

# 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	<b>Wireshark</b>
Threat Intelligence	<b>VirusTotal</b> , OSINT research
Packet Filtering	Wireshark Display Filters
File Analysis	Hash extraction, file signature inspection
Decoding Tool	<b>CyberChef</b> (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:

Wireshark - Conversations - 2023-02-03.pcap

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter
- Copy
- Follow Stream...
- Graph...
- Protocol: Ethernet
- Filter list for specific type

Ethernet · 8	IPv4 · 150	IPv6	TCP · 762	UDP · 722			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	
10.0.0.149	10.0.0.6	12,040	8 MB	8,036	7 MB	4,004	
10.0.0.149	208.187.122.74	9,806	7 MB	4,712	474 kB	5,094	
10.0.0.149	5.75.205.43	4,127	3 MB	1,878	3 MB	2,249	
10.0.0.149	74.6.143.26	2,747	2 MB	1,314	75 kB	1,433	
10.0.0.149	128.254.207.55	1,924	2 MB	639	35 kB	1,285	
10.0.0.149	13.107.42.14	1,449	1 MB	674	53 kB	775	
10.0.0.149	23.58.117.164	1,020	722 kB	497	32 kB	523	
10.0.0.149	209.131.162.45	1,047	710 kB	470	34 kB	577	
10.0.0.149	102.156.32.143	892	680 kB	471	655 kB	421	
10.0.0.149	23.214.54.85	877	657 kB	411	28 kB	466	
10.0.0.149	69.58.187.40	880	650 kB	400	25 kB	480	
10.0.0.149	20.10.31.115	1,024	598 kB	350	40 kB	674	
10.0.0.149	184.86.169.24	764	550 kB	375	26 kB	389	
10.0.0.149	78.31.67.7	3,913	439 kB	1,947	311 kB	1,966	
10.0.0.149	23.64.146.226	524	376 kB	244	19 kB	280	
10.0.0.149	23.111.114.52	2,342	335 kB	1,071	235 kB	1,271	
10.0.0.149	96.6.184.69	404	282 kB	194	14 kB	210	

### 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

Wireshark - Protocol Hierarchy Statistics - 2023-02-03.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	B
Frame	100.0	55207	100.0	31172531	2
Ethernet	100.0	55207	2.5	772898	5
Internet Protocol Version 4	96.3	53164	3.4	1063308	8
User Datagram Protocol	3.1	1730	0.0	13840	1
Transmission Control Protocol	93.1	51423	93.2	29062433	2
Transport Layer Security	13.2	7277	62.2	19375514	1
Simple Mail Transfer Protocol	0.1	37	0.0	2196	1
NetBIOS Session Service	1.6	884	17.6	5485249	4
SMB2 (Server Message Block Protocol version 2)	1.3	744	17.6	5471348	4
Data	0.1	38	17.0	5286439	4
SMB (Server Message Block Protocol)	0.2	126	0.1	16167	1
SMB Pipe Protocol	0.1	28	0.0	406	0
Microsoft Windows Lanman Remote API Protocol	0.1	28	0.0	468	0
Lightweight Directory Access Protocol	2.3	1278	2.7	840142	6
Malformed Packet	0.0	4	0.0	0	0
Kerberos	0.1	46	0.2	56566	4
Hypertext Transfer Protocol	0.0	4	5.7	1763357	1

No display filter.

