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 21/03 to 28/03 .
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	njRAT (ID Mitre: S0385)
2	RedLine (NC)
3	Emotet(ID Mitre: S0367)
4	Formbook (NC)
5	Vidar (NC)
6	Nanocore (ID Mitre: S0336)
7	LokiBot (ID Mitre: S0447)
8	Remcos (ID Mitre: S0332)
9	Ursnif (ID Mitre: S0386)
10	Hancitor (ID Mitre: S0499)

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	T1056: Input Capture	T1056.001: Keylogging	T1041: Exfiltration Over C2 Channel	T1105: Ingress Tool Transfer	
			T1059.001: PowerShell			T1055: Process Injection		T1112: Modify Registry		T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers	T1083: File and Directory Discovery		T1113: Screen Capture			T1071: Application Layer Protocol	T1071.001: Web Protocols
			T1059.005: Visual Basic					T1070: Indicator Removal on Host	T1070.004: File Deletion			T1082: System Information Discovery		T1125: Video Capture			T1571: Non-Standard Port	
		T1106: Native API						T1140: Deobfuscate/Decode Files or Information				T1012: Query Registry					T1132: Data Encoding	
		T1204: User Execution	T1204.002: Malicious File					T1497: Virtualization/Sandbox Evasion				T1033: System Owner/User Discovery						

Technique shared by …

9 8 7 6 5 4 3 … malwares

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	**T1083**	File and Directory Discovery	**T1566.001**	Spearphishing Attachment
T1027	Obfuscated Files or Information	**T1082**	System Information Discovery	**T1027.002**	Software Packing
T1547	Boot or Logon Autostart Execution	**T1012**	Query Registry	**T1132**	Data Encoding
T1056	Input Capture	**T1041**	Exfiltration Over C2 Channel	**T1125**	Video Capture
T1547.001	Registry Run Keys / Startup Folder	**T1070.004**	File Deletion	**T1021**	Remote Services
T1112	Modify Registry	**T1140**	Deobfuscate/Decode Files or Information	**T1033**	System Owner/User Discovery
T1105	Ingress Tool Transfer	**T1497**	Virtualization/Sandbox Evasion		
T1059.003	Windows Command Shell	**T1071**	Application Layer Protocol		
T1057	Process Discovery	**T1071.001**	Web Protocols		
T1070	Indicator Removal on Host	**T1571**	Non-Standard Port		
T1055	Process Injection	**T1059.005**	Visual Basic		
T1059.001	PowerShell	**T1204.002**	Malicious File		
T1106	Native API	**T1555**	Credentials from Password Stores		
T1204	User Execution	**T1555.003**	Credentials from Web Browsers		
T1056.001	Keylogging	**T1560**	Archive Collected Data		
T1113	Screen Capture	**T1566**	Phishing		

What's new?

Vidar (NC)

A new phishing campaign exploiting help files distributes Vidar spyware.

Based on #Trustwave blog post, a new malicious email campaign aimed at spreading the #Vidar spyware in what appears to be a compiled HTML help file from Microsoft is underway. First observed in the wild in late 2018, according #Infoblox cloud security vendor, Vidar is a variant of #Arkei infostealer. The spyware is sold in online forums.

The campaign uses a novel technique involving Microsoft Compiled #HTML help files. The help files, which use the "CHM" suffix, are packaged in an ISO with the Vidar payload in a Word document. The "CHM" file is mainly a copy of a legitimate CHM file, but it also contains #HTML application code, which silently executes the payload.

The version of the malware used for this campaign is 50.3 and synchronizes with its #C2 servers which are hosted on the Mastodon social network. Once the malware is installed on the machine and then launched, its configuration file is retrieved from #Mastodon, and then the work of the spyware begins: collects system information and password data from browsers and other applications, sends this data as a #ZIP file to C2 server, and then deletes itself on the compromised host. Other malware may be downloaded to the targeted machine.

https://www.csoonline.com/article/3654849/microsoft-help-files-repurposed-to-contain-vidar-malware-in-new-campaign.html#tk.rss_all