VMRAY

Connecting Sandboxing and Threat Intelligence

Ertugrul Kara

Senior PMM | VMRay

Tallinn, Estonia | ATEA Action 2024

Agenda today

1 **Infostealers Under Spotlight**

2 Threat Landscape Overview

3 Getting Proactive with Malware Config Extraction

4 Extracting Hidden Intelligence | Real Cases

The infostealer surge

Gateway to ransomware

266% increase
in infostealer related activity in 2023*

* IBM X-Force Threat Intelligence Index

Stolen Credentials

10% of intrusions
began with evidence of stolen credentials*

* Mandiant M-Trends

2024 | Top 4 Infostealers

Redline
Lumma
RisePro
Agent Tesla

* VMRay Labs

Redline

One of the most used infostealer in 2024

Recent uptick: FakeBat used as a loader

via SEO poisoning | Malvertising | Code Injection

Efficient data theft

Passwords, browser history/cookies, VPN clients

Widely available on underground forums

Offering as-a-Service making it easy to deploy

Agent Tesla

Excel Exploitation

Spreading by crafted Excel document, leveraging old yet effective vulnerabilities

(CVE-2017-11882 / 2018-0802)

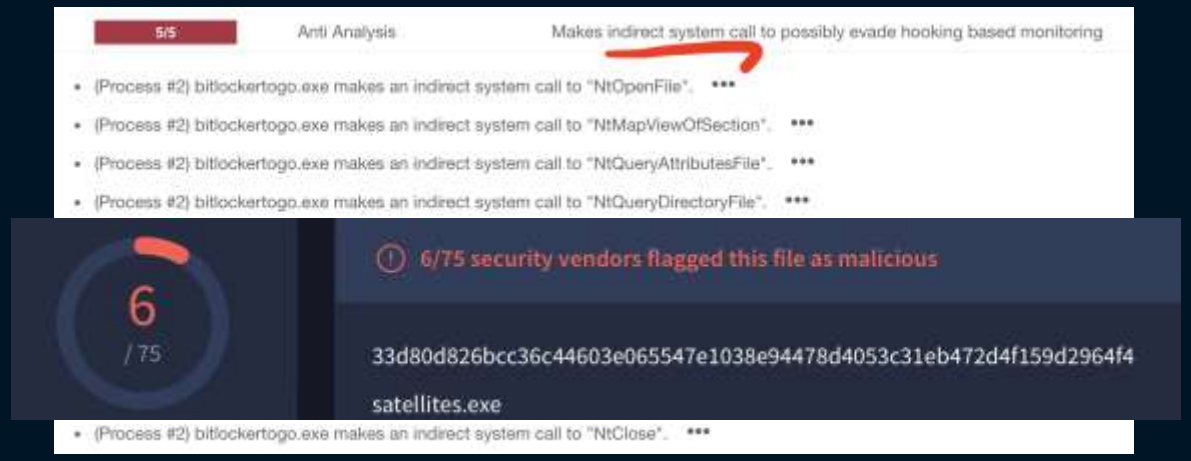
Stealthy Exfiltration

Utilizes various channels, including HTTP(S), SMTP, FTP, and Telegram.

Enhanced Obfuscation

Deployed sophisticated obfuscation through steganography and process injection.

Running the extra mile to be a market-leading infostealer



Evading hooking based sandboxes

With indirect syscalls

Monitoring global headlines to use as a lure

e.g. Falcon EDR client update

Paving way to a series of breaches

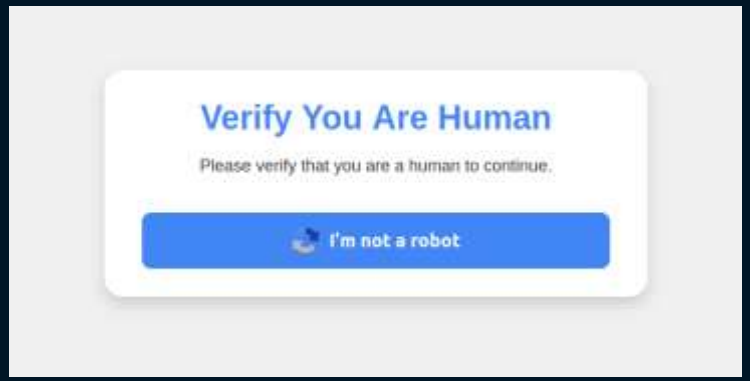
Stealer logs including Cloud SaaS platforms

