Red Team

Soheil Hashemi

@huntlearn

Who am I?

- Soheil Hashemi
- MSC Network Computers
- Red Team | Penetration Testing | purple Team
- @soheilsec

Agenda

1. What is Red Team
2. why red team is important?
3. pyramid of pain
4. APT Groups
5. APT timeline in IRAN
6. type of hackers group
7. Red team Methodologies
8. Red Team vs penetration testing vs Bug bounty
9. Red Team Infrastrucure
10. Adversary Emulation Platforms
11. Red Team Tools
12. Cost of Data breach
13. APT 38
14. Red Team Roadmap
15. Red Team Interview
16. QA

1. What is Red Team

The Process of Emulation APT Attacks

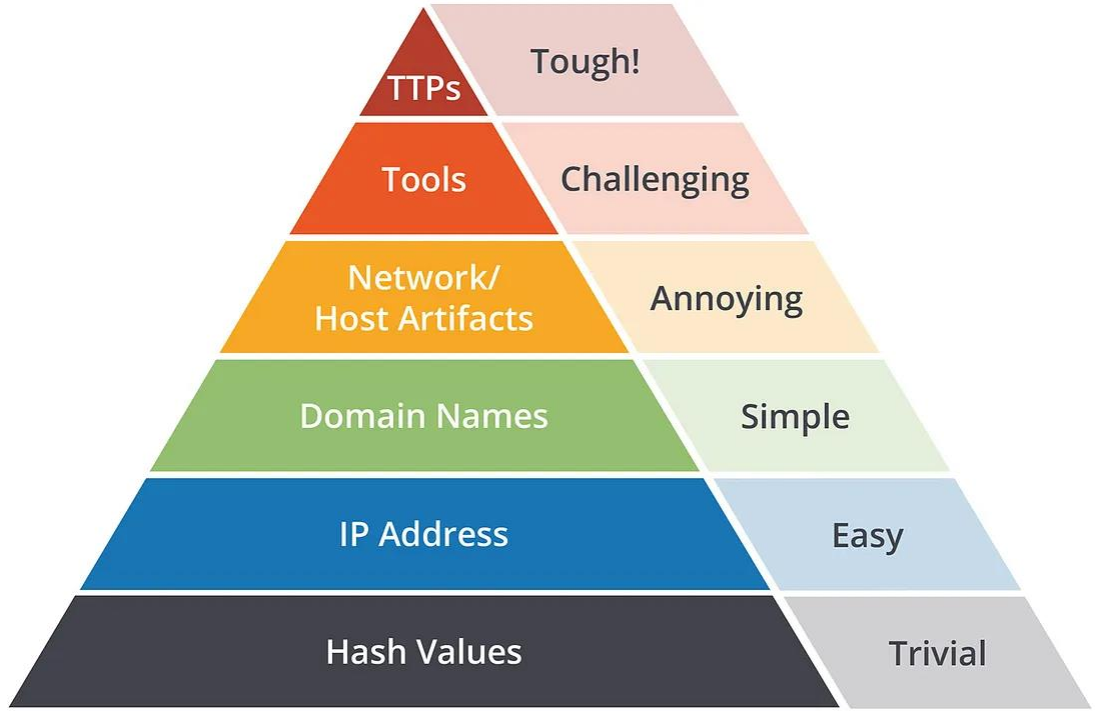
- Invented on 19th Century by German Army

- Used on DOD during COLD war 1960

2. Why Red Team is important?

Espionage

Sabotage



Source: David J. Bianco, personal blog

3. Pyramid of pain

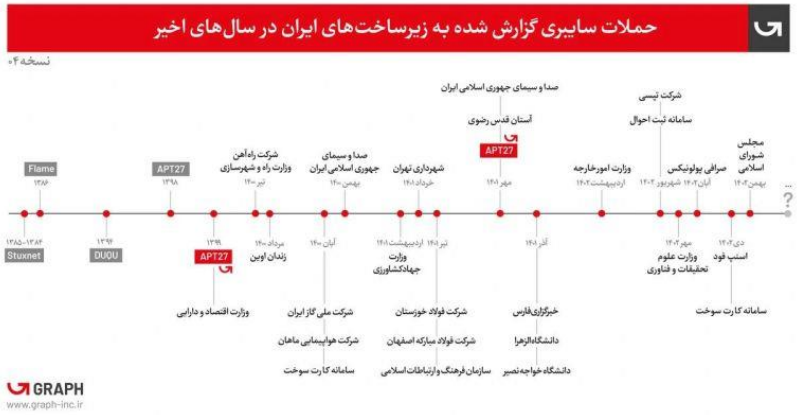
4. APT Groups

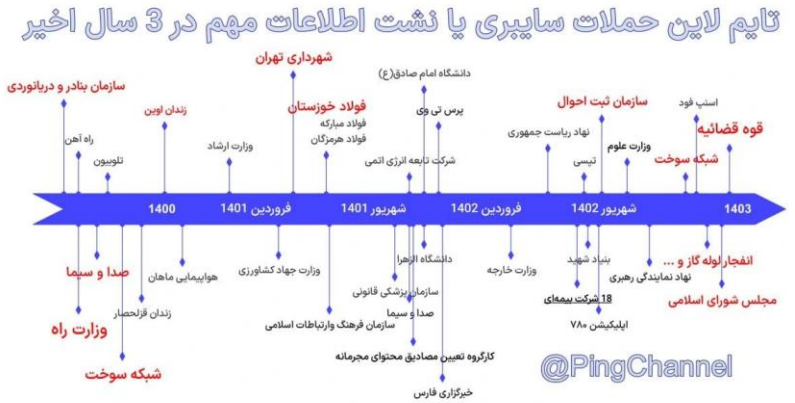
Advanced Persistence Threat

Advanced = Goal

- Persistence = Week, Month, Year [APT29 - nobelium Solarwinds]

