Global Information Security Society for Professionals of Pakistan

Topic : Introduction to MITRE ATT@CK Frame work –A holistic overview




Global Information Security Society for Professionals of Pakistan

Introduction to Mitre Att@ck Frame Work

| A Holistic overview|

Presenter: Sajjad Haider

MSc Information Security /MSCE NT4 ,2000, SIX Sigma yellow belt

Threat Monitoring Lead CISCO

How to use Zoom Client for New Comers

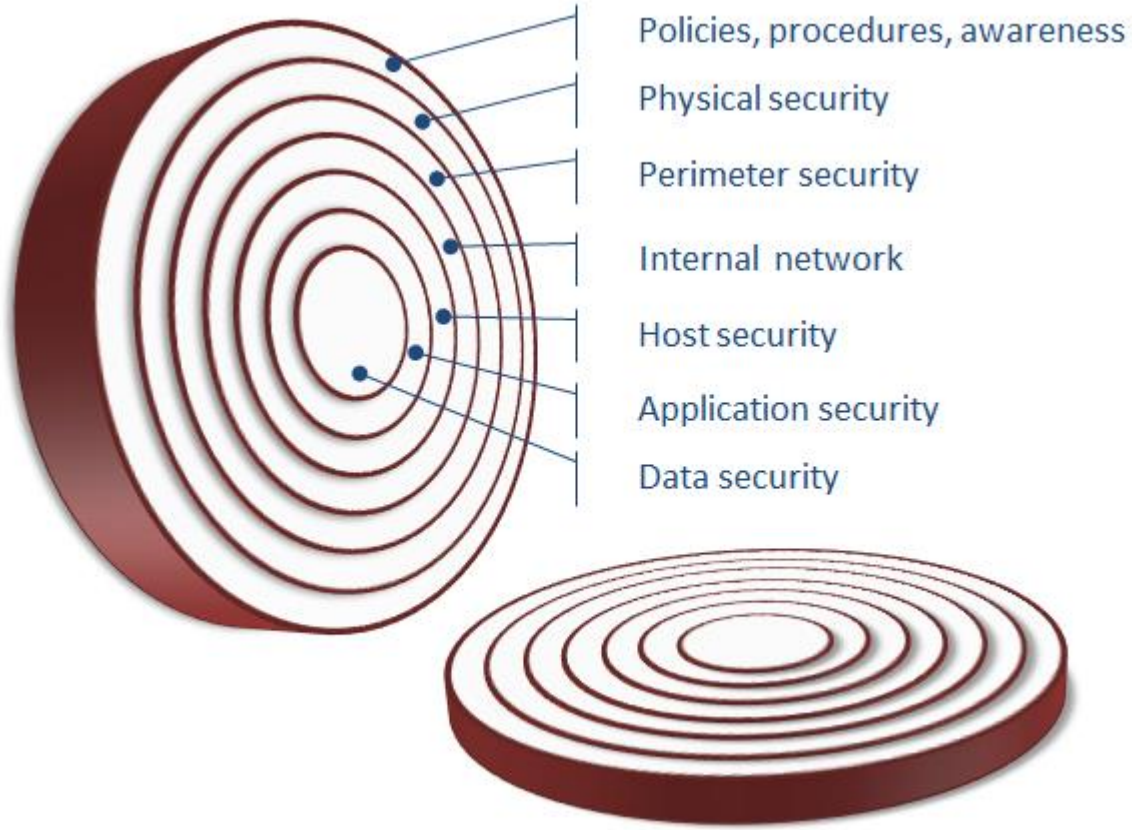
If you are using Zoom for the first time than these points will be useful for you .

- If you are unable to hear audio than you need to connect via device audio . Look at the bottom left corner .
- Kindly turn off your camera while connecting to Zoom as we respect your privacy .
- The Speaker will keep you muted during the session however if you want to ask any question during QA session ,you can click on the three dots and “raise hand” so that the speaker can unmute you .
- You can click on the participants tab to chat with host or to send a member to all participants
- If you are attending the session while doing some other work ,kindly mute yourself in case if the host unmutes all users during QA session
- Your session might be disconnected after 40 minute however you can use the same link to join the meeting again . Most of our sessions are longer than 40 minutes so always keep in mind to check if the meeting is still ON .

What we are protecting

- PCI –DSS
- OWASP
- Compliance
- Because InfoSec says so

The Death of Defense in Depth (Layered Security Model)



What we are protecting

- PCI –DSS
- OWASP
- Compliance
- Because InfoSec says so
- average time an attacker is active inside your network is 191 days as most (IBM)

- Sun Tzu said in Art of war if you know your enemy and know yourself you need now fear the result of a hundred battles if you know yourself but not the enemy for every victory gained you will also suffer a defeat in the cybersecurity

What we are protecting

- To find an attacker, you must think like an attacker
  - What steps do they take?
- Know how they operate
- Know their techniques
- Know their tools
- Know what they are looking for
- Essentially, know what they look like
  - If you know they have a capability for initial compromise with an infected USB drive…
    - Emails might not be the best place to start looking for evidence of compromise

What are we dealing with (Threats)

- In order to prepare for an incident, we must know what is out there
- Wide range of malicious
  - Botnets
  - Phishers
  - Ransomware
  - Insider Threats (elevation of privilege, data theft, unauthorized access, etc)
  - Hackers
  - "APT's"
  - Malware outbreak
  - Etc…
- Consider as many vectors as possible when preparing

Vulnerabilities

- Software bugs
- Broken processes
- Ineffective controls
- Hardware flaws
- Legacy systems
- Human error

Risks

- Business disruptions
- Financial losses
- Privacy loss
- Reputation loss
- Impaired growth
- Loss of life
- Others?

Information Gathering

- Adversary is gathering information about your network
- Passive Recon
  - Never touching the customer
  - Customer should have no idea you're gathering info on them
- Active Recon
  - Touching the customer/equipment
  - Customer could (should) know you're gathering info on them.

- Enumeration
  - Scans!