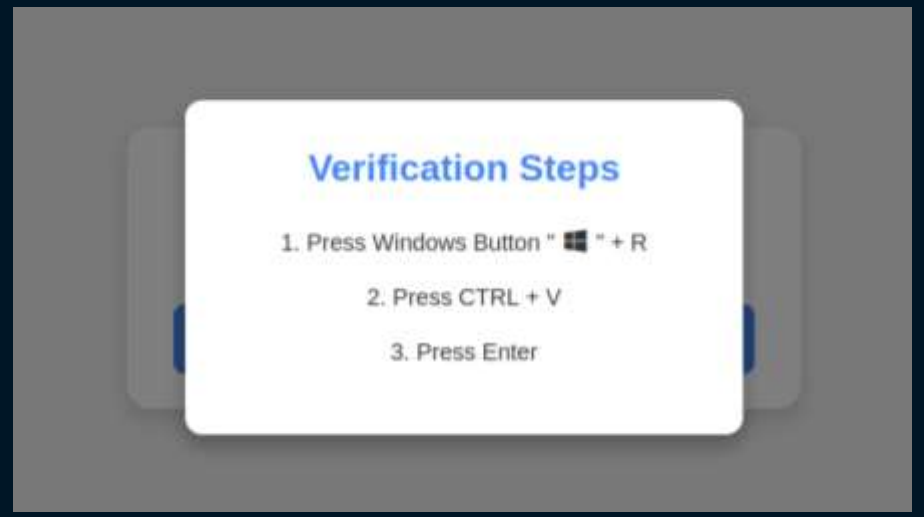
Lumma | Delivery via keyboard input

Clever delivery tactic

- Leveraging the virtual clipboard of the browser
- Running powershell command to download **Lumma**

GitHub-themed malicious emails





** Screenshots taken from KrebsonSecurity, by Brian Krebs

Malware Insights
For CTI Analysts

WHAT | Malware Configuration Extraction

1

Process of extracting configuration details embedded in malware samples

2

Understand C2 (Command & Control) communication, data exfiltration methods, and more.

3

Enhances threat hunting and incident response by providing insights into attack infrastructure and tactics

HOW | Malware Config Data Helps in Threat Hunting

Extract

IPs | Domains | Ports

BLOCK or MONITOR

Identify

Exfiltration channels

Telegram
Discord
HTTP/S
FTP
SMTP
...

Track

Malware | Infostealers

C2 patterns
Encryption algorithms
Campaigns

Winning Solution | Static + Dynamic

1

Malware authors often evolve their techniques around encryption, obfuscation, and compression. This makes it difficult to extract configurations using static methods

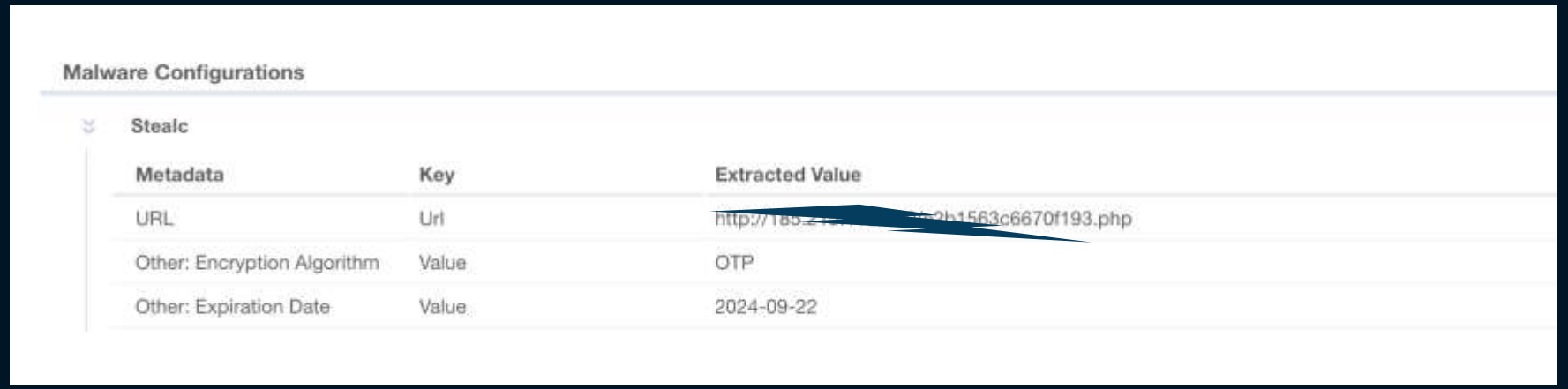
2

While static extraction is often blocked by protection techniques, extracting configurations directly from memory via dynamic analysis is a more effective route

3

Some of the configurations may not be visible during dynamic analysis, so a combination of static and dynamic analysis is the winning solution

