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 11/01 to 18/01.
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	Nanocore (ID Mitre: S0336)
^	4	Emotet (ID Mitre: S0367)
^	5	FormBook (NC)
v	6	AsyncRAT (NC)
^	7	Lokibot (ID Mitre : S0447)
^	8	Orcus (NC)
v	9	Vidar (NC)
^	10	Snake (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 ©.

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	T1083 : File and Directory 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		T1055 : Process Injection		T1112 : Modify Registry		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		T1070 : Indicator Removal on Host	T1070 : Indicator Removal on Host	T1552 : Unsecured Credentials		T1012 : Query Registry		T1113 : Screen Capture		T1071 : Application Layer Protocol	T1071.001 : Web Protocols	
		T1204 : User Execution	T1204.002 : Malicious File					T1562 : Impair Defenses	T1562.004 : Disable or Modify System Firewall			T1082 : System Information Discovery		T1125 : Video Capture		T1132 : Data Encoding		
		T1106 : Native API						T1055 : Process Injection				T1087 : Account Discovery						
		T1053 : Scheduled Task/Job										T1120 : Peripheral Device Discovery						
												T1033 : System Owner/User Discovery						
												T1124 : System Time 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).

T1059	Command and scripting interpreter	T1555	Credentials from Password Stores	T1041	Exfiltration Over C2 Channel
T1547	Boot or Logon Autostart Execution	T1555.003	Credentials from Web Browsers		
T1056	Input Capture	T1552	Unsecured Credentials		
T1059.003	Windows Command Shell	T1021	Remote Services		
T1547.001	Registry run keys/Startup folder	T1113	Screen capture		
T1112	Modify registry	T1571	Non-standard port		
T1057	Process discovery	T1053	Scheduled Task/Job		
T1012	Query registry	T1204	User Execution		
T1027	Obfuscated files or information	T1070	indicator Removal on host		
T1056.001	Keylogging	T1552.001	Credentials In Files		
T1083	File and Directory Discovery	T1087	Account Discovery		
T1082	System Information Discovery	T1120	Peripheral Device Discovery		
T1560	Archive Collected Data	T1021.001	Remote Desktop Protocol		
T1125	Video capture	T1123	Audio Capture		
T1105	Ingress tool transfer	T1132	Data Encoding		
T1055	Process injection	T1573	Encrypted Channel		

What's new?

Nanocore (ID Mitre: S0336) / AsyncRAT (NC)

Nanocore, Netwire and AsyncRAT spreading campaign uses public cloud infrastructure

#Cisco Talos analyzed a malicious campaign spotted at the end of October 2021 that delivered some Remote Access Trojan (#RAT), mostly across United States, Italy and Singapore.
The threat actor, which has not been named by Talos, deployed a distributed infrastructure depending on cloud resources such as #Amazon AWS EC2 or #Microsoft Azure instances to host their Command-And-Control (#C&C) servers and even deployed some web servers to host malwares like #Nanocore, #AsyncRAT or #Netwire. They created malicious DNS subdomains via #DuckDNS, a free dynamic DNS service, to resolve download servers.
A #PowerShell dropper has been identified, built with #Hcrypt crypter, in the infection chain which was already been spotted by #TrendMicro researchers in a previous campaign named Water Basilisk (source). Hcrypt is considered as a #crypter-as-a-service and give access to sophisticated malware deployment with a minimal investment to several threat actors having not enough time or resources for that.

https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html