- Threat = espionage, Sabotage





5. APT timeline in IRAN

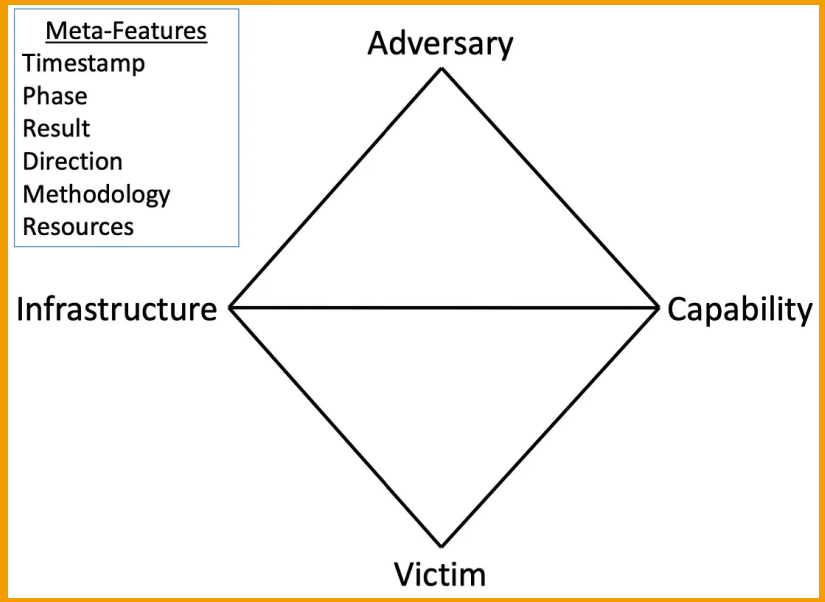
6.Type of hackers group

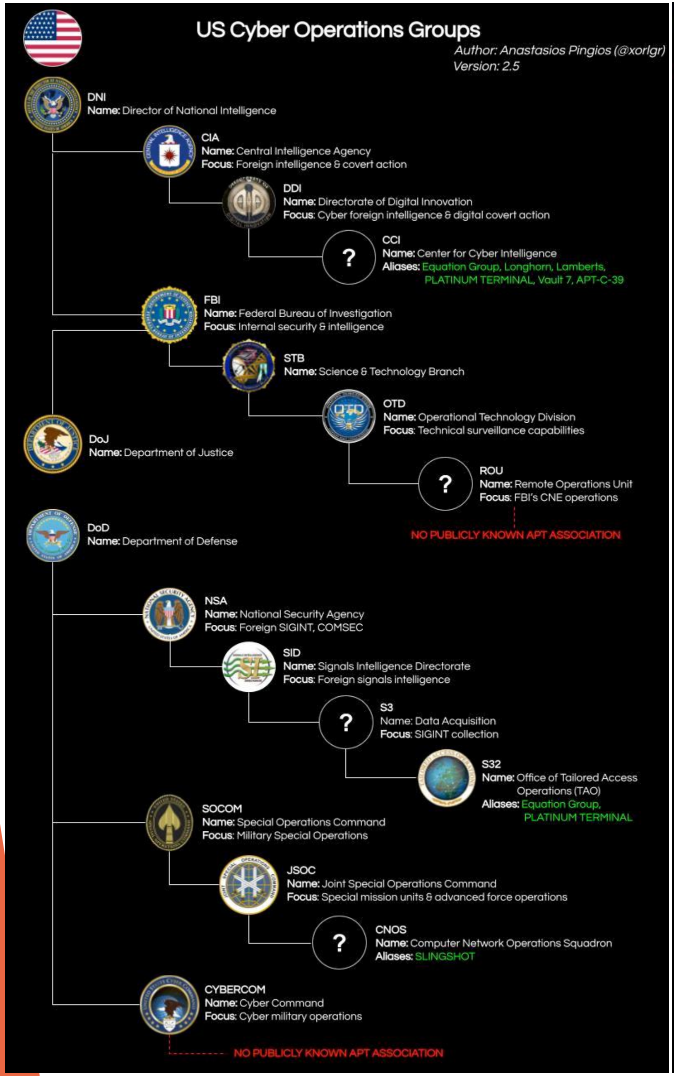
- APT
- Ransomware Gangs
- Organized Cyber Crime
- hacktivist

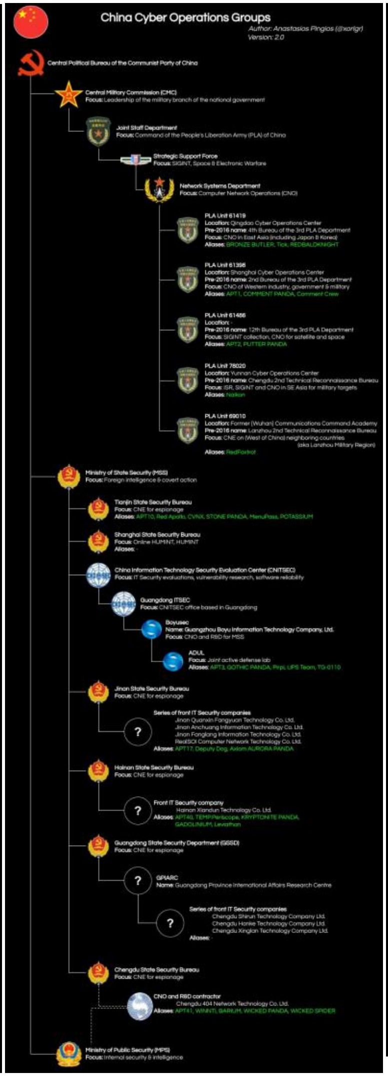
Diamond Model in Cyber Threat Intelligence

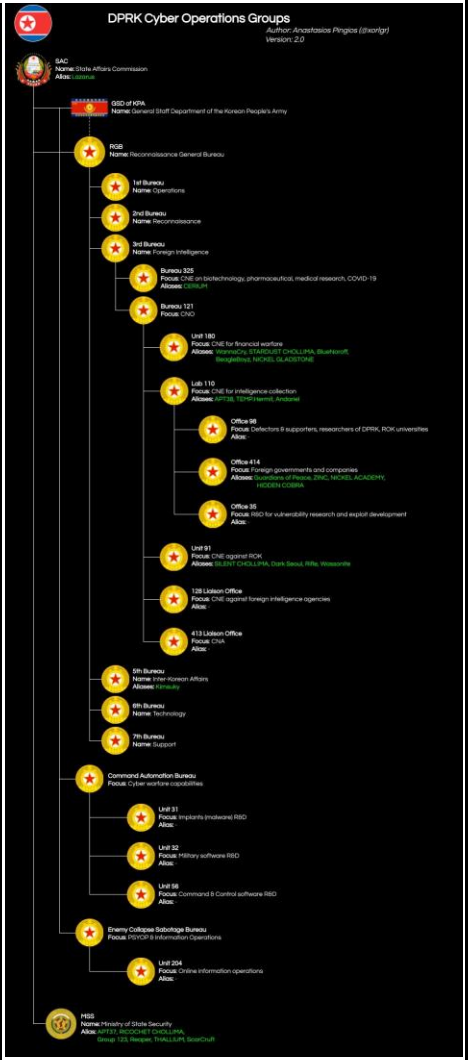
- Timestamp: date and time intrusion event occurred
- Phase: which event, in the chain of events, is represented by this particular model
- Result: outcome of intrusion (e.g., success, failure, or unknown; or confidentiality compromised, integrity compromised, and/or availability compromised)
- Direction: how event moved through network or host (e.g., Victim-to-Infrastructure, Adversary-to-Infrastructure, Bidirectional)
- Methodology: category of event (e.g., spearphishing, port scan)
- Resources: elements required for intrusion (e.g., particular software, hardware, knowledge, funds, facilities, access)
- Social-political: relationship between adversary and victim, based on victim's needs and aspirations
- Technology: tech involved in adversary's capabilities and use of infrastructure

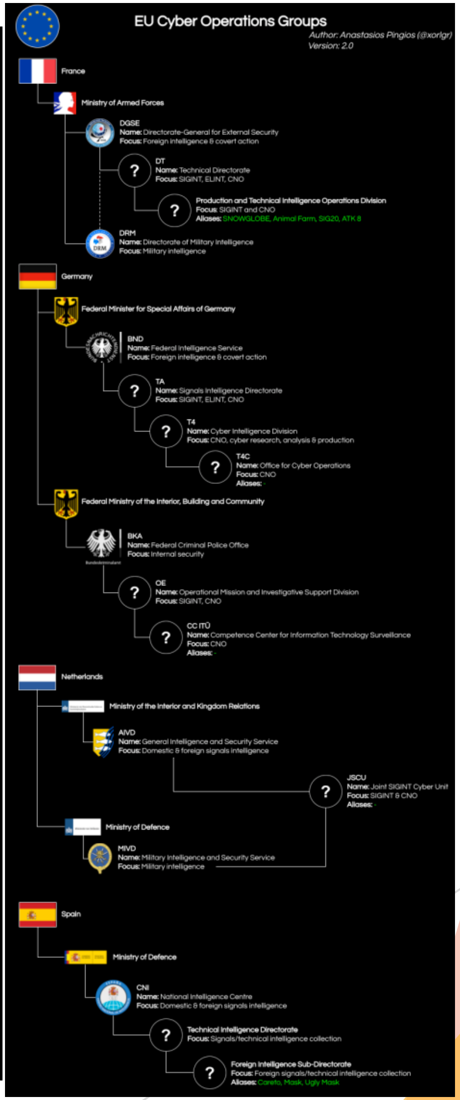
https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585




US Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 2.5
DNI
Name: Director of National Intelligence
CIA
Name: Central Intelligence Agency
Focus: Foreign intelligence & covert action
DDI
Name: Directorate of Digital Innovation
Focus: Cyber foreign intelligence & digital covert action
CCI
Name: Center for Cyber Intelligence
Aliases: Equation Group, Longhorn, Lamberts, PLATINUM TERMINAL, Vault 7, APT-C-39
FBI
Name: Federal Bureau of Investigation
Focus: Internal security & intelligence
STB
Name: Science & Technology Branch
OTD
Name: Operational Technology Division
Focus: Technical surveillance capabilities
DoJ
Name: Department of Justice
ROU
Name: Remote Operations Unit
Focus: FBI's CNE operations
NO PUBLICLY KNOWN APT ASSOCIATION
DoD
Name: Department of Defense
NSA
Name: National Security Agency
Focus: Foreign SIGINT, COMSEC
SID
Name: Signals Intelligence Directorate
Focus: Foreign signals intelligence
S3
Name: Data Acquisition
Focus: SIGINT collection
S32
Name: Office of Tailored Access Operations (TAO)
Aliases: Equation Group, PLATINUM TERMINAL
SOCOM
Name: Special Operations Command
Focus: Military Special Operations
JSOC
Name: Joint Special Operations Command
Focus: Special mission units & advanced force operations
CNOS
Name: Computer Network Operations Squadron
Aliases: SLINGSHOT
CYBERCOM
Name: Cyber Command
Focus: Cyber military operations
NO PUBLICLY KNOWN APT ASSOCIATION


China Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 2.0

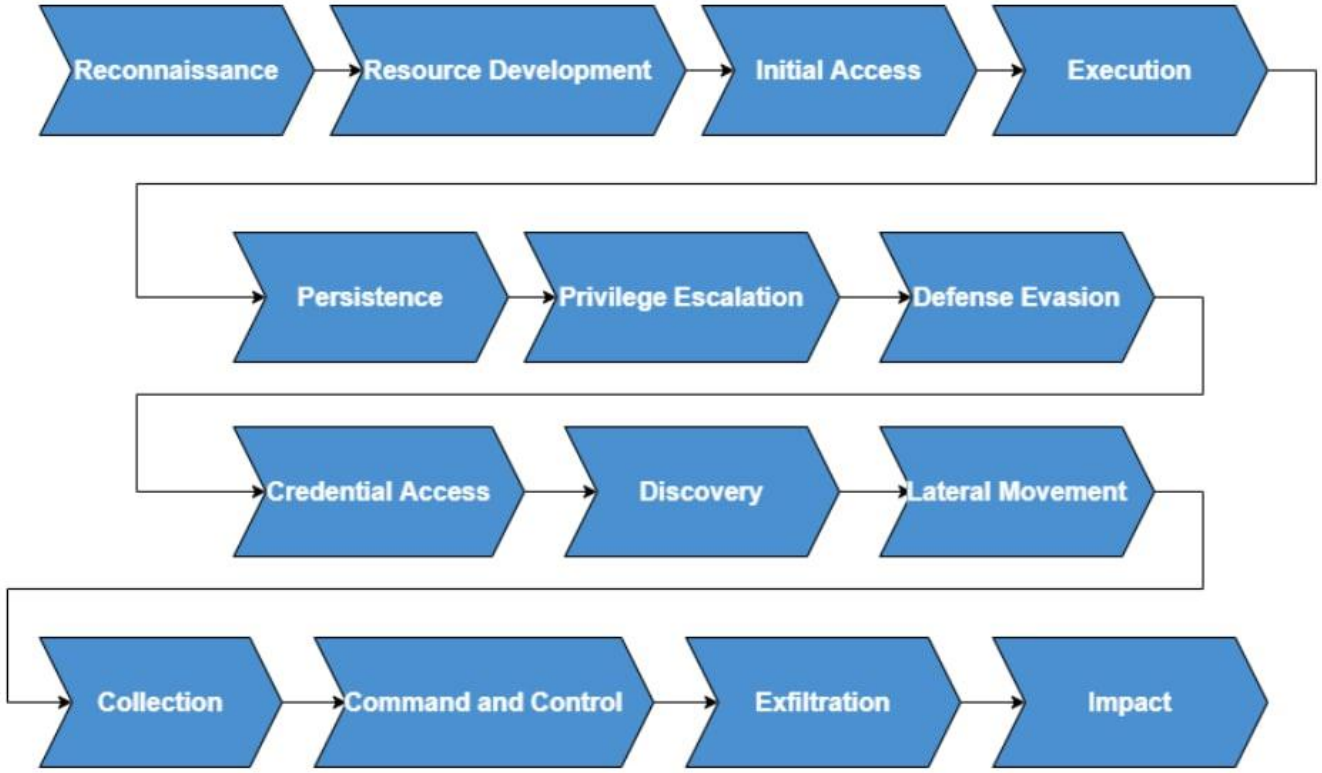

DPRK Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 2.0


EU Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 2.0

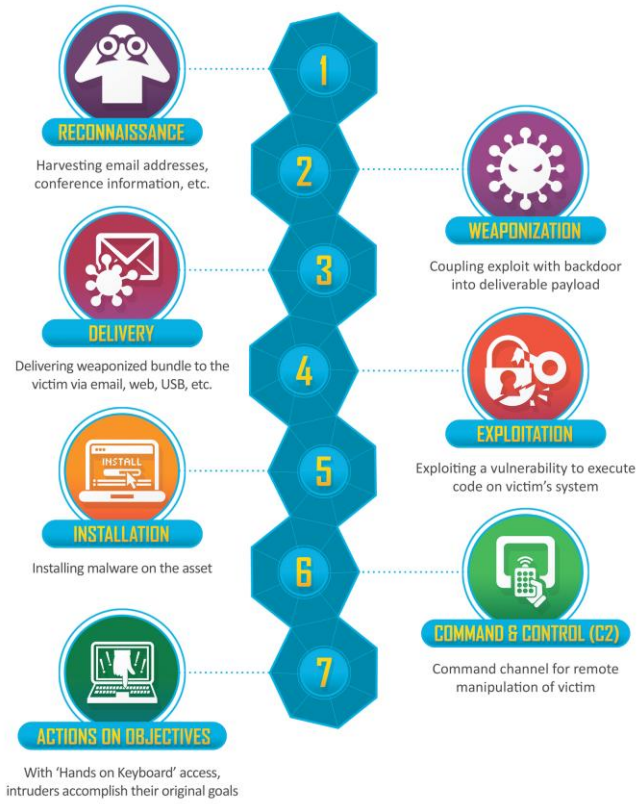
7. Red team Methodologies

- Methodologies [MITRE, Cyber Kill Chain attack]

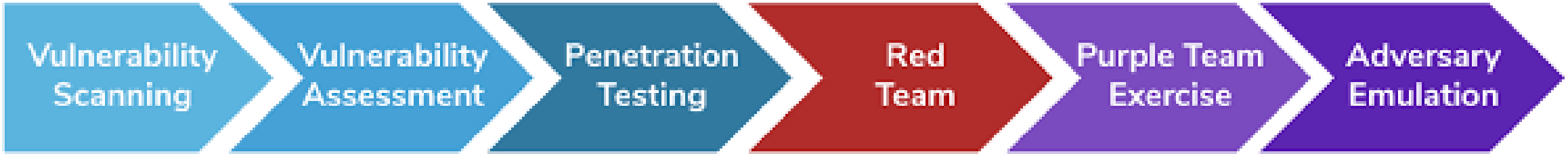
MITRE Att&ck


Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Cyber Kill chain



8. Red Team vs penetration testing vs Bug bounty



9. Red Team Infrastructure

Resource and Development [Domain, Mail Server, Smtp relay, C2 server, Forwarder]

For building Infrastructure Using Terraform IAC on AWS,AZURE,...