STEALC | Config Data

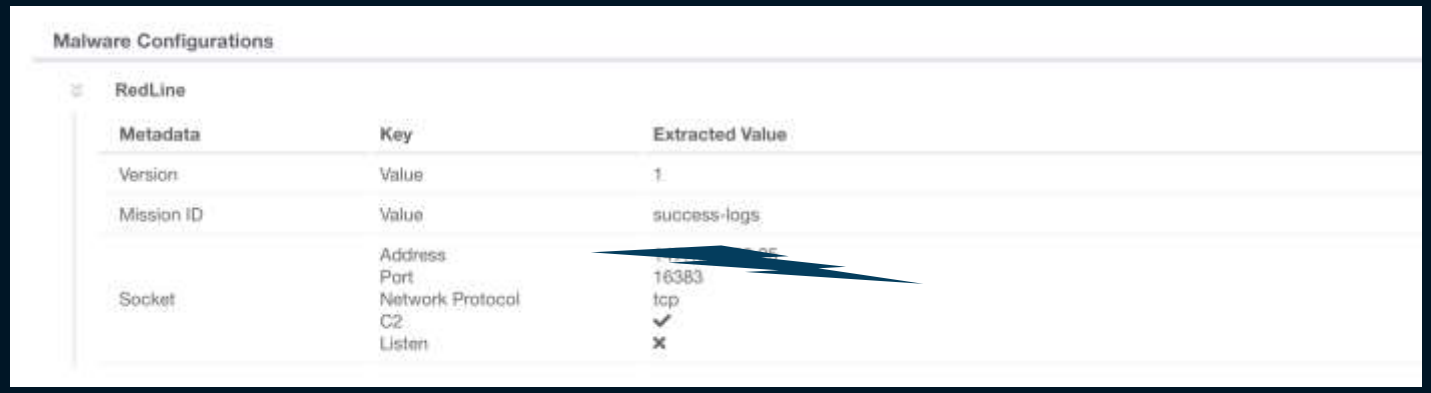


URL: http://185..../e2b1563...php

Encryption algorithm: OTP

Expiration date: 2024-09-22

REDLINE | Config Data



Version: 1

Mission ID: success-logs

Socket

Address: 147...

Port: 16383

Network Protocol: TCP

C2: ☑

Listen: X

LUMMA | Config Data

Sample 1

URL: ..site

URL: ..site

URL: ..site

.. ..

Sample 2

Mission ID: BVn..--@Bruno...

URL: ..shop

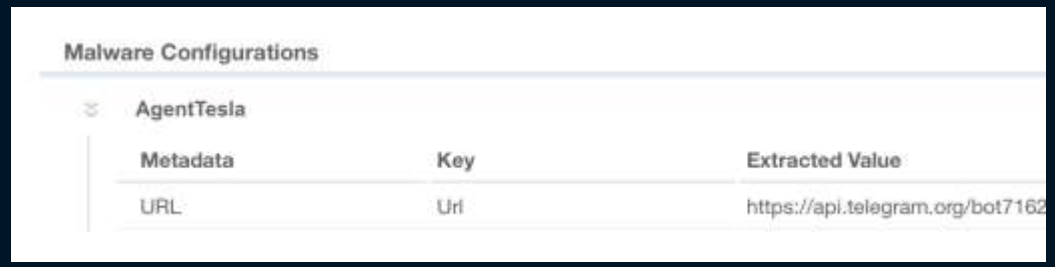
URL: ..shop

URL: ..shop

.. ..

