

# Phishing Email Investigation Report

**Analyst:** Seif Tuhul

**Date:** August 9, 2025

---

## Overview

Phishing remains one of the most common and dangerous cybersecurity threats, where attackers impersonate trusted entities to steal sensitive information such as credentials, financial data, or install malware. This report analyzes three phishing URLs sourced from PhishTank, a reputable community-driven phishing repository. Using VirusTotal and Any.Run sandbox tools, the URLs were scanned and analyzed for indicators of compromise (IOCs). Two URLs showed suspicious characteristics, while one appeared clean. The goal is to extract relevant IOCs, summarize findings, and recommend mitigations.

---

## Tools Used

- **PhishTank:** For gathering active phishing URL samples
  - **VirusTotal:** Multi-engine URL and file scanning
  - **Any.Run:** Dynamic sandbox analysis for behavioral insights
  - **MXToolbox:** Email header analysis (not applied here as no email samples)
- 

## URL Analysis

**URL 1:** <https://nvq0ac.top/DylBDPO9HV/login&getFlg=on/>

- **VirusTotal:** No significant detections; rated clean to medium risk
- **Sandbox:** No suspicious activity detected during dynamic analysis
- **Notes:** URL may be inactive or low-risk phishing landing page

**URL 2:** <https://serviceuzg.cyou/us/index.html>

- **VirusTotal:** Flagged as suspicious by multiple detection engines
- **Sandbox:** Browser process (msedge.exe) executed; network connections to suspicious IPs; multiple dropped files observed
- **Notes:** Potential phishing landing page with associated malicious scripts

**URL 3:** <http://daspol-eu.s10.hostcreators.sk/img/fi/>

- **VirusTotal:** Flagged suspicious by multiple engines
  - **Sandbox:** Similar behavior to URL 2 with dropped files and network connections
  - **Notes:** Active phishing URL hosting potentially malicious content
- 

## Indicators of Compromise (IOCs)

For <https://serviceuzg.cyou/us/index.html>

- **Phishing URL:** <https://serviceuzg.cyou/us/index.html>
- **Dropped files (SHA256):**
  - cc6aecf8-6480-4eb0-94fe-30fcdeecf5f0.tmp —  
cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
  - coupons\_data.db\000017.ldb —  
50d42197b44f33e1a778c82a210db43dde3e3972716bbfe41f71a86ae1a1e03a
  - Last Browser — 9c70f766d3b84fc2bb298efa37cc9191f28bec336329cc11468cfadbc3b137f4
  - page\_embed\_script.js —  
8ba9b01fe8eb16e6673b7e5341697ec449026ca902d3f16305924d853a339ad8
  - service\_worker\_bin\_prod.js —  
58bf445f708c392ab82e2cdd45e3633bb5e83252f5eeac897d90eb65b0d16151
  - offscreenocument\_main.js —  
8000ba1c3e8a760839707872c5efd133077ab39ef1ff53b818a3ffacea5021d4
  - the-real-index — 7c336dd1b93b3f0ed5e368d566653e7a8bdb552287d050f56dd9db1dd249fb7c
- **DNS Request Domain:** serviceuzg.cyou
- **Network Connection IP:** 43.130.60.113

For <http://daspol-eu.s10.hostcreators.sk/img/fi/>

- **Phishing URL:** <http://daspol-eu.s10.hostcreators.sk/img/fi/>
- **Dropped files (SHA256):**
  - 0a5d4b45-2357-4aca-a426-519cac723032.tmp —  
cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
  - coupons\_data.db\000017.ldb —  
50d42197b44f33e1a778c82a210db43dde3e3972716bbfe41f71a86ae1a1e03a
  - Last Browser — 9c70f766d3b84fc2bb298efa37cc9191f28bec336329cc11468cfadbc3b137f4
  - page\_embed\_script.js —  
8ba9b01fe8eb16e6673b7e5341697ec449026ca902d3f16305924d853a339ad8
  - service\_worker\_bin\_prod.js —  
58bf445f708c392ab82e2cdd45e3633bb5e83252f5eeac897d90eb65b0d16151
  - offscreenocument\_main.js —  
8000ba1c3e8a760839707872c5efd133077ab39ef1ff53b818a3ffacea5021d4
- **DNS Request Domain:** daspol-eu.s10.hostcreators.sk
- **Network Connection IP:** 193.163.77.16

---

## Recommendations

- Block the phishing URLs and related domains at the network perimeter firewall and web filters.
- Implement user awareness training focused on phishing detection and safe email practices.

