MITRE

- research in cybersecurity, artificial intelligence, health informatics, space security
- US based non-profit Corporation
- some projects are
    - ATT&CK (Adversarial Tactics, Techniques and Common Knowledge)
    - CAR (Cyber Analytics Repository) Knowledge Base
    - ENGAGE
    - D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)
    - AEP (ATT&CK Emulation Plans)

BASIC TERMINOLOGY

- APT (Advanced Persistent Threat) - team or country that engages in long term attacks against organizations or countries

    - not called advanced due to superweapon/zero day exploit
    - techniques used are common and can be detected using right implementations
    - APT28 (FancyBear) - Russia's GRU
    - APT33 (Elfin) - Iranian group
    - APT34 (OilRig) - Iranian group

- TTP - Tactics, Techniques, Procedures

    - Tactic - adversary's goal or objective
    - Technique - how adversary achieves goal
    - Procedure - how technique is executed

ATT&CK FRAMEWORK

- globally-accessible knowledge base of adversary tactics and techniques based on real-world observations
- due to need to document common TTPs and APTs used against enterprise Windows networks
- started with internal project known as FMX (Fort Meade Experiment)
    - security professionals asked to emulate TTPs against network and collect data from the attack on the network
    - used to create ATT&CK Framework
- initially focused on Windows but now covers macOS and Linux
- contributed by security researchers and intelligence reports
- useful for both red and blue teamers
- 14 stages
    - Reconnaisance - gathering target information (scanning, social engineerin)
    - Resource Development - acquiring infrastructure tools and credentials
    - Initial Access - gaining entry (phishing, exploits, credential theft)
    - Execution - running malicious code on target
    - Persistence - maintaining access through backdoors (rootkits)
    - Privilege Escalation - gaining higher privileges within system

    - Defense Evasion - avoid detection using obfuscation and disabling security tools
    - Credential Access - stealing passwords, hashes
    - Discovery - learn about network, users, security measures used
    - Lateral Movement - expand access to multiple systems
    - Collection - gather sensitive data from compromised systems
    - Command and Control - establish remote control over network
    - Exfiltration - Transferring stolen data
    - Impact - disrupting, modifying, destroying systems
- MITRE ATT&CK Navigator - used for basic navigation and annotation of ATT&CK matrices

CAR KNOWLLEDGE BASE

- knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model
- provides analytics for identifying TTPs used by attackers
    - Analytics - predefined detection rules for identifying suspicious activities based on logs
    - Mapping to ATT&CK - links each analytic to specific ATT&CK technique
    - Provides pseudocode or structured queries to implement detection in SIEM (Splunk)
    - defines log sources required for detection (Sysmon, Windows Event Logs)
- full analytic list to see what implementations are available for any analytic
- eg. Scheduled Task - FileAccess

MITRE ENGAGE

- framework for active cyber defense focusing on adversary engagement through deception and manipulation
    - prepare - prepare and deploy deception techniques to mislead attackers
    - expose - identify adversaries when they interact with the deception
    - affect - perform action with negative impact on the attackers operations
    - elicit - gather intelligence about the attackers TTPs
    - understand - the outcomes of the operational activities

MITRE D3FEND

- knowledge graph of cybersecurity countermeasures
- currently in beta
- funded by Cybersecurity Directorate of NSA
- eg. Decoy File

MITRE ATT&CK EMULATION PLANS

- Center of Threat-Informed Defense (CTID)
    - various companies and vendors across globe
    - conduct research on cyber threats and their TTPs and share research to improve cyber defense
    - Verizon, Splunk, Microsoft (founder), Red Canary (founder), AttackIQ (founder)
- Adversary Emulation Library and ATT&CK Emulation Plans

    - public library of free emulation plans for blue/red teamers
    - contribution from CTID
    - step by step guide to mimic specific threat group