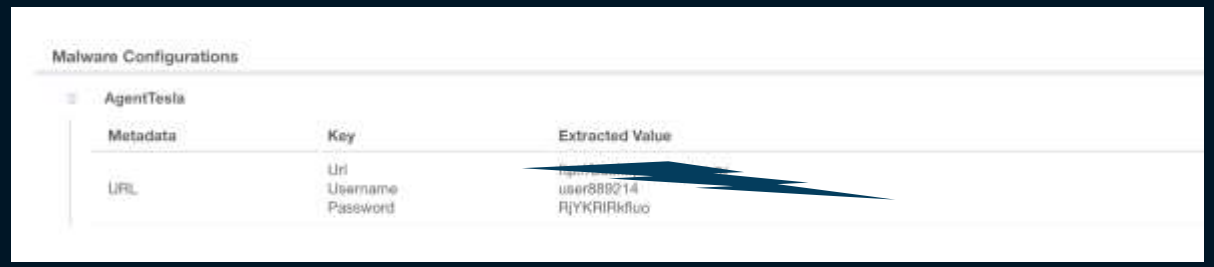
AGENT TESLA | Config Data

Sample 1




```
URL: https://api.telegram.org/bot...
```

Sample 2

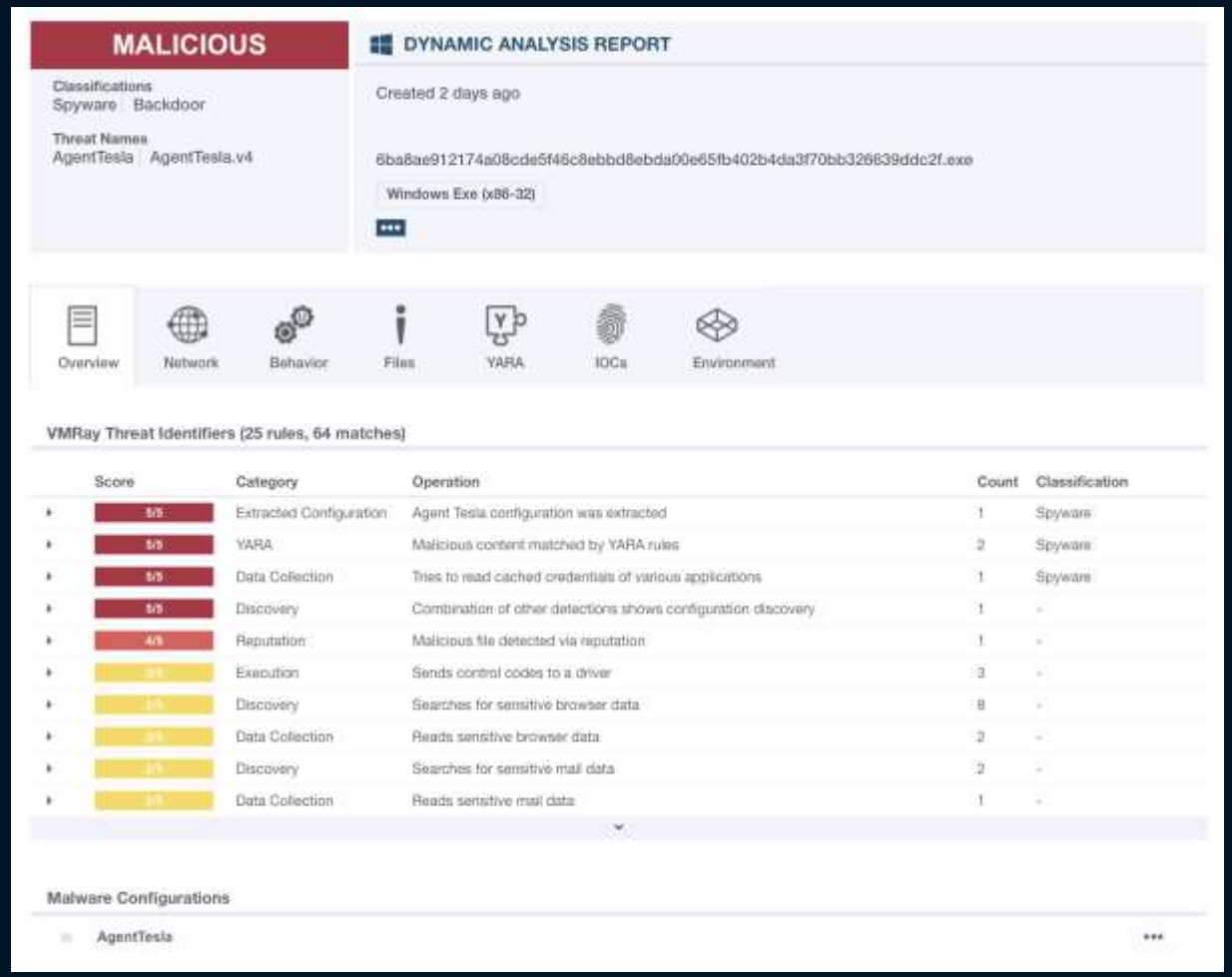



```
URL: ftp://backup...ru
```

```
username: ..
```

```
password: ..
```

Finding patterns > connecting dots



MALICIOUS

DYNAMIC ANALYSIS REPORT

Classifications
Spyware | Backdoor

Threat Names
AgentTesla | AgentTesla.v4

Created 2 days ago

6ba8ae912174a08cde5f46c8ebbd8ebda00e65fb402b4da3f70bb326639ddc2f.exe

Windows Exe (x86-32)

