



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 07/03 to 14/03. 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	Emotet (ID Mitre: S0367)
	3	njRAT (ID Mitre: S0385)
	4	FormBook (NC)
	5	AsyncRAT (NC)
	6	Lokibot (ID Mitre : S0447)
	7	Nanocore (ID Mitre: S0336)
	8	OrcusRAT (NC)
	9	Remcos (ID Mitre : S0332)
	10	DcRAT (NC)



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	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	T1027 : Obfuscated Files or Information	T1027.002 : Software Packing	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		T1112 : Modify Registry	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		T1012 : Query Registry		T1113 : Screen Capture		T1571 : Non-Standard Port			
			T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task				T1140 : Deobfuscate/Decode Files or Information				T1082 : System Information Discovery		T1125 : Video Capture					
			T1204 : User Execution	T1204.002 : Malicious File				T1562 : Impair Defenses				T1033 : System Owner/User Discovery							
			T1106 : Native API					T1070 : Indicator Removal on Host				T1087 : Account Discovery							
								T1497 : Virtualization/Sandbox Evasion				T1016 : System Network Configuration Discovery							
												T1124 : System Time Discovery							
												T1497 : Virtualization/Sandbox Evasion							

Technique shared by ...



... malwares



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

What's new?

[Redline](#) (NC)

Fake Valorant cheats on YouTube infect you with RedLine stealer

#ASEC security analysts, from #South Korea discovered a malware campaign that tries to exploit #Valorant game fame to lure victims.

Threat actor creates #Youtube content to promote a new auto-aiming cheat on this First Person Shooter (#FPS) and gives future victim a link to the package on #Anonfile.com, a file sharing platform, in the description of the video. The #RAR file contains an executable named "Cheat installer.exe".

Malware campaign previously spotted in October 2021 led to #Raccoon or #Redline Stealer. This one is "only" leading to #Redline.

#Redline is an information stealer following a Malware-as-a-Service model (#MaaS) and running at least since 2020. It steals #credentials, #browser history, #credit card information, #vpn client configuration as well as taking desktop #screenshots or saving #keystrokes. The stolen information is packed and delivered to the threat actor using a #Webhook API post request to a #Discord channel. Redline also allows to execute commands on the victims' machines and upload or download files.

<https://www.bleepingcomputer.com/news/security/fake-valorant-cheats-on-youtube-infect-you-with-redline-stealer/>