Weaponize CVE

Keep FUD payloads

Social Media Accounts and one time sim card for OSINT

10.Adversary Emulation Platforms

- Caldera - MITRE ATT&CK https://github.com/mitre/caldera
- Atomic Red Team - Red Canary - https://github.com/redcanaryco/atomic-red-team
- Hunter Forge's Mordor
- Metta - https://github.com/uber-common/metta
- APTSimulator - https://github.com/NextronSystems/APTSimulator
- Red Team Automation (RTA) - MITRE ATT&CK -https://github.com/endgameinc/RTA
- Infection Monkey - https://github.com/guardicore/monkey
- AutoTTP - https://github.com/jymcheong/AutoTTP
- RedHunt OS - Red Team TOOLS

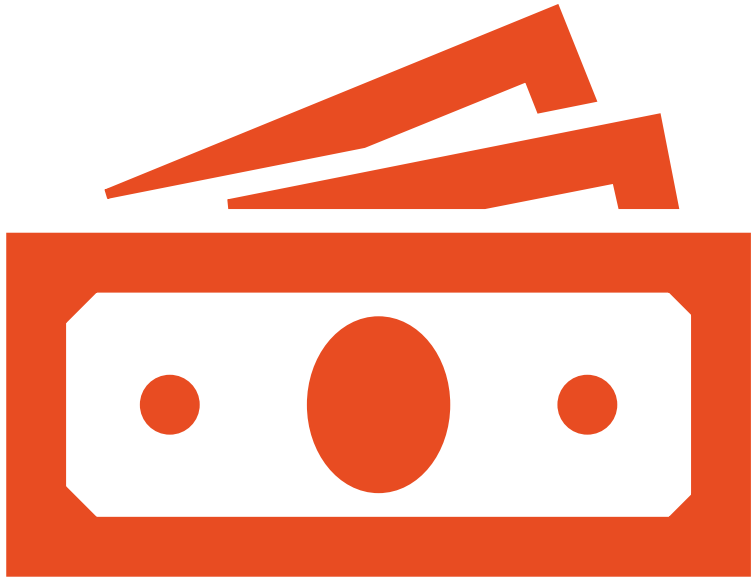
11.Red Team Framework

- Cobalt strike
- Brutal ratel c4
- AttackIQ FireDrill
- Cymulate

11.Red Team Tools

Meterpreter vs cobalt strike beacon detection rate	HTTP / HTTPs / TCP / UDP Detection rate	Macro	Cobaltstrike
Covenant	Sillenttrinity	Koadic	Metasploit
Merlin			

12.Cost of Data breach

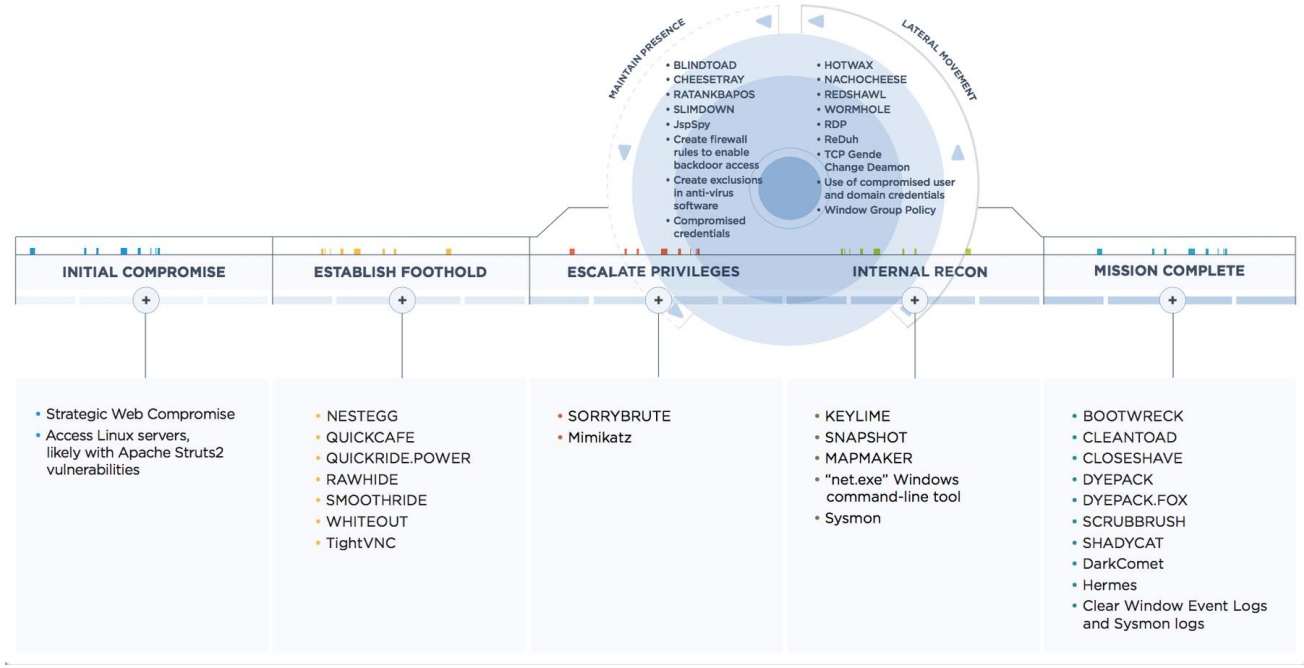


- **4.35 million USD Average total cost of a data breach**
- **4.82 million USD Average cost of a critical infrastructure data breach**
- **4.54 million USD Average cost of a ransomware attack, not including the cost of the ransom itself**
- **1 million USD Average difference in cost where remote work was a factor in causing the breach versus when it wasn't a factor**
- **2.66 million USD Average cost savings associated with an incident response (IR) team and regularly tested IR plan**
- **4.35 million USD Global average total cost of a data breach**
- **4.91 million USD Average cost of data breach with a phishing initial attack vector**
- **5.57 million USD Average cost of a breach for organizations with high levels of compliance failures**

