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 09/05 to 16/05 .
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	RedLine (NC)
2	Formbook (NC)
3	njRAT (ID Mitre: S0385)
4	Agent Tesla (ID Mitre: S0331)
5	Emotet (ID Mitre: S0367)
6	LokiBot (ID Mitre: S0447)
7	Remcos (ID Mitre: S0332)
8	Nanocore (ID Mitre: S0336)
9	Quasar RAT (NC)
10	Ave Maria (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	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	T1027: Obfuscated Files or Information	T1027.002: Software Packing	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			T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control	T1070: Indicator Removal on Host	T1070.004: File Deletion	T1552: Unsecured Credentials	T1552.001: Credentials In Files	T1083: File and Directory Discovery			T1560: Archive Collected Data			T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1204: User Execution	T1204.002: Malicious File					T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control			T1012: Query Registry			T1113: Screen Capture			T1573: Encrypted Channel	
		T1053: Scheduled Task/Job	T1053.005: Scheduled Task									T1124: System Time Discovery							
		T1106: Native API										T1033: System Owner/User Discovery							
												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
T1547	Boot or Logon Autostart Execution
T1059	Command and Scripting Interpreter
T1112	Modify Registry
T1056.001	Keylogging
T1105	Ingress Tool Transfer
T1027	Obfuscated Files or Information
T1125	Video Capture
T1547.001	Registry Run Keys / Startup Folder
T1055	Process Injection
T1057	Process Discovery
T1082	System Information Discovery
T1059.003	Windows Command Shell
T1083	File and Directory Discovery
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1021	Remote Services
T1560	Archive Collected Data
T1113	Screen Capture
T1053	Scheduled Task/Job
T1053.005	Scheduled Task
T1571	Non-Standard Port
T1012	Query Registry
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1204	User Execution
T1070	Indicator Removal on Host
T1070.004	File Deletion
T1021.001	Remote Desktop Protocol
T1041	Exfiltration Over C2 Channel
T1548	Abuse Elevation Control Mechanism
T1548.002	Bypass User Account Control
T1071	Application Layer Protocol
T1071.001	Web Protocols
T1573	Encrypted Channel
T1124	System Time Discovery
T1033	System Owner/User Discovery
T1497	Virtualization/Sandbox Evasion
T1016	System Network Configuration Discovery
T1059.001	PowerShell
T1059.005	Visual Basic
T1106	Native API
T1204.002	Malicious File
T1027.002	Software Packing
T1562	Impair Defenses
T1566	Phishing
T1566.001	Spearphishing Attachment

What's new?

Redline (NC)

RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload

During April 2022, several campaigns through YouTube tutorials have been identified by Netskope Threat Labs, that were aimed to infect victims with #RedLine, a malware used for #data harvesting and #exfiltration as well as #remote control.
Those tutorials target a very specific audience by featuring a fake bot to buy #Binance NFT Mystery boxes.
A link to a #Github repository in the description allows the victims to download the malicious files along with a README and a setup file for #Microsoft Visual C++ Redistributable.
Executing the given file will decrypt and load a first stage of RedLine Stealer into another process. The malware then attempts to delay execution to evade sandboxes and then begins decrypting the next stage using a simple rolling XOR algorithm. It also decrypts and executes a shellcode and finally injects its payload into "RegSvcs.exe" process.
The malware also checks for #blocklisted countries and exits if finding a match with the OS region, mostly Commonwealth of Independent States (CIS) countries.
When inspecting the GitHub account repositories linked, they found five distinct RedLine loaders, two of which being digitally signed and all pretending to be some kinds of bots.

https://www.netskope.com/blog/redline-stealer-campaign-using-binance-mystery-box-videos-to-spread-github-hosted-payload