CounterCraft

Extending MITRE ATT&CK for better adversary profiling

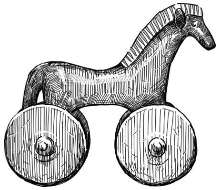
EU MITRE ATT&CK Community Workshop

Mikel Gastesi

Cyber Deception Platform

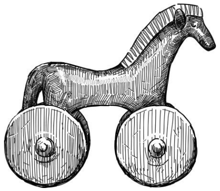
$ whoami

- ✓ Mikel Gastesi
- ✓ Threat Researcher at CounterCraft
- ✓ Contact: mgastesi@countercraftsec.com



Agenda

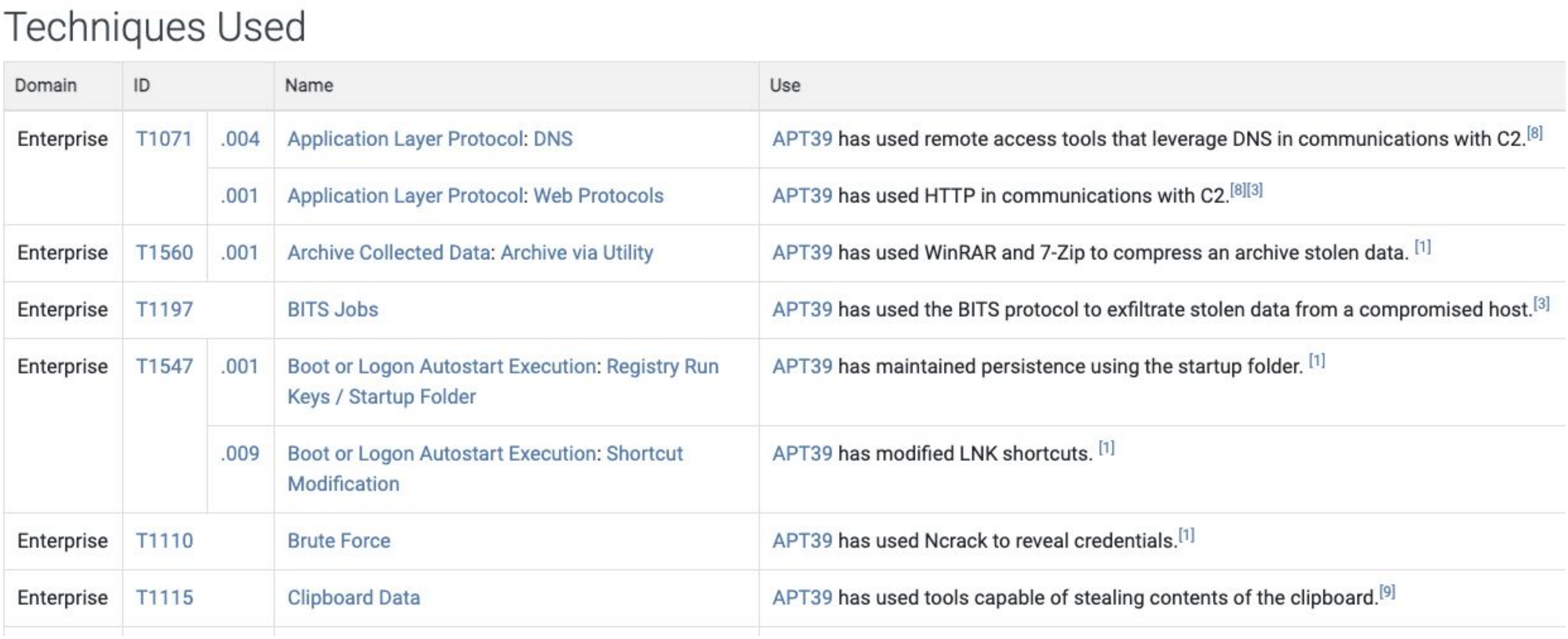
- ✓ TTP related public information format
- ✓ Problems / Limitations
- ✓ How we obtain TTP information
- ✓ Our approach to solve the issues