13.APT 38

https://attack.mitre.org/groups/G/0082

- Operation Troy
- Sony Pictures
- bank heist



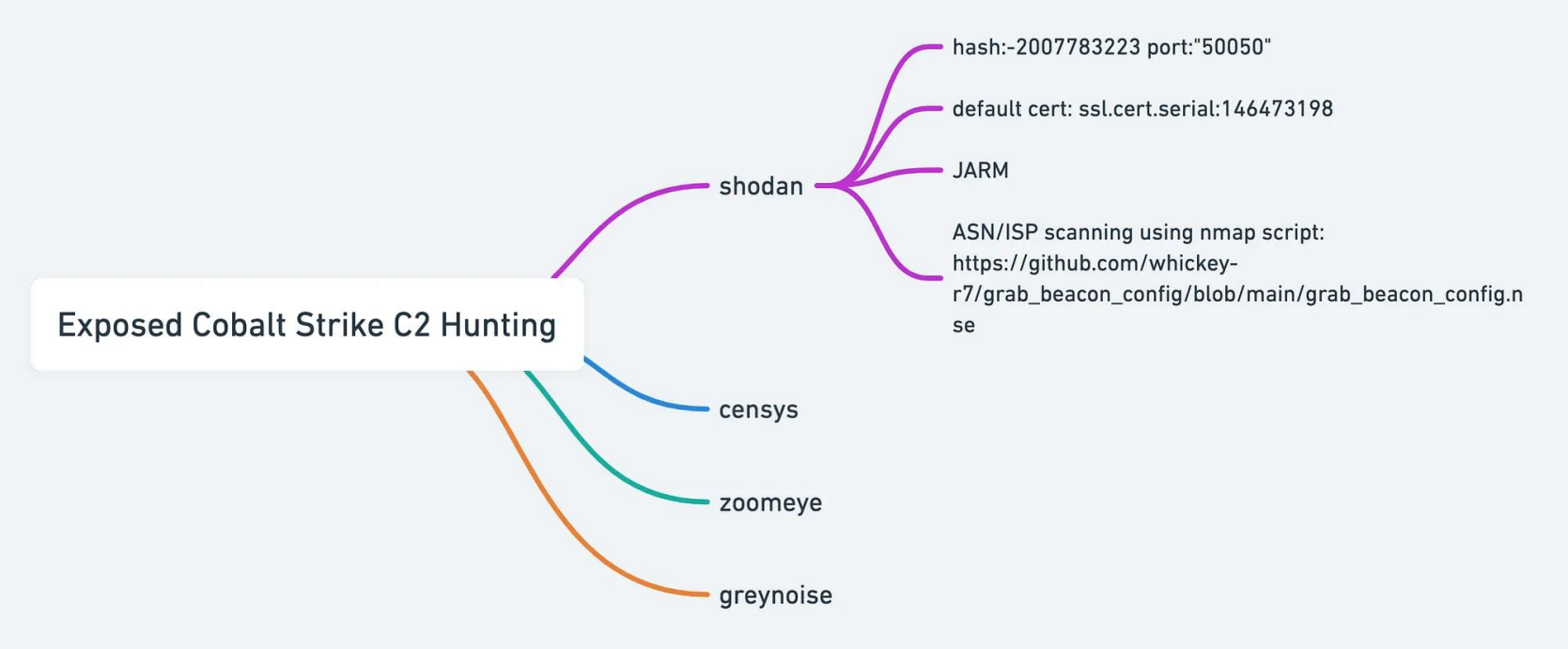
APT38 Attack Lifecycle

C2 Matrix

- https://howto.thec2matrix.com/
- https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4lgPsSc/edit?gid=0#gid=0
- https://ask.thec2matrix.com/

Cobalt Strike Offensive

- Listener
- Beacon
- Team server
- Stageless / stager
- Aggressor Script
- Maleable C2 profile



Cobalt strike Detection

Resource Development [public tools]

- DarkComet
- ECCENTRICBANDWAGON (RAT)
- HOPLIGHT (backdoor)
- KillDisk (wiper)
- mimikatz
- net

Initial Access

- Drive by compromise T1189
- Spear-Phishing Attachment T1566.001

- T1059.001 is a technique under the MITRE ATT&CK framework that involves using PowerShell, a powerful command-line interface and scripting environment in Windows, for malicious purposes. Adversaries can abuse PowerShell to execute commands, evade defenses, and carry out various post-exploitation activities.
- Executing malicious scripts
- Obfuscating commands
- Bypassing security controls
- Living-off-the-land
- Emulation

Execution - T1059.001- Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation): Look for suspicious PowerShell processes and command-line arguments.
- Event ID 7 (Image Loaded): Check for unusual DLLs loaded by PowerShell.
- Event ID 10 (Process Access): Monitor PowerShell accessing other processes or being accessed by other processes.
- Event ID 13 (Registry Event): Monitor registry modifications by PowerShell.
- Windows Event Logs:
- Event ID 4104 (PowerShell Script Block Logging): Enable PowerShell logging and monitor for suspicious script executions.
- Event ID 4688 (New Process Creation): Check for PowerShell creating new processes.
- Event ID 4689 (Process Termination): Monitor PowerShell process terminations.

Execution - T1059.001- Detection

- T1059.005 is a technique under the MITRE ATT&CK framework that involves using Visual Basic (VB) for malicious purposes. VB is a programming language that can be used to create executable files, macros in Microsoft Office documents, and scripts. Adversaries can abuse VB to execute commands, evade defenses, and carry out various post-exploitation activities.
- Malicious macros in Office documents
- Executing Visual Basic scripts (VBS)
- Obfuscating commands
- Bypassing security controls
- Living-off-the-land
- Emulation

Execution - T1059.005 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Image Loaded)
- Event ID 10 (Process Access)
- Event ID 13 (Registry Event)
- Windows Event Logs:
- Event ID 4688 (New Process Creation)
- Event ID 4689 (Process Termination)

Execution - T1059.005 - Detection

- T1059.003 is a technique under the MITRE ATT&CK framework that involves using the Windows Command Shell (cmd.exe) for malicious purposes. Cmd.exe is a command-line interpreter that can be used to execute commands, scripts, and batch files. Adversaries can abuse cmd.exe to execute commands, evade defenses, and carry out various post-exploitation activities.
- Executing commands directly
- Executing scripts and batch files
- Obfuscating commands
- Bypassing security controls
- Emulation

Execution - T1059.003 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Image Loaded)
- Event ID 10 (Process Access)
- Event ID 13 (Registry Event)
- Windows Event Logs:
- Event ID 4688 (New Process Creation)
- Event ID 4689 (Process Termination)

Execution - T1059.003 - Detection

- T1106 is a technique under the MITRE ATT&CK framework that involves using Native Application Programming Interfaces (APIs) for malicious purposes. Native APIs are functions and services provided by the operating system that allow applications to interact with system resources and perform various tasks. Adversaries can abuse native APIs to execute code, evade defenses, and carry out various post-exploitation activities.
- Direct system calls
- Evading defenses
- Code injection
- Process manipulation
- Emulation

Execution – T1106 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Image Loaded)
- Event ID 10 (Process Access)
- Event ID 13 (Registry Event)
- Windows Event Logs:
- Event ID 4688 (New Process Creation)
- Event ID 4689 (Process Termination)

Execution – T1106 - Detection

- T1053.003 is a technique under the MITRE ATT&CK framework that involves using cron jobs for malicious purposes on Linux and Unix-based systems. Cron is a time-based job scheduler in Unix-like operating systems that allows users to schedule tasks or scripts to run automatically at specific times or intervals. Adversaries can abuse cron to execute code, establish persistence, or carry out various post-exploitation activities.
- Executing malicious scripts
- Establishing persistence
- Bypassing security controls
- Emulation

Execution – T1053.003 - Offensive

- Monitor syslog for suspicious events related to cron job creation, modification, or deletion.
- Review authentication logs for unusual user activity or privileges that may indicate unauthorized modification of cron jobs.
- Analyze cron logs (e.g., /var/log/cron) to identify suspicious job executions or patterns.
- Monitor changes to cron-related files and directories, such as /etc/crontab and /etc/cron.*/*, using tools like auditd

Execution – T1053.003 - Detection

- T1053.005 is a technique under the MITRE ATT&CK framework that involves using scheduled tasks for malicious purposes on Windows systems. The Windows Task Scheduler is a built-in utility that allows users to schedule tasks or scripts to run automatically at specific times or intervals. Adversaries can abuse scheduled tasks to execute code, establish persistence, or carry out various post-exploitation activities.
- Executing malicious scripts
- Establishing persistence
- Bypassing security controls
- Emulation

Execution – T1053.005 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Access)
- Windows Event Logs:
- Event ID 106 (Scheduled Task Creation)
- Event ID 107 (Scheduled Task Modified)
- Event ID 4698 (Scheduled Task Created)

Execution – T1053.005 - Detection

- T1569.002 is a technique under the MITRE ATT&CK framework that involves using service execution for malicious purposes. Services are background processes designed to perform specific functions without requiring user interaction. Adversaries can abuse services to execute code, establish persistence, or carry out various post-exploitation activities.
- Creating new services
- Modifying existing services
- Bypassing security controls
- Emulation

Execution – T1569.002 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 6 (Driver Loaded)
- Event ID 10 (Process Access)
- Windows Event Logs:
- Event ID 7045 (Service Start/Stop)
- Event ID 4697 (Service Installation)

Execution – T1569.002 - Detection

- T1024.002 is a technique under the MITRE ATT&CK framework that involves using malicious files for various purposes, such as delivering malware, executing code, or evading defenses. These files can be in different formats, such as executables (.exe), scripts (.bat, .ps1, etc.), or document files with macros (.doc, .xls, etc.).
- Email attachments
- Drive-by downloads
- Exploit kits
- Supply chain attacks
- Emulation