Attacker focus

- Adversary is mapping vulnerabilities to exploits

- This is really done on their side
- Nothing that you're going to see in your systems

- …Except maybe determining vulnerable systems

Exploitation

- Exploits traversing the network or hitting the border
- Sometimes easy to see them
  - IDS's may catch them
  - Signatures
  - Anomalies
- Newer exploits or custom exploits may not get caught
  - No signatures for them
- Some exploits just take advantage of poor configuration
  - Probably looks like mostly normal or legit traffic

Post-Exploitation

- Three P's
  - Privilege Escalation
  - Pivoting
  - Persistence
- Command and Control (C2)
- Things can become difficult here
  - Covert Channels
  - Encryption
- Who's connecting to who?
  - Is it anomalous?
  - There's so much of this data on modern networks…

Cyber Kill chain in a nutshell

1 Reconnaissance

Gathering email addresses, conference information, etc.

2 Weaponization

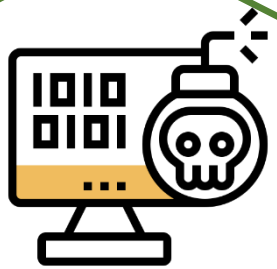
Delivering weaponized bundle to the victim via email, web, USB, etc

3 Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 Exploitation

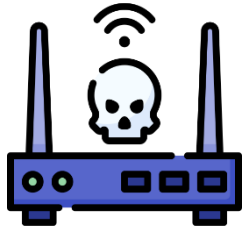
Exploiting a vulnerability to execute code on victim's system
.



5 Installation

Installing malware on the Target.

6 Command and Control



Command channel for remote manipulation Of victim
.

7 Action on objectives

With 'Hands on Keyboard' access, intruders accomplish their original goals
Coupling exploit with backdoor into deliverable payload
.

Cyber Kill Chain limitations

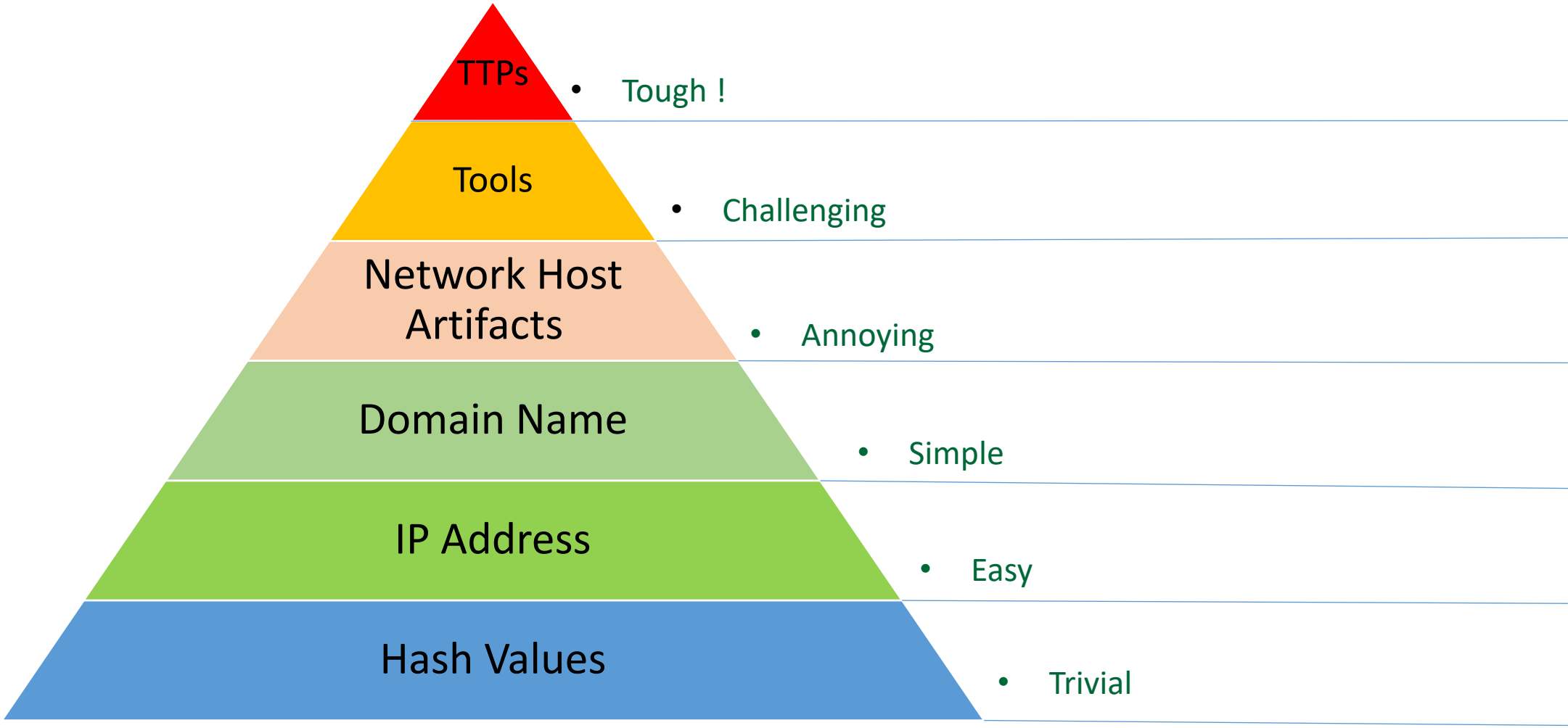
- The Cyber Kill Chain assumes a traditional perimeter-focused defense where a firewall is the main line of defense and so fails to cover other attack vectors and internal attack paths; modern organizations need to leverage defensive solutions within the perimeter.

- The Cyber Kill Chain does not focus enough on what to do after an attacker has broken into your network successfully, which they inevitably can with enough persistence.

- The Cyber Kill Chain's phase sequence cannot accurately depict all attacks as several kill chain phases can be bypassed entirely.

- Once inside a victim's network, the timing of each attack phase is inconsistent. Phases can take anywhere from minutes to months to years. Attackers could lay dormant for prolonged periods of time waiting for the optimal window to launch the final phase of their attack to apply the most impact on their target.