Help Protocols Copy Close

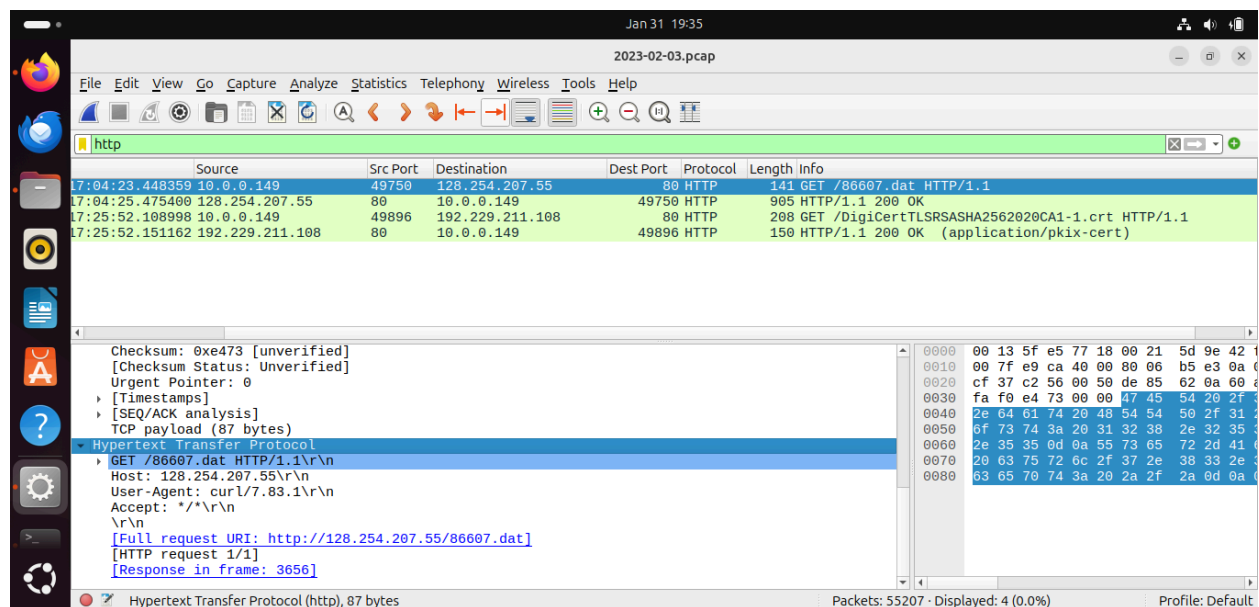
Since HTTP traffic is unencrypted and had fewer packets, it was analyzed first.

# Malicious File Download via HTTP

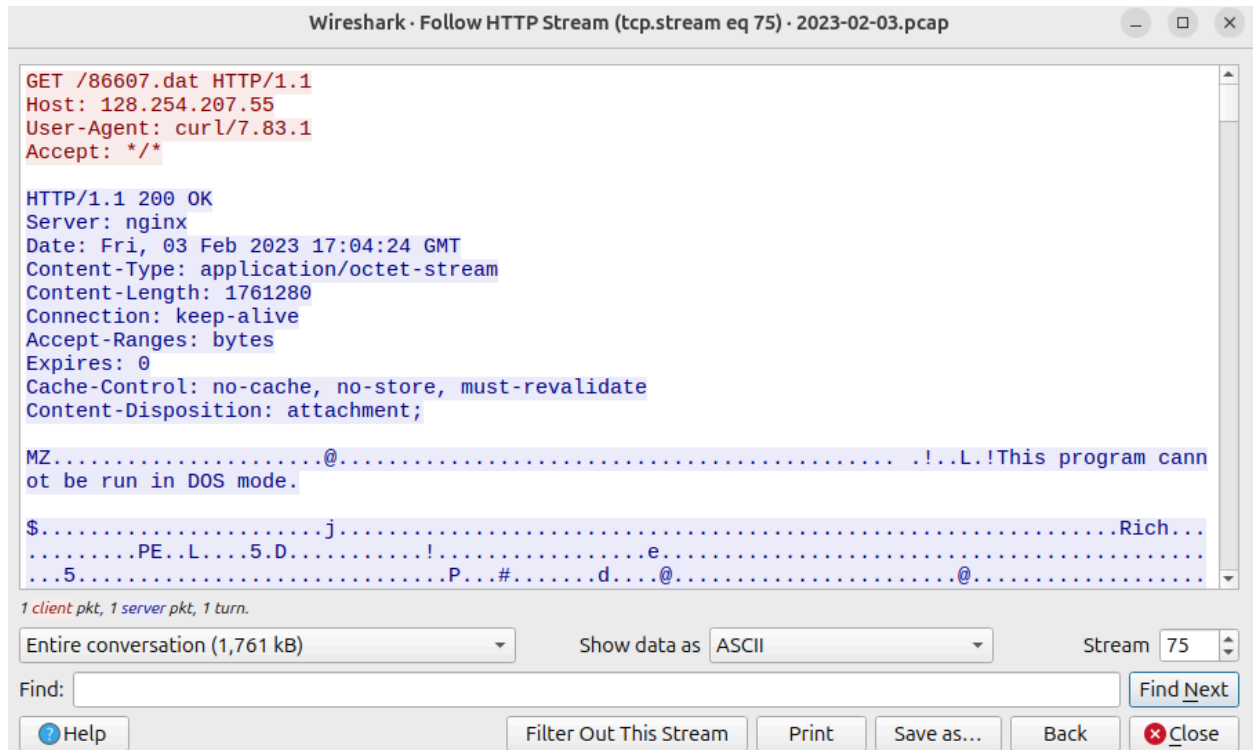
Filtering for HTTP traffic revealed **4 packets**.

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)



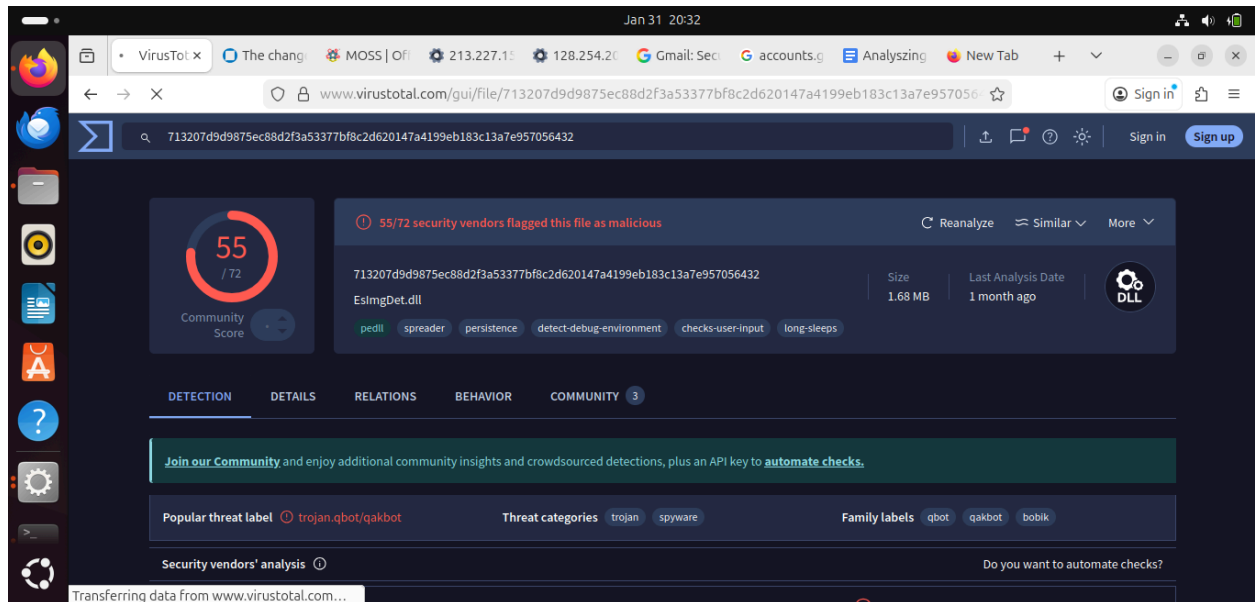
Inspection of the file contents revealed the “MZ” file signature, indicating the .dat file is actually a **Windows executable**.



