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 18/01 to 25/01.
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.

You can click here to know more about a way of analysing TTPs of malwares.

Most Recurrent Malwares

=	1	Redline (NC)
⌃	2	Emotet (ID Mitre: S0367)
⌄	3	njRAT (ID Mitre: S0385)
⌃	4	FormBook (NC)
⌃	5	AsyncRAT (NC)
⌃	6	Remcos (ID Mitre : S0332)
=	7	Lokibot (ID Mitre : S0447)
⌃	8	Nanocore (ID Mitre: S0336)
⌄	9	AgentTesla (ID Mitre: S0331)
⌄	10	Vidar (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 ©.

TA0002 : Execution		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	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	T1027.002 : Software Packing	T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1083 : File and Directory Discovery		T1560 : Archive Collected Data		T1071 : Application Layer Protocol	T1071.001 : Web Protocols	
			T1059.005 : Visual Basic			T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1055 : Process Injection		T1552 : Unsecured Credentials		T1082 : System Information Discovery		T1113 : Screen Capture		T1571 : Non-Standard Port		
		T1204 : User Execution	T1204.002 : Malicious File					T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1012 : Query Registry		T1125 : Video Capture		T1132 : Data Encoding		
		T1106 : Native API						T1140 : Deobfuscate/Decode Files or Information				T1087 : Account Discovery		T1123 : Audio Capture				
		T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task					T1562 : Impair Defenses				T1033 : System Owner/User Discovery						
								T1497 : Virtualization/Sandbox Evasion				T1120 : Peripheral Device Discovery						
												T1016 : System Network Configuration Discovery						
												T1124 : System Time Discovery						
												T1497 : Virtualization/Sandbox Evasion						

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	T1555.003	Credentials from Web Browsers	T1106	Native API
T1056	Input Capture	T1012	Query registry	T1053	Scheduled Task/Job
T1059	Command and scripting interpreter	T1113	Screen capture	T1053.005	Scheduled Task
T1547.001	Registry run keys/Startup folder	T1125	Video capture	T1140	Deobfuscate/Decode Files or Information
T1112	Modify registry	T1566	Phishing	T1562	Impair Defenses
T1027	Obfuscated files or information	T1566.001	Spearphishing Attachment	T1497	Virtualization/Sandbox Evasion
T1057	Process discovery	T1204.002	Malicious File	T1027.002	Software Packing
T1059.003	Windows Command Shell	T1070	indicator Removal on host	T1070.004	File Deletion
T1055	Process injection	T1087	Account Discovery	T1552	Unsecured Credentials
T1056.001	Keylogging	T1033	System Owner/User Discovery	T1120	Peripheral Device Discovery
T1083	File and Directory Discovery	T1071	Application Layer Protocol	T1016	System Network Configuration Discovery
T1082	System Information Discovery	T1071.001	Web Protocols	T1124	System Time Discovery
T1560	Archive Collected Data	T1571	Non-standard port	T1021	Remote Services
T1105	Ingress tool transfer	T1041	Exfiltration Over C2 Channel	T1123	Audio Capture
T1204	User Exécution	T1059.001	PowerShell	T1132	Data Encoding
T1555	Credentials from Password Stores	T1059.005	Visual Basic		

What's new?

Emotet (ID Mitre: S0367)

Emotet Spam Abuses Unconventional IP Address Formats to Spread Malware

#TrendMicro observed latest #Emotet spam campaign and found that a new #obfuscation technique has been used to evade classic detection measures.
The malicious actor exploited #Excel 4.0 old macro, in this case auto_open, delivered via email attachment. The novelty is that the URL is obfuscated with carets and the IP address is defined in octal or hexadecimal. The code is automatically converted by the operating system into classic decimal format. The following actions are more common and will download a HTML application code as the next stage.
This discovery of this mechanism is occurring when #Microsoft communicated that they disable Excel 4.0 macros by default in the build 16.0.14427.10000 of Excel.
Despite the 10-months hiatus, Emotet is constantly evolving as the tactic of #Cobalt Strike beacon dropping discovered in December 2021.

https://www.trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html