David Bianco's Pyramid of Pain



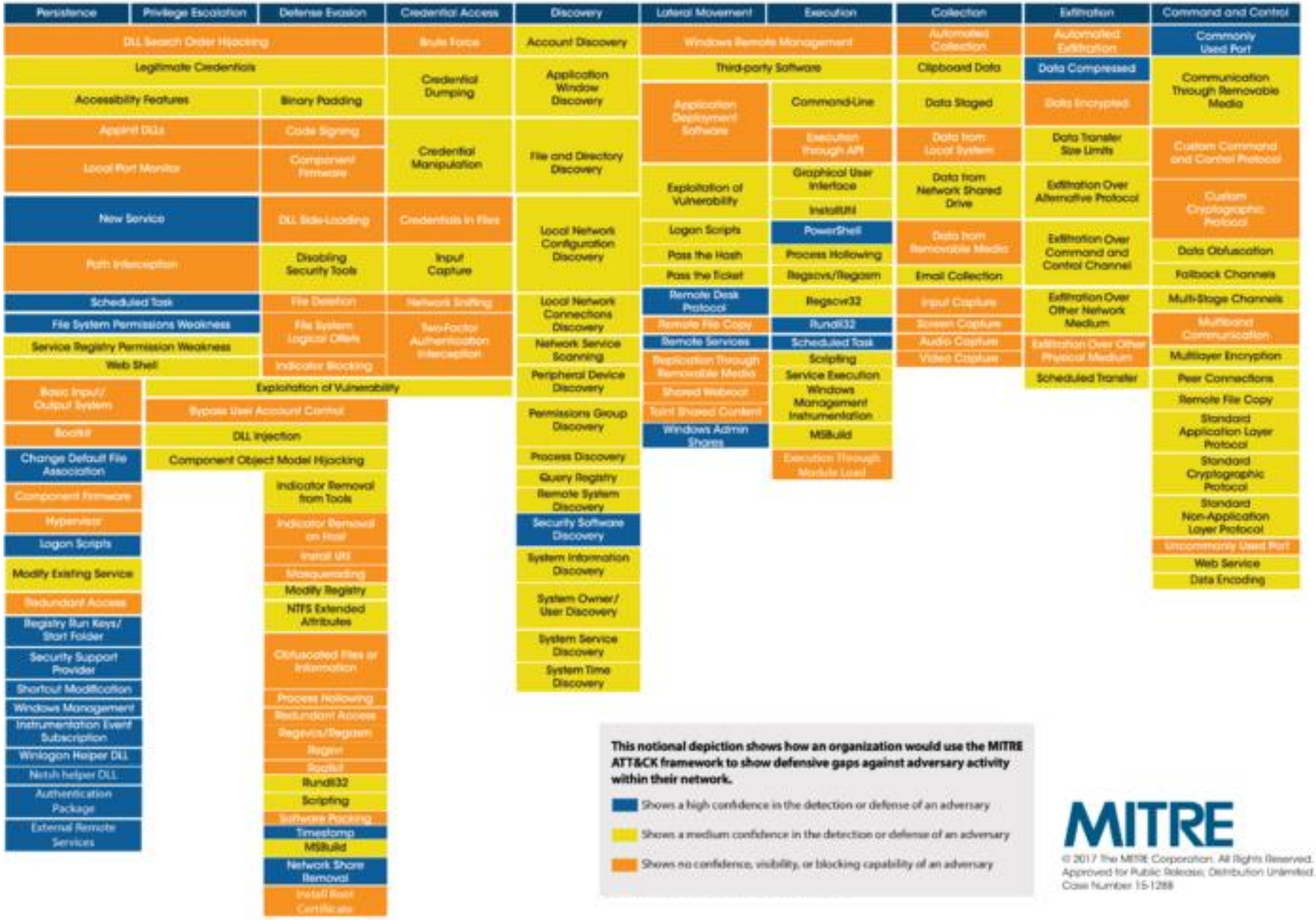
MITRE ATT&CK

Cyber Kill chain		MITRE ATT&CK
• Reconnaissance • Weaponization • Delivery • Exploitation • Installation • Command & Control • Actions of objectives	VS	• Initial access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral moment • Collection • Exfiltration • Command and Control • Impact

MITRE ATT&CK

- The MITRE Corporation, a not-for-profit org that manages FFRDCs, released the ATT&CK Framework in 2015.
- ATT&CK is a living, growing framework of common tactics, techniques, and procedures (TTP) used by advanced persistent threats (APTs) and other cybercriminals.
- MITRE ATT&CK makes their matrices accessible to the private sector, governments, the cybersecurity product and service community, and the general public.
- The ATT&CK matrix provides a framework for identifying tactics and techniques used by threat actors

MITRE ATT&CK


Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control
DLL Search Order Hijacking
Legitimate Credentials
Accessibility Features
Binary Padding
AppInit DLLs
Code Signing
Local Port Monitor
Component Firmware
New Service
DLL Side-Loading
Path Interception
Disabling Security Tools
Scheduled Task
File System Permissions Weakness
Service Registry Permission Weakness
Web Shell
File Deletion
File System Logical Offsets
Indicator Blocking
Exploitation of Vulnerability
Basic Input/ Output System
Bootkit
Change Default File Association
Component Firmware
Hypervisor
Logon Scripts
Modify Existing Service
Redundant Access
Registry Run Keys/ Start Folder
Security Support Provider
Shortcut Modification
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL
Netsh helper DLL
Authentication Package
External Remote Services
Bypass User Account Control
DLL Injection
Component Object Model Hijacking
Indicator Removal from Tools
Indicator Removal on Host
Install Util
Masquerading
Modify Registry
NTFS Extended Attributes
Obfuscated Files or Information
Process Hollowing
Redundant Access
Regsvcs/Regasm
Regsvr
Rootkit
Rundll32
Scripting
Software Packing
Timestomp
MSBuild
Network Share Removal
Install Root Certificate
Brute Force
Credential Dumping
Credential Manipulation
Credentials in Files
Input Capture
Network Sniffing
Two-Factor Authentication Interception
Account Discovery
Application Window Discovery
File and Directory Discovery
Local Network Configuration Discovery
Local Network Connections Discovery
Network Service Scanning
Peripheral Device Discovery
Permissions Group Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Owner/ User Discovery
System Service Discovery
System Time Discovery
Windows Remote Management
Third-party Software
Application Deployment Software
Command-Line
Execution through API
Exploitation of Vulnerability
Graphical User Interface
InstallUtil
Logon Scripts
PowerShell
Pass the Hash
Process Hollowing
Pass the Ticket
Regsvcs/Regasm
Remote Desk Protocol
Regsvr32
Remote File Copy
Rundll32
Remote Services
Scheduled Task
Replication Through Removable Media
Scripting
Shared Webroot
Service Execution
Taint Shared Content
Windows Management Instrumentation
Windows Admin Shares
MSBuild
Execution Through Module Load
Automated Collection
Clipboard Data
Data Staged
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Email Collection
Input Capture
Screen Capture
Audio Capture
Video Capture
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Other Physical Medium
Scheduled Transfer
Commonly Used Port
Communication Through Removable Media
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Obfuscation
Fallback Channels
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Peer Connections
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Data Encoding
This notional depiction shows how an organization would use the MITRE ATT&CK framework to show defensive gaps against adversary activity within their network.
Shows a high confidence in the detection or defense of an adversary
Shows a medium confidence in the detection or defense of an adversary
Shows no confidence, visibility, or blocking capability of an adversary
MITRE
© 2017 The MITRE Corporation. All Rights Reserved.
Approved for Public Release; Distribution Unlimited.
Case Number 15-1288