Execution – T1024.002 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Image Loaded)
- Event ID 10 (Process Access)
- Windows Event Logs:
- Event ID 4688 (New Process Creation)

Execution – T1024.002 - Detection

- T1543.003 is a technique under the MITRE ATT&CK framework that involves creating or modifying Windows services for malicious purposes. Windows services are background processes designed to perform specific functions without requiring user interaction. Adversaries can abuse Windows services to execute code, establish persistence, or carry out various post-exploitation activities.
- Creating new services
- Modifying existing services
- Bypassing security controls
- Emulation

Execution – T1024.002 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 6 (Driver Loaded)
- Event ID 10 (Process Access)
- Windows Event Logs:
- Event ID 7045 (Service Start/Stop)
- Event ID 4697 (Service Installation)

Execution – T1024.002 - Detection

Persistence

- T1543.003 Windows Service
- T1053.003 Cron
- T1053.005 Schedule Task

- T1505.003 is a technique under the MITRE ATT&CK framework that involves the use of web shells for malicious purposes. A web shell is a malicious script or program that an attacker can upload to a web server to gain remote access and execute arbitrary commands. These scripts are often written in server-side scripting languages like PHP, ASP, or JSP.
- File upload vulnerabilities
- Stolen credentials
- Social engineering and phishing
- Emulation

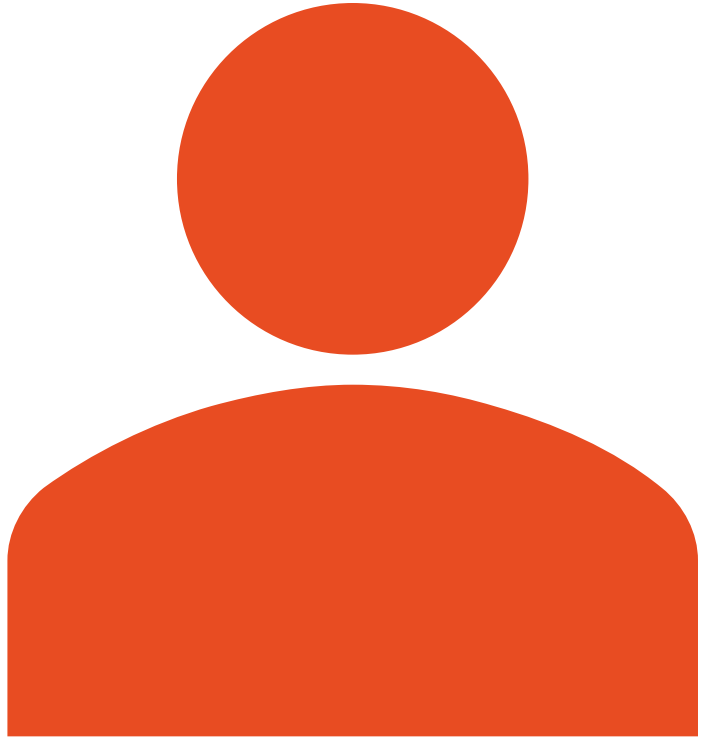
Persistence – T1505.003 - Offensive

- Monitor web server access logs for unusual HTTP requests or patterns, such as those accessing unusual file paths or making unexpected POST requests, which may indicate web shell activity.
- Check for HTTP error codes (e.g., 404, 500) that could be associated with web shell uploads or execution.
- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Access)
- FIM

Persistence – T1505.003 - Detection

Privilege Escalation

- T1543.003 Windows Service
- T1053.003 Cron
- T1053.005 Schedule Task



Defense Evasion

- T1562.004 Disable or modify system firewall
- Emulation
- Search for events with Event ID 5031 (Windows Firewall blocked an application from accepting incoming connections) and other firewall-related Event IDs in Splunk. Ensure that your systems are logging firewall configuration changes and forwarding these logs to your Splunk instance. For Windows systems, you can use Sysmon Event ID 17 (Rule-Level Policy Change) and Event ID 4870 (Change to firewall exception list).

- T1562.004 is a technique under the MITRE ATT&CK framework that involves disabling or modifying system firewalls for malicious purposes. A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Adversaries may disable or modify firewall settings to weaken the security posture of a system, allowing unauthorized access or data exfiltration.
- Disabling the firewall
- Modifying firewall rules
- Bypassing firewall restrictions
- Emulation

Defense Evasion – T1562.004 - Offensive

- Sysmon Event IDs:
- Event ID 12 (Registry Event)
- Event ID 1 (Process Creation)
- Windows Firewall Logs:
- Event ID 4948 (Change in Firewall Settings)
- Event ID 4950 (Windows Firewall Settings were restored)
- Firewall Logs
- FIM

Defense Evasion – T1562.004 - Detection

- T1562.003 is a technique under the MITRE ATT&CK framework that involves impairing command history logging for malicious purposes. Command history logging is a feature of many operating systems and applications that records commands executed by users or processes. Adversaries may attempt to disable, modify, or delete command history logs to hinder forensic analysis and hide their actions during an intrusion.
- Disabling logging
- Modifying log settings
- Clearing or deleting logs
- Emulation

Defense Evasion – T1562.003 - Offensive

- Sysmon Event IDs:
- Event ID 12 (Registry Event)
- Event ID 1 (Process Creation)
- Windows Firewall Logs:
- Event ID 1102 (Audit Log Cleared)
- Event ID 4719 (System Audit Policy Changed)
- FIM

Defense Evasion – T1562.003 - Detection

- T1070.001 is a technique under the MITRE ATT&CK framework that involves clearing Windows logs for malicious purposes. Windows logs record various events and activities on a system, including user actions, process execution, and network connections. Adversaries may attempt to clear Windows logs to hinder forensic analysis and hide their actions during an intrusion.
- Clearing specific log entries
- Clearing entire log files
- Modifying log settings
- Emulation

Defense Evasion – T1070.001 - Offensive

- Sysmon Event IDs:
- Event ID 12 (Registry Event)
- Event ID 1 (Process Creation)
- Windows Firewall Logs:
- Event ID 1102 (Audit Log Cleared)
- Event ID 4719 (System Audit Policy Changed)

Defense Evasion – T1070.001 - Detection

- T1070.004 is a technique under the MITRE ATT&CK framework that involves file deletion for malicious purposes. File deletion is the process of removing a file from a file system, making it no longer accessible to users or applications. Adversaries may delete files to hinder forensic analysis, hide their actions, or remove evidence of their presence on a system.
- Removing malware artifacts
- Cleaning up post-exploitation
- Obfuscating data exfiltration
- Disrupting system functionality
- Emulation

Defense Evasion – T1070.004 - Offensive

- Sysmon Event IDs:
- Event ID 23 (File Delete)
- Event ID 1 (Process Creation)
- Windows Firewall Logs:
- Event ID 4663 (Object Access)
- Event ID 4660 (Object Access Attempt)
- FIM

Defense Evasion – T1070.004 - Detection

- T1070.006 Timestomp is a technique under the MITRE ATT&CK framework that involves modifying file timestamps to hide new or changes to existing files. Adversaries may manipulate file timestamps, such as the modified, accessed, created, and changed times, to make it more difficult for defenders to identify malicious activity and reconstruct the sequence of events during an intrusion.
- Altering file timestamps to match those of legitimate files
- Masking file creation or modification dates
- Obfuscating data exfiltration
- Emulation

Defense Evasion – T1070.006 - Offensive

- Sysmon Event IDs:
- Event ID 2 (File Creation Time Changed)
- Event ID 3 (Network Connections)
- Windows Firewall Logs:
- Event ID 5145 (File Creation Time Modified)
- FIM

