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 20/12 to 27/12.
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	AsyncRAT (NC)
^	4	Nanocore (ID Mitre: S0336)
v	5	FormBook (NC)
^	6	Vidar (NC)
^	7	Orcus (NC)
^	8	Quasar (ID Mitre: S0262)
=	9	Remcos (ID Mitre : S0332)
v	10	Snake (NC)

TLP:WHITE

Most observed malware'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	T1083 : File and Directory Discovery	T1021 : Remote Services	T1021.001 : Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer
T1204 : User Execution				T1055 : Process Injection		T1027 : Obfuscated Files or Information		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1012 : Query Registry			T1113 : Screen Capture		T1132 : Data Encoding
						T1070 : Indicator Removal on Host	T1070.004 : File Deletion	T1552 : Unsecured Credentials		T1082 : System Information Discovery			T1125 : Video Capture		T1571 : Non-Standard Port
						T1562 : Impair Defenses	T1562.004 : Disable or Modify System Firewall			T1057 : Process Discovery			T1560 : Archive Collected Data		
						T1055 : Process Injection				T1120 : Peripheral Device Discovery			T1123 : Audio Capture		
										T1124 : System Time Discovery					

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).

T1547	Boot or Logon Autostart Execution
T1056	Input Capture
T1547.001	Registry run keys/Startup folder
T1059	Command and scripting interpreter
T1112	Modify registry
T1056.001	Keylogging
T1083	File and Directory Discovery
T1012	Query registry
T1082	System Information Discovery
T1059.003	Windows Command Shell
T1027	Obfuscated files or information
T1057	Process discovery
T1113	Screen capture
T1125	Video capture
T1105	Ingress tool transfer
T1070	indicator Removal on host
T1560	Archive Collected Data
T1204	User Execution
T1055	Process injection
T1070.004	File Deletion
T1562	Impair defenses
T1562.004	Disable or Modify System Firewall
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1552	Unsecured Credentials
T1120	Peripheral Device Discovery
T1124	System Time Discovery
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1123	Audio Capture
T1132	Data Encoding
T1571	Non-standard port

What's new?

FormBook (NC)

Attackers test "CAB-less 40444" exploit in a dry run

During September 2021, the main issue Cyber security researcher faced was #CVE-2021-40444, a vulnerability impacting all the #Microsoft Office products and allowing a Remote Code Execution (#RCE). This vulnerability was used as an initial access vector targeting the #Russian Ministry of Interior and #State Rocket Center. It was patched by #Microsoft in September's Patch Tuesday. However, attackers were trying to exploit this vulnerability before the patch is applied and some mitigations involving #ActiveX installation deactivation had to be performed to prevent exploitation via an initial #CAB file method.

#Sophos Labs discovered a campaign that attempted to bypass mitigation measures in place at this time by packaging the exploit inside a #RAR archive file. The adversary could take advantage of the fact that in RAR5 standard, any code before RAR magic bytes will not be treated. Therefore, it is possible to insert a #Visual Basic script which will be executed when the word document inside the archive is extracted and opened, triggering the download of #Formbook malware. This technique will not work on a fully patched system at the time of writing of this article.

Formbook is active since 2016 and is one of the most established #information stealer constantly evolving to stay attractive to attackers.

https://news.sophos.com/en-us/2021/12/21/attackers-test-cab-less-40444-exploit-in-a-dry-run/