MITRE ATT&CK

What is ATT&CK?	Why did MITRE develop ATT&CK?
ATT&CK is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle. ATT&CK has two parts: **ATT&CK for Enterprise,** which covers behavior against enterprise IT networks and cloud, and **ATT&CK for Mobile**, which focuses on behavior against mobile devices.	MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks. It was created out of a need to document adversary behaviors for use within a MITRE research project called FMX. The objective of FMX was to investigate use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating within enterprise networks. ATT&CK was used as the basis for testing the efficacy of the sensors and analytics under FMX and served as the common language both offense and defense could use to improve over time.

MITRE ATT&CK

What are "tactics"?	What are "techniques"?
Tactics represent the “why” of an ATT&CK technique or sub-technique. It is the adversary’s tactical goal: the reason for performing an action. For example, an adversary may want to achieve **credential access**.	Techniques represent “how” an adversary achieves a tactical goal by performing an action. For example, an adversary may **dump credentials** to achieve credential access.
What are "sub-techniques"?	**What are "procedures"?**
Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique. For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.	Procedures are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorized in ATT&CK as the observed in the wild use of techniques in the "Procedure Examples" section of technique pages.

MITRE Cyber Analytics Repository (CAR)

CAR is a knowledge base of analytics developed by MITRE and is based on the MITRE ATT&CK adversary model. Analytics stored in CAR contain the following information for each analytic:

- A hypothesis which explains the idea behind an analytic.
- The information or primary domain the analytic is designed to operate within (this could be host, network, process, external, etc.)
- References to ATT&CK Techniques and Tactics that the analytic detects
- The Glossary
- A pseudocode description of how the analytic might be implemented
- A unit test which can be run to trigger the analytic

MITRE ATT&CK Navigator

- The MITRE ATT&CK Navigator is designed to provide basic navigation and annotation of the ATT&CK matrix. The tool is used as a simple way to visualize the ATT&CK matrix and make it easier to use. One of the many useful features of the ATT&CK Navigator is using the provided filters to highlight techniques used by a particular threat group. This is helpful in identifying the techniques that may be important to your organization.

