

Module 2

Typical goals of malware and their
implementations

https://github.com/hasherezade/malware_training_voll

Introduction

Malware: missions and tactics



Malware: missions and tactics

- First questions that we need to answer analyzing malware: WHAT?
 - What is the main purpose (mission) of the malware?
 - What is the malware family?
- Other questions that follow: HOW?
 - How are the goals implemented?
 - Are the used techniques novel/similar to known implementations?
- Possible actor: WHO?
 - Cybercrime? Nation-State? Level of sophistication?



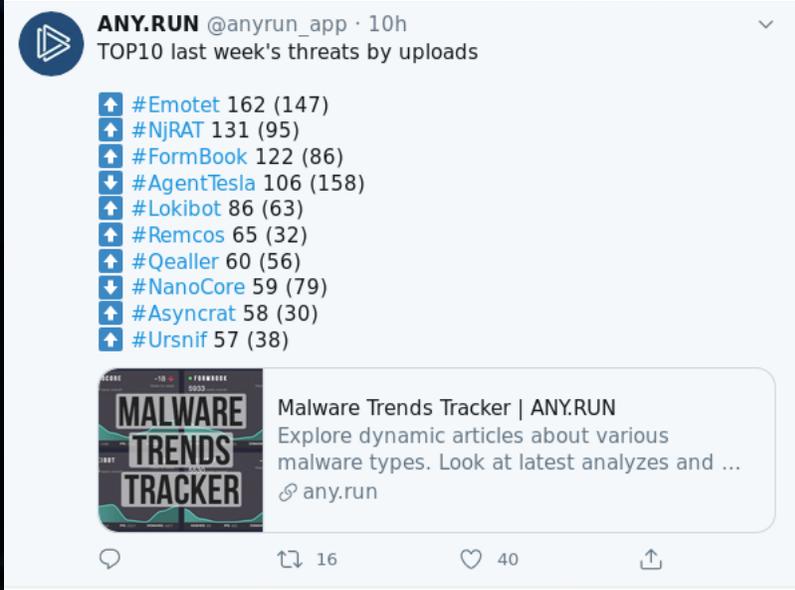
Malware: missions

- Most common malware missions:
 - Extortion (ransomware)
 - Financial fraud and stealing of credentials (i.e. Banking trojans, card number stealers)
 - Long-run espionage operations (RATs, spyware)
 - Short run-espionage operations (stealing documents)
 - Botnets for other attacks (i.e. DDoS bots, spamming bots, click-fraud, loading of secondary malware)
 - Illegitimate usage of resources (i.e. proxy botnets, cryptocurrency miners)
- Sometimes multiple goals can be implemented in one executable

Malware: families

- Trending malware families

- <https://any.run/malware-trends/>
- <https://blog.malwarebytes.com/reports/2020/02/malwarebytes-labs-releases-2020-state-of-malware-report/>



ANY.RUN @anyrun_app · 10h
TOP10 last week's threats by uploads

↑	#Emotet	162	(147)
↑	#NjRAT	131	(95)
↑	#FormBook	122	(86)
↓	#AgentTesla	106	(158)
↑	#Lokibot	86	(63)
↑	#Remcos	65	(32)
↑	#Qealler	60	(56)
↓	#NanoCore	59	(79)
↑	#Asyncrat	58	(30)
↑	#Ursnif	57	(38)

 Malware Trends Tracker | ANY.RUN
Explore dynamic articles about various malware types. Look at latest analyzes and ...
any.run

16 40

Malware: tactics

- MITRE database (<https://attack.mitre.org/tactics>) –set of common tactics used by malware
- Depending on malware family, the authors may be interested in achieving different goals, i.e.
 - Persistence
 - Defense Evasion
 - Stealing Credentials
 - Exfiltration
 - Lateral Movements
 - Manipulation/Destruction



Malware: tactics

Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

© 2015-2020, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

From: <https://attack.mitre.org/tactics>