TTP-related public information format

Threat Actor Groups - TTP Info

- A list of techniques per actor



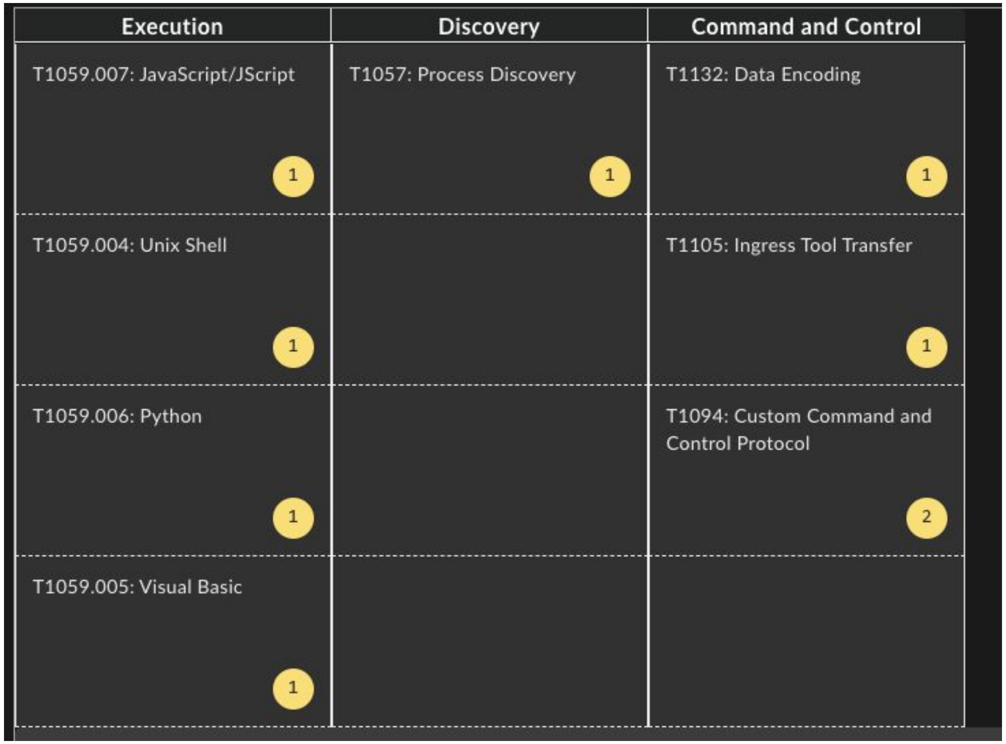
Techniques Used

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	APT39 has used remote access tools that leverage DNS in communications with C2.[8]
		.001	Application Layer Protocol: Web Protocols	APT39 has used HTTP in communications with C2.[8][3]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT39 has used WinRAR and 7-Zip to compress an archive stolen data. [1]
Enterprise	T1197		BITS Jobs	APT39 has used the BITS protocol to exfiltrate stolen data from a compromised host.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT39 has maintained persistence using the startup folder. [1]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT39 has modified LNK shortcuts. [1]
Enterprise	T1110		Brute Force	APT39 has used Ncrack to reveal credentials.[1]
Enterprise	T1115		Clipboard Data	APT39 has used tools capable of stealing contents of the clipboard.[9]