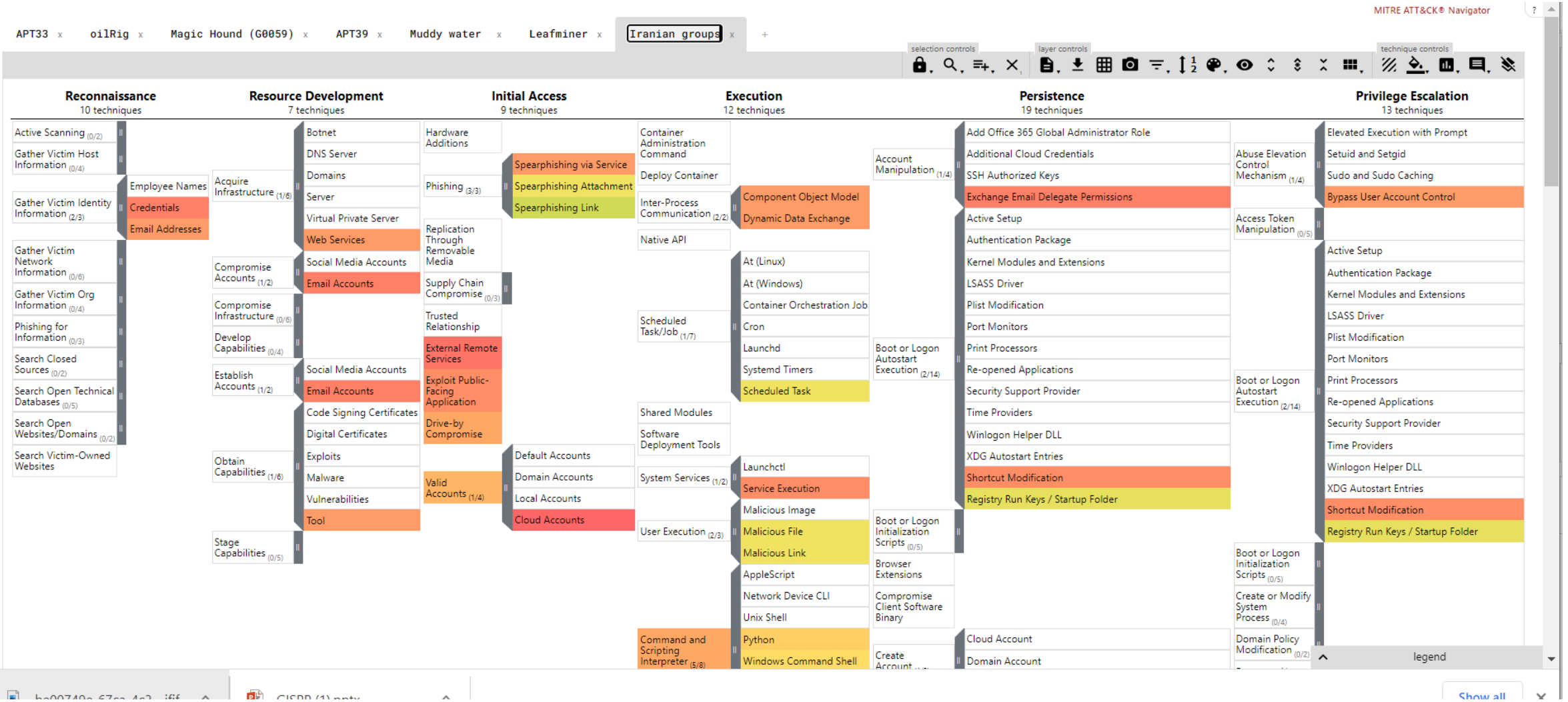
Tools Identification in MITRE ATT&CK

ID	Name	Tactic	Tools
T1002	Data Compressed	Exfiltration	PowerShell,rar
T1003	Credential Dumping	Credential Access	PowerShell, Mimikatz, Gsecdump, Windows Credential Editor
T1007	System Service Discovery	Discovery	tasklist_exq sc.exe, wmic
T1012	Query Registry	Discovery	reg,cmd
T1015	Accessibility Features	Persistence, Privilege Escalation	reg,cmd
T1016	System Network Configuration Discovery	Discovery	cmd,ipconfig,netsh,arp,nbtstat,net
T2018	Remote System Discovery	Discovery	net,ping,arp
T1028	Windows Remote Management	Execution, Lateral Movement	PowerShell,Wmic,Mimikatz,WinRM
T1033	System Owner/User Discovery	Discovery	cmd,wmic,quser,qwinsta
T1035	Service Execution	Execution	PsExec
T1042	Change Default File Association	Persistence	cmd,reg,assoc
T1047	Windows Management Instrumentation	Execution	wmic
T1050	New Service	Persistence, Privilege Escalation	sc.exe,PowerShell
T1053	Scheduled Task	Execution, Persistence, Privilege Escalation	at.exe,schtask,net
T1055	Process Injection	Defense Evasion, Privilege Escalation	PowerSploit

Example Technique used by OilRig

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	OilRig has run net user, `net user /domain`, `net group "domain admins" /domain`, and net group "Exchange Trusted Subsystem" /domain to get account listings on a victim.
		.002	Account Discovery: Domain Account	OilRig has run net user, net user /domain, net group "domain admins" /domain, and net group "Exchange Trusted Subsystem" /domain to get account listings on a victim.
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	OilRig has used HTTP for C2
		.004	Application Layer Protocol: DNS	OilRig has used DNS for C2
Enterprise	T1110		Brute Force	OilRig has used brute force techniques to obtain credentials.
	T1059	.001		OilRig has used PowerShell scripts for execution, including use of a macro to run a PowerShell command to decode file contents

Heat Map of few Iranian Groups

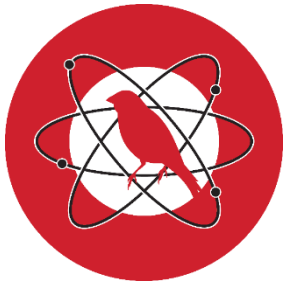


APT33 TTPs, MITRE ATT&CK (FireEye)

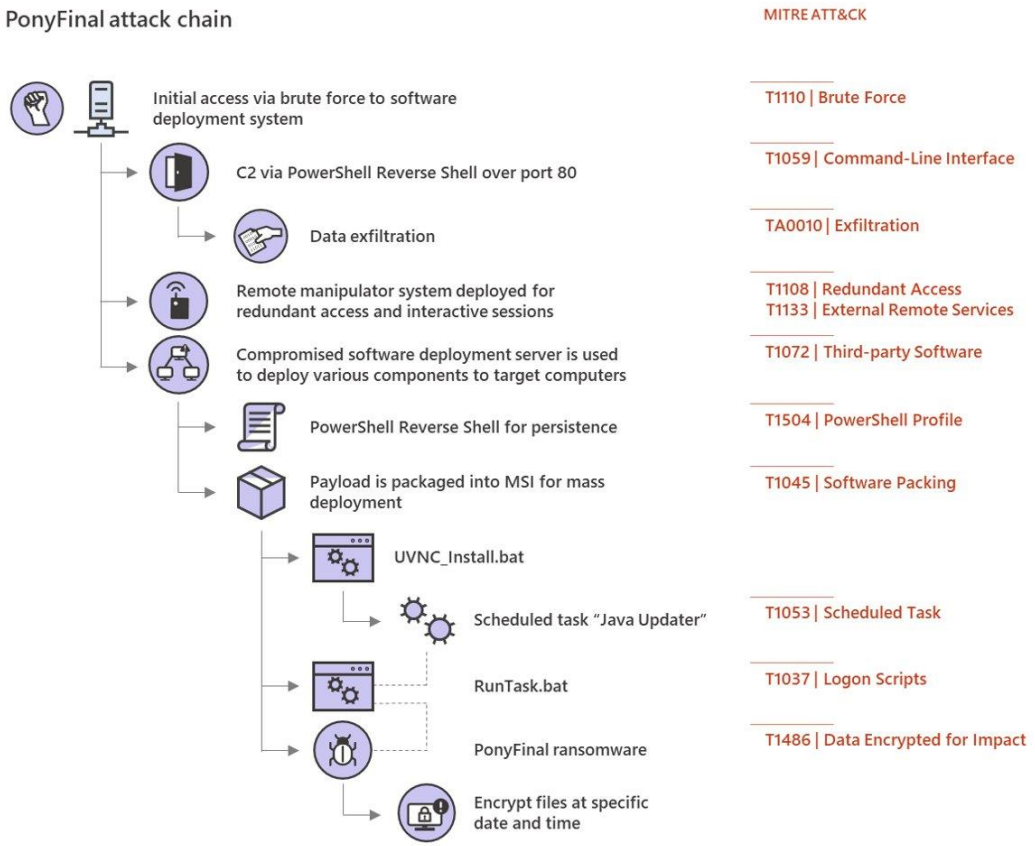
DOMAIN	ID	NAME	USE
