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

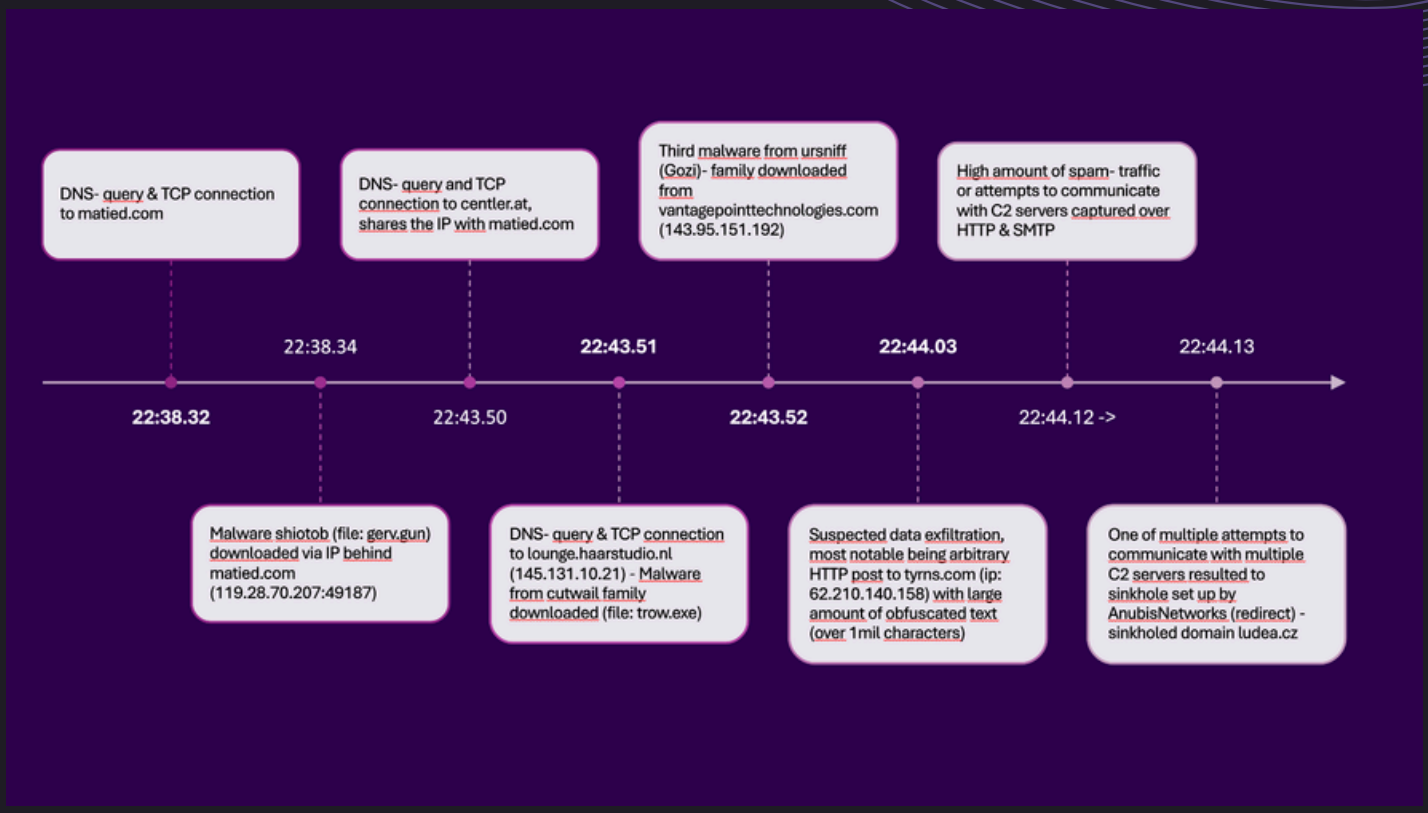
5. Communication and Reporting

- Internal Notification
- External Notification

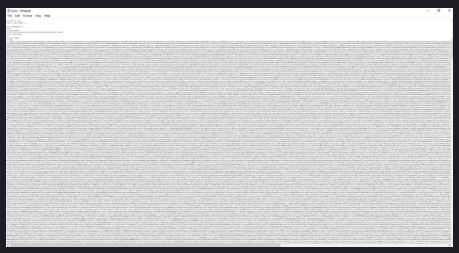
Areas of concern:

- 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



SO - alerts

	Count	rule.name	event.module	event.severity_label	rule.uuid
	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 .biz TLD	suricata	medium	2027863
	2	ET INFO Packed Executable Download	suricata	low	2014819
	2	ET INFO HTTP Request to a *.tw domain	suricata	medium	2032987
	2	ET INFO External IP Lookup Domain (myip .opendns .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

