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 27/12 to 04/01.
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	Redline (NC)
2	njRAT (ID Mitre: S0385)
3	AsyncRAT (NC)
4	Nanocore (ID Mitre: S0336)
5	Quasar (ID Mitre: S0262)
6	Vidar (NC)
7	DcRAT (NC)
8	Remcos (ID Mitre : S0332)
9	Orcus (NC)
10	FormBook (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 ©.

TA0002 : Execution		TA0003 : Persistence		TA0004 : Privilege Escalation		TA0005 : Defense Evasion	TA0006 : Credential Access		TA0007 : Discovery	TA0008 : Lateral Movement		TA0009 : Collection		TA0011 : Command and Control
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	T1012 : Query Registry	T1021 : Remote Services	T1021.001 : Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer
T1053 : Scheduled Task/Job		T1053 : Scheduled Task/Job		T1055 : Process Injection		T1027 : Obfuscated Files or Information	T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1083 : File and Directory Discovery			T1125 : Video Capture		T1132 : Data Encoding
				T1053 : Scheduled Task/Job		T1070 : Indicator Removal on Host	T1552 : Unsecured Credentials		T1057 : Process Discovery			T1560 : Archive Collected Data		T1571 : Non-Standard Port
						T1055 : Process Injection			T1082 : System Information Discovery			T1113 : Screen Capture		
									T1120 : Peripheral Device Discovery			T1123 : Audio Capture		

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).

T1547	Boot or Logon Autostart Execution
T1056	Input Capture
T1012	Query registry
T1547.001	Registry run keys/Startup folder
T1112	Modify registry
T1059	Command and scripting interpreter
T1059.003	Windows Command Shell
T1027	Obfuscated files or information
T1056.001	Keylogging
T1083	File and Directory Discovery
T1057	Process discovery
T1082	System Information Discovery
T1125	Video capture
T1105	Ingress tool transfer
T1560	Archive Collected Data
T1113	Screen capture
T1053	Scheduled Task/Job
T1055	Process injection
T1070	indicator Removal on host
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1552	Unsecured Credentials
T1120	Peripheral Device Discovery
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1123	Audio Capture
T1132	Data Encoding
T1571	Non-standard port

What's new?

njRAT (ID Mitre: S0385)

Crowdstrike Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt

Since the discovery of Log4Shell vulnerabilities (#CVE-2021-44228, #CVE-2021-45105) in December 2021, all cyber security teams are dealing with multiple threats starting with the exploitation of those ones. In this context, #Crowstrike Falcon OverWatch claims to have disrupted a recent malware campaign based on an early detect of the exploitation attempt through a vulnerable #Apache Tomcat process. The attacker tried to execute suspicious Linux commands before connect to an infrastructure managed by a poorly known threat actor dubbed #Aquatic Panda. Overwatch has observed through investigation that #Aquatic Panda tried to figure out after downloading several scripts from remote, then they tried to understand and harvested information about the server such as credentials, system or domain information.

#Aquatic Panda is a Chinese Advanced Persistent Threat (#APT) with intelligence gathering and industrial espionage missions first spotted around May 2020. They heavily relied on Cobalt Strike as well as unique tools like a famous Cobalt Strike downloader, #FishMaster. They have been observed dropping #NjRAT, a remote access trojan (#RAT) which has information gathering or process/registry manipulation capabilities.

https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/