Briefing Malware

CERT Capgemini CIS

From January 1st, 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 14/02 to 21/02.
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	Redline (NC)
2	njRAT (ID Mitre: S0385)
3	FormBook (NC)
4	Emotet (ID Mitre: S0367)
5	Lokibot (ID Mitre : S0447)
6	AsyncRAT (NC)
7	Orcus (NC)
8	Remcos (ID Mitre : S0332)
9	Nanocore (ID Mitre: S0336)
10	AgentTesla (ID Mitre: S0331)

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

What's new?

FormBook (NC)

Cybercrime, "Payment Advice for Outstanding Invoices" conveys Formbook

A new malware campaign has been spotted by #difesaesicurezza researcher Francesco Bussoletti that delivers the malware #Formbook.

The #phishing campaign named "**Payment Advice for Outstanding Invoices**" tries to attract the potential victim with the promise that a large amount of money have been transferred to its account. The "#GZ" file shown as a receipt of the transfer contains an executable with the malware inside.

Formbook is a Malware-as-a-Service (#MaaS), active since 2016, dedicated to steal personal information from the victims such as #credentials or #credit card saved in web browser, as well as #keystrokes or #screenshots of the desktop. They can also perform actions from Command and Control (#C2) servers and collect those information through #ftp.

https://www.difesaesicurezza.com/en/defence-and-security/cybercrime-payment-advice-for-outstanding-invoices-conveys-formbook/