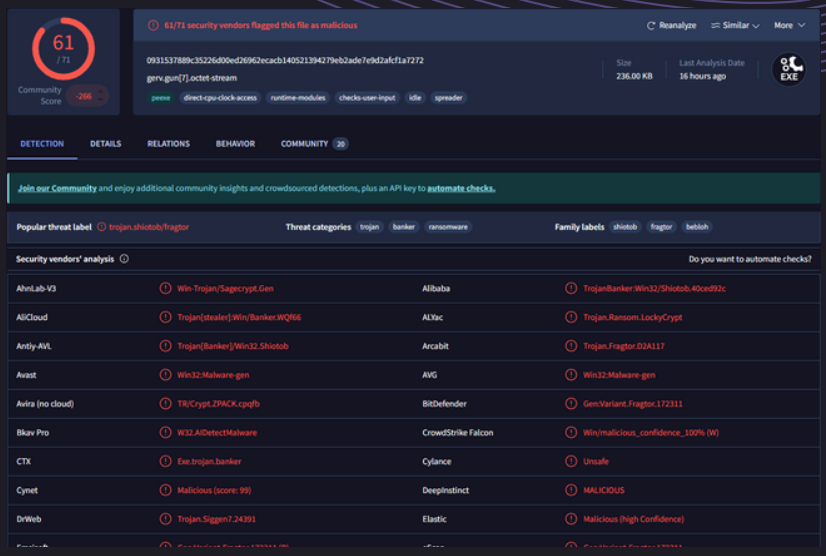
Trojans

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

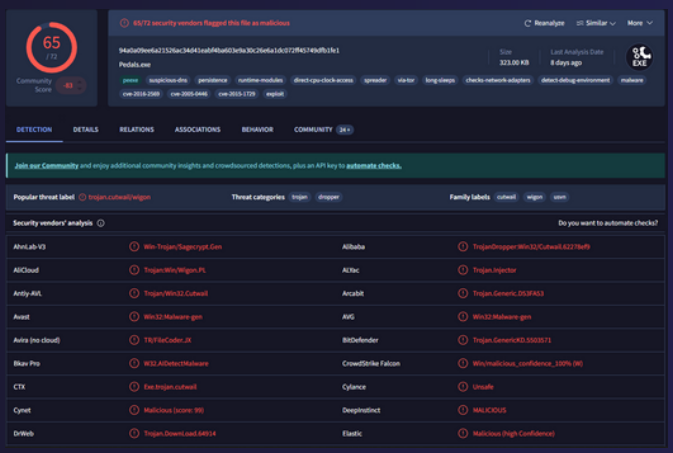


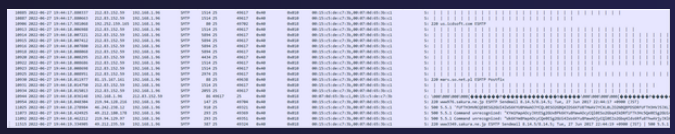
2. Cutwail/wigon

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



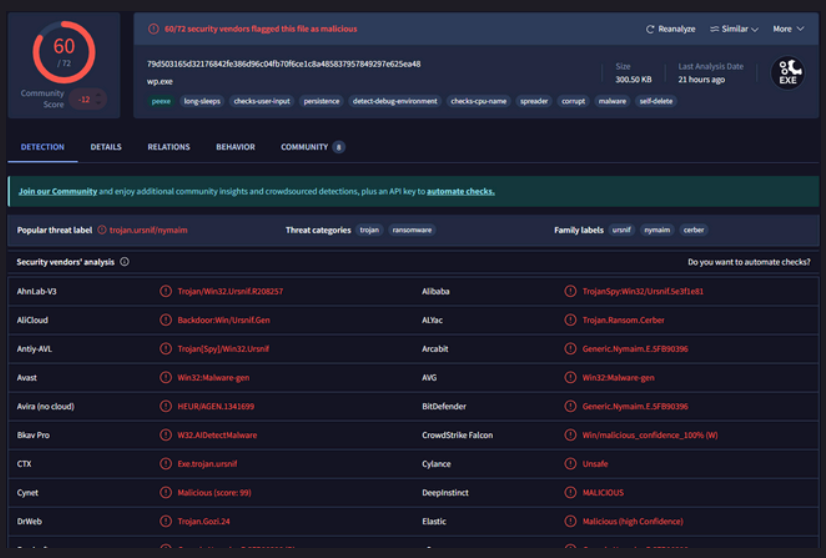


3. Ursniff/gozi

Role: Final-stage data theft and persistence

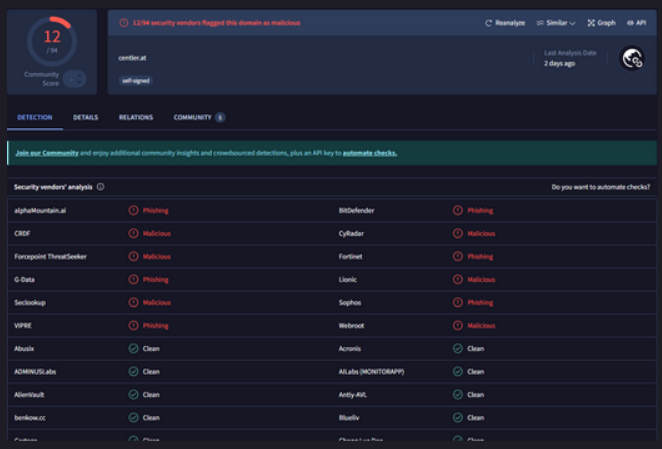
- Potential theft of sensitive information
- Defense evasion via DGA (Domain Generation Algorithm)
- C2 communication over HTTP

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

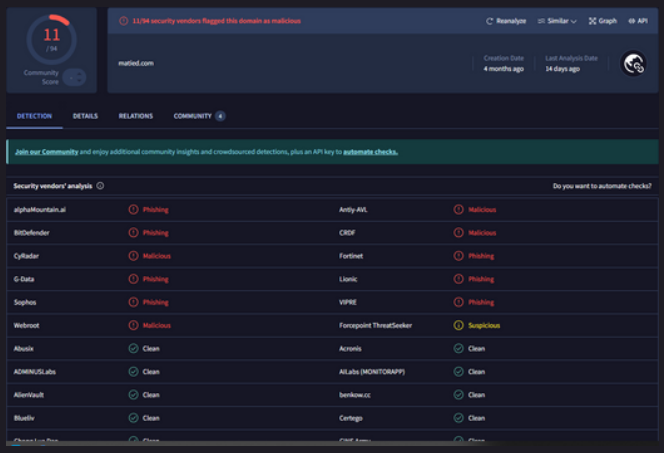


C2 & Malicious domains

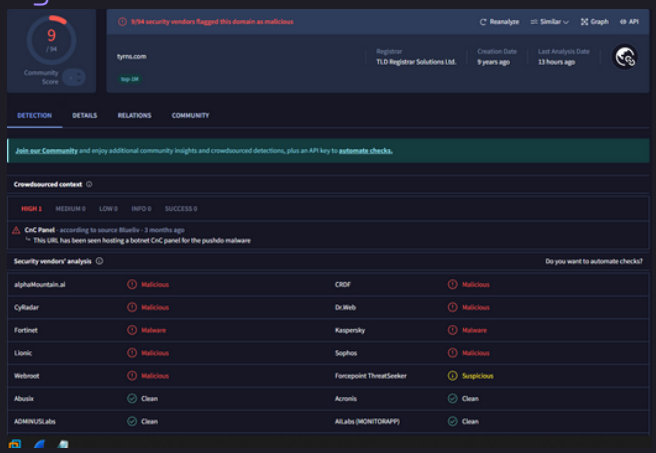
Centler.at



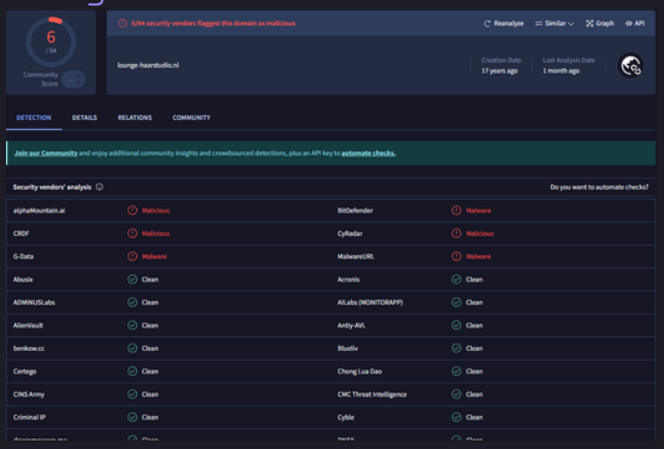
matied.com



Tyrns.com



lounge-haarstudio.nl



Technical tables

Information about malicious components found

IP	AbuselPdb	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
trow.exe	trojan.ursnif/nymaim	lounge-haarstudio.nl 145.131.10.21	79d503165d32176842fe386d96c04fb70f6ce1c8a4858379578492 97e625ea48	60/72
wp.exe	trojan.shiotob/fragtor	vantagepointtechnologies.com 143.95.151.192	0931537889c35226d00ed26962ecacb1405 21394279eb2ade7e9d2afcf1a7272	61/72

Tools

Tools used:

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