- Monitor DNS and network logs for traffic related to the listed domains and IP addresses.
- Use advanced endpoint protection tools capable of detecting script-based attacks and suspicious file drops.

Attachments

https://nvq0ac.top/DyIBDPO9HV/login&getFlg=on/

0 / 97

Community Score

No security vendors flagged this URL as malicious

Reanalyze Search More

https://nvq0ac.top/DyIBDPO9HV/login&getFlg=on/nvq0ac.top

Status 403Content type text/html; charset=utf-8Last Analysis Date a moment ago

DETECTIONDETAILSCOMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Abusix	Spam	Fortinet	Spam
Sophos	Spam	Trustwave	Suspicious
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean
Cybereason	Clean	Cybereason	Clean

Screenshot 1:  
VirusTotal scan results showing detection status for https://nvq0ac.top/DyIBDPO9HV/login&getFlg=on/

https://serviceuzg.cyou/us/index.html

5 / 97

Community Score

5/97 security vendors flagged this URL as malicious

Reanalyze Search More

https://serviceuzg.cyou/us/index.htmlserviceuzg.cyou

Status 200Content type text/htmlLast Analysis Date 5 hours ago

DETECTIONDETAILSCOMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Emsisoft	Phishing	Fortinet	Phishing
Netcraft	Malicious	Trustwave	Phishing
Webroot	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean

Screenshot 2:

VirusTotal scan results showing suspicious flags for <https://serviceuzg.cyou/us/index.html>

9/97

Community Score

9/97 security vendors flagged this URL as malicious

Reanalyze Search More

http://daspol-eu.s10.hostcreators.sk/img/fi/

daspol-eu.s10.hostcreators.sk

Status: 200

Content type: text/html; charset=UTF-8

Last Analysis Date: 2 hours ago

text/html

password input

DETECTION

DETAILS

COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	CyRadar	Malicious
Emsisoft	Phishing	Fortinet	Phishing
G-Data	Phishing	Kaspersky	Phishing
Netcraft	Malicious	OpenPhish	Phishing
Sophos	Phishing	Gridinsoft	Suspicious
URLQuery	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean

Screenshot 3:

VirusTotal scan results showing suspicious flags for <http://daspol-eu.s10.hostcreators.sk/img/fi/>

Tracking | UPS - US

https://serviceuzg.cyou/us/index.html

ups

Your shipment  
1ZT9B3N70333613034  
**Delivery Failed**  
Friday, 8/8/2025 at 3:38 P.M.  
The recipient was unavailable.  
Please reschedule the package delivery time to prevent the package from being returned.

Delivery To  
ROMA, 62 IT

Label Created

We Have Your Package

On the Way

Out for Delivery

HTTP Requests

Connections

DNS Requests

Threats

Filter by PID, name or url

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5425 ms	GET 200 OK	6680	msedge.exe			http://edge.microsoft.com/browse/networktime/time/1/current?cpu2key=2.Tu.Dm.1dJohFfc31LOBNvayZFku3FZ...	100 b + text
7925 ms	GET 200 OK	1268	svchost.exe			http://cf.micrsoft.com/pk/crl/products/MicrosoftAut2011_2011.03.22.crl	825 b + binary
7942 ms	GET 200 OK	1268	svchost.exe			http://www.microsoft.com/pkcsps/crl/MicSecSerCA2011_2011-10-18.crl	814 b + binary