THREAT INTELLIGENCE

- information or TTPs attributed to adversary
- use TI for better decision making regarding defense strategy
- teams in organizations dedicated to gathering TI for others teams in organization
- can be open source or through subscription with vendor like CrowdStrike
- goal is to make TI actionable

YARA

- help researchers identify and classify malware samples
- create descriptions of malware families based on textual or binary patterns
    - a rule; consists of set of strings a boolean expression which determines logic
- typical yara command contains
    - the rule file (myrule.yar)
    - target file (file, directory, process)
    - yara myrule.yar somedirectory
- every yara rule has a name and condition
    - the rule describes patterns to search for in files, directories, processes
    - rule examplerule { condition: true }
    - name : examplerule
    - condition - true
    - Simply, the rule we have made checks to see if the file/directory/PID that we specify exists via condition: true. If the file does exist, we are given the output of examplerule

YARA Keywords

- Meta - reserved for descriptive information by author of rule
    - desc - short for description, summarize what your rule checks for
    - like commenting code
- Strings - usign strings to search for specific text or hexadecimal in files or programs
    - case sensitive

```
rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"

    condition:
        $hello_world
}
```

```
rule helloworld_checker{
    strings:
        $hello_world = "Hello World!"
        $hello_world_lowercase = "hello world"
        $hello_world_uppercase = "HELLO WORLD"

    condition:
        any of them
}
```

CONDITIONS

- <= or >= or != can be used
- condition : #hello_world <= 10
    - matches if there are less than or equal to ten occurrences of the "Hello World"
- and, not, or
    - to combine multiple conditions
    - condition : $hello_world and filesize < 10KB

YARA TOOLS

- LOKI - open-source IOC (Indicator of Compromise) scanner
    - File Name IOC Check - scans files for names that match known IOCs as malicious software often uses specific file names
    - Yara Rule Check - use Yara rules to scan files for patterns or signautres associated with malware
    - Hash Check - compare file hashes against database of known malicious hashes
    - C2 Back Connect Check - detect attempts made by compromised systems to connect to external C2 serers
- THOR - multi-platform IOC and YARA scanner
    - precompiled for Windows, Linux and macOS
    - scan throttling to prevent excessive CPU usage
- FENRIR - address limitations of previous tools

    - bash script tool
    - works on any system supporting bash including Windows

- YAYA - Yet Another Yara Automation

    - open source tool for managing YARA rule repoisitories
    - allows users to import, modify, disable rules and scan files with custom/existing YARA rules

NOTE : IOCs - hashes, IP addresses, domain names, etc

- typically we need to add our own rules based on our Threat Intelligence from incident response engagement

    - Yara has rules we can use to start scanning for evil straightaway

- yarGen - tool that helps generate YARA rules for detecting malware by removing strings from suspicious files and removing common goodware strings to reduce false positives

- yarAnalyzer - another tool for analyzing and refining YARA rules

- Valhalla - online Yara feed; collection of thousands of hand-crafted high quality YARA rules for enhanced detection

    - users can search based on
        - keywords
        - tags
        - ATT&CK techniques
        - SHA-256 hashes
        - rule names
    - centralized repository of YARA rules
        - easier to identify suspicious activity with community driven rules

ZERO LOGON

- allowed an attacker to go from zero to domai admin in one minute

    - dubbed zero logonPP

- statistics based attack

- abuses feature within MS-NRPC (Microsoft NetLogon Remote Protocol)

    - authentication component of Active Directory for User and Machine accounts
    - focuses on poor implementation of cryptographu
    - Microsoft chose AES-CFB* for ComputeNetlogonCredential
        - this is usually fine but they hardcoded Initialization Vectort to use all zeroes instead of random string
        - a message of all zeroes and IV zero has 1/256 of having ciphertext as zero

- machine accounts - 64+ alphanumeric password, difficult to break into

    - no lockout attempts
    - not meant for end user access
    - can use Mimikatz to dump password but at this point we want persistence not lateral movement

- by abusing ZeroLogon, you can bypass Domