Briefing Malware

CERT Sogeti ESEC

TLP:GREEN

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 15/11 to 22/11.
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	Emotet (ID Mitre: S0367)
=	3	FormBook (NC)
v	4	njRAT (ID Mitre: S0385)
^	5	Lokibot (ID Mitre: S0447)
v	6	Nanocore (ID Mitre: S0336)
v	7	Remcos (ID Mitre : S0332)
v	8	AsyncRAT (NC)
v	9	Vidar (NC)
^	10	Raccoon (NC)

TLP:GREEN

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 ©.

TA0001 : Initial Access	TA0002 : Execution		TA0003 : Persistence		TA0004 : Privilege Escalation		TA0005 : Defense Evasion		TA0006 : Credential Access		TA0007 : Discovery	TA0008 : Lateral Movement	TA0009 : Collection		TA0011 : Command and Control	TA0010 : Exfiltration
T1566 : Phishing	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	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer	T1041 : Exfiltration Over C2 Channel
		T1059.001 : Powershell	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1055 : Process Injection		T1027 : Obfuscated Files or Information		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1012 : Query Registry		T1560 : Archive Collected Data		T1571 : Non-Standard Port	
		T1059.005 : Visual Basic			T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1083 : File and Directory Discovery		T1113 : Screen Capture			
	T1106 : Native API						T1562 : Impair Defenses				T1082 : System Information Discovery		T1125 : Video Capture			
	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task					T1055 : Process Injection				T1120 : Peripheral Device Discovery		T1123 : Audio Capture			
	T1204 : User Execution															

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:GREEN

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
T1547.001	Registry run keys/Startup folder
T1112	Modify registry
T1057	Process discovery
T1012	Query registry
T1059.003	Windows Command Shell
T1027	Obfuscated files or information
T1056.001	Keylogging
T1083	File and Directory Discovery
T1560	Archive Collected Data
T1105	Ingress tool transfer
T1070	indicator Removal on host
T1070.004	File Deletion
T1082	System Information Discovery
T1113	Screen capture
T1125	Video capture
T1571	Non-standard port
T1566	Phishing
T1059.001	Powershell
T1059.005	Visual Basic
T1106	Native API
T1053	Scheduled Task/Job
T1053.005	Scheduled Task
T1204	User execution
T1562	Impair defenses
T1055	Process injection
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1120	Peripheral Device Discovery
T1021	Remote Services
T1123	Audio capture
T1041	Exfiltration Over C2 Channel

What's new?

Emotet (ID Mitre: S0367)

Netskope Threat Coverage: The Return of Emotet

#Netskope published a report about the return of one of the most important threat of the beginning of this year, #Emotet. This threat has been spotted again in a campaign delivered by the #Trickbot botnet infrastructure.
Emotet is active since 2014 and was initially a #banking trojan that has evolved in a botnet used to delivered other loaders such as Trickbot or IcedID but also ransomware payloads namely #Ryuk before being taken down by law enforcement agencies in January 2021.
The new campaign lure victims to active macros in Microsoft Office to execute obfuscated #Powershell scripts which will download malicious DLLs ending the process with a packed DLL; the last step being Emotet execution in memory. After that, Emotet will start its communications with Command and control (#C&C) servers. As of writing, there's 13 servers online .

https://www.netskope.com/blog/netskope-threat-coverage-the-return-of-emotet