

CASE 4

2022/06/28

JYRI PUURUNEN
KRISTIAN SIKANEN

Summary

Mr. Oswald Cobblepot,

We've reason to believe that Haitek Ltd. was targeted by severe layered cyberattack.

Attack / chain of events included:

- Suspected social engineering as initial entry-point
- 3 different potent trojans delivered in phases (see technical section)
 - Resilient C2 infrastructure
 - Suspected data exfiltration
 - Suspected resource hijacking
 - Stealthy TTPs & defense evasion

Threat-actor:

- Moderate to advanced in skill
- Most likely motivated by financial gain (banking trojans or capabilities of wide data harvesting & exfil)
- Most likely organized cybercrime or well-funded individual

Likely objectives:

- Initial compromise & Recon
 - basic system access
- Data Harvesting & resource utilization
 - e.g, credential theft, keylogging, or browser history scraping
- Persistence and Spread
 - ensure persistence & additional payload deployments

Immediate actions:

1. Containment

- Isolate Infected System(s)
- Block Malicious Communication

2. Investigation

- DFIR
- Identify Phishing Entry Point
- Network Traffic Analysis

3. Eradication

- Remove Malware
- Patch Possible Vulnerabilities

4. Recovery

- Restore affected device from backup
- Reset Credentials

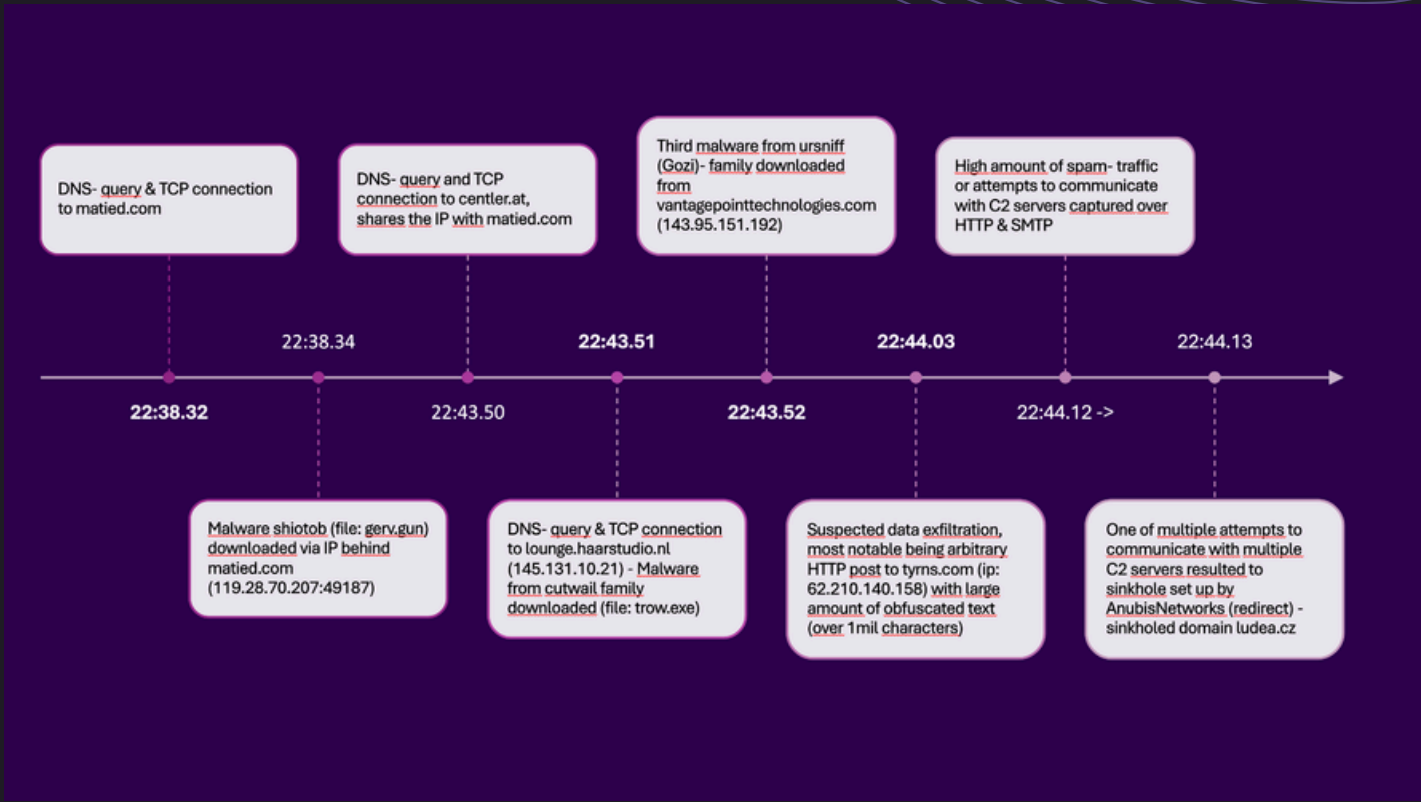
5. Communication and Reporting

- Internal Notification
- External Notification

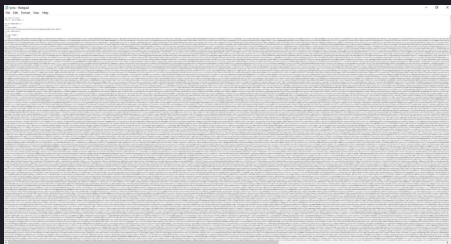
Areas of concern:

- Trojans may have propagated themselves over the spam to other hosts on the network
- Characteristics of trojans include tampering with firewall
- Potential reputational damage if sensitive customer data has been exfiltrated

Timeline



Obfuscated data - tyrns.com



50 - alerts

Count	rule.name	event.module	event.severity_label	rule.sid
637	ET MALWARE Backdoor Win32 Pushdo s Checkin	suricata	high	2016867
4	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959
4	ET INFO Observed DNS Query to bz TLD	suricata	medium	2027863
2	ET INFO Packed Executable Download	suricata	low	2014819
2	ET INFO HTTP Request to a *.fr domain	suricata	medium	2032987
2	ET INFO External IP Lookup Domain (myip. opensns .com in DNS lookup)	suricata	medium	2023472
1	ET JA3 Hash - [Abuse ch] Possible Gozi	suricata	low	2028814
1	ET INFO Windows Powershell User-Agent Usage	suricata	low	2033355
1	ET INFO WinHttpRequest Downloading EXE	suricata	low	2019822
1	ET INFO TLS possible TOR SSL traffic	suricata	low	2018789

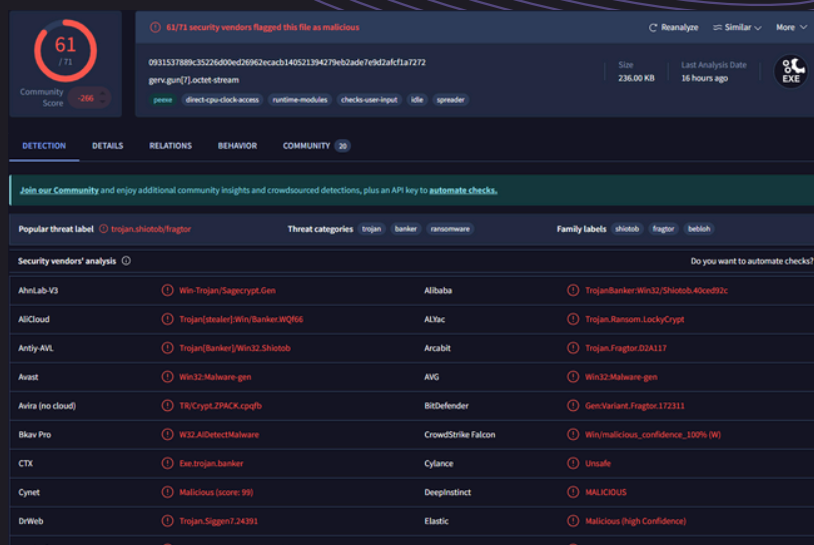
Trojans

1. Shiotob/fragtor

Role: Establish foothold and reconnaissance.

