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 28/02 to 07/03.
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	Emotet (ID Mitre: S0367)
2	njRAT (ID Mitre: S0385)
3	Redline (NC)
4	FormBook (NC)
5	Nanocore (ID Mitre: S0336)
6	Lokibot (ID Mitre : S0447)
7	Vidar (NC)
8	Remcos (ID Mitre : S0332)
9	Quasar (ID Mitre : S0262)
10	AgentTesla (ID Mitre: S0331)

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	T1059 : Command and Scripting Interpreter	T1547 : Boot or Logon Autostart Execution	T1547 : Boot or Logon Autostart Execution	T1112 : Modify Registry	T1056 : Input Capture	T1057 : Process Discovery	T1021 : Remote Services	T1056 : Input Capture	T1105 : Ingress Tool Transfer	T1041 : Exfiltration Over C2 Channel
T1566.001 : Spearphishing Attachment	T1059.003 : Windows Command Shell	T1547.001 : Registry Run Keys / Startup Folder	T1547.001 : Registry Run Keys / Startup Folder	T1027 : Obfuscated Files or Information	T1056.001 : Keylogging	T1082 : System Information Discovery	T1021.001 : Remote Desktop Protocol	T1056.001 : Keylogging	T1071 : Application Layer Protocol	T1071.001 : Web Protocols
	T1059.001 : PowerShell	T1053 : Scheduled Task/Job	T1055 : Process Injection	T1027.002 : Software Packing	T1555 : Credentials from Password Stores	T1083 : File and Directory Discovery		T1560 : Archive Collected Data	T1571 : Non-Standard Port	
	T1059.005 : Visual Basic	T1053.005 : Scheduled Task	T1053 : Scheduled Task/Job	T1055 : Process Injection	T1555.003 : Credentials from Web Browsers	T1012 : Query Registry		T1113 : Screen Capture	T1573 : Encrypted Channel	
	T1053 : Scheduled Task/Job		T1053.005 : Scheduled Task	T1140 : Deobfuscate/ Decode Files or Information	T1552 : Unsecured Credentials	T1033 : System Owner/User Discovery		T1125 : Video Capture		
	T1053.005 : Scheduled Task			T1562 : Impair Defenses	T1552.001 : Credentials In Files	T1087 : Account Discovery				
	T1204 : User Execution			T1070 : Indicator Removal on Host		T1016 : System Network Configuration Discovery				
	T1204.002 : Malicious File			T1497 : Virtualization /Sandbox Evasion		T1124 : System Time Discovery				
	T1106 : Native API					T1497 : Virtualization/Sandbox Evasion				

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	**T1113**	Screen capture	**T1106**	Native API
T1056	Input Capture	**T1125**	Video capture	**T1059.001**	PowerShell
T1059.003	Windows Command Shell	**T1566**	Phishing	**T1059.005**	Visual Basic
T1547	Boot or Logon Autostart Execution	**T1566.001**	Spearphishing Attachment	**T1140**	Deobfuscate/Decode Files or Information
T1112	Modify registry	**T1053**	Scheduled Task/Job	**T1562**	Impair Defenses
T1027	Obfuscated files or information	**T1204**	User Execution	**T1070**	indicator Removal on host
T1056.001	Keylogging	**T1053.005**	Scheduled Task	**T1497**	Virtualization/Sandbox evasion
T1547.001	Registry run keys/Startup folder	**T1204.002**	Malicious File	**T1027.002**	Software Packing
T1555	Credentials from Password Stores	**T1552**	Unsecured Credentials	**T1552.001**	Credentials In Files
T1555.003	Credentials from Web Browsers	**T1012**	Query registry	**T1087**	Account Discovery
T1057	Process discovery	**T1033**	System Owner/User Discovery	**T1016**	System Network Configuration Discovery
T1082	System Information Discovery	**T1021**	Remote Services	**T1124**	System Time Discovery
T1105	Ingress tool transfer	**T1071**	Application Layer Protocol	**T1021.001**	Remote Desktop Protocol
T1055	Process injection	**T1571**	Non-standard port	**T1573**	Encrypted Channel
T1083	File and Directory Discovery	**T1071.001**	Web Protocols		
T1560	Archive Collected Data	**T1041**	Exfiltration Over C2 Channel		

What's new?

FormBook (NC)

Beware of malware offering "Warm greetings from Saudi Aramco"

Last week, #MalwareBytes Threat Intelligence Team discovered a malware campaign targeting #Oil and Gas Sector compagnies.

This targeted email campaign exploited an old vulnerability, #CVE-2017-11882, through an embedded #Microsoft Excel object inside a #pdf file. When opened, the file tries to download the remote template which exploits the vulnerability and then downloads the malware, #Formbook. This vulnerability allows an attacker to execute code with current context of the user. If this user has administrator rights, the malware will take control of the system. There's also an Excel file in attachment which is a copy of the embedded one functionalities.

The email impersonates a Saudi Arabian public petroleum, #Saudi Aramco, claiming a flash and big opportunity for refinery renovation was possible.

#Formbook is active since 2016 and is one of the most established #information stealer constantly evolving to stay attractive to attackers.

https://cisotimes.com/email-which-claims-to-come-from-saudi-aramco-delivers-malware/