



Briefing Malware

CERT Sogeti ESEC

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 27/09 to 04/10.

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	Vidar (NC)
∨	4	FormBook (NC)
∧	5	Remcos (ID Mitre : S0332)
∨	6	AsyncRAT (NC)
∨	7	Lokibot (ID Mitre: S0447)
∧	8	Gandcrab (NC)
∧	9	Nanocore (ID Mitre: S0336)
∨	10	Snake (NC)



Most observed malwares'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 ©.

TA0002 : Execution		TA0003 : Persistence		TA0004 : Privilege Escalation		TA0005 : Defense Evasion		TA0006 : Credential Access		TA0007 : Discovery	TA0009 : Collection		TA0011 : Command and Control		TA0010 : Exfiltration
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	T1012 : Query Registry	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer		T1041 : Exfiltration Over C2 Channel
T1106 : Native API				T1055 : Process Injection		T1027 : Obfuscated Files or Information				T1083 : File and Directory Discovery	T1560 : Archive Collected Data		T1071 : Application Layer Protocol	T1071.001 : Web Protocols	
						T1055 : Process Injection				T1057 : Process Discovery	T1113 : Screen Capture		T1571 : Non-Standard Port		
						T1562 : Impair Defenses				T1082 : System Information Discovery	T1125 : Video Capture				
						T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1120 : Peripheral Device Discovery	T1123 : Audio Capture				
												T1005 : Data from Local System			

Legend

 Technique shared by 9 malwares	 Technique shared by 6 malwares	
 Technique shared by 8 malwares	 Technique shared by 5 malwares	
 Technique shared by 7 malwares	 Technique shared by 4 malwares	 Technique shared by 3 malwares



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
T1547	Boot or Logon Autostart Execution	T1125	Video capture
T1056	Input Capture	T1041	Exfiltration over C2 channel
T1112	Modify registry	T1106	Native API
T1027	Obfuscated files or information	T1070	Indicator Removal on host
T1012	Query registry	T1070.004	File Deletion
T1547.001	Registry run keys/Startup folder	T1120	Peripheral Device Discovery
T1055	Process injection	T1123	Audio Capture
T1056.001	Keylogging	T1005	Data from Local System
T1083	File and Directory Discovery	T1071	Application Layer Protocol
T1057	Process discovery	T1071.001	Web Protocols
T1082	System Information Discovery	T1571	Non-standard port
T1105	Ingress tool transfer		
T1059.003	Windows Command Shell		
T1562	Impair defense		
T1560	Archive Collected Data		

What's new?

FormBook (NC)

FormBook Adds Latest Office 365 0-Day Vulnerability (CVE-2021-40444) to Its Arsenal

#Trend Micro researchers unveil a new #Formbook campaign in which its developer weaponized such #infostealer with the recent #Office 365 MSHTML vulnerability (#CVE-2021-40444) instead of #CVE-2017-019. Both vulnerabilities allow a Remote Code Execution (#RCE) via crafted Office documents.

Formbook is an information stealer that is active since 2016 but is constantly evolving such as the recent addition of #MacOS support (via the fork #Xloader) or the addition of #Cobalt strike beacons. Formbook is well-known for its use of vulnerabilities involving Office Documents.

In this new campaign, the malware (#Formbook version 4.1) is delivered through a two-layer of #PowerShell scripts; the first one downloading the second one being hosted on #Discord. As previously reported, the malware is injected into a Calculator while the obfuscation was applied this time over a #.Net injector. As often the entry vector was a phishy email where a victim has downloaded and opened a maldoc attached followed by a successful exploitation of the vulnerability.

https://www.trendmicro.com/en_us/research/21/i/formbook-adds-latest-office-365-0-day-vulnerability-cve-2021-404.html