## Malware Confirmation

The file was exported and hashed.  
VirusTotal results showed:

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



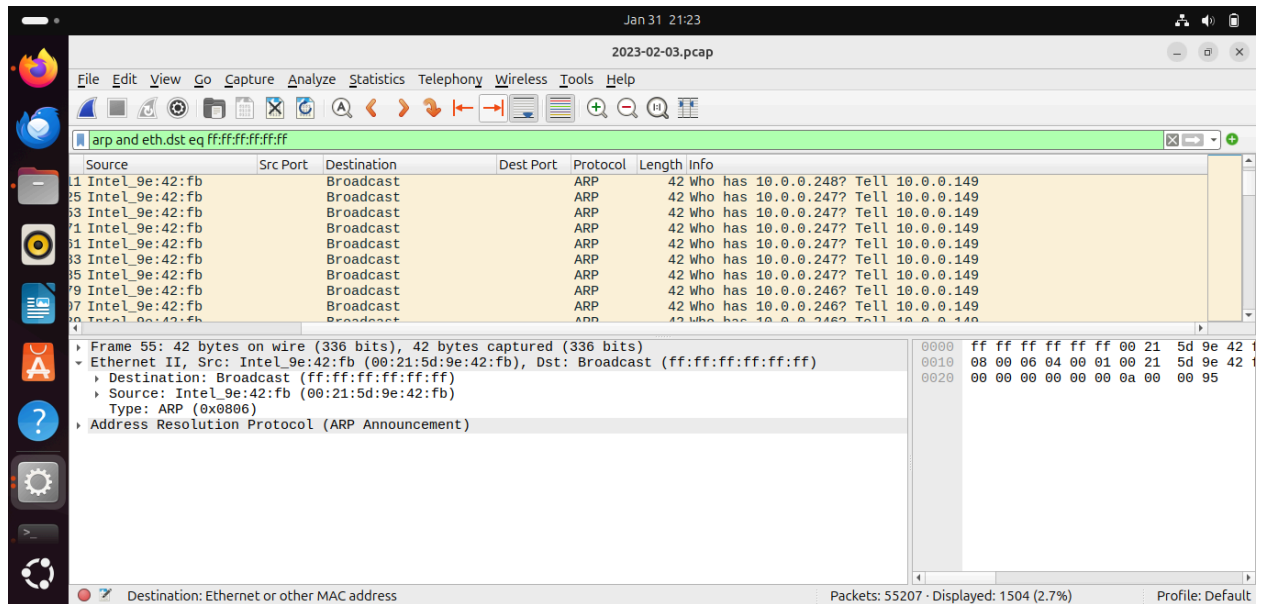
## Post-Infection Behavior — ARP Scanning

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**.

