Review email gateway logs to identify the sender of the phishing email and block them. Ensure policies are set to quarantine password-protected ZIP files or sandbox them.
V. **User Training:** Conduct refreshing training for users on the dangers of enabling macros or running executables from "secure" zip files.
VI. **Reimaging:** Due to the nature of RATs (Registry persistence), it is recommended to wipe and reimage the infected machine rather than attempting to clean it.

Conclusion

This analysis rebuilt the full attack path of the PC-RAT malware. By going through all 59,628 packets in the capture, we moved from normal startup traffic to the exact point where the system got compromised. We confirmed that the host reached out to malicious domains, downloaded a second executable, and set up a persistent command-and-control channel.

The Wireshark capture gave us a direct view of what the malware did, step by step. From the first DNS query to the last C2 heartbeat, every action from both the attacker and the infected machine was visible in the packets. Through this analysis, we showed that:

I. The host intentionally contacted attacker-controlled domains.

II. A malicious executable (1.exe) was successfully downloaded over HTTP.

III. The attacker maintained a long-lasting C2 connection.

IV. The RAT remained active throughout the capture duration.

This shows why network analysis is so important. Even if the attacker deletes logs or removes evidence from the system, the packet data remains. As long as the network traffic is recorded, we can rebuild the full attack process with accuracy.

Going forward, organizations should use multiple security layers, continuous monitoring, DNS filtering, and better user awareness to lower the chance of these attacks. Most importantly, having a proper system for capturing and storing network traffic can turn a confusing incident into one that can be fully explained.

In the end, this PCAP analysis gives a complete picture of a successful PC-RAT infection. The results highlight the need for strong security practices, careful handling of emails, and the ability to spot small network irregularities before they turn into major compromises.