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 21/02 to 28/02.
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	Emotet (ID Mitre: S0367)
4	FormBook (NC)
5	Lokibot (ID Mitre : S0447)
6	Orcus (NC)
7	Nanocore (ID Mitre: S0336)
8	Vidar (NC)
9	Remcos (ID Mitre : S0332)
10	Quasar (ID Mitre : S0262)

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		TA0010 : Exfiltration	TA0011 : Command and Control	
T1566 : Phishing	T1566.001 : Phishing: Spearphishing Attachment	T1059 : Command and Scripting Interpreter	T1059.003 : Command and Scripting Interpreter: Windows Com...	T1547 : Boot or Logon Autostart Execution	T1547.001 : Boot or Logon Autostart Execution: Registry Ru...	T1547 : Boot or Logon Autostart Execution	T1547.001 : Boot or Logon Autostart Execution: Registry Ru...	T1027 : Obfuscated Files or Information	T1027.002 : Obfuscated Files or Information: Software Packing	T1056 : Input Capture	T1056.001 : Input Capture: Keylogging	T1083 : File and Directory Discovery	T1021 : Remote Services	T1021.001 : Remote Services: Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Input Capture: Keylogging	T1041 : Exfiltration Over C2 Channel	T1105 : Ingress Tool Transfer	T1071.001 : Application Layer Protocol: Web Protocols
		T1053 : Scheduled Task/Job	T1059.001 : Command and Scripting Interpreter: PowerShell	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task/Job: Scheduled Task	T1055 : Process Injection	T1053.005 : Scheduled Task/Job: Scheduled Task	T1112 : Modify Registry		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Password Stores: Credentials ...	T1057 : Process Discovery			T1560 : Archive Collected Data			T1571 : Non-Standard Port	
		T1204 : User Execution	T1059.005 : Command and Scripting Interpreter: Visual Basic			T1053 : Scheduled Task/Job		T1055 : Process Injection		T1552 : Unsecured Credentials		T1012 : Query Registry			T1113 : Screen Capture			T1071 : Application Layer Protocol	
		T1106 : Native API	T1053.005 : Scheduled Task/Job: Scheduled Task					T1070 : Indicator Removal on Host				T1082 : System Information Discovery			T1125 : Video Capture			T1573 : Encrypted Channel	
			T1204.002 : User Execution: Malicious File									T1033 : System Owner/User Discovery							

Technique shared by …

9 8 7 6 5 4 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	T1041	Exfiltration Over C2 Channel	T1566	Phishing
T1547	Boot or Logon Autostart Execution	T1571	Non-Standard Port	T1566.001	Spearphishing Attachment
T1059.003	Windows Command Shell	T1055	Process Injection	T1021.001	Remote Desktop Protocol
T1056	Input Capture	T1021	Remote Services	T1053.005	Scheduled Task
T1027	Obfuscated Files or Information	T1053	Scheduled Task/Job	T1033	System Owner/User Discovery
T1547.001	Registry run keys/Startup folder	T1113	Screen Capture	T1552	Unsecured Credentials
T1056.001	Input Capture: Keylogging	T1204	User Execution	T1204.002	Malicious File
T1112	Modify Registry	T1125	Video Capture		
T1555	Credentials from Password Stores	T1071	Application Layer Protocol		
T1555.003	Credentials from Web Browsers	T1071.001	Web Protocols		
T1083	File and Directory Discovery	T1059.001	PowerShell		
T1105	Ingress Tool Transfer	T1059.005	Visual Basic		
T1057	Process Discovery	T1573	Encrypted Channel		
T1012	Query Registry	T1070	Indicator Removal on Host		
T1082	System Information Discovery	T1106	Native API		
T1560	Archive Collected Data	T1027.002	Software Packing		

What's new?

Emotet (ID Mitre: S0367)

TrickBot operators slowly abandon the botnet and replace it with Emotet

Last week, samples from #Conti's internal chats leaked. Among various addressed subjects, the group confirmed that the botnet #Trickbot has shut down this month. In addition, conversations showed relationships between #Conti ransomware group ,#Trickbot group, and #Emotet operators.

#Emotet malware is a #loader operated by the eponymous group on the loader-as-a-service model. After a takedown in January 2021, #Emotet malware came back in November 2021 with new features and techniques. The malware is now reemerging on the threat landscape, reaching Any.run submissions top 3 at this day.

Before disappearing, #Trickbot operators might move infected assets to other #botnets such as #Emotet to keep some monetization value, as suggested by #Intel 471 researchers. Historically, #Trickbot and #Emotet were distributing each other on infected targets, facilitating the transition.
It could sign a new rise of a Emotet.

https://www.csoonline.com/article/3651492/trickbot-operators-slowly-abandon-the-botnet-and-replace-it-with-emotet.html