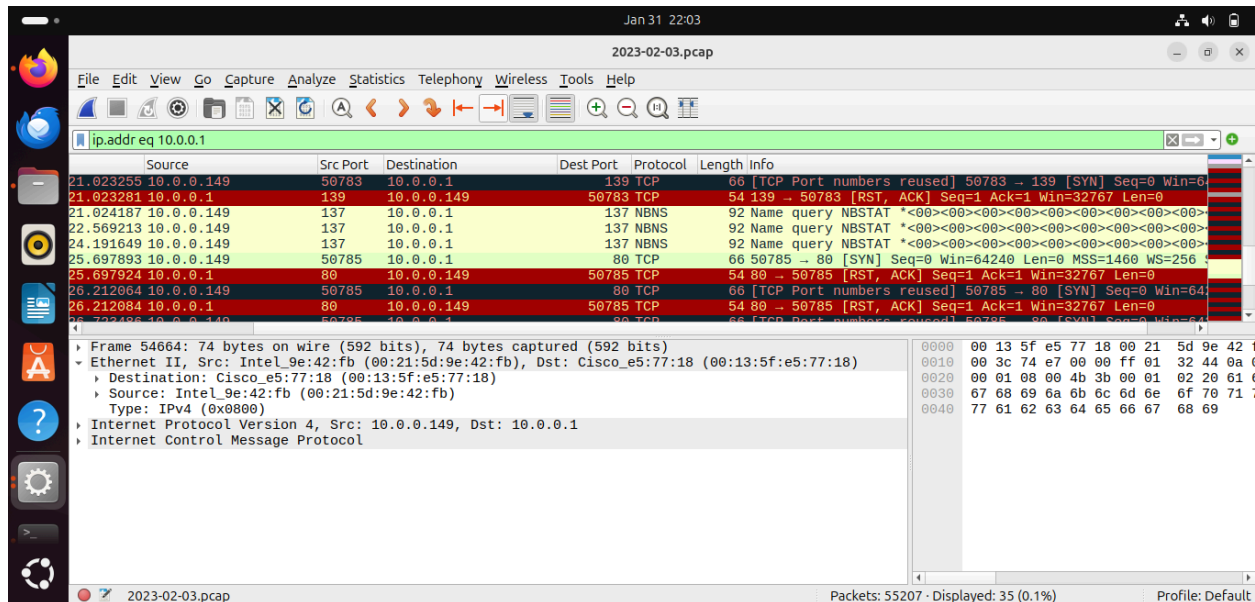


## ICMP & Port Scanning Activity

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@macnells.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 ESMTTP 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
YXJ0aG10QG1hY25lbHMuY28udGg=
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)  
Offset Number: 254 (relative ack number)

Packets: 55207 · Display

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

Recipe	Input
<p>From Base64</p> <p>Alphabet A-Za-z0-9+/=</p> <p><input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode</p>	<p>VXNlcm5hbWU6</p> <p>YXJ0aG10QG1hY25lbHMuY28udGg=</p> <p>UGFzc3dvcmQ6</p> <p>QXJ0MTIzNDU2</p>

Output

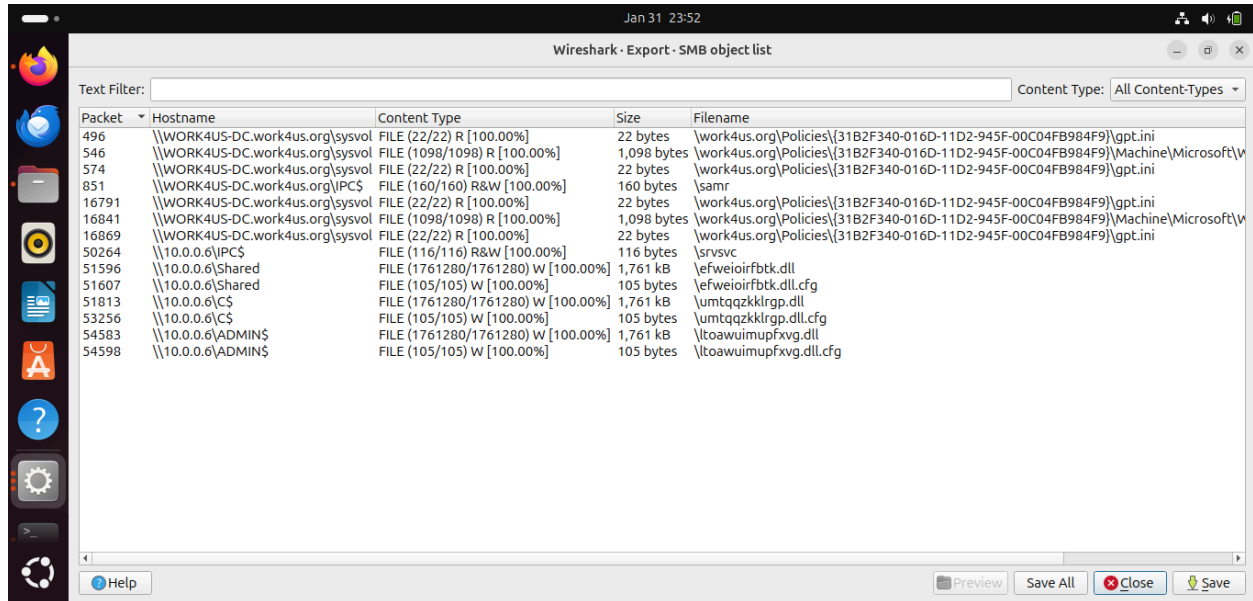
Username:arthit@macnells.co.thPassword:Art123456