Win10 64bit

00:26

CPU 0%

RAM 46%

Processes 15

Actions 0

Filter by PID or name

Only important

PID	Process name	Working set	Private bytes	Page faults	Working set	Private bytes	Page faults
6254	msedge.exe	https://serviceuzg.cyou/us/index.html	17k	2k	164		
4188	msedge.exe	-type=cashpad-handler ~user-data-dir=C:\Users\admin\AppData\Local\Micros...	236	15	25		
4072	msedge.exe	-type=cpu-process ~string=annotations ~gpu-preferences=UAAAAAAAAAAdgAAA...	437	23	48		
6680	msedge.exe	-type=utility ~utility-sub-type=network.mojom.NetworkService ~lang=en-US ~ser...	1k	211	47		
4224	msedge.exe	-type=utility ~utility-sub-type=storage.mojom.StorageService ~lang=en-US ~serv...	310	15	30		
440	msedge.exe	-type=renderer ~string=annotations ~video-capture-use-gpu-memory-buffer ~lang...	272	18	34		
2628	msedge.exe	-type=renderer ~string=annotations ~video-capture-use-gpu-memory-buffer ~lan...	202	18	34		
3148	msedge.exe	-type=renderer ~string=annotations ~extension-process ~renderer-sub-type=exte...	170	18	34		
7452	msedge.exe	-type=utility ~utility-sub-type=asset_store.mojom.AssetStoreService ~lang=en U...	124	15	30		
7404	msedge.exe	-type=utility ~utility-sub-type=entity_extraction_service.mojom.Extractor ~lang=en...	138	15	31		
7330	msedge.exe	-type=utility ~utility-sub-type=data_decoder.mojom.DataDecoderService ~lang=en...	122	15	30		
7812	identity_helper.exe	-type=utility ~utility-sub-type=winrt_app_id.mojom.WinrtAppIdService ~lan...	1	0	2		
7624	identity_helper.exe	-type=utility ~utility-sub-type=winrt_app_id.mojom.WinrtAppIdService ~lan...	1k	370	76		

Screenshot 4:

Any.Run sandbox overview capturing browser process activity for <https://serviceuzg.cyou/us/index.html>

	HTTP Requests	3	Connections	44	DNS Requests	34	Threats	12		Filter by PID, domain, name or ip	PCAP
	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
	BEFORE	TCP	✓	1268	svchost.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data
	BEFORE	UDP	✓	4	System		192.168.100.255	137	—	—	↑ 1020 b ↓ —
	BEFORE	TCP	✓	5944	MoUsrCoreWorker.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data
	BEFORE	TCP	✓	6388	RUXIMICS.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data
	2297 ms	UDP	✓	4	System		192.168.100.255	138	—	—	↑ 2 Kb ↓ —
	5353 ms	TCP	✓	6680	msedge.exe		150.171.22.17	443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 3 Kb ↓ 8 Kb
	5420 ms	TCP	✓	6680	msedge.exe		150.171.27.11	80	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 653 b ↓ 861 b

	HTTP Requests	3	Connections	44	DNS Requests	34	Threats	12		Filter by IP or domain	PCAP
	Timeshift	Status	Rep	Domain					IP		
	BEFORE	Responded	✓	settings-win.data.microsoft.com					4.231.128.59		
	BEFORE	Responded	✓	google.com					142.250.186.46		
	5298 ms	Responded	✓	edge.microsoft.com					150.171.27.11		
									150.171.28.11		
	5300 ms	Requested	✓	edge.microsoft.com					IP Addresses not found		
	5300 ms	Responded	✓	config.edge.skype.com					150.171.22.17		
	5301 ms	Requested	✓	config.edge.skype.com					IP Addresses not found		

Screenshot 5: Any.Run sandbox network connections and DNS requests for <https://serviceuzg.cyou/us/index.html>

d8a7e1e3-3fdb-4bdd-b9e8-f0cb2d321306.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter

<<Ctrl>

No.

Time

Source

Destination

Protocol

Length

Info

1 0.000000 192.168.100.6 192.168.100.2 DNS 91 Standard query 0xa6a6 A settings-win.data.microsoft.com

2 0.000753 192.168.100.2 192.168.100.6 DNS 225 Standard query response 0xa6a6 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settings-prod-neu-3.northeurope.cloudapp.azure.com A 4.231.128.59

3 0.0009124 192.168.100.6 4.231.128.59 TCP 66 49721 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

4 0.0009733 192.168.100.6 4.231.128.59 TCP 66 49722 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

5 0.161159 192.168.100.6 4.231.128.59 TCP 66 49723 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

6 0.232936 fe80::a828:c478:5c2::ff02::1:fff4:d7f7 ICHPV6 86 Neighbor Solicitation for fe80::ac25:95d6:e7d4:d7f7 from f2:88:df:d5:5f:5c

7 0.233093 fe80::a828:c478:5c2::ff02::1:fff4:4a78 ICHPV6 86 Neighbor Solicitation for fe80::2ee4:156c:ce74:4a78 from f2:88:df:d5:5f:5c

8 0.5902518 192.168.100.6 192.168.100.255 NBNS 110 Registration NB WORKGROUP<00>

9 0.592748 192.168.100.6 192.168.100.255 NBNS 110 Registration NB DESKTOP-3GLL3LD<00>

10 0.592791 192.168.100.6 192.168.100.255 NBNS 110 Registration NB DESKTOP-3GLL3LD<20>

11 0.951878 fe:88:df:d5:5f:5c Spanning-tree-(for...) STP 52 Conf. Root = 32768/0/52:54:00:2f:9f:a3 Cost = 0 Port = 0x0006

12 0.998604 192.168.100.6 4.231.128.59 TCP 66 [TCP Retransmission] 49721 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

13 1.002440 192.168.100.6 4.231.128.59 TCP 66 [TCP Retransmission] 49722 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

14 1.155701 192.168.100.6 192.168.100.2 DNS 70 Standard query 0xa6508 A google.com

15 1.159372 192.168.100.2 192.168.100.6 DNS 86 Standard query response 0xa6508 A google.com A 142.250.186.46

16 1.170624 192.168.100.6 4.231.128.59 TCP 66 [TCP Retransmission] 49723 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

▼ Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Aug 9, 2025 22:06:58.817063000 Central Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1754795218.817063000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 91 bytes (728 bits)

Capture Length: 91 bytes (728 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

> Ethernet II, Src: f2:88:df:d5:5f:5c (f2:88:df:d5:5f:5c), Dst: d4:da:6d:a6:d5:dc (d4:da:6d:a6:d5:dc)

0000 d4 da 6d a6 d5 dc f2 88 df d5 5f 5c 00 00 45 00 . . m . . . . . \ . E .

0010 00 4d 00 7b 00 00 00 11 20 cb c0 a8 64 06 c0 a8 . N { . . . . . d . .

0020 64 02 c9 74 00 35 00 39 8a c6 a6 a6 01 00 00 01 d . t 5 9 . . . . .

0030 00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2d . . . . . s ettings-