Defense Evasion – T1070.006 - Detection

- T1112 Modify Registry is a technique under the MITRE ATT&CK framework that involves modifying the Windows Registry to hide malicious activity, establish persistence, or disrupt system functionality. The Windows Registry is a hierarchical database that stores system settings, configuration information, and user preferences. Adversaries may add, modify, or delete registry keys and values to achieve their objectives.
- Altering system settings
- Establishing persistence
- Disrupting system functionality
- Emulation

Defense Evasion – T1112 - Offensive

- Sysmon Event IDs:
- Event ID 2 (File Creation Time Changed)
- Event ID 1 (Process Creation)
- Windows Firewall Logs:
- Event ID 4657 (Registry Value Changed)
- Event ID 4663 (Object Access Attempt)

Defense Evasion – T1112 - Detection

- T1027.002 Software Packing is a technique under the MITRE ATT&CK framework that involves packing malicious software, such as malware payloads or malicious executables, to evade detection by security tools. Software packing is a method of compressing or encrypting executable code, which makes it more difficult for antivirus software and other security tools to analyze the code and identify potential threats.
- Obfuscating malware payloads
- Packing malicious executables
- Bypassing security controls
- Delaying code execution
- Emulation

Defense Evasion – T1027.002 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Process Image Loaded)
- Windows Firewall Logs:
- Event ID 4688 (Process Creation)

Defense Evasion – T1027.002 - Detection

- T1218.001 Compiled HTML File is a technique under the MITRE ATT&CK framework that involves using Compiled HTML (CHM) files for malicious purposes. CHM files are executable files that contain compressed HTML, JavaScript, and other web-based content. Adversaries may use CHM files to execute code or deliver malware payloads while evading detection by security tools.
- Delivering malware payloads
- Obfuscating malicious code
- Bypassing security controls
- Delivering malicious documents
- Emulation

Defense Evasion – T1218.001 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Process Image Loaded)
- Windows Firewall Logs:
- Event ID 4688 (Process Creation)

Defense Evasion – T1218.001 - Detection

- T1218.011 Rundll32 is a technique under the MITRE ATT&CK framework that involves using the rundll32.exe process to execute code or load DLLs. rundll32.exe is a legitimate Windows program that can be used to run DLL files as if they were executables. Adversaries may abuse rundll32.exe to execute malicious code or load malicious DLLs while evading detection by security tools.
- Executing malicious code
- Loading malicious DLLs
- Bypassing security controls
- Obfuscating malware artifacts
- Emulation

Defense Evasion – T1218.011 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 7 (Process Image Loaded)
- Windows Firewall Logs:
- Event ID 4688 (Process Creation)

Defense Evasion – T1218.011 - Detection

- T1110 Brute Force is a technique under the MITRE ATT&CK framework that involves guessing the password or passphrase of a user, system, or service by trying a large number of possibilities. Brute force attacks can be conducted using various methods, such as dictionary attacks (using common passwords or phrases) or generating all possible combinations of characters until the correct credentials are found.
- Password spraying
- Credential stuffing
- Emulation

Credential Access– T1110 - Offensive

- Sysmon Event IDs:
- Event ID 12 (Logon Attempt Failed)
- Event ID 10 (Process Terminated)
- Windows Firewall Logs:
- Event ID 4625 (Logon Failure)
- Event ID 4624 (Logon Success)
- Web Application logs

Credential Access– T1110- Detection

- T1056.001 Keylogging is a technique under the MITRE ATT&CK framework that involves capturing and recording user keystrokes to obtain sensitive information, such as credentials, financial data, or other confidential information. Keylogging can be achieved through hardware or software-based methods and is often used by adversaries to collect valuable data for further exploitation.
- Malware-based keylogging
- Hardware keyloggers
- Browser-based keylogging
- Social engineering
- Emulation

Credential Access– T1056.001 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Firewall Logs:
- Event ID 4688 (Process Creation)
- Event ID 7045 (Service Installation)

Credential Access– T1056.001- Detection

- T1217 Browser Information Discovery is a technique under the MITRE ATT&CK framework that involves gathering information about a user's web browser, such as browser type, version, plugins, and preferences. Adversaries may use this information to tailor their attacks or exploit known vulnerabilities in specific browser configurations.
- JavaScript fingerprinting
- Web server logs
- Social engineering
- Emulation

Discovery– T1217 - Offensive

- Web application logs
- Network Traffic logs
- Antivirus logs & EDR logs
- Proxy logs

Discovery– T1217- Detection

- T1135 Network Share Discovery is a technique under the MITRE ATT&CK framework that involves adversaries identifying and enumerating network shares on a system or within a network. Network shares are resources (such as directories or files) that are accessible over a network, typically using the Server Message Block (SMB) or Common Internet File System (CIFS) protocols. Adversaries may use this technique to map out network resources and look for sensitive information or potential targets for further attacks.
- Using built-in operating system tools
- Network scanning tools
- Malicious scripts
- Emulation

Discovery– T1135 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 3 (Network Connection)
- Windows Event Logs:
- Event ID 5140 (Network Share Object Accessed)
- Network Traffic Analysis
- Antivirus and EDR logs

Discovery– T1135- Detection

- T1057 Process Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to obtain information about running processes on a system. This information can help attackers understand the system's configuration, identify potential targets for further attacks, or find ways to blend in with normal system activity to avoid detection.
- Using built-in operating system tools
- Malicious scripts
- Emulation

Discovery– T1057 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4689 (Process Termination)
- Antivirus and EDR logs

Discovery– T1057- Detection

- T1518.001 Security Software Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to identify and enumerate security software installed on a system or within a network. This information can help attackers understand the defensive capabilities of their targets and devise strategies to bypass or disable security measures.
- Using built-in operating system tools
- Malicious scripts
- System calls and API queries
- Emulation

Discovery- T1518.001 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4697 (Service Installed)
- Antivirus and EDR logs

Discovery– T1518.001- Detection

- T1082 System Information Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to gather information about a target system's hardware, software, and network configuration. This information can help attackers understand the environment and identify potential vulnerabilities or areas to exploit.
- Using built-in operating system tools
- Malicious scripts
- System calls and API queries
- Emulation

Discovery– T1082 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4697 (Service Installed)
- Antivirus and EDR logs

Discovery - T1082 - Detection

- T1049 System Network Connections Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to gather information about active network connections on a system. This information can help attackers understand the network environment, identify potential targets, or look for opportunities to pivot within the network.
- Using built-in operating system tools
- Malicious scripts
- System calls and API queries
- Emulation

Discovery– T1049 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 3 (Network Connection)
- Windows Event Logs:
- Event ID 5156 (Windows Filtering Platform Connection)
- Antivirus and EDR logs

Discovery – T1049 - Detection

- T1049 System Network Connections Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to gather information about active network connections on a system. This information can help attackers understand the network environment, identify potential targets, or look for opportunities to pivot within the network.
- Using built-in operating system tools
- Malicious scripts
- System calls and API queries
- Emulation

Discovery– T1049 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 3 (Network Connection)
- Windows Event Logs:
- Event ID 5156 (Windows Filtering Platform Connection)
- Antivirus and EDR logs

Discovery – T1049 - Detection

- T1033 System Owner/User Discovery is a technique under the MITRE ATT&CK framework that involves adversaries attempting to gather information about the owner or users of a system. This information can help attackers understand the system's context, identify potential targets for social engineering or credential theft, or gain insight into the privileges and access levels associated with the users.
- Using built-in operating system tools
- Malicious scripts
- System calls and API queries
- Emulation

Discovery– T1033 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Event Logs:
- Event ID 4648 (Logon Attempt)
- Event ID 4624 (Logon Success)
- Antivirus and EDR logs