# SMB Malware Propagation

SMB traffic analysis showed file transfers. Exported files revealed:

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

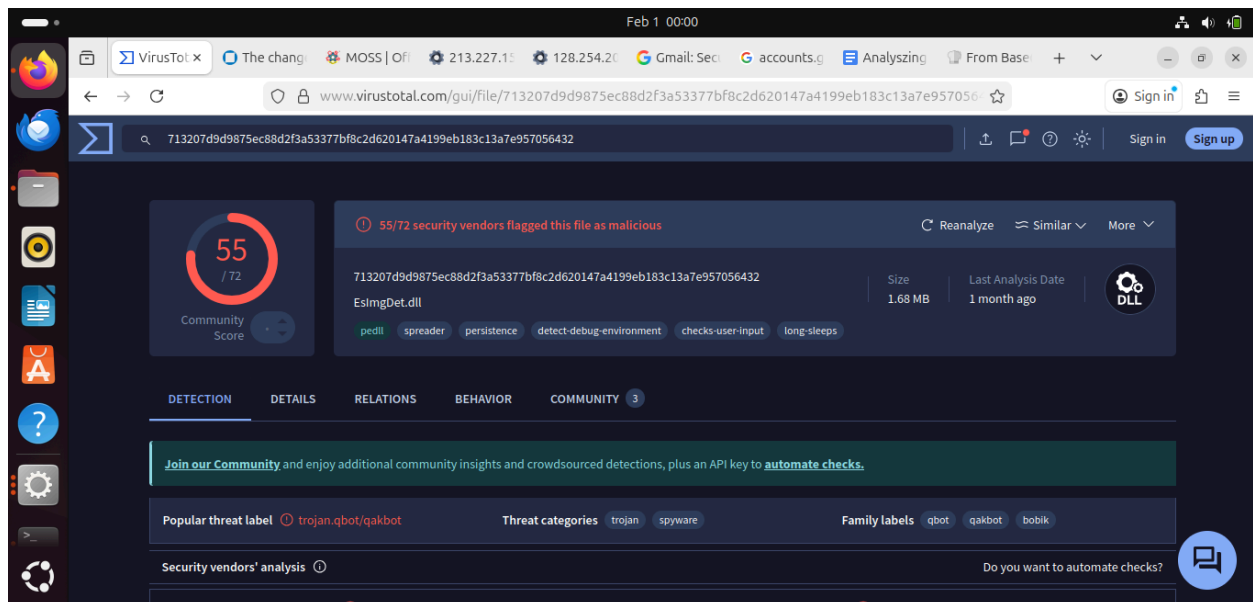


Wireshark - Export - SMB object list

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\MicrosoftV
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\MicrosoftV
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	\\srsvcs
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	\\umtqqzkkllrgp.dll
53256	\\10.0.0.6\C\$	FILE (105/105) W [100.00%]	105 bytes	\\umtqqzkkllrgp.dll.cfg
54583	\\10.0.0.6\ADMIN\$	FILE (1761280/1761280) W [100.00%]	1,761 KB	\\toawuimupfxvg.dll
54598	\\10.0.0.6\ADMIN\$	FILE (105/105) W [100.00%]	105 bytes	\\toawuimupfxvg.dll.cfg

Help Preview Save All Close Save



Feb 1 00:00

www.virustotal.com/gui/file/713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432

713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432

Community Score: 55 / 72

55/72 security vendors flagged this file as malicious

Reanalyze Similar More

713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432

Size: 1.68 MB Last Analysis Date: 1 month ago

Dll

pedi spreader persistence detect-debug-environment checks-user-input long-sleeps

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 bobik

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@macnells.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.