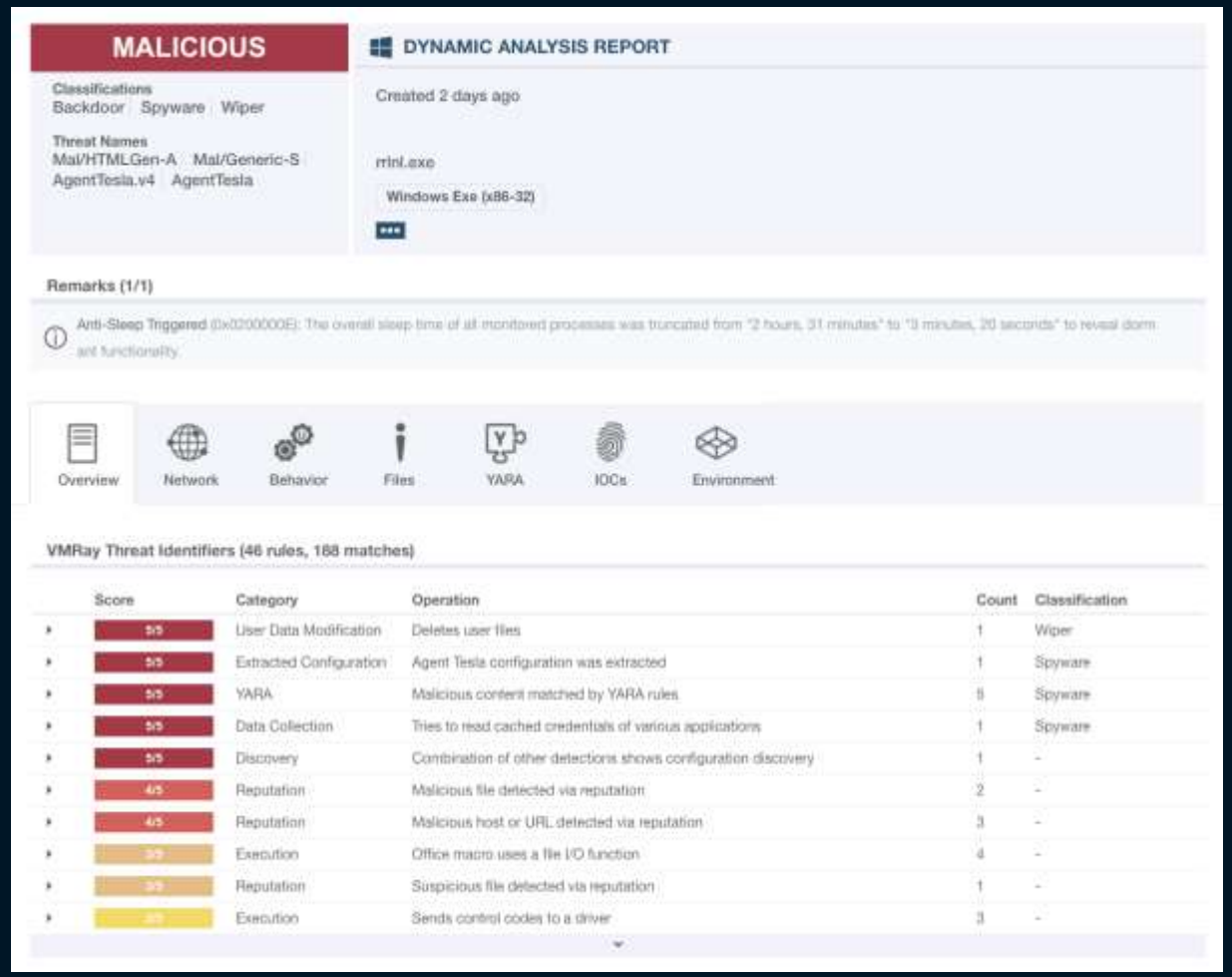
Overview | Network | Behavior | Files | YARA | IOCs | Environment

VMRay Threat Identifiers (25 rules, 64 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
4/5	Reputation	Malicious file detected via reputation	1	-
3/5	Execution	Sends control codes to a driver	3	-
3/5	Discovery	Searches for sensitive browser data	8	-
3/5	Data Collection	Reads sensitive browser data	2	-
3/5	Discovery	Searches for sensitive mail data	2	-
3/5	Data Collection	Reads sensitive mail data	1	-

Malware Configurations

AgentTesla



MALICIOUS

DYNAMIC ANALYSIS REPORT

Classifications
Backdoor | Spyware | Wiper

Threat Names
Mal/HTMLGen-A | Mal/Generic-S
AgentTesla.v4 | AgentTesla

Created 2 days ago

rrlnl.exe

Windows Exe (x86-32)

Remarks (1/1)