Enterprise	T1110	Brute Force	APT33 has used password spraying to gain access to target systems.
Enterprise	T1043	Commonly Used Port	APT33 has used port 443 for command and control.
Enterprise	T1003	Credential Dumping	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, Gpppassword, SniffPass, and ProcDump to dump credentials.
Enterprise	T1002	Data Compressed	APT33 has used WinRAR to compress data prior to exfil.
Enterprise	T1132	Data Encoding	APT33 has used base64 to encode command and control traffic.
Enterprise	T1480	Execution Guardrails	APT33 has used kill dates in their malware to guardrail execution.
Enterprise	T1048	Exfiltration Over Alternative Protocol	APT33 has used FTP to exfiltrate files (separately from the C2 channel).
Enterprise	T1203	Exploitation for Client Execution	APT33 has attempted to exploit a known vulnerability in WinRAR (CVE-2018-20250).
Enterprise	T1068	Exploitation for Privilege Escalation	APT33 has used a publicly available exploit for CVE-2017-0213 to escalate privileges on a local system.
Enterprise	T1040	Network Sniffing	APT33 has used SniffPass to collect credentials by sniffing network traffic.
Enterprise	T1027	Obfuscated Files or Information	APT33 has used base64 to encode payloads.
Enterprise	T1086	PowerShell	APT33 has utilized PowerShell to download files from the C2 server and run various scripts.
Enterprise	T1060	Registry Run Keys / Startup Folder	APT33 has deployed a tool known as DarkComet to the Startup folder of a victim.
Enterprise	T1105	Remote File Copy	APT33 has downloaded additional files and programs from its C2 server.
Enterprise	T1053	Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day.
Enterprise	T1192	Spearphishing Link	APT33 has sent spearphishing emails containing links to tht files.
Enterprise	T1071	Standard Application Layer Protocol	APT33 has used HTTP for command and control.
Enterprise	T1032	Standard Cryptographic Protocol	APT33 has used AES for encryption of command and control traffic.
Enterprise	T1065	Uncommonly Used Port	APT33 has used ports 808 and 880 for command and control.
Enterprise	T1204	User Execution	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails.

