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 06/08 to 13/09.
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)
v	3	Raccoon (NC)
^	4	Vidar (NC)
v	5	FormBook (NC)
v	6	**Nanocore** (ID Mitre: S0336)
v	7	AsyncRAT (NC)
=	8	**Remcos** (ID Mitre : S0332)
=	9	**Lokibot** (ID Mitre: S0447)
=	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
				T1055 : Process Injection		T1027 : Obfuscated Files or Information		T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers	T1082 : System Information Discovery	T1560 : Archive Collected Data		T1571 : Non-Standard Port	
						T1055 : Process Injection		T1552 : Unsecured Credentials	T1552.001 : Credentials In Files	T1057 : Process Discovery	T1113 : Screen Capture			
						T1562 : Impair Defenses				T1083 : File and Directory 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 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
T1012	Query registry
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
T1059.003	Windows Command Shell
T1055	Process injection
T1083	File and Directory Discovery
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1105	Ingress tool transfer
T1562	Impair defense
T1070	indicator Removal on host
T1070.004	File Deletion
T1555	Credential from Password Stores
T1555.003	Credential from Web browsers
T1552	Unsecured Credentials
T1552.001	Credentials In Files
T1120	Peripheral Device Discovery
T1123	Audio Capture
T1005	Data from Local System
T1571	Non-standard port
T1041	Exfiltration over C2 channel

What's new?

Remcos (ID Mitre : S0332)

New Remcos campaign in Italy

Remcos has entered the index for the first time in 2021 though is operational since 2016. **Remcos** was developed by an **Italian malware developer Viotto** and advertised as remote control and surveillance software and available for purchase on underground hacking forums.

This malware is now actively **maintained up to date** by the **firm "breaking security"** (registered in **Germany**) with a **Free and Pro version** made available as well as a **manual**. Remcos is "an extensive and powerful **Remote-Control tool**, which can be used to fully administrate one or many computers, remotely". The latter can be purchased in **cryptocurrencies** supposedly for legal purposes such as pen-testing or audits , unfortunately it is or has been also **leveraged by malicious actors** such as **APT33**, **SilverTerrier** and the **Gordon group**.

Recently, malware Hunter **@JAMESWT** studied a global malware campaign spread via phishing email. The attack consisted in a series of three emails sent by a credible sender **"COSCO ASIA MANAGEMENT LTD"** with the same subject "Request for quotation". Even if the request id was different, content of those emails remain the same and with a compressed **#archive file** (.TAR) attachment. The latter will drop **Remcos**, which will collect **use activity** as well as **credentials** and **audio or video content**.

https://www.difesaesicurezza.com/areariservatacat/cybercrime-triplo-attacco-remcos-anche-in-italia-via-rfq/
https://breakingsecurity.net/remcos/