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 08/11 to 15/11.
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	njRAT (ID Mitre: S0385)
↓	3	FormBook (NC)
↑	4	**Nanocore** (ID Mitre: S0336)
=	5	**Remcos** (ID Mitre : S0332)
↑	6	AsyncRAT (NC)
=	7	Vidar (NC)
↑	8	Avemaria (NC)
↑	9	Orcus (NC)
↓	10	**Lokibot** (ID Mitre: S0447)

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	TA0008 : Lateral Movement		TA0009 : Collection		TA0011 : Command and Control
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	T1012 : Query Registry	T1021 : Remote Services	T1021.001 : Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer
T1106 : Native API				T1548 : Abuse Elevation Control Mechanism	T1548.002 : Bypass User Account Control	T1070 : Indicator Removal on Host	T1070.004 : File Delection		T1056.004 : Credential API Hooking	T1083 : File and Directory Discovery	-	-		T1056.004 : Credential API Hooking	T1571 : Non-Standard Port
				T1055 : Process Injection		T1548 : Abuse Elevation Control Mechanism	T1548.002 : Bypass User Account Control			T1057 : Process Discovery	-	-	T1560 : Archive Collected Data		
						T1027 : Obfuscated Files or Information				T1082 : System Information Discovery	-	-	T1113 : Screen Capture		
						T1055 : Process Injection				T1120 : Peripheral Device Discovery	-	-	T1125 : Video Capture		

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
T1112	Modify registry
T1083	File and Directory Discovery
T1057	Process discovery
T1547.001	Registry run keys/Startup folder
T1105	Ingress tool transfer
T1070	indicator Removal on host
T1070.004	File Deletion
T1056.001	Keylogging
T1082	System Information Discovery
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1106	Native API
T1059.003	Windows Command Shell
T1548	Abuse Elevation Control Mechanism
T1548.002	Bypass User Account Control
T1055	Process injection
T1027	Obfuscated files or information
T1056.004	Credential API Hooking
T1120	Peripheral Device Discovery
T1021	Remote Services
T1021.003	Remote Desktop Protocol
T1571	Non-standard port

What's new?

njRAT (ID Mitre: S0385) /
AsyncRAT (NC)

HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks

#Microsoft 365 Defender Threat Intelligence Team published a report about an evasive technique, #HTML smuggling. This technique permit to use #HTML5 and #JavaScript legitimate features to generate malicious files on the victim behind the firewall and execute them. The main objective of this technique is to bypass most of standard security controls performed by pattern or signature that could use email gateway or web proxies by using features like JavaScript Blob or the "download" attribute of a href HTML object.
Microsoft Threat Intelligence Center (#MSTIC) published a detailed analysis of sophisticated email attack from threat actor #NOBELIUM where HMTL smuggling was used to deliver some Remote Access Trojan such as #AsyncRAT or #NjRAT and more recently to delivers #Trickbot in a campaign related to a new threat actor tracked by MSTIC as #DEV-0193.

https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/