0040 77 69 6e 64 64 61 74 61 09 6d 69 63 72 6f 73 6f . win data microso

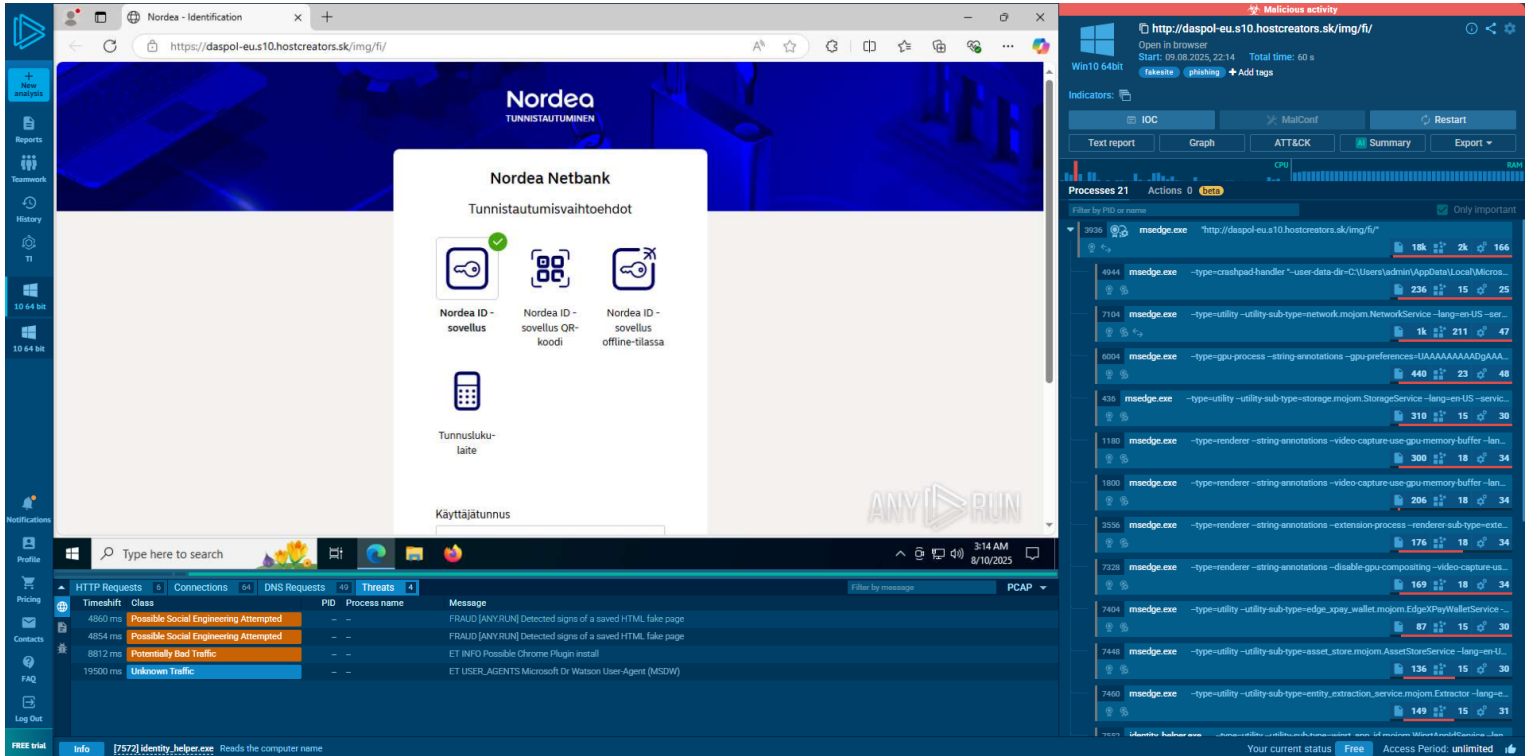
0050 66 74 63 63 6f 6d 00 00 01 00 01 ft:com . . . . .

d8a7e1e3-3fdb-4bdd-b9e8-f0cb2d321306.pcap

Packets: 3766 • Displayed: 3766 (100.0%)

Profile: Default

Screenshot 6: Wireshark DNS request capture showing lookup for domain serviceuzg.cyou during sandbox analysis



Screenshot 7:

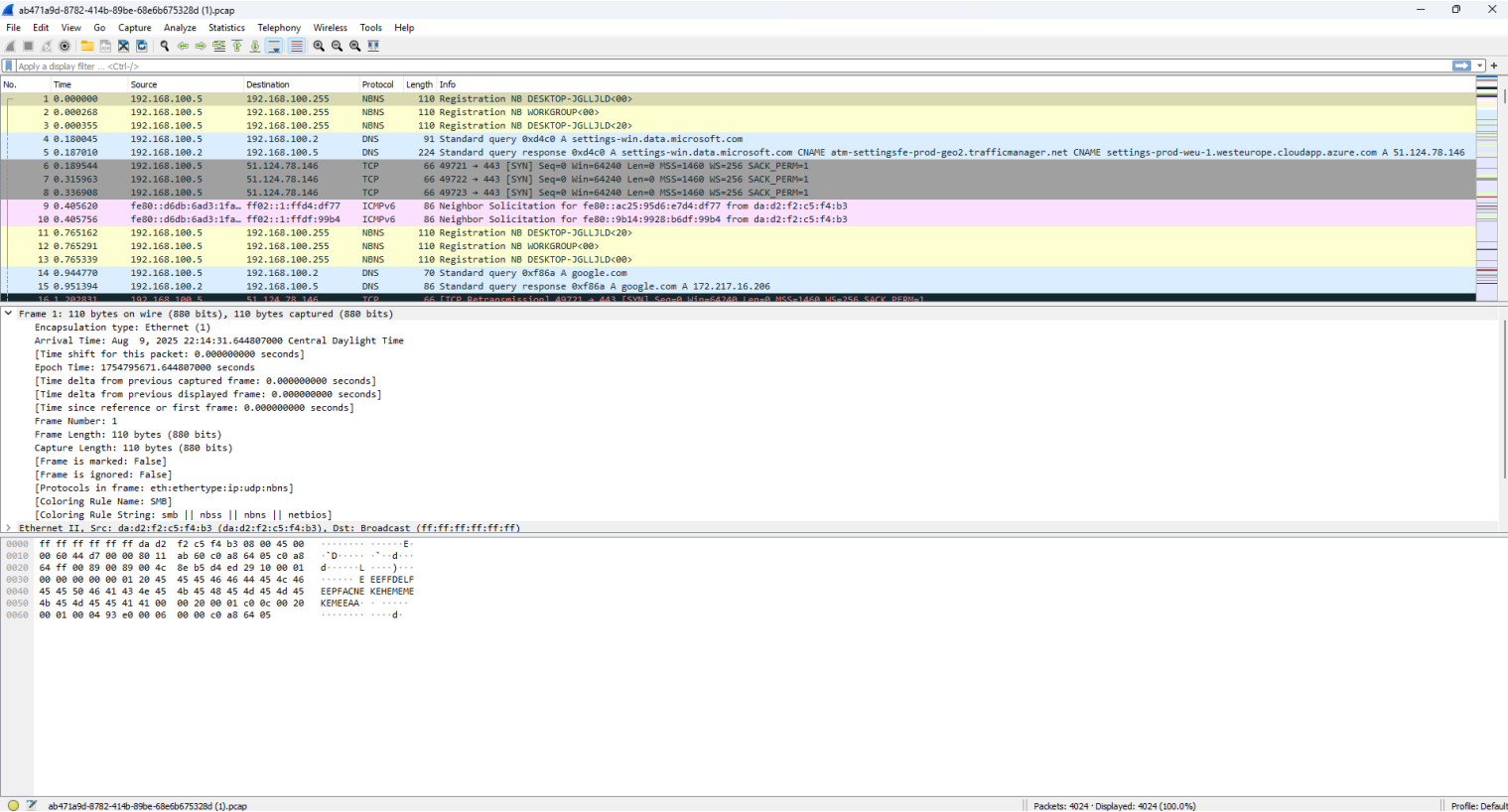
Any.Run sandbox overview capturing browser process activity for <http://daspol-eu.s10.hostcreators.sk/img/fi/>

HTTP Requests 6   Connections 64   DNS Requests 49   Threats 4											Filter by PID, domain, name or ip	PCAP
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic		
BEFORE	TCP	✓	5944	MoUsoCoreWorker.exe		51.124.78.146	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data		
BEFORE	UDP	✓	4	System		192.168.100.255	137			↑ 1 Kb ↓		
BEFORE	TCP	✓	1268	svchost.exe		51.124.78.146	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data		
BEFORE	TCP	✓	1040	RUXIMICS.exe		51.124.78.146	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Waiting for the Data		
2255 ms	UDP	✓	4	System		192.168.100.255	138			↑ 2 Kb ↓		
4409 ms	TCP	✓	7104	msedge.exe		150.171.27.11	80	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 653 b ↓ 859 b		
4426 ms	TCP	✓	7104	msedge.exe		150.171.22.17	443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 3 Kb ↓ 8 Kb		

