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 25/04 to 02/05 .
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	njRAT (ID Mitre: S0385)
2	RedLine (NC)
3	Agent Tesla (ID Mitre: S0331)
4	Formbook (NC)
5	Emotet (ID Mitre: S0367)
6	Nanocore (ID Mitre: S0336)
7	LokiBot (ID Mitre: S0447)
8	Quasar RAT (NC)
9	Remcos (ID Mitre: S0332)
10	Orcus RAT (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 ©.

TA0003: Initial Access		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	
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	T1082: System Information 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	T1057: Process 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			T1113: Screen Capture			T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1053: Scheduled Task/Job	T1053.005: Scheduled Task									T1012: Query Registry			T1560: Archive Collected Data			T1573: Encrypted Channel	
		T1204: User Execution	T1204.002: Malicious File									T1033: System Owner/User Discovery							
		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).

T1056	Input Capture	**T1571**	Non-Standard Port	**T1059.005**	Visual Basic
T1547	Boot or Logon Autostart Execution	**T1204**	User Execution	**T1106**	Native API
T1027	Obfuscated Files or Information	**T1053.005**	Scheduled Task	**T1204.002**	Malicious File
T1112	Modify Registry	**T1113**	Screen Capture	**T1552**	Unsecured Credentials
T1059	Command and Scripting Interpreter	**T1560**	Archive Collected Data	**T1552.001**	Credentials In Files
T1056.001	Keylogging	**T1021**	Remote Services	**T1021.001**	Remote Desktop Protocol
T1547.001	Registry Run Keys / Startup Folder	**T1083**	File and Directory Discovery	**T1033**	System Owner/User Discovery
T1105	Ingress Tool Transfer	**T1012**	Query Registry	**T1016**	System Network Configuration Discovery
T1059.003	Windows Command Shell	**T1562**	Impair Defenses	**T1566**	Phishing
T1055	Process Injection	**T1070**	Indicator Removal on Host	**T1566.001**	Spearphishing Attachment
T1053	Scheduled Task/Job	**T1070.004**	File Deletion	**T1041**	Exfiltration Over C2 Channel
T1555	Credentials from Password Stores	**T1497**	Virtualization/Sandbox Evasion		
T1555.003	Credentials from Web Browsers	**T1071**	Application Layer Protocol		
T1125	Video Capture	**T1071.001**	Web Protocols		
T1082	System Information Discovery	**T1573**	Encrypted Channel		
T1057	Process Discovery	**T1059.001**	PowerShell		

What's new?

RedLine (NC)

RedLine Stealer Resurfaces in Fresh RIG Exploit Kit Campaign

#RedLine is a popular #stealer malware, cheap but powerful, with the ability to steal various information from crypto wallets to emails or VPN credentials. This diversity of stolen information makes it attractive to operators for monetization. #Bitdefender detected more than 10 000 Redline attacks this April 2022. Additionally, the editor identified a campaign at the start of the year using exploits for #CVE-2021-26411 found in #Internet Explorer (triggered when viewing a specially crafted website), that are part of #RIG Exploit Kit which is used to deliver the stealer. Once the exploit kit is successfully executed, it drops a #JScript file in the temporary folder and executes it with wscript.exe to download the payload and decrypt it with the #RC4 encryption key provided as parameter.
#Recorded Future estimated that the vast majority of stolen credentials currently sold on two dark web underground markets were collected using the RedLine Stealer malware.
Even if #Microsoft strongly advises to not use Internet Explorer, the browser is still largely used in the industry for operational reasons, so it is important to keep it updated. Moreover, it could be relevant noting that IE will end support in June 2022 and will stop receiving security patches in 2023.

https://www.bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/