Briefing Malware

CERT Sogeti ESEC

TLP:WHITE

About this report

This report aims to identify the Tactics, Techniques and Procedures (TTP's) of the most known malwares along this year on the *ANY.RUN* platform © from the 04/10 to 11/10.
This analysis is based on the *MITRE ATT&CK* © matrix in the evaluation of the TTP's most exploited by cyber actors in order to prioritize the vigilance effort of the detection and incident response teams.
A remediation solution is proposed in the "Mitigations" tab for each technique.

Please note that the sub-techniques are now available for the Enterprise Matrix of Mitre ATT&CK. We work on it to add more and more details about these sub-techniques in the present communication. You can click here to know more about this new way of analysing TTPs of malwares.

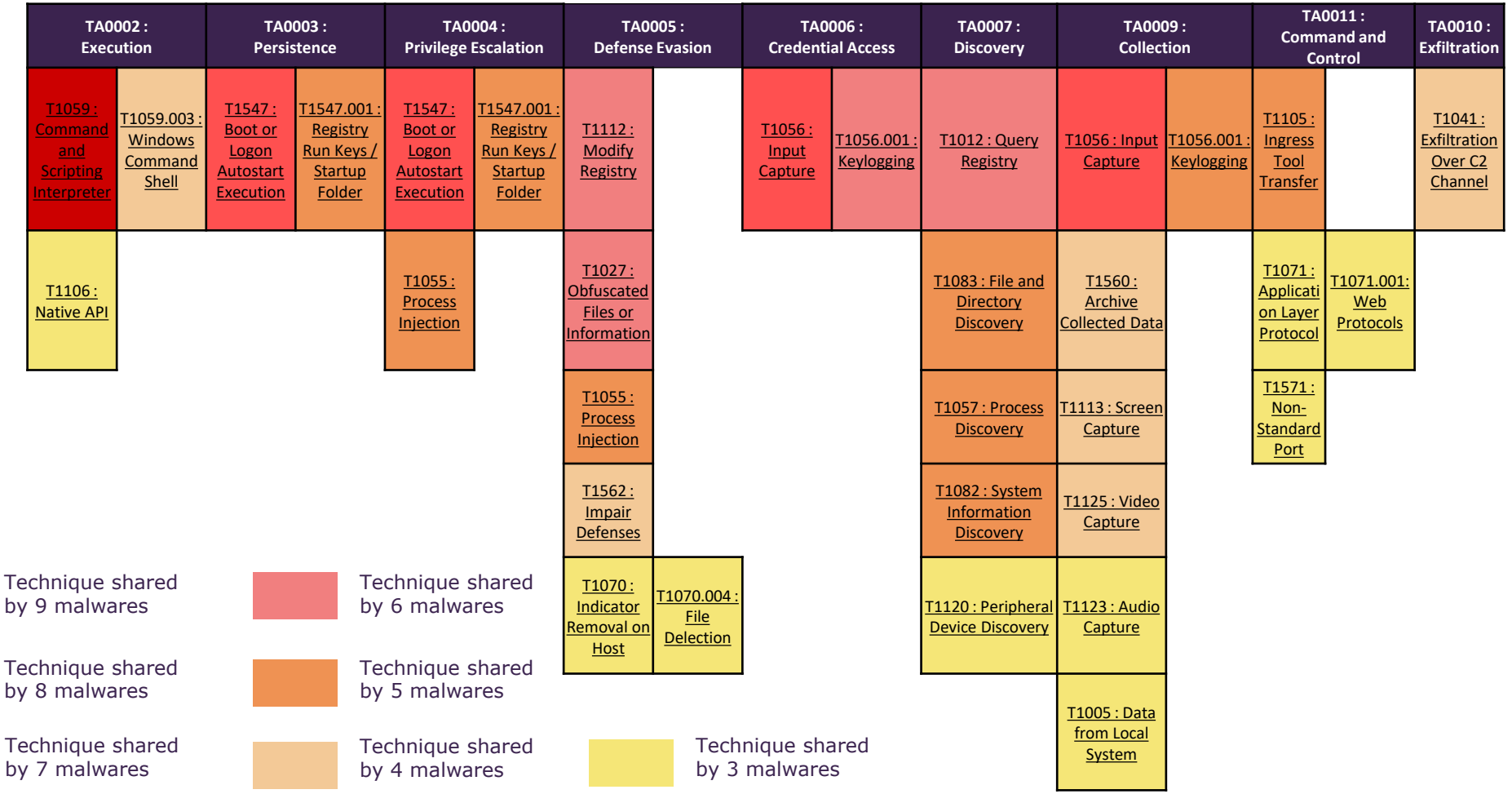
Most Recurrent Malwares

=	1	Redline (NC)
=	2	njRAT (ID Mitre: S0385)
^	3	FormBook (NC)
^	4	**Nanocore** (ID Mitre: S0336)
^	5	Snake (NC)
=	6	AsyncRAT (NC)
v	7	Vidar (NC)
^	8	**Lokibot** (ID Mitre: S0447)
^	9	**Remcos** (ID Mitre : S0332)
v	10	Raccoon (NC)

TLP:WHITE

Most observed malwares's TTPs overlaps

A graphic presentation of TTPs overlaps between malwares is available in the next pages. For each tactic, you can find the listing of the names and the IDs of the techniques.
Credits from The Mitre Corporation ©.



Legend

- Technique shared by 9 malwares
- Technique shared by 8 malwares
- Technique shared by 7 malwares
- Technique shared by 6 malwares
- Technique shared by 5 malwares
- Technique shared by 4 malwares
- Technique shared by 3 malwares

TLP:WHITE

List of most leveraged techniques

To optimize the visibility of the results, only techniques shared by at least 3 malwares are listed here (from the most to the less shared).

T1059	Command and scripting interpreter
T1547	Boot or Logon Autostart Execution
T1056	Input Capture
T1012	Query registry
T1082	System Information Discovery
T1547.001	Registry run keys/Startup folder
T1112	Modify registry
T1027	Obfuscated files or information
T1056.001	Keylogging
T1057	Process discovery
T1059.003	Windows Command Shell
T1055	Process injection
T1083	File and Directory Discovery
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1105	Ingress tool transfer
T1562	Impair defense
T1070	indicator Removal on host
T1070.004	File Deletion
T1555	Credential from Password Stores
T1555.003	Credential from Web browsers
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1120	Peripheral Device Discovery
T1123	Audio Capture
T1005	Data from Local System
T1571	Non-standard port
T1041	Exfiltration over C2 channel

What's new?

Vidar (NC)

Vidar Stealer Abuses Mastadon Social Network

#Cyberint researchers unveil a new **#Vidar malware** campaign. The specificity of this campaign is that the list of Command and Control (**#C2**) is dynamically retrieved from a **#Mastodon** instance.

Mastodon is a social network, usually compared to **#Twitter** and most of the time a trusted destination network even in a professional context. This configuration permit the infected to connect to a pre-defined Mastodon profile with a POST request containing the Vidar campaign ID and receive the C2 configuration.

Any C2 involved had between 500 and 1500 campaign IDs with indicates the popularity of the stealer.

Vidar is an **information stealer** that is active since October 2018 and linked to the former **#Arkei Stealer**. The simplicity and his ongoing development has made Vidar a popular stealer. Vidar is sold on underground forums or some **#Telegram** channels from $150 to $750 and is totally independent.

Vidar is mostly used to steal web browser personal information like **credentials**, **cookies** or **credit cards** details, **cryptocurrency wallets** or **files** according to pre-defined regex from streamers, social media influencers or just private people.

https://blog.cyberint.com/vidar-stealer-abuses-mastadon-social-network