Source: https://attack.mitre.org/groups/G0087/

Threat Actor Groups - TTP Info

- A list of techniques linked to indicators

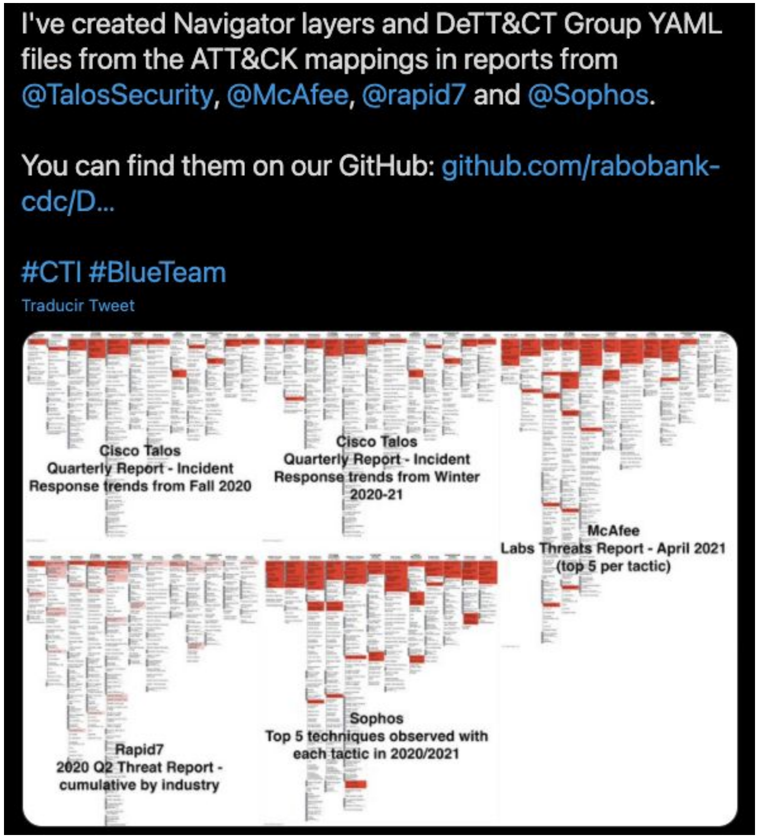


Execution	Discovery	Command and Control
T1059.007: JavaScript/JScript 1	T1057: Process Discovery 1	T1132: Data Encoding 1
T1059.004: Unix Shell 1		T1105: Ingress Tool Transfer 1
T1059.006: Python 1		T1094: Custom Command and Control Protocol 2
T1059.005: Visual Basic 1		

Source: https://unit42.paloaltonetworks.com/atoms/chafer/

Threat Actor Groups - TTP Info

- A list of techniques / layers per report /incident



I've created Navigator layers and DeTT&CT Group YAML files from the ATT&CK mappings in reports from @TalosSecurity, @McAfee, @rapid7 and @Sophos.

You can find them on our GitHub: github.com/rabobank-cdc/D...

#CTI #BlueTeam

Traducir Tweet

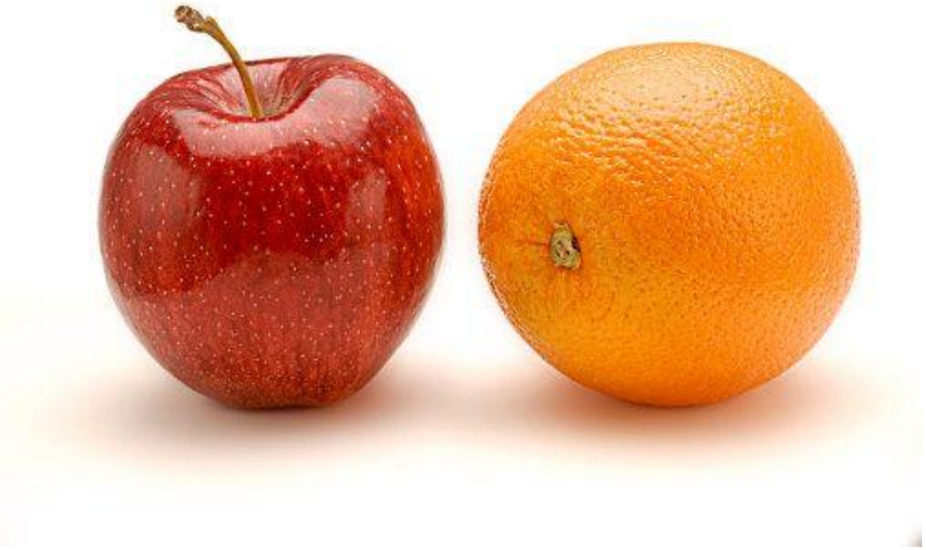
Cisco Talos
Quarterly Report - Incident Response trends from Fall 2020
Cisco Talos
Quarterly Report - Incident Response trends from Winter 2020-21
McAfee
Labs Threats Report - April 2021 (top 5 per tactic)
Rapid7
2020 Q2 Threat Report - cumulative by industry
Sophos
Top 5 techniques observed with each tactic in 2020/2021

Source: https://twitter.com/Bakk3rM/status/1398293628074790913

Problems

Problems?

- Without context, the information it is not easy to compare



✓ Data sources

✓ Bias?

✓ Incomplete?