Discovery – T1033 - Detection

- RDP Hijacking is a technique under the MITRE ATT&CK framework that involves adversaries attempting to take control of a legitimate Remote Desktop Protocol (RDP) session to gain unauthorized access to a system. This technique leverages the lack of security measures or misconfigurations in RDP implementations, allowing attackers to hijack active sessions without needing to authenticate themselves.
- Session takeover
- Network sniffing
- Social engineering and phishing
- Emulation

Lateral Movement– T1563.002 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 3 (Network Connection)
- Windows Event Logs:
- Event ID 21 (Remote Desktop Services: Session logon succeeded)
- Event ID 4624 (Logon Success)
- Event ID 4625 (Logon Failure)
- Event ID 4778 (logon RDP)
- Event ID 4779 (logoff RDP)
- Antivirus and EDR logs

Lateral Movement– T1563.002 - Detection

- T1115 Clipboard Data is a technique under the MITRE ATT&CK framework that involves adversaries abusing the clipboard functionality to steal or manipulate sensitive information. The clipboard is a temporary storage area used to store copied data, such as text, images, or files, for easy transfer between applications. Attackers may target the clipboard to obtain credentials, intercept data, or insert malicious content.
- Data theft
- Malicious content injection
- Clipboard hijacking
- Emulation

Collection- T1115 - Offensive

- Sysmon Event IDs:
- Event ID 13 (Clipboard Changed)
- Windows Event Logs:
- Antivirus and EDR logs

Collection– T1115 - Detection

- T1005 Data from Local System is a technique under the MITRE ATT&CK framework that involves adversaries collecting data from a local system to gather information about the target environment or facilitate further attacks. This technique encompasses various sub-techniques, such as querying system information, collecting file and directory listings, or reading configuration files.
- System information collection
- File and directory listing
- Configuration file access
- Emulation

Collection– T1005 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 10 (Process Terminated)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4656 (File Access)
- Antivirus and EDR logs

Collection– T1005 - Detection

- T1071.001 Web Protocols is a technique under the MITRE ATT&CK framework that involves adversaries using standard web protocols, such as HTTP(S), to communicate with command and control (C2) servers or exfiltrate data. This technique leverages common web traffic to blend in with regular network activity and evade detection.
- C2 communication
- Data exfiltration
- Tunneling and proxies
- Emulation

C2- T1071.001 - Offensive

- Network Traffic Analysis
- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 3 (Network Connection)
- Proxy and firewall logs
- Web server and web application logs

C2- T1071.001 - Detection

- T1105 Ingress Tool Transfer is a technique under the MITRE ATT&CK framework that involves adversaries transferring tools or other files from an external system into a compromised network or host. This technique allows attackers to bring in additional tools, malware, or utilities to facilitate further attacks or maintain persistence within the target environment.
- File downloads
- Email attachments
- Exploit kits
- Lateral movement
- Emulation

C2- T1105 - Offensive

- Sysmon Event IDs:
- Event ID 1 (Process Creation)
- Event ID 11 (File Creation)
- Event ID 13 (File Update)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4656 (File Access)
- Antivirus and EDR logs
- Network Traffic Analysis
- Email Security solutions

C2- T1105 - Detection

- T1485 Data Destruction is a technique under the MITRE ATT&CK framework that involves adversaries deliberately destroying or manipulating data on a target system or network. This technique is often used to disrupt business operations, impair system functionality, or conceal an attacker's activities during an intrusion.
- File deletion
- Disk wiping
- Encryption and ransomware
- Data corruption
- Emulation

Impact- T1485 - Offensive

- Sysmon Event IDs:
- Event ID 23 (File Delete)
- Event ID 2 (File Creation Time Modified)
- Windows Event Logs:
- Event ID 4663 (File Access)
- Event ID 5140 (Network Share Object Access)
- Antivirus and EDR logs
- Backup & recovery monitoring

Impact- T1485 - Detection

- T1486 Data Encrypted for Impact is a technique under the MITRE ATT&CK framework that involves adversaries encrypting data on a target system or network to disrupt system operations, render data inaccessible, or pressure victims into complying with their demands. This technique often involves ransomware, where attackers encrypt data and demand payment in exchange for the decryption key.
- Ransomware attacks
- Targeted data encryption
- Supply chain attacks
- Emulation

Impact- T1486 - Offensive

- Sysmon Event IDs:
- Event ID 2 (File Creation Time Modified)
- Event ID 11 (File Create)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Event ID 4656 (File Access)
- Antivirus and EDR logs
- Backup & recovery monitoring
- Network Traffic Analysis

Impact- T1486 - Detection

- T1565.003 Runtime Data Manipulation is a technique under the MITRE ATT&CK framework that involves adversaries manipulating data during the runtime of a process or application to gain unauthorized access, elevate privileges, or conceal their actions. This technique can be achieved through memory injection, function hooking, or other forms of runtime modification.
- Memory injection
- Function hooking
- DLL injection
- API hooking
- Emulation

Impact- T1565.003 - Offensive

- Sysmon Event IDs:
- Event ID 7 (Process Access)
- Event ID 8 (CreateRemoteThread)
- Windows Event Logs:
- Event ID 4688 (Process Creation)
- Antivirus and EDR logs
- Memory Forensic
- Code Integrity Monitoring

Impact- T1565.003 - Detection

- T1565.001 Stored Data Manipulation is a technique under the MITRE ATT&CK framework that involves adversaries manipulating stored data on a target system or network to gain unauthorized access, elevate privileges, or conceal their actions. This technique can be achieved through file manipulation, database tampering, or other forms of stored data modification.
- File tampering
- Registry key modification
- Configuration file alteration
- Emulation

Impact- T1565.001 - Offensive

- Sysmon Event IDs:
- Event ID 2 (File Creation Time Modified)
- Event ID 11 (File Create)
- Event ID 13 (File Update)
- Windows Event Logs:
- Event ID 4663 (File Access)
- Event ID 4657 (Registry Value Modified)
- Antivirus and EDR Logs
- Database Logs

Impact- T1565.001 - Detection

- T1565.002 Transmitted Data Manipulation is a technique under the MITRE ATT&CK framework that involves adversaries manipulating data during transmission on a target system or network to gain unauthorized access, elevate privileges, or conceal their actions. This technique can be achieved through network traffic manipulation, protocol manipulation, or other forms of data tampering during transmission.
- Network traffic interception and modification
- Protocol manipulation
- Man-in-the-Middle (MitM) attacks
- Emulation

Impact- T1565.002 - Offensive

- Sysmon Event IDs:
- Event ID 3 (Network Connect)
- Event ID 22 (DNS Query)
- Windows Event Logs:
- Event ID 5157 (IPsec Security Association Negotiation)
- Event ID 5061 (Cryptographic Operation)
- Network Traffic Analysis
- IDS/IPS and Firewall Logs

Impact- T1565.002 - Detection

- T1529 System Shutdown / Reboot is a technique under the MITRE ATT&CK framework that involves adversaries shutting down or rebooting systems on a target network to interrupt business operations, impede security controls, or facilitate other attack techniques. This technique can be achieved through direct system commands, exploiting vulnerabilities, or leveraging compromised credentials.
- Manual shutdown or reboot
- Exploiting vulnerabilities
- Leveraging malware or ransomware
- Using remote management tools
- Emulation

Impact- T1529 - Offensive

- Sysmon Event IDs:
- Event ID 10 (Process Access)
- Event ID 12 (Process Terminate)
- Windows Event Logs:
- Event ID 1074 (System Shutdown)
- Event ID 6006 (Event Log Shutdown)
- Antivirus and EDR Logs
- Network Traffic Analysis

Impact- T1529 - Detection

14. Red Team Roadmap

- Basic knowledge on Os,Network
- Automation
- MTRE Attack
- Pen200, Pen300
- Sec565
- ...

https://github.com/soheilsec/Red-Team-Roadmap

15.Red Team Interview

https://github.com/soheilsec/RedTeam-Interview

16.Any Question?