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 29/11 to 06/12.
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	Emotet (ID Mitre: S0367)
v	3	FormBook (NC)
v	4	njRAT (ID Mitre: S0385)
^	5	Nanocore (ID Mitre: S0336)
v	6	Lokibot (ID Mitre: S0447)
=	7	AsyncRAT (NC)
=	8	Vidar (NC)
=	9	Snake (NC)
^	10	Quasar (ID Mitre : S0262)

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 ©.

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	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	T1057 : Process Discovery	T1021 : Remote Services	T1021.001 : Remote Desktop Protocol	T1056 : Input Capture	T1056.001 : Keylogging	T1105 : Ingress Tool Transfer		T1041 : Exfiltration Over C2 Channel
		T1059.001 : Powershell	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task	T1027 : Obfuscated Files or Information		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1012 : Query Registry			T1560 : Archive Collected Data		T1571 : Non-Standard Port		
		T1059.005 : Visual Basic					T1562 : Impair Defenses		T1552 : Unsecured Credentials		T1082 : System Information Discovery			T1113 : Screen Capture		T1071 : Application Layer Protocol	T1071.001 : Web Protocols	
	T1106 : Native API						T1070 : Indicator Removal on Host	T1070.004 : File Delection			T1083 : File and Directory Discovery			T1125 : Video Capture		T1132 : Data Encoding	T1132 : Standard Encoding	
	T1053 : Scheduled Task/Job	T1053.005 : Scheduled Task									T1120 : Peripheral Device Discovery							
	T1204 : User Execution										T1033 : System Owner/User 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).

T1059	Command and scripting interpreter
T1547	Boot or Logon Autostart Execution
T1056	Input Capture
T1057	Process discovery
T1112	Modify registry
T1012	Query registry
T1082	System Information Discovery
T1059.003	Windows Command Shell
T1547.001	Registry run keys/Startup folder
T1056.001	Keylogging
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1552	Unsecured Credentials
T1083	File and Directory Discovery
T1021	Remote Services
T1059	Command and scripting interpreter
T1560	Archive Collected Data
T1105	Ingress tool transfer
T1571	Non-standard port
T1059.001	Powershell
T1106	Native API
T1027	Obfuscated files or information
T1120	Peripheral Device Discovery
T1113	Screen capture
T1125	Video capture
T1041	Exfiltration Over C2 Channel
T1566	Phishing
T1059.005	Visual Basic
T1053	Scheduled Task/Job
T1053.005	Scheduled Task
T1562	Impair defenses
T1560	Archive Collected Data
T1070	indicator Removal on host
T1070.004	File Deletion
T1033	System Owner/User Discovery
T1021.001	Remote Desktop Protocol
T1071	Application Layer Protocol
T1071.001	Web Procotols
T1132	Data Encoding
T1132.001	Standard Encoding

What's new?

Redline (NC)

Magnat malvertising campaigns spreads malicious Chrome extensions, backdoors and info stealers

Researchers at #Cisco Talos discovered a new wave of malware campaigns that can be attributed to a threat actor tracked as #Magnat.
The main objective of those campaigns is to lure victims through #online advertising to download an installer, which will infect its computer with a password stealer (#Redline), an #AutoIt-based backdoor and a malicious #browser extension dubbed #MagnatExtension that can take #screenshot or perform #key stroke logging. The #C2 used to communicate with victims is hardcoded but can be used to upload additional ones. There is also a #Twitter hashtag translation mechanism to get additional C2 address.
The threat actor, #Magnat, is active since the end of 2018 but do not have constant activity. It was first spotted in late 2019 and at the beginning of 2020 before resurfacing in April 2021. The group primarily targets North America, Australia Italy, Spain and Norway.

https://securityaffairs.co/wordpress/125297/cyber-crime/magnat-malvertising-campaigns.html