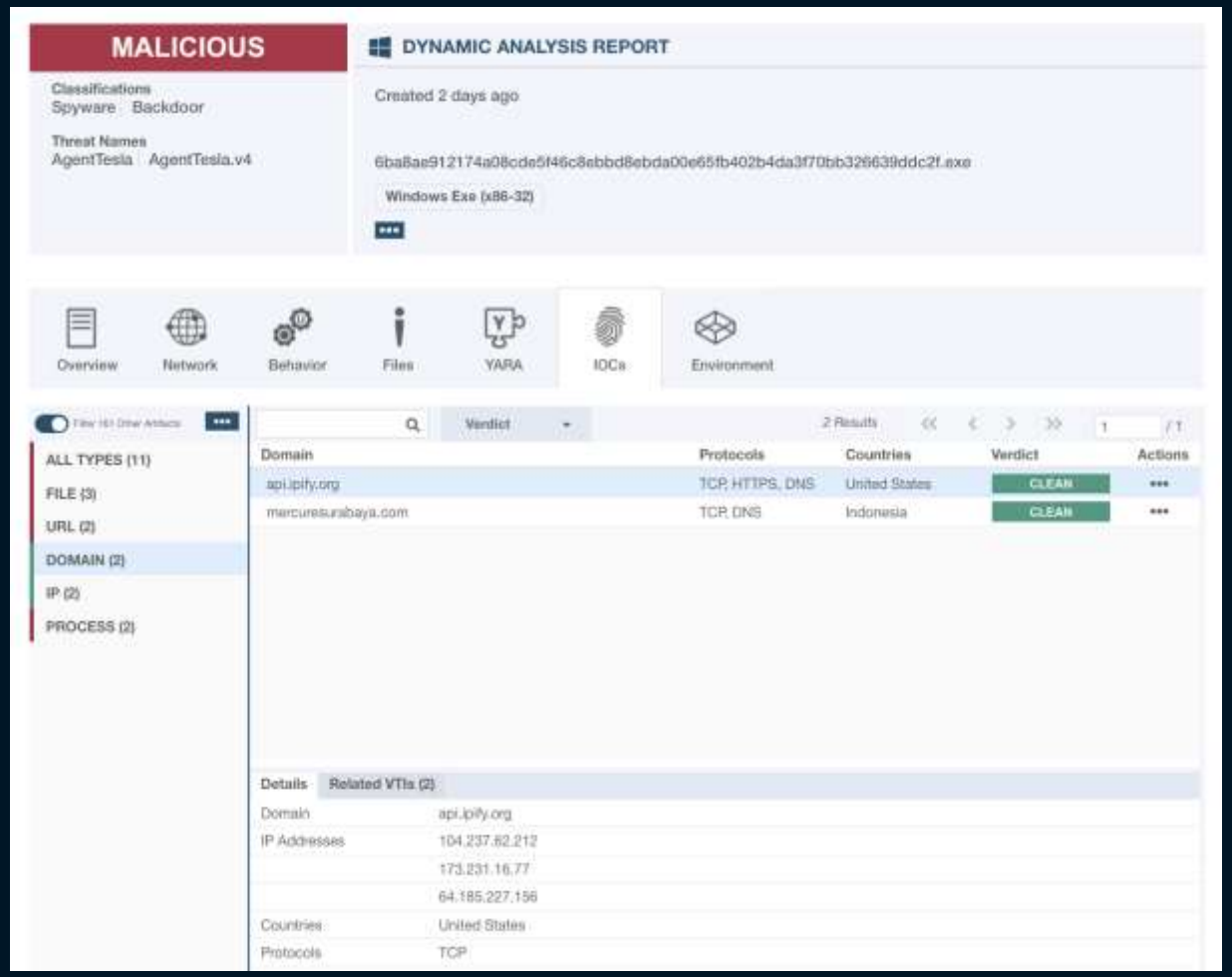
Anti-Sleep Triggered (0x0200000E): The overall sleep time of all monitored processes was truncated from "2 hours, 31 minutes" to "3 minutes, 20 seconds" to reveal dormant functionality

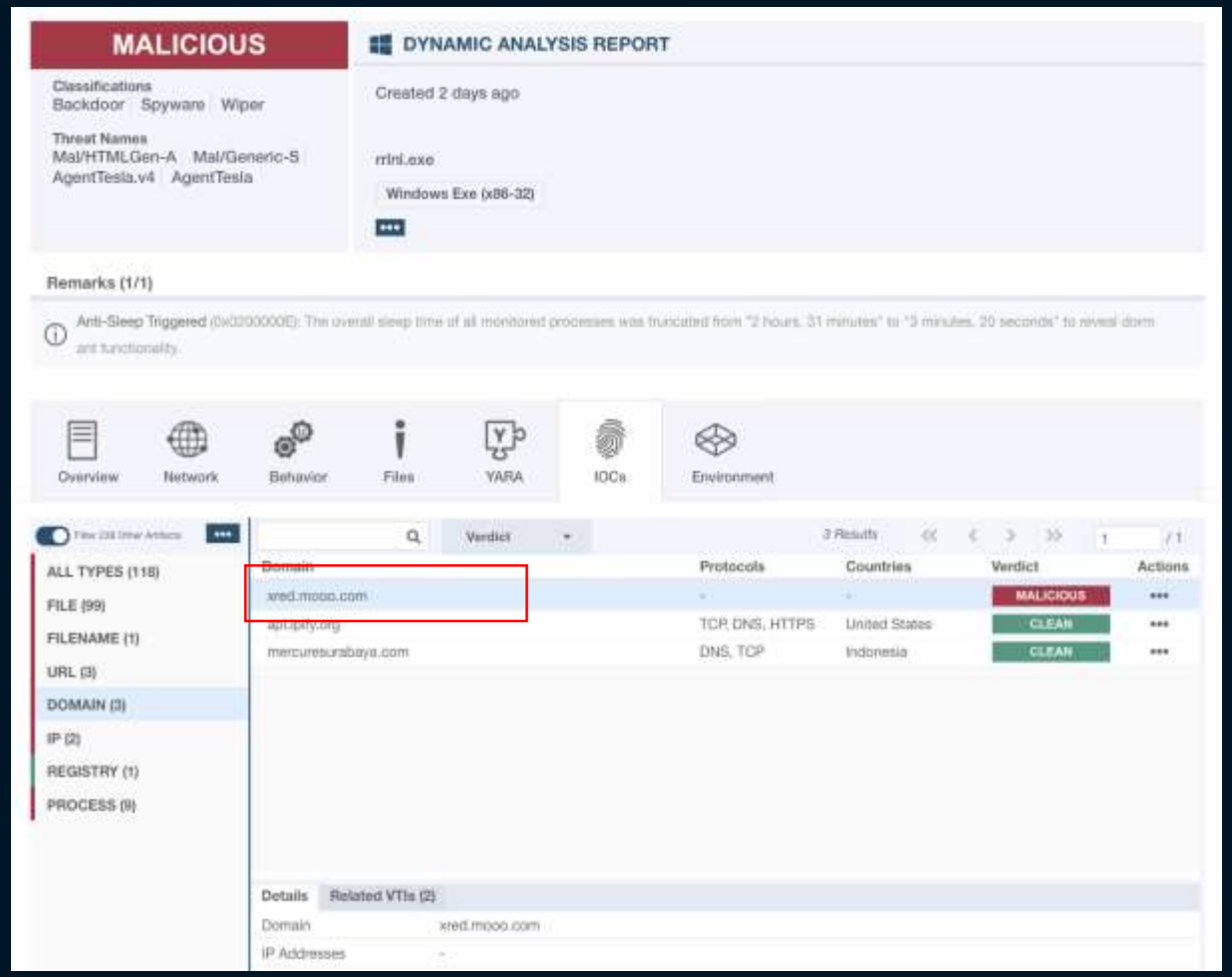
Overview | Network | Behavior | Files | YARA | IOCs | Environment

