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 21/09 to 27/09.
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	Avemaria (NC)
=	5	AsyncRAT (NC)
v	6	**Lokibot** (ID Mitre: S0447)
^	7	Vidar (NC)
^	8	Snake (NC)
=	9	**Remcos** (ID Mitre : S0332)
=	10	**Nanocore** (ID Mitre: S0336)

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 ©.

TA0002 : Execution		TA0003 : Persistence		TA0004 : Privilege Escalation		TA0005 : Defense Evasion		TA0006 : Credential Access		TA0007 : Discovery	TA0009 : Lateral movement		TA0009 : Collection		TA0011 : Command and Control	TA0010 : Exfiltration
T1059 : Command and Scripting Interpreter	T1059.003 : Windows Command Shell	T1547 : Boot or Logon Autostart Execution	T1547.001 : Registry Run Keys / Startup Folder	T1547 : Boot or Logon Autostart Execution	T1547.001 : Registry Run Keys / Startup Folder	T1112 : Modify Registry		T1056 : Input Capture	T1056.001 : Keylogging	T1057 : Process Discovery	T1021 : Remote Services	T1021.001 : Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer	T1041 : Exfiltration Over C2 Channel
				T1055 : Process Injection		T1027 : Obfuscated Files or Information			T1056.004 : Credential API Hooking	T1012 : Query Registry				T1056.004 : Credential API Hooking	T1571 : Non-Standard Port	
						T1055 : Process Injection				T1083 : File and Directory Discovery			T1125 : Video Capture			
						T1562 : Impair Defenses				T1082 : System Information Discovery			T1560 : Archive Collected Data			
						T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1120 : Peripheral Device Discovery			T1113 : Screen Capture			
													T1123 : Audio Capture			
													T1005 : Data from Local System			

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).

T1056	Input Capture
T1547	Boot or Logon Autostart Execution
T1059	Command and scripting interpreter
T1112	Modify registry
T1027	Obfuscated files or information
T1057	Process discovery
T1012	Query registry
T1547.001	Registry run keys/Startup folder
T1055	Process injection
T1056.001	Keylogging
T1083	File and Directory Discovery
T1125	Video capture
T1105	Ingress tool transfer
T1562	Impair defense
T1082	System Information Discovery
T1560	Archive Collected Data
T1113	Screen capture
T1059.003	Windows Command Shell
T1070	indicator Removal on host
T1070.004	File Deletion
T1056.004	Credential API Hooking
T1120	Peripheral Device Discovery
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1123	Audio Capture
T1005	Data from Local System
T1571	Non-standard port
T1041	Exfiltration over C2 channel

What's new?

Vidar (NC)

New Vidar Stealer Evasion Arsenal
A new anti analysis technic has been spotted while investigating **#Vidar Stealer** by **#Minerva** analysts. Those **#anti debugging** technics are used to prevent detection by security products which performs their analysis inside an **#emulator** environment like a sandbox but, usually, with some specific's configuration. The analyzed sample of **#Vidar** contains 3 distinct methods to prevent the detection, such as the use of IsDebuggerPresent **#API** call as well as the username and the hostname used by **#Microsoft Defender** inside the emulator (**#JohnDoe** and **#HAL9TH**).
Vidar, a malware as a Service (**#MaaS**) is deployed to steal sensitive information such as **#banking credential**, **#saved password**, **#browser history** or **#crypto wallet**.

https://blog.minerva-labs.com/vidar-stealer-evasion-arsenal