Briefing Malware

CERT Capgemini CIS

From January 1, 2022, Capgemini is bringing together its cybersecurity forces, originating from Sogeti and Capgemini Cloud Infrastructure Services, into a single entity, which operates under the Capgemini brand.

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 31/01 to 07/02.
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	Emotet (ID Mitre: S0367)
2	Redline (NC)
3	njRAT (ID Mitre: S0385)
4	FormBook (NC)
5	Remcos (ID Mitre : S0332)
6	Lokibot (ID Mitre : S0447)
7	Nanocore (ID Mitre: S0336)
8	AsyncRAT (NC)
9	DcRAT (NC)
10	Snake (NC)

Capgemini

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 ©.

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	T1566.001 : Spearphishing Attachment	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	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer	T1041 : Exfiltration Over C2 Channel
			T1059.001 : PowerShell	T1053 : Scheduled Task/Job		T1055 : Process Injection		T1070 : Indicator Removal on Host	T1070.004 : File Deletion	T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1057 : Process Discovery		T1560 : Archive Collected Data		T1571 : Non-Standard Port	
			T1059.005 : Visual Basic			T1053 : Scheduled Task/Job		T1027 : Obfuscated Files or Information		T1552 : Unsecured Credentials	T1552.001 : Credentials In Files	T1012 : Query Registry		T1113 : Screen Capture		T1132 : Data Encoding	
		T1053 : Scheduled Task/Job						T1055 : Process Injection				T1082 : System Information Discovery		T1125 : Video Capture			
		T1204 : User Execution	T1204.002 : Malicious File					T1562 : Impair Defenses	T1562.004 : Disable or Modify System Firewall			T1120 : Peripheral Device Discovery		T1123 : Audio Capture			
		T1106 : Native API										T1016 : System Network Configuration Discovery					

Technique shared by …

9 8 7 6 5 4 3 … malwares

Capgemini

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
T1059.003	Windows Command Shell
T1055	Process injection
T1070	indicator Removal on host
T1027	Obfuscated files or information
T1057	Process discovery
T1012	Query registry
T1082	System Information Discovery
T1105	Ingress tool transfer
T1053	Scheduled Task/Job
T1204	User Execution
T1070.004	File Deletion
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1571	Non-standard port
T1566	Phishing
T1566.001	Spearphishing Attachment
T1106	Native API
T1059.001	PowerShell
T1059.005	Visual Basic
T1204.002	Malicious File
T1562	Impair Defenses
T1562.004	Disable or Modify System Firewall
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1120	Peripheral Device Discovery
T1016	System Network Configuration Discovery
T1021	Remote Services
T1123	Audio Capture
T1132	Data Encoding
T1041	Exfiltration Over C2 Channel

What's new?

Emotet (ID Mitre: S0367)

Microsoft disables MSIX protocol handler abused in Emotet attacks

#Microsoft has announced that they will disable the #MSIX ms-appinstaller protocol handler to limit malware exploitation of the #Windows AppX Installer spoofing vulnerability tracked as #CVE-2021-43890.

Even if this vulnerability has been handled through December 2021 Patch Tuesday, Microsoft has justified this action by the massive exploitation of this flaw by #Emotet as well as #BazarLoader and, also to protect users that did not install the security patch or workaround to disable the handler.

In December 2021, #Emotet disguises its middle stage payloads as an installation of #Adobe PDF component to exploit this vulnerability and then install #Trickbot or #Qbot.

#Emotet is one of the most effective #botnets which has resurrected in mid-November after being taken down by law enforcement during Operation #LadyBird in the end of January 2021. The botnet which started as a #banking trojan is active since at least 2014, operated by the threat actor #TA542 (aka #Mummy Spider) and observed delivering payloads such as #Trickbot and #QBot droping ransomware such as #Conti, #Ryuk or #Egregor.

https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-msix-protocol-handler-abused-in-emotet-attacks/