- Initial infection vector
- most likely delivered via phishing / spearphishing (DNS- query to matied.com)

Further characteristics:
<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Shiotob>

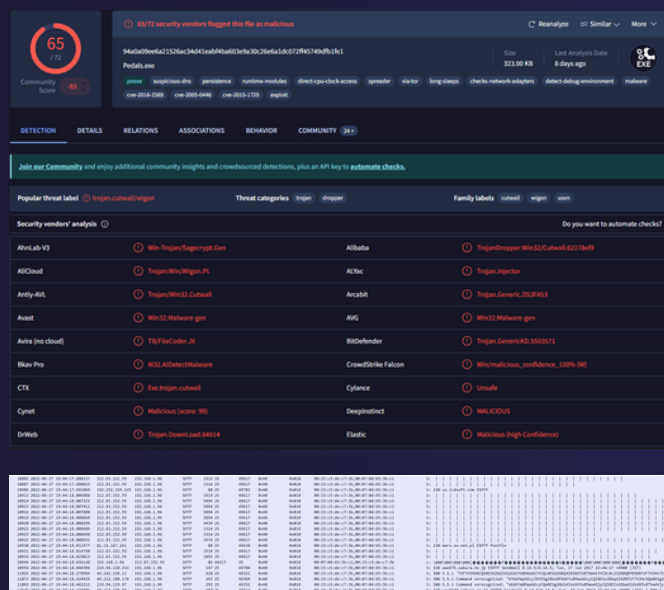


2. Cutwail/wigon

Role: Amplification and propagation

- Propagate the attack further via phishing spam or secondary infection attempts. (Captured arbitrary SMTP-traffic)
- Act as a relay for Ursniff deployment.

Further characteristics:
<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Cutwail.A>

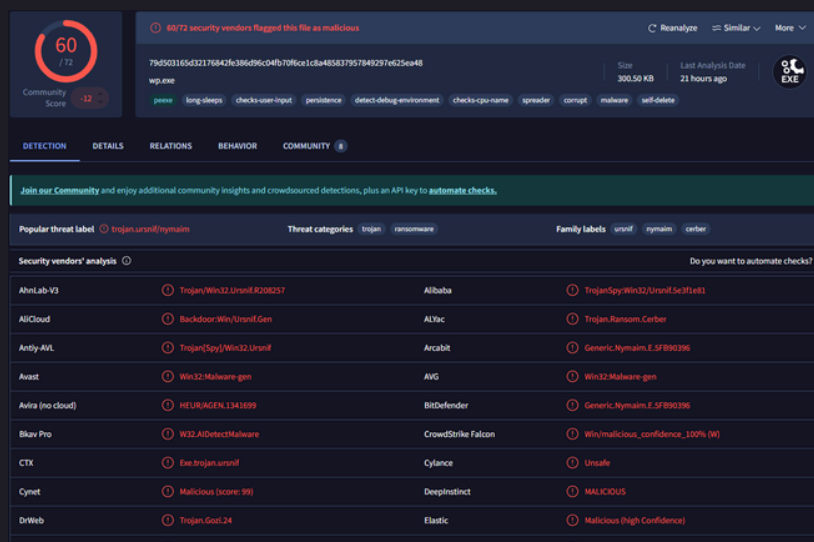


3. Ursniff/gozi

Role: Final-stage data theft and persistence

- Potential theft of sensitive information
- Defense evasion via DGA (Domain Generation Algorithm)
- C2 communication over HTTP

Further characteristics:
<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Ursniff>



C2 & Malicious domains

Centler.at

12

7/14

Community Score

12/14 security vendors flagged this domain as malicious

Reanalyze

Similar

Graph

API

centler.at

self-signed

Last Analysis Date
2 days ago

DETECTION

DETAILS

RELATIONS

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.at	Phishing	BitDefender	Phishing
CDF	Malicious	CyRadar	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Phishing
G-Data	Phishing	Lionic	Malicious
Seclookup	Malicious	Sophos	Phishing
VPRE	Phishing	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AL Labs (MONTORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	Blueliv	Clean
Phishing Link Proxy	Phishing	Phishing Link Proxy	Phishing

matied.com

11

7/14

Community Score

11/14 security vendors flagged this domain as malicious

Reanalyze

Similar

Graph

API

matied.com

Creation Date
4 months ago

Last Analysis Date
14 days ago

DETECTION

DETAILS

RELATIONS

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.at	Phishing	Antiy-AVL	Malicious
BitDefender	Phishing	CDF	Malicious
CyRadar	Malicious	Fortinet	Phishing
G-Data	Phishing	Lionic	Phishing
Sophos	Phishing	VPRE	Phishing
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AL Labs (MONTORAPP)	Clean
AlienVault	Clean	benkow.cc	Clean
Blueliv	Clean	Cartago	Clean
Phishing Link Proxy	Phishing	CDF Army	Phishing

Tyrns.com

9

7/14

Community Score

8/14 security vendors flagged this domain as malicious

Reanalyze

Similar

Graph

API

tyrns.com

Registrar
TLD Registrar Solutions Ltd

Creation Date
9 years ago

Last Analysis Date
13 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

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

Crowdsourced content

HIGH 1

MEDIUM 0

LOW 0

INFO 0

SUCCESS 0

CnC Panel: according to source Blueliv - 1 month ago
This URL has been seen hosting a botnet CnC panel for the portable malware

Security vendors' analysis

Do you want to automate checks?

alphaMountain.at	Malicious	CDF	Malicious
CyRadar	Malicious	Dr.Web	Malicious
Fortinet	Malware	Kaspersky	Malware
Lionic	Malicious	Sophos	Malicious
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AL Labs (MONTORAPP)	Clean

lounge-haarstudio.nl

6

7/14

Community Score

6/14 security vendors flagged this domain as malicious

Reanalyze

Similar

Graph

API

lounge-haarstudio.nl

Creation Date
17 years ago

Last Analysis Date
1 month ago

DETECTION

DETAILS

RELATIONS

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.at	Malicious	BitDefender	Malware
CDF	Malicious	CyRadar	Malicious
G-Data	Malware	MalwareURL	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AL Labs (MONTORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	Blueliv	Clean
Cartago	Clean	Chong-Luo-Bao	Clean
CMV Army	Clean	CMC Threat Intelligence	Clean
Criminal IP	Clean	Cyble	Clean
Phishing Link Proxy	Phishing	Phishing Link Proxy	Phishing

Technical tables

Information about malicious components found

IP	AbuseIPdb	Domain	Desc
119.28.70.207	0% abuse	matied.com, centler.at	First malware (Shiotob)
145.131.10.21	0% abuse	lounge-haarstudio.nl	Second malware (Cutwail)
208.83.223.34	0% abuse	-	C2/Data Exfiltration channel for Gozi
62.210.140.158	0% abuse	tyrns.com	C2-srvr, huge HTML-file with obfuscated content
212.61.180.100	0% abuse	ludea.cz	C2 with AnubisNetworks sinkhole in middle
143.95.151.192	0% abuse	vantagepointtechnologies.com	Third malware (Ursniff / Gozi)

File	Desc	Loaded	HASH - SHA1	Virustotal
gerv.gun	trojan.cutwail/wigon	matied.com 119.28.70.207	94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1	65/72
trou.exe	trojan.ursnif/nymaim	lounge-haarstudio.nl 145.131.10.21	79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48	60/72
wp.exe	trojan.shiotob/fragtor	vantagepointtechnologies.com 143.95.151.192	0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272	61/72

Tools

Tools used:

- Security onion
- Kibana
- Wireshark
- Whois
- Virustotal
- Abuseipdb
- Malpedia
- <https://sslbl.abuse.ch>
- Microsoft malware encyclopedia

