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 18/10 to 25/10.
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	**Lokibot** (ID Mitre: S0447)
^	5	AsyncRAT (NC)
v	6	FormBook (NC)
v	7	**Nanocore** (ID Mitre: S0336)
^	8	Raccoon (NC)
=	9	**Remcos** (ID Mitre : S0332)
^	10	**DcRAT** (NC)

TLP:WHITE

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
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
T1106 : Native API		T1053 : Scheduled Task/Job		T1055 : Process Injection		T1070 : Indicator Removal on Host	T1070.004 : File Deletion			T1083 : File and Directory Discovery	T1560 : Archive Collected Data		T1571 : Non-Standard Port
T1053 : Scheduled Task/Job				T1053 : Scheduled Task/Job		T1027 : Obfuscated Files or Information				T1057 : Process Discovery	T1113 : Screen Capture		
						T1562 : Impair Defenses				T1082 : System Information Discovery	T1125 : Video Capture		
						T1055 : Process Injection				T1120 : Peripheral Device Discovery	T1123 : Audio Capture		

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
T1112	Modify registry
T1547.001	Registry run keys/Startup folder
T1056.001	Keylogging
T1105	Ingress tool transfer
T1059.003	Windows Command Shell
T1070	Indicator Removal on Host
T1070.004	File Deletion
T1027	Obfuscated files or information
T1082	System Information Discovery
T1560	Archive Collected Data
T1113	Screen capture
T1125	Video capture
T1106	Native API
T1053	Scheduled Task/Job
T1055	Process injection
T1562	Impair defense
T1120	Peripheral Device Discovery
T1123	Audio capture
T1571	Non Standard Port

What's new?

Redline (NC)

Google unmasks two-year-old phishing & malware campaign targeting YouTube users

#Google Threat analysis Group (TAG) released a report about a malware campaign targeting **#Youtube** creators for 2 years.
Contacted by email to advertise a new product by a fake company, victims were redirected to a malware landing page to download the software. **#Cookies** and **#credentials** were stolen by its execution and uploaded to **#Command & Control** servers, performing all those actions in non-persistent mode (**#smash-and-grab technique**) in order to let lesser trace if not detected.
With those stolen goods, **#Youtube** channels was sold (from $3 to $4000 USD) and rebranded for **#cryptocurrency** scam live-streaming promising to victim giveaways on cryptocurrency after an initial contribution.
More than 15000 actors and 1000 domains have been identified for this campaign. Some legitimate software were impersonated such as **#Cisco VPN** or **#Luminar**, going as far as copying a social media page from an existing company.
Various information stealer were observed during this campaign such as **#RedLine**, **#Vidar**, **#Raccoon** or open-source malware like **#Sorano** and **#AdamantiumThief**.

https://blog.google/threat-analysis-group/phishing-campaign-targets-youtube-creators-cookie-theft-malware/