MITRE ATT&CK

- Several open-source tools are available for testing an organization's detection capabilities based on the matrix
  - MITRE Caldera
  - Red Team Automation
  - Atomic Red Team
- These tools can be used to generate event information to test alerts and search capabilities
- .

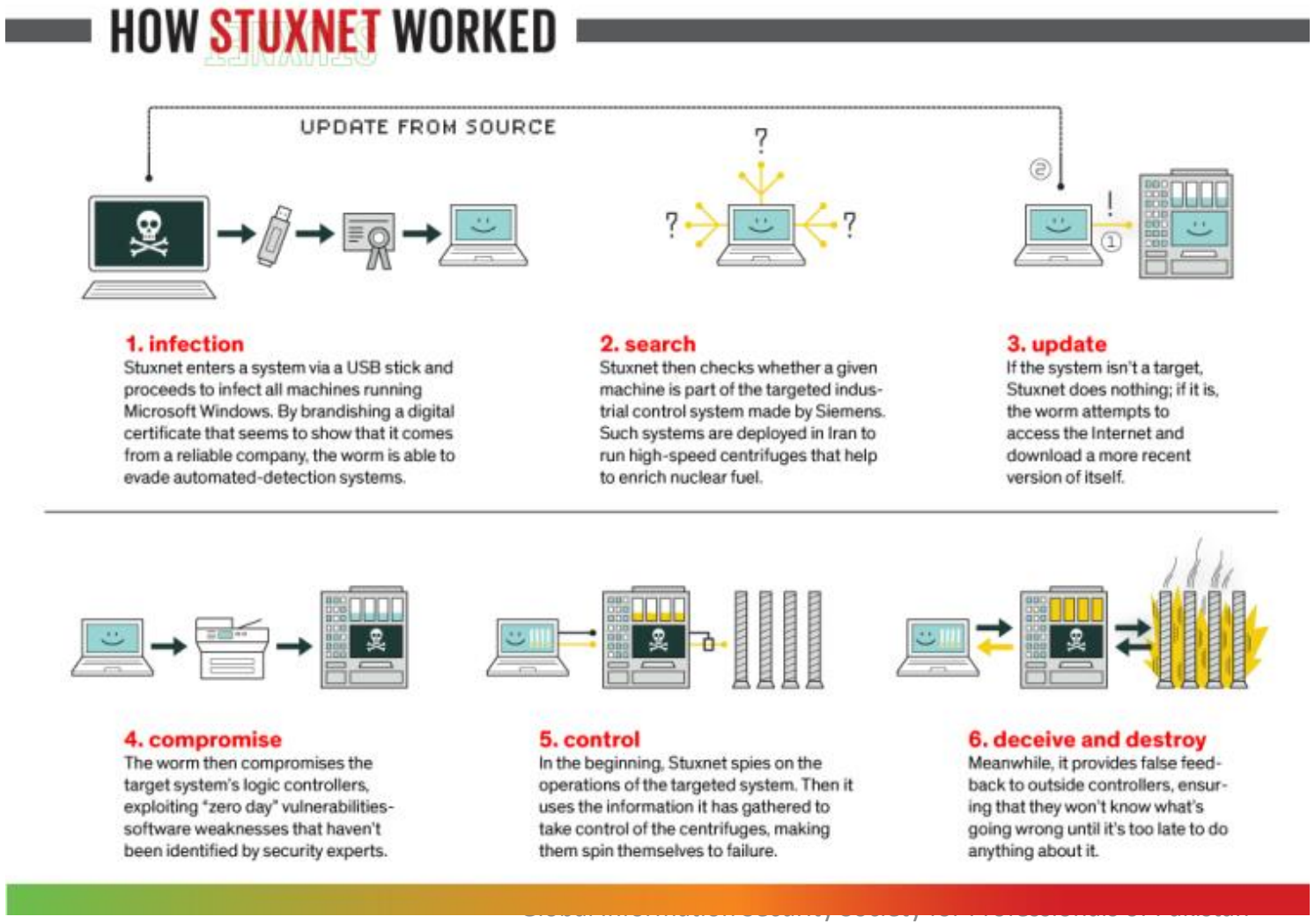


Pony Final Attack Chain

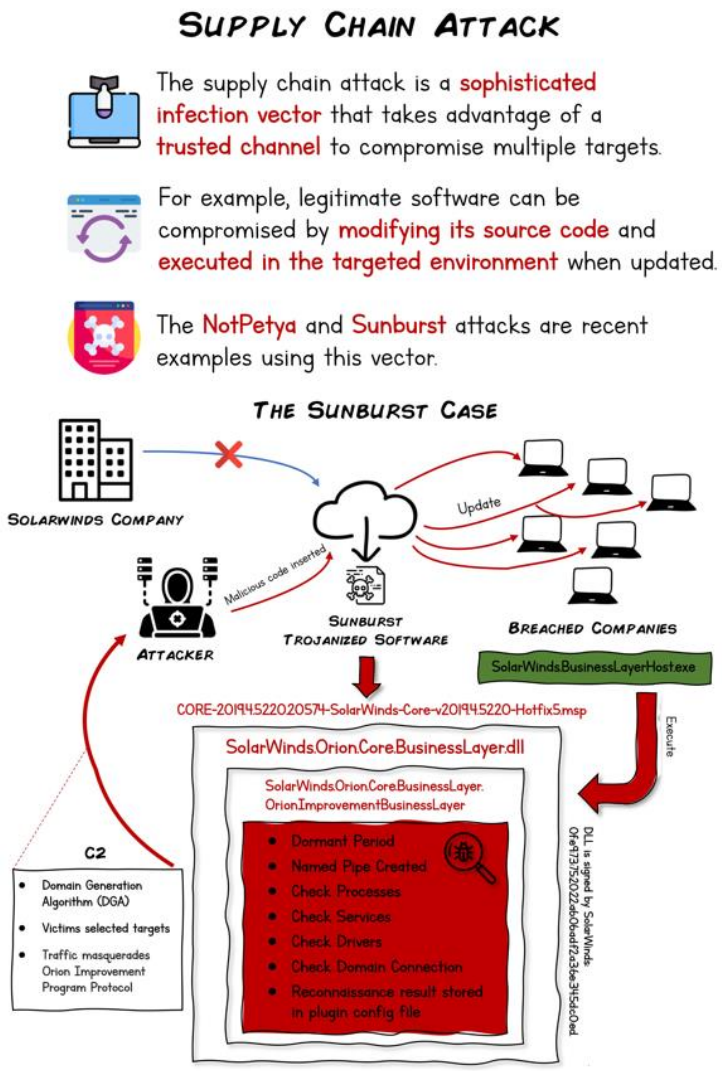


Wanna Cry Attack Chain

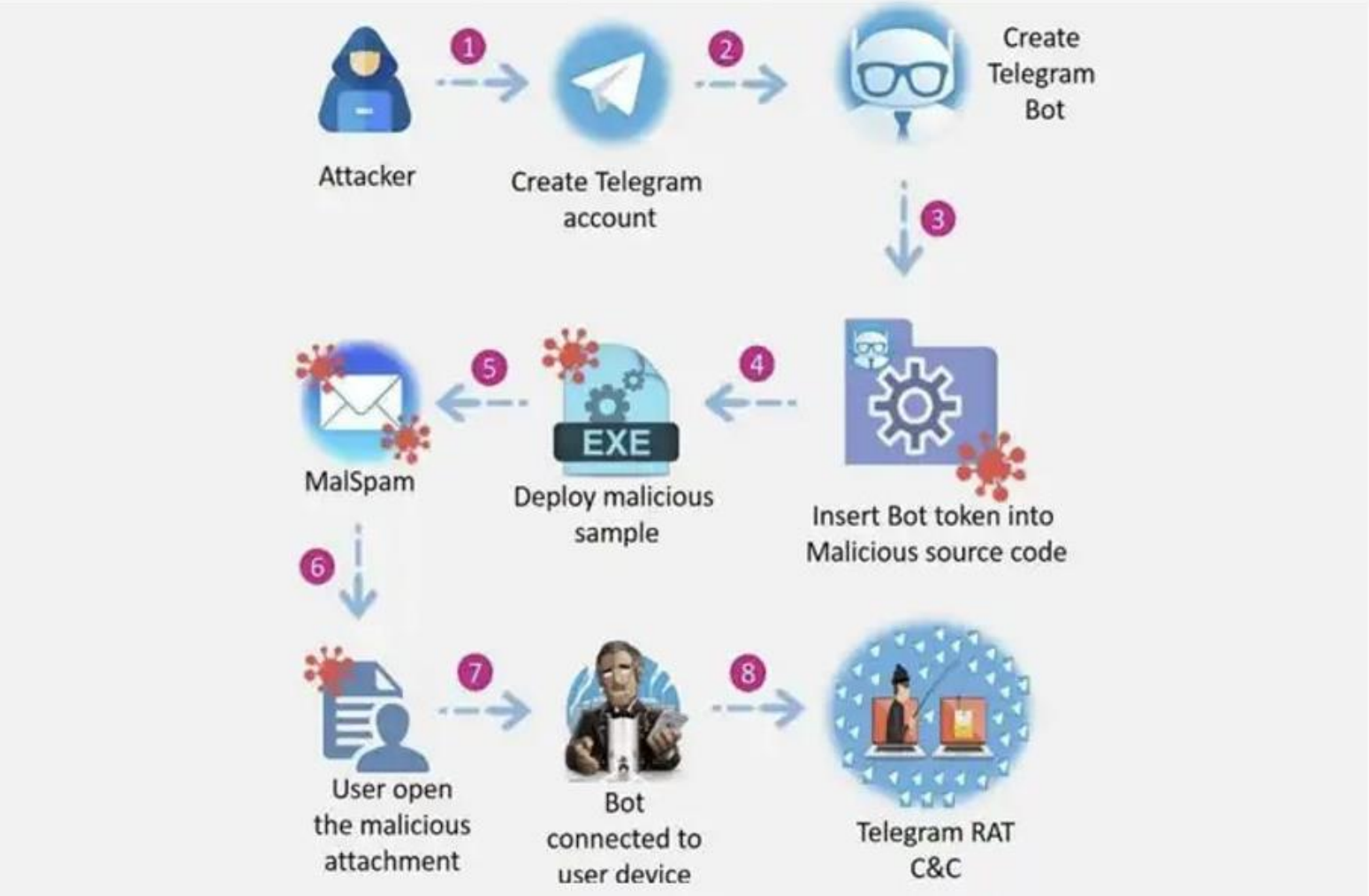
Few major Malware before MITRE

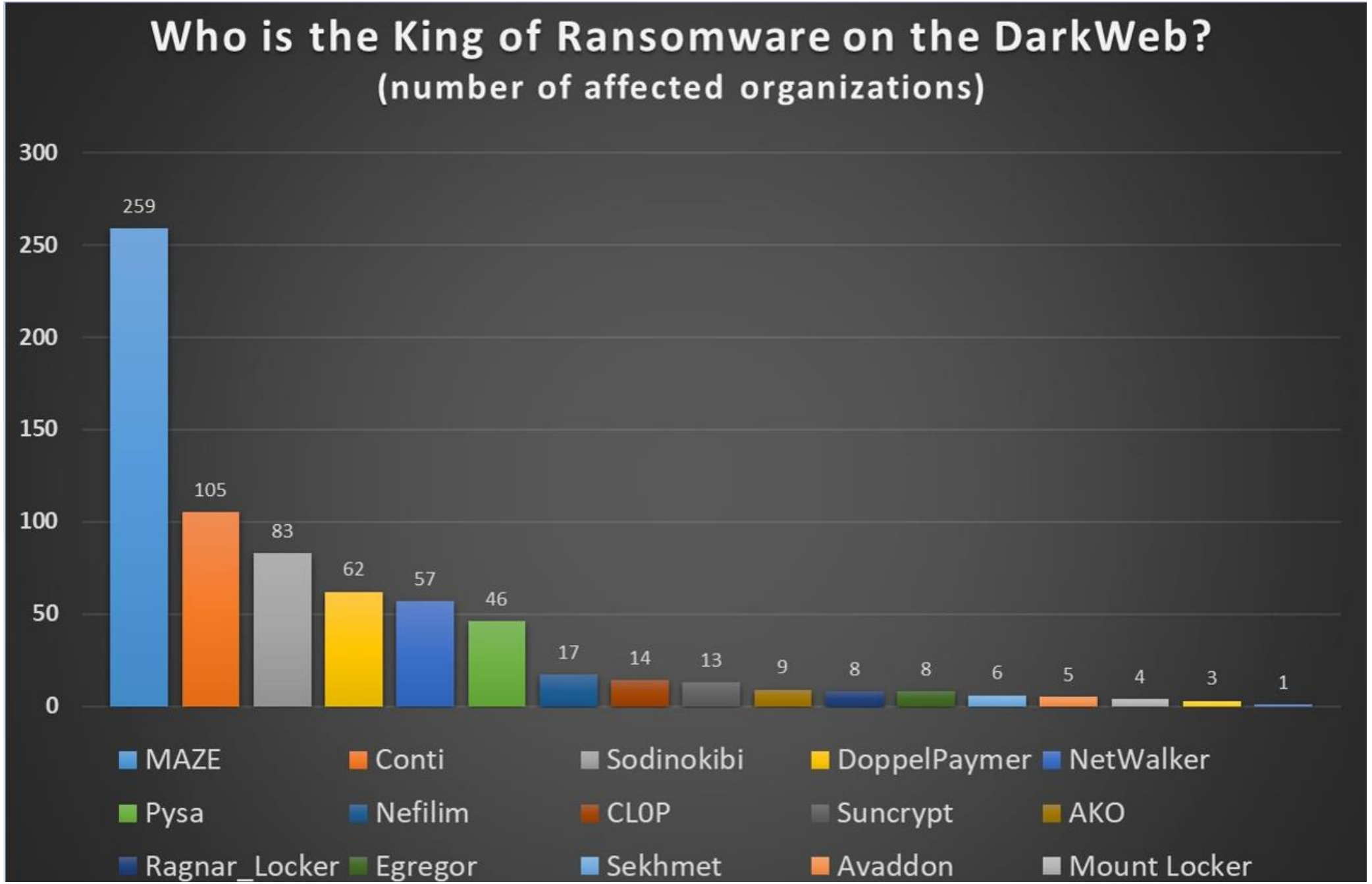


Solar Wind Supply Attack chain overview



Telegram Remote Access Trogan




Who is the King of Ransomware on the DarkWeb?
(number of affected organizations)
300
250
200
150
100
50
0
259
105
83
62
57
46
17
14
13
9
8
8
6
5
4
3
1
MAZE
Conti
Sodinokibi
DoppelPaymer
NetWalker
Pysa
Nefilim
CL0P
Suncrypt
AKO
Ragnar_Locker
Egregor
Sekhmet
Avaddon
Mount Locker

Useful URLS

- https://attack.mitre.org/resources/faq/ Frequently asked questions
- https://attack.mitre.org/matrices/enterprise/pre/ Pre Attack
- https://mitre-attack.github.io/attack-navigator/ Attack Navigator
- https://mitre-engenuity.org/mad/ new Certifications announced 90 days validation free
- https://d3fend.mitre.org/ NCA funded knowledge graph of cybersecurity countermeasures
- https://attackiq.com/mitre-attack/
- https://github.com/austinsonger/Incident-Playbook/tree/main/Pl aybooks/MITRE-ATTACK
- https://github.com/austinsonger/Incident-Playbook MITRE Incident response playbooks
- https://saf.mitre.org/ **Security Automation Framework based on MITRE**
- https://ctid.mitre-engenuity.org/our-work/attack-workbench/
- https://atomicredteam.io/testing.html running tests on lab environment for checking quality of SIEM /EDR use cases . Reduce noise and identifying true positives