VMRay Threat Identifiers (46 rules, 188 matches)

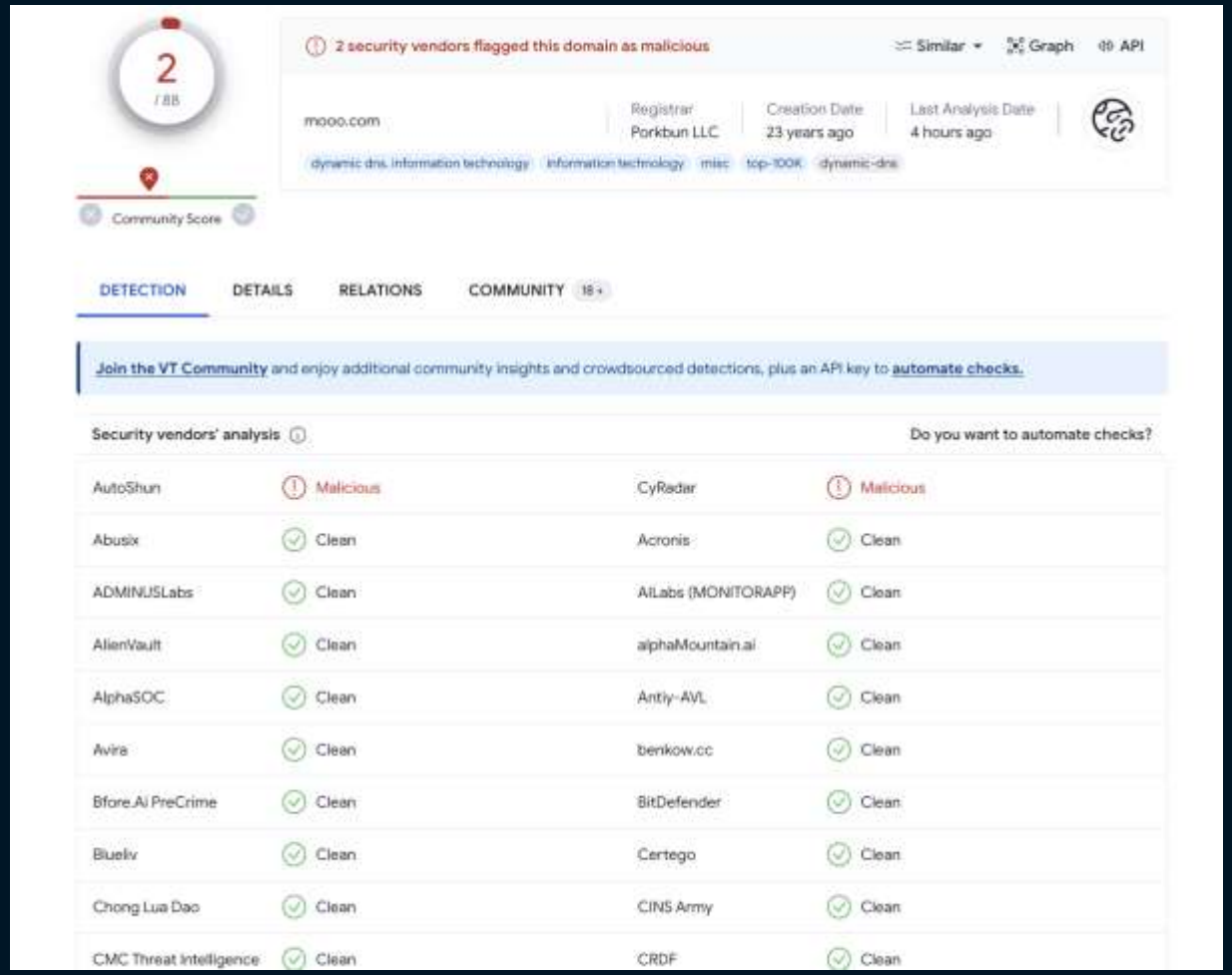
Score	Category	Operation	Count	Classification
5/5	User Data Modification	Deletes user files	1	Wiper
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
5/5	YARA	Malicious content matched by YARA rules	5	Spyware
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
4/5	Reputation	Malicious file detected via reputation	2	-
4/5	Reputation	Malicious host or URL detected via reputation	3	-
3/5	Execution	Office macro uses a file I/O function	4	-
3/5	Reputation	Suspicious file detected via reputation	1	-
3/5	Execution	Sends control codes to a driver	3	-

