



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 [23/05](#) to [30/05](#) . 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	Agent Tesla (ID Mitre: S0331)
v	3	Formbook (NC)
^	4	njRAT (ID Mitre: S0385)
^	5	Emotet (ID Mitre: S0367)
v	6	LokiBot (ID Mitre: S0447)
☰	7	Remcos (ID Mitre: S0332)
☰	8	Nanocore (ID Mitre: S0336)
☰	9	Quasar RAT (NC)
^	10	Ave Maria (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 ©.

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
T1566.001: Spearphishing Attachment	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1112: Modify Registry	T1056: Input Capture	T1057: Process Discovery	T1021: Remote Services	T1056: Input Capture	T1041: Exfiltration Over C2 Channel	T1105: Ingress Tool Transfer
T1566: Phishing	T1059.003: Windows Command Shell	T1547.001: Registry Run Keys / Startup Folder	T1547.001: Registry Run Keys / Startup Folder	T1027: Obfuscated Files or Information	T1056.001: Keylogging	T1082: System Information Discovery	T1021.001: Remote Desktop Protocol	T1056.001: Keylogging		T1571: Non-Standard Port
	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1055: Process Injection	T1055: Process Injection	T1555.003: Credentials from Web Browsers	T1083: File and Directory Discovery		T1125: Video Capture		T1071.001: Web Protocols
	T1204: User Execution	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1070.004: File Deletion	T1555: Credentials from Password Stores	T1012: Query Registry		T1560: Archive Collected Data		T1071: Application Layer Protocol
	T1053: Scheduled Task/Job		T1053: Scheduled Task/Job	T1070: Indicator Removal on Host	T1552.001: Credentials In Files	T1497: Virtualization/Sandbox Evasion		T1113: Screen Capture		T1573: Encrypted Channel
	T1204.002: Malicious File		T1548.002: Bypass User Account Control	T1497: Virtualization/Sandbox Evasion	T1552: Unsecured Credentials	T1124: System Time Discovery				
	T1106: Native API		T1548: Abuse Elevation Control Mechanism	T1562: Impair Defenses		T1033: System Owner/User Discovery				
	T1059.001: PowerShell			T1027.002: Software Packing		T1016: System Network Configuration Discovery				
	T1059.005: Visual Basic			T1548.002: Bypass User Account Control						
				T1548: Abuse Elevation Control Mechanism						

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).

T1056	Input Capture	T1021	Remote Services	T1071.001	Web Protocols
T1547	Boot or Logon Autostart Execution	T1560	Archive Collected Data	T1071	Application Layer Protocol
T1112	Modify Registry	T1113	Screen Capture	T1573	Encrypted Channel
T1059	Command and Scripting Interpreter	T1053.005	Scheduled Task	T1497	Virtualization/Sandbox Evasion
T1056.001	Keylogging	T1053	Scheduled Task/Job	T1124	System Time Discovery
T1105	Ingress Tool Transfer	T1571	Non-Standard Port	T1033	System Owner/User Discovery
T1027	Obfuscated Files or Information	T1012	Query Registry	T1016	System Network Configuration Discovery
T1125	Video Capture	T1552.001	Credentials In Files	T1562	Impair Defenses
T1547.001	Registry Run Keys / Startup Folder	T1552	Unsecured Credentials	T1027.002	Software Packing
T1055	Process Injection	T1070.004	File Deletion	T1204.002	Malicious File
T1057	Process Discovery	T1070	Indicator Removal on Host	T1106	Native API
T1082	System Information Discovery	T1204	User Execution	T1059.001	PowerShell
T1059.003	Windows Command Shell	T1021.001	Remote Desktop Protocol	T1059.005	Visual Basic
T1083	File and Directory Discovery	T1041	Exfiltration Over C2 Channel	T1566.001	Spearphishing Attachment
T1555.003	Credentials from Web Browsers	T1548.002	Bypass User Account Control	T1566	Phishing
T1555	Credentials from Password Stores	T1548	Abuse Elevation Control Mechanism		

What's new?

Redline (NC)

NEW SYK CRYPTER DISTRIBUTED VIA DISCORD

[#Morphisec's Threat Labs team](#) released a report about a current threat regarding popular attack chain with a new SYK crypter.

Starting from a phishing infection with a common subject as such as "New order", this attack uses the content delivery network of [#Discord](#) to download the next stage and, then assembles what will be the [#.NET](#) crypter named SYK because of the name of the decryptor resource. The last step delivers the malware which could be [#AsyncRAT](#), [#njRAT](#), [#QuasarRAT](#), [#WarzoneRAT](#), [#NanoCoreRAT](#) or [#RedLine](#). In addition to the crypter mechanism, it also has an anti-debugging and a persistence function to avoid antivirus detection.

This type of attack chain is an answer to the massive use of signature based detection tools.

<https://blog.morphisec.com/syk-crypter-discord>