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 31/05 to 07/06 .
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	Agent Tesla (ID Mitre: S0331)
4	Formbook (NC)
5	LokiBot (ID Mitre: S0447)
6	Emotet (ID Mitre: S0367)
7	Nanocore (ID Mitre: S0336)
8	Remcos (ID Mitre: S0332)
9	Qbot (NC)
10	Ave Maria (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 ©.

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: 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	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	
			T1059.005: Visual Basic	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1055: Process Injection	T1055.012: Process Hollowing	T1112: Modify Registry			T1056.004: Credential API Hooking	T1082: System Information Discovery				T1056.004: Credential API Hooking		T1571: Non-Standard Port	
			T1059.001: PowerShell			T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1055: Process Injection	T1055.012: Process Hollowing	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers	T1083: File and Directory Discovery			T1125: Video Capture			T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1204: User Execution	T1204.002: Malicious File			T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control	T1070: Indicator Removal on Host	T1070.004: File Deletion	T1552: Unsecured Credentials	T1552.001: Credentials In Files	T1012: Query Registry			T1560: Archive Collected Data				
		T1106: Native API						T1562: Impair Defenses	T1562.001: Disable or Modify Tools			T1033: System Owner/User Discovery			T1113: Screen Capture				
		T1053: Scheduled Task/Job	T1053.005: Scheduled Task					T1140: Deobfuscate/ Decode Files or Information				T1124: System Time Discovery							
		T1047: Windows Management Instrumentation						T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control			T1016: System Network Configuration Discovery							
												T1120: Peripheral Device 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).

T1056	Input Capture
T1547	Boot or Logon Autostart Execution
T1027	Obfuscated Files or Information
T1112	Modify Registry
T1059	Command and Scripting Interpreter
T1547.001	Registry Run Keys / Startup Folder
T1055	Process Injection
T1105	Ingress Tool Transfer
T1057	Process Discovery
T1056.001	Keylogging
T1082	System Information Discovery
T1125	Video Capture
T1083	File and Directory Discovery
T1012	Query Registry
T1070	Indicator Removal on Host
T1070.004	File Deletion
T1059.003	Windows Command Shell
T1204	User Execution
T1560	Archive Collected Data
T1113	Screen Capture
T1053	Scheduled Task/Job
T1053.005	Scheduled Task
T1571	Non-Standard Port
T1033	System Owner/User Discovery
T1497	Virtualization/Sandbox Evasion
T1124	System Time Discovery
T1016	System Network Configuration Discovery
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1027.002	Software Packing
T1562	Impair Defenses
T1059.005	Visual Basic
T1106	Native API
T1204.002	Malicious File
T1021	Remote Services
T1566	Phishing
T1566.001	Spearphishing Attachment
T1056.004	Credential API Hooking
T1041	Exfiltration Over C2 Channel
T1055.012	Process Hollowing
T1548	Abuse Elevation Control Mechanism
T1548.002	Bypass User Account Control
T1071	Application Layer Protocol
T1071.001	Web Protocols
T1120	Peripheral Device Discovery
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1562.001	Disable or Modify Tools
T1140	Deobfuscate/Decode Files or Information
T1059.001	PowerShell
T1047	Windows Management Instrumentation
T1021.001	Remote Desktop Protocol

What's new?

Formbook (NC)

XLoader Botnet: Find Me If You Can

#Checkpoint research team uncovered new versions of #XLoader with updated protection mechanism and camouflaging capabilities.
#XLoader is based off #Formbook and receive updates much more frequently than its predecessor. The last version observed go back to early 2020 which suggests it is now discontinued in favor of #XLoader.
In their article they explain the changes, especially the process of camouflaging C&C servers as web hosting domains (fake Hostinger and Namecheap being the most common), in v.2.5. They also provide ways to identify C&C domains among others.
This new version brings the most changes, but a v.2.6 was also spotted, bringing minor improvement to the way it communicates.

https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/