IOC Commonality





IOC Enrichment using TI tools



The same domain zone was used by **Winnti group / PlugX**

Typically motivated by espionage targeting Europe and South Asia and financial gain

Seamless integrations with Threat Intel tools

1) Malware
2) Suspicious files
3) URLs

Windows
Linux
MacOS

VOLUMETRIC SUBMISSIONS

Threat Intelligence Extraction

TotalInsight

Verdict
IOCs
Malware Classification

Incident Response

Hashes files

CTI Team

ANOMALI THREATSTREAM
MISP Threat Sharing
ThreatConnect

Connect the dots

Malware
Threat group

Automations

Enrich data using 3rd party APIs

Enrich data using native data

Resources from Community

[1] https://blog.eclecticiq.com/redline-stealer-variants-demonstrate-a-low-barrier-to-entry-threat

[2] https://www.trendmicro.com/tr_tr/research/23/i/redline-vidar-first-abuses-ev-certificates.html

[3] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/

[4] https://krebsonsecurity.com/2024/09/this-windows-powershell-phish-has-scary-potential/

[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

[6] https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

[7] https://www.bleepingcomputer.com/news/security/adobe-acrobat-sign-abused-to-push-redline-info-stealing-malware/

[8] https://unit42.paloaltonetworks.com/teasing-secrets-malware-configuration-parsing/

[9] https://www.bleepingcomputer.com/news/security/infostealer-malware-bypasses-chromes-new-cookie-theft-defenses/

[10] https://www.vmray.com/obfuscated-batch-file-downloads-open-source-stealer-straight-from-github/

EBOOK
Malware Configurations
How to find and use them?

https://www.vmray.com/resources/malware-configuration/

Free Access | VMRay Sandbox Reports

STEALC
https://www.vmray.com/analyses/4b7c4f962efb/report/overview.html

AGENT TESLA
1 https://www.vmray.com/analyses/34aa26c19b5f/report/overview.html
2 https://www.vmray.com/analyses/6d0c73cca21a/report/overview.html

SOCKS5SYSTEMZ
https://www.vmray.com/analyses/fc91fbd564a8/report/overview.html

REMCOS
https://www.vmray.com/analyses/1a7f73810fe7/report/overview.html

REDLINE
https://www.vmray.com/analyses/_vt/0e1fb62097c1/report/overview.html

LUMMA
1 https://www.vmray.com/analyses/_vt/e0486e2b9833/report/overview.html
2 https://www.vmray.com/analyses/_vt/3df25eeded4d/report/overview.html

NANOCORE
https://www.vmray.com/analyses/47f3fb622c45/report/overview.html

Key takeaways

- Malware like **infostealer needs a broader lens** when it comes to threat intelligence and threat modeling.
- **Threat Hunting Tip**: Malware C2 infrastructure to operate, whether through IP addresses, domains, FTP, or dynamic DNS services.
- Continually extracted **behaviors/IOCs**, such as persistence techniques and encryption usage, can help analysts **anticipate the attacks and get proactive.**

Thank you.

Q&A

VMRAY | vmray.com

Next?

To request a **free trial**, please visit our website.

Access Public Threat Feed

For millions of **malware analysis** reports, check out our community portal: **threatfeed.vmray.com**

Latest detection & YARA updates (09/24)

Blog post by VMRay Labs

Turn uncertainty into clarity

Files

URLs

Emails

- Infostealer
- Dropper
- Phishing URL
- Backdoor
- Banking trojan
- Exploit
- Hacktool
- Ransomware
- RAT
- Rootkit
- Spyware
- Trojan
- Worm
- Wiper
- Adware
- Cryptominer
- Bot

FinalVerdict

DeepResponse

TotalInsight

Accurate Verdict

MALICIOUS

Actionable Insights & IOCs