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 20/07 to 27/07.
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	FormBook (NC)
^	4	Raccoon (NC)
^	5	Nanocore (ID Mitre: S0336)
v	6	Lokibot (ID Mitre: S0447)
^	7	Vidar (NC)
v	8	AsyncRAT (NC)
v	9	Remcos (ID Mitre : S0332)
=	10	Agent Tesla (ID Mitre : S0331)

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	T1082 : System Information Discovery	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer		T1041 : Exfiltration Over C2 Channel
				T1055 : Process Injection		T1027 : Obfuscated Files or Information		T1552 : Unsecured Credentials	T1552.001 : Credentials In Files	T1057 : Process Discovery	T1560 : Archive Collected Data		T1071 : Application Layer Protocol	T1071.001 : Web Protocols	
						T1055 : Process Injection		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1012 : Query Registry	T1113 : Screen Capture		T1571 : Non-Standard Port		
						T1562 : Impair Defenses				T1083 : File and Directory Discovery	T1125 : Video Capture				
						T1564 : Hide Artefacts				T1120 : Peripheral Device Discovery	T1123 : Audio Capture				
						T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1016 : System Network Configuration Discovery	T1005 : Data from Local System				
										T1033 : System Owner / User Discovery					
										T1124 : System Time Discovery					

Legend

- Technique shared by 9 malwares
- Technique shared by 8 malwares
- Technique shared by 7 malwares
- Technique shared by 6 malwares
- Technique shared by 5 malwares
- Technique shared by 4 malwares
- Technique shared by 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).

T1547	Boot or Logon Autostart Execution
T1056	Input Capture
T1059	Command and scripting interpreter
T1082	System Information Discovery
T1547.001	Registry run keys/Startup folder
T1112	Modify registry
T1027	Obfuscated files or information
T1056.001	Keylogging
T1057	Process discovery
T1012	Query registry
T1055	Process injection
T1552	Unsecured Credentials
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1105	Ingress tool transfer
T1059.003	Windows Command Shell
T1562	Impair defense
T1555	Credential from Password Stores
T1552.001	Credentials In Files
T1555.003	Credential from Web browsers
T1083	File and Directory Discovery
T1071	Application Layer Protocol
T1564	Hide Artefacts
T1070	indicator Removal on host
T1070.004	File Deletion
T1120	Peripheral Device Discovery
T1016	System Network Configuration Discovery
T1033	System Owner/User Discovery
T1124	System Time Discovery
T1123	Audio Capture
T1005	Data from Local System
T1571	Non-standard port
T1071.001	Web Protocols
T1041	Exfiltration over C2 channel

What's new?

FormBook (NC)

New variant of Formbook spotted

#Quick Heal Security Labs studied a new variant of #Formbook information #stealer. Even if the malware born 5 years ago and can also target #MAcOS systems via its forked version #Xloader, Formbook developers remain active as a new variant using steganography was recently spotted by researchers. Formbook is known to be used to steal credentials from web browser, capture screenshots, record keystrokes, download and execute files from victim side. According to the author, the initial vector seems to be, as usual, via malicious XML/DOC files or email attachments.

https://blogs.quickheal.com/formbook-malware-returns-new-variant-uses-steganography-and-in-memory-loading-of-multiple-stages-to-steal-data/

Lokibot (ID Mitre : S0447)

Lokibot delivered by email in Italy

The independent malware hunter @JAMESWT alerts on another email campaign that reached Italy according to @Fbussoletti by delivering a binary EXE file containing #LokiBot malware. The email is constructed as an answer of a Purchase order containing pictures of works of art. As a reminder, Lokibot is an Android banker #Trojan with core capabilities of stealing sensitive data, as such as credentials and cryptocurrency wallets.

https://www.difesaesicurezza.com/areariservatacat/cybercrime-lokibot-ora-e-veicolato-anche-attraverso-opere-darte/