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 14/03 to 21/03 .
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	Nanocore (ID Mitre: S0336)
7	Remcos (ID Mitre: S0332)
8	Raccoon (NC)
9	QuasarRAT (NC)
10	OrcusRAT (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 ©.

TA0004 : Execution		TA0005 : Persistence		TA0006 : Privilege Escalation		TA0007 : Defense Evasion		TA0008 : Credential Access		TA0009 : Discovery	TA0010 : Lateral Movement		TA0011 : Collection		TA0012 : Exfiltration	TA0013 : 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	T1057: Process Discovery	T1021: Remote Services	T1021.001: Remote Desktop Protocol	T1056: Input Capture	T1056.001: Keylogging	T1041: Exfiltration Over C2 Channel	T1105: Ingress Tool Transfer
	T1059.001: PowerShell	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1070: Indicator Removal on Host	T1070.004: File Deletion	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers	T1082: System Information Discovery			T1125: Video Capture			T1571: Non-Standard Port
	T1059.005: Visual Basic					T1497: Virtualization/Sandbox Evasion		T1552: Unsecured Credentials	T1552.001: Credentials In Files	T1083: File and Directory Discovery			T1560: Archive Collected Data			T1573: Encrypted Channel
T1053: Scheduled Task/Job	T1053.005: Scheduled Task									T1012: Query Registry			T1113: Screen Capture			
T1106: Native API										T1033: System Owner/User Discovery						
T1204: User Execution	T1204.002: Malicious File									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).

T1059	Command and Scripting Interpreter
T1056	Input Capture
T1056.001	Keylogging
T1059.003	Windows Command Shell
T1547	Boot or Logon Autostart Execution
T1547.001	Registry Run Keys / Startup Folder
T1105	Ingress Tool Transfer
T1027	Obfuscated Files or Information
T1112	Modify Registry
T1125	Video Capture
T1057	Process Discovery
T1082	System Information Discovery
T1555	Credentials from Password Stores
T1560	Archive Collected Data
T1113	Screen Capture
T1053	Scheduled Task/Job
T1053.005	Scheduled Task
T1055	Process Injection
T1571	Non-Standard Port
T1083	File and Directory Discovery
T1012	Query Registry
T1555.003	Credentials from Web Browsers
T1070	Indicator Removal on Host
T1021	Remote Services
T1041	Exfiltration Over C2 Channel
T1071.001	Web Protocols
T1573	Encrypted Channel
T1033	System Owner/User Discovery
T1497	Virtualization/Sandbox Evasion
T1016	System Network Configuration Discovery
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1070.004	File Deletion
T1059.001	PowerShell
T1059.005	Visual Basic
T1106	Native API
T1204	User Execution
T1204.002	Malicious File
T1021.001	Remote Desktop Protocol

What's new?

Emotet (ID Mitre: S0367)

Emotet malware campaign impersonates the IRS for 2022 tax season

Threat researchers from #Black Lotus Labs observe a regain of the number of emails sent by Emotet in March. This supports the resurgence of #Emotet botnet since November 2021, counting approximatively 130,000 unique bots spread across 179 countries since. #Tripwire estimated that the malware was involved in 30% of all malware attacks in 2021.

Emotet is a malware botnet distributed by phishing emails containing malicious Excel or Word documents with #macros. Once the malware compromised a target, it can install additional malware like #Cobalt Strike beacons, #ransomware or #RAT, but also send other spam mails and even spoof user's email threads to distribute itself to the other recipients. Last version (Epoch 5) includes new functionalities and improvements, especially in its network encryption.

As US tax season begins, the malicious mails distributing Emotet embodied the #IRS (US Internal Revenue Service), sending documents related to taxation forms. This campaign either sends a password encrypted zip file or a HTML file, both file format being hard to detect by security email gateways. The growth of Emotet bots might be helped by new #Conti group members joining Emotet operators as the close relationship between Conti and Emotet was recently confirmed by the Conti Leaks.

https://www.bleepingcomputer.com/news/security/emotet-malware-campaign-impersonates-the-irs-for-2022-tax-season/