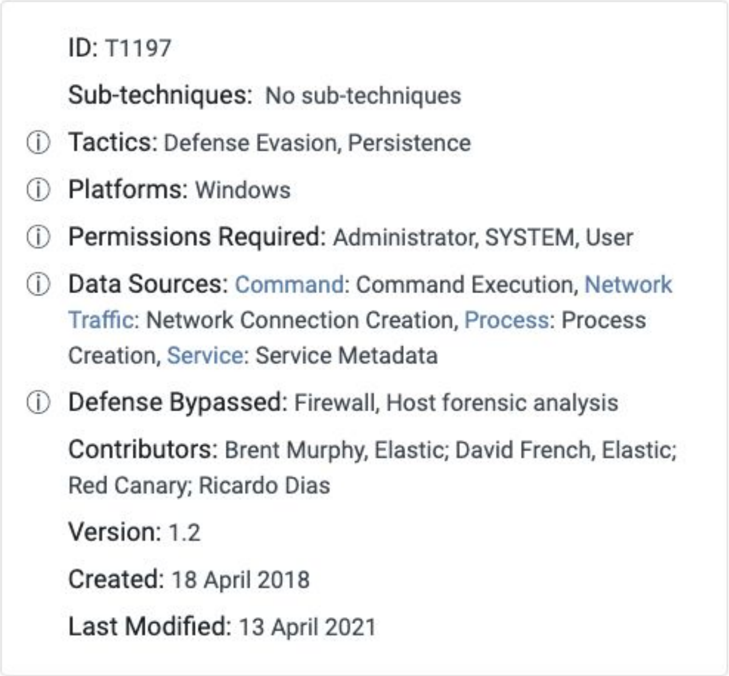
✓ Mistake / NDA / partial vision

Ask for your money back!

Problems?

- Out of scope for today; techniques are not OS agnostic

BITS Jobs



ID: T1197

Sub-techniques: No sub-techniques

Tactics: Defense Evasion, Persistence

Platforms: Windows

Permissions Required: Administrator, SYSTEM, User

Data Sources: Command: Command Execution, Network Traffic: Network Connection Creation, Process: Process Creation, Service: Service Metadata

Defense Bypassed: Firewall, Host forensic analysis

Contributors: Brent Murphy, Elastic; David French, Elastic; Red Canary; Ricardo Dias