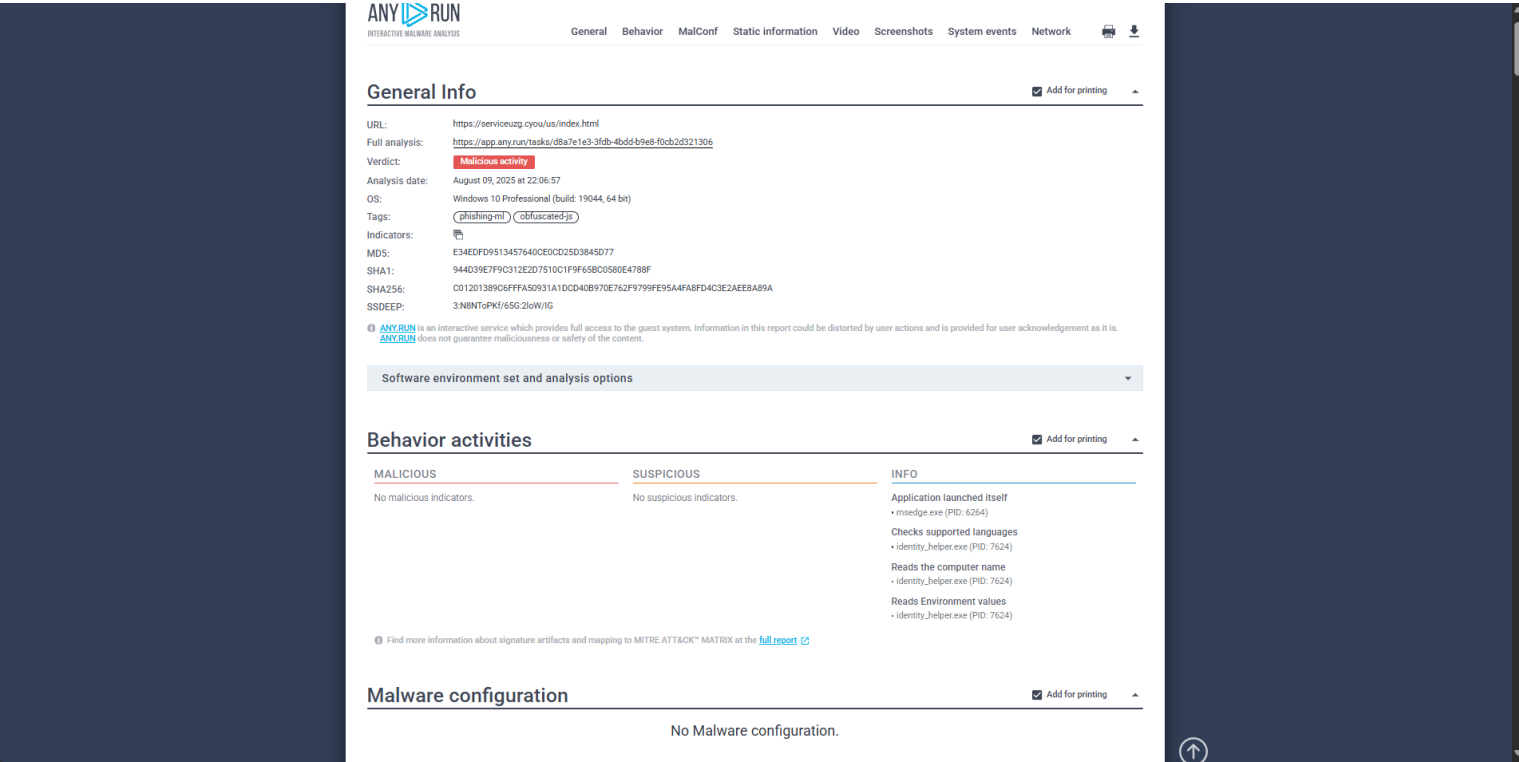
HTTP Requests 6   Connections 64   DNS Requests 49   Threats 4					Filter by IP or domain		PCAP
Timeshift	Status	Rep	Domain	IP			
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.124.78.146			
BEFORE	Responded	✓	google.com	172.217.16.206			
4354 ms	Responded	✓	edge.microsoft.com	150.171.27.11			
4356 ms	Requested	✓	edge.microsoft.com	150.171.28.11			
4356 ms	Requested	✓	edge.microsoft.com	IP Addresses not found			
4356 ms	Responded	✓	config.edge.skype.com	150.171.22.17			
4357 ms	Requested	✓	config.edge.skype.com	IP Addresses not found			

Screenshot 8:

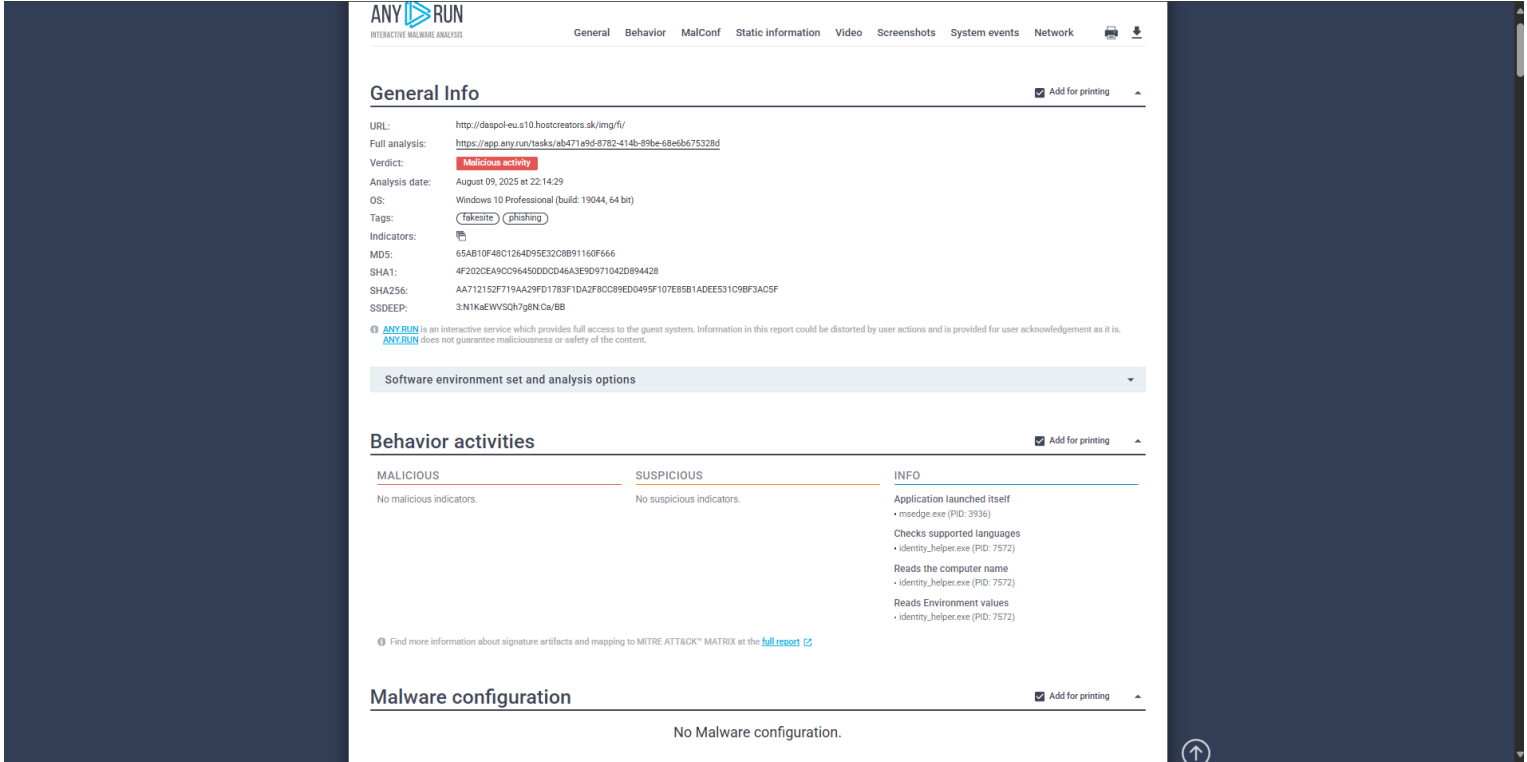
Any.Run sandbox network connections and DNS requests for <http://daspol-eu.s10.hostcreators.sk/img/fi/>



**Screenshot 9:** Wireshark DNS request capture showing lookup for domain daspol-eu.s10.hostcreators.sk during sandbox analysis



**Screenshot 10:** Any.Run dynamic analysis report excerpt for <https://serviceuzg.cyou/us/index.html>



**Screenshot 11:**  
Any.Run dynamic analysis report excerpt for <http://daspol-eu.s10.hostcreators.sk/img/fi/>