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 20/06 to 27/06 .
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	Emotet (ID Mitre: S0367)
4	Agent Tesla (ID Mitre: S0331)
5	Formbook (NC)
6	Quasar RAT (NC)
7	Remcos (ID Mitre: S0332)
8	Nanocore (ID Mitre: S0336)
9	DarkComet (ID Mitre: S0334)
10	Sodinokibi (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 ©.

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	
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	T1562: Impair Defenses	T1562.001: Disable or Modify Tools	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						T1562.004: Disable or Modify System Firewall	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
T1106: Native API										T1012: Query Registry			T1113: Screen Capture			T1573: Encrypted Channel	
T1204: User Execution	T1204.002: Malicious File									T1033: System Owner/User Discovery			T1115: Clipboard Data				
T1053: Scheduled Task/Job	T1053.005: Scheduled Task												T1123: Audio Capture				
T1047: Windows Management Instrumentation																	

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).

T1547.001	Registry Run Keys / Startup Folder	T1555	Credentials from Password Stores	T1070.004	File Deletion
T1105	Ingress Tool Transfer	T1555.003	Credentials from Web Browsers	T1059.001	PowerShell
T1027	Obfuscated Files or Information	T1562	Impair Defenses	T1059.005	Visual Basic
T1059	Command and Scripting Interpreter	T1562.001	Disable or Modify Tools	T1106	Native API
T1059.003	Windows Command Shell	T1021.001	Remote Desktop Protocol	T1204	User Execution
T1125	Video Capture	T1115	Clipboard Data	T1204.002	Malicious File
T1057	Process Discovery	T1123	Audio Capture	T1047	Windows Management Instrumentation
T1082	System Information Discovery	T1041	Exfiltration Over C2 Channel	T1566.001	Spearphishing Attachment
T1055	Process Injection	T1053	Scheduled Task/Job		
T1021	Remote Services	T1053.005	Scheduled Task		
T1560	Archive Collected Data	T1071	Application Layer Protocol		
T1113	Screen Capture	T1573	Encrypted Channel		

What's new?

Emotet (ID Mitre: S0367)

Malicious Windows "LNK" attacks simplified with new Quantum builder

#Malware researchers have spotted a new tool that helps #cybercriminals to create malicious #.LNK files to provide #payloads for the early stages of an attack.
LNKs are widely used for malware distribution, particularly in phishing campaigns, with some notable malware families currently using them being #Emotet , #Bumblebee , #Qbot and #IcedID. Quantum offers User Account Control (#UAC) bypass, #Windows Smartscreen bypass, the ability to load multiple #payloads onto a single LNK file, post-execution masking, delayed start or execution. The authors claim that files generated with Quantum are completely #undetectable, indicating that antivirus engines and operating system protection mechanisms fail to flag them as suspicious or dangerous.
The #PowerShell script that runs when the LNK file is opened is very similar to the scripts used by #Lazarus in recent campaigns, indicating a possible connection. As long as the use of #LNK files is effective for malicious actors, the upward trend in their deployment should continue.

https://www.bleepingcomputer.com/news/security/malicious-windows-lnk-attacks-made-easy-with-new-quantum-builder/