Version: 1.2

Created: 18 April 2018

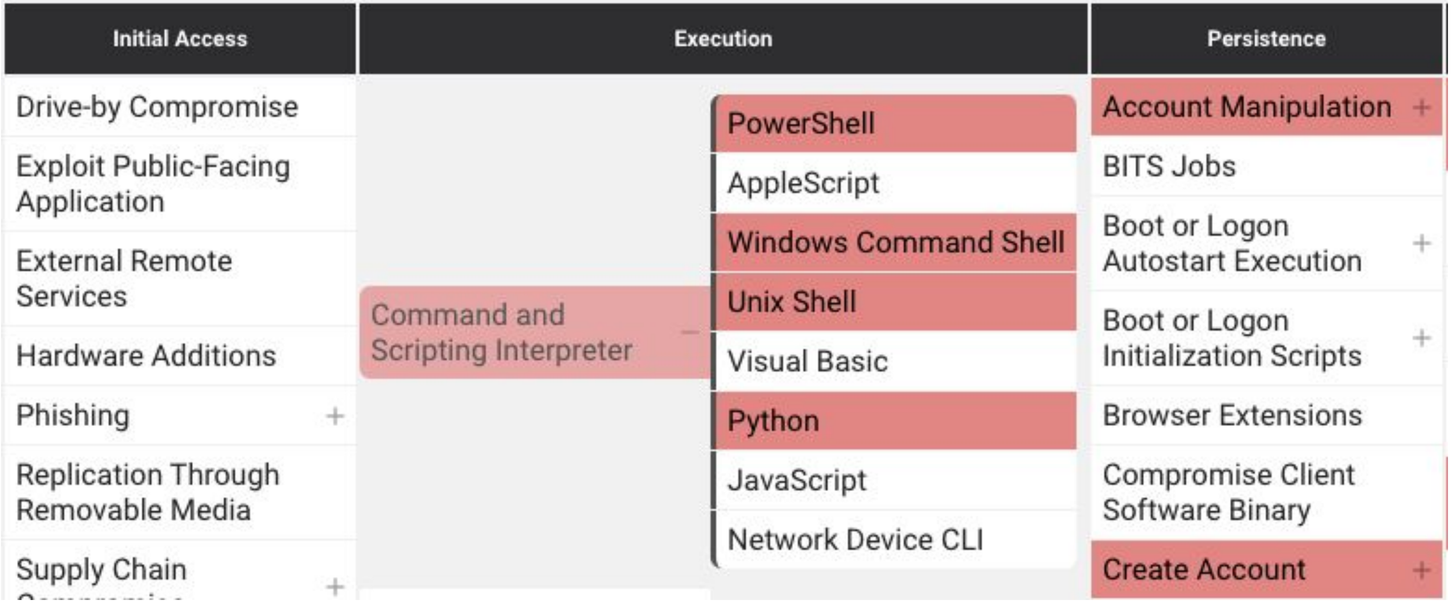
Last Modified: 13 April 2021

Source: https://attack.mitre.org/techniques/T1197/

How we obtain TTP information

How we obtain TTP information

- Fully monitorized environment
- ‘Auto-magic’ TTP detection in real time



Initial Access	Execution		Persistence
Drive-by Compromise		PowerShell	Account Manipulation +
Exploit Public-Facing Application		AppleScript	BITS Jobs
External Remote Services		Windows Command Shell	Boot or Logon Autostart Execution +
Hardware Additions	Command and Scripting Interpreter –	Unix Shell	Boot or Logon Initialization Scripts +
Phishing +		Visual Basic	Browser Extensions
Replication Through Removable Media		Python	Compromise Client Software Binary
Supply Chain Compromise +		JavaScript	Create Account +
		Network Device CLI	

TTP detection example

Our approach

Our approach

- ✓ We have context, so we added context.

- ✓ Grouping:
    - By campaign / attack

- ✓ Adding context value (I):
    - Timestamp / order
    - Host
    - User session/privileges
    - User connection type

- ✓ New TTPs (I)

Our approach

- ✓ Timestamp / order
  - How many times
  - Helpful for software
  - Not always meaningful, but is adds information

- ✓ Host
  - Linux? Windows?

- ✓ User session/privileges
  - Unprivileged user/root

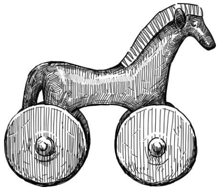
- ✓ User connection type
  - Local? Network? External?

Our approach

- ✓ New TTPs
  - Suspicious processes
  - Suspicious file creation
  - Suspicious network connections
  - Suspicious script execution

- ✓ Suspicious behaviour != malicious != technique
  - Map when possible

Conclusions

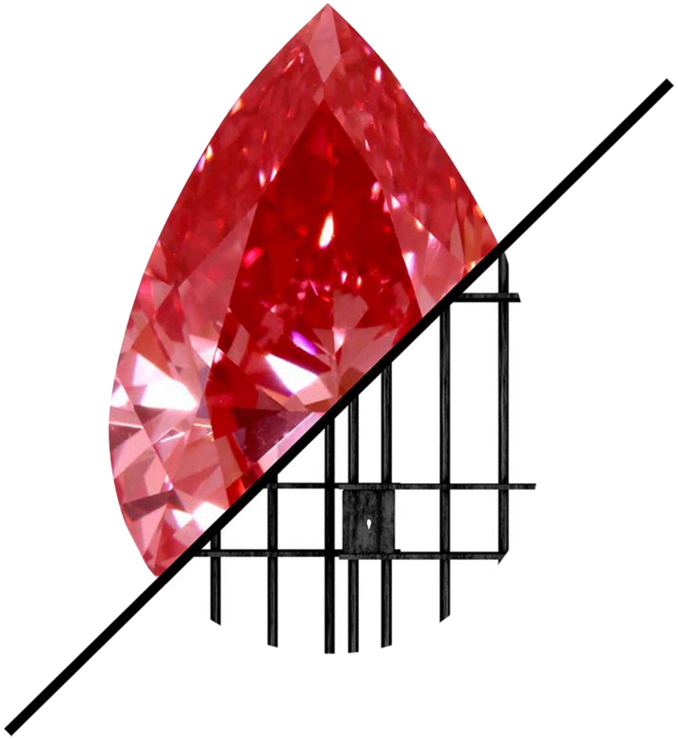


- ✓ There is a lack of context that could help to make information more complete
  - Do you think it is contradictory to add more specific information to an abstract model?
- ✓ Techniques vs Suspicious activity
  - Investigate suspicious, confirm malicious

Thank you!!

Mikel Gastesi
mgastesi@countercraftsec.com

Counter
Craft



craft@countercraftsec.com

www.countercraftsec.com