



# Briefing Malware

CERT Capgemini CIS



From January 1, 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 [25/01](#) to [31/01](#). 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	<a href="#">Emotet</a> (ID Mitre: <a href="#">S0367</a> )
↓	2	<a href="#">Redline</a> (NC)
↑	3	<a href="#">FormBook</a> (NC)
↓	4	<a href="#">njRAT</a> (ID Mitre: <a href="#">S0385</a> )
↓	5	<a href="#">Lokibot</a> (ID Mitre : <a href="#">S0447</a> )
↑	6	<a href="#">Snake</a> (NC)
↓	7	<a href="#">Remcos</a> (ID Mitre : <a href="#">S0332</a> )
↓	8	<a href="#">AsyncRAT</a> (NC)
▬	9	<a href="#">AgentTesla</a> (ID Mitre: <a href="#">S0331</a> )
↓	10	<a href="#">Nanocore</a> (ID Mitre: <a href="#">S0336</a> )



# 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 Assistant Execution	T1547.001 : Registry Run Keys / Startup Folder	T1547 : Boot or Logon Assistant Execution	T1547.001 : Registry Run Keys / Startup Folder	T1112 : Modify Registry	T1027 : Obfuscated Files or Information	T1024 : Ingest Capture	T1056.001 : Keylogging	T1083 : File and Directory Discovery	T1021 : Remote Services	T1024 : Ingest 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	T1055 : Process Injection	T1027 : Obfuscated Files or Information		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1057 : Process Discovery	T1560 : Archive Collected Data	T1571 : Non-Standard Port				
			T1059.005 : Visual Basic			T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1055 : Process Injection		T1552 : Unsecured Credentials	T1552.001 : Credentials In Files	T1082 : System Information Discovery	T1113 : Screen Capture	T1071 : Application Layer Protocol	T1071.001 : Web Protocols			
			T1204 : User Execution	T1204.002 : Malicious File				T1070 : Indicator Removal on Host		T1070.004 : File Deletion			T1012 : Query Registry	T1125 : Video Capture	T1132 : Data Encoding			
			T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task				T1562 : Impair Defenses		T1562.004 : Disable or Modify System Firewall			T1016 : System Network Configuration Discovery	T1123 : Audio Capture				
			T1106 : Native API							T1562.001 : Disable or Modify Tools			T1087 : Account Discovery	T1115 : Clipboard Data				
							T1497 : Virtualization/Sandbox Evasion					T1120 : Peripheral Device Discovery						
												T1033 : System Owner/User 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).

<b>T1547</b>	Boot or Logon Autostart Execution	<b>T1125</b>	Video capture	<b>T1562.001</b>	Disable or Modify Tools
<b>T1056</b>	Input Capture	<b>T1566</b>	Phishing	<b>T1497</b>	Virtualization/Sandbox Evasion
<b>T1547.001</b>	Registry run keys/Startup folder	<b>T1566.001</b>	Spearphishing Attachment	<b>T1552</b>	Unsecured Credentials
<b>T1112</b>	Modify registry	<b>T1204.002</b>	Malicious File	<b>T1552.001</b>	Credentials In Files
<b>T1056.001</b>	Keylogging	<b>T1053</b>	Scheduled Task/Job	<b>T1087</b>	Account Discovery
<b>T1059</b>	Command and scripting interpreter	<b>T1053.005</b>	Scheduled Task	<b>T1120</b>	Peripheral Device Discovery
<b>T1055</b>	Process injection	<b>T1562</b>	Impair Defenses	<b>T1033</b>	System Owner/User Discovery
<b>T1027</b>	Obfuscated files or information	<b>T1070.004</b>	File Deletion	<b>T1124</b>	System Time Discovery
<b>T1083</b>	File and Directory Discovery	<b>T1555</b>	Credentials from Password Stores	<b>T1021</b>	Remote Services
<b>T1057</b>	Process discovery	<b>T1555.003</b>	Credentials from Web Browsers	<b>T1123</b>	Audio Capture
<b>T1082</b>	System Information Discovery	<b>T1012</b>	Query registry	<b>T1115</b>	Clipboard Data
<b>T1105</b>	Ingress tool transfer	<b>T1016</b>	System Network Configuration Discovery	<b>T1071</b>	Application Layer Protocol
<b>T1204</b>	User Execution	<b>T1571</b>	Non-standard port	<b>T1071.001</b>	Web Protocols
<b>T1059.003</b>	Windows Command Shell	<b>T1059.001</b>	PowerShell	<b>T1132</b>	Data Encoding
<b>T1070</b>	indicator Removal on host	<b>T1059.005</b>	Visual Basic	<b>T1041</b>	Exfiltration Over C2 Channel
<b>T1560</b>	Archive Collected Data	<b>T1106</b>	Native API		
<b>T1113</b>	Screen capture	<b>T1562.004</b>	Disable or Modify System Firewall		

## What's new?

### [AsyncRAT](#) (NC)

#### **New threat campaign identified: ASYNCRAT introduces a new delivery technique**

[#Morphisec](#) have successfully identified a new campaign with a new elaborated technic to evade detection that the final objective was to deliver [#AsyncRAT](#), a Remote Access Trojan ([#RAT](#)).

Most of the malware attack use external server to download payload and pass to the next step of the infection chain. In this case, the attacker locally create an [#ISO](#) from a [#Base64](#) string using [#JavaScript](#) and simulate the download process. The iso file is mount as a drive which contain a [#VBS](#) or [#BAT](#) file executed via [#PowerShell](#) command. This will initiate a chain of execution that will be ended by [#AsyncRAT](#) execution.

[#AsyncRAT](#) is a RAT with control and monitoring of the victim as main objective. Its features include [#keylogging](#), [#antivirus management](#), [#password recovery](#) as well as a client-server chat window.

<https://blog.morphisec.com/asynccrat-new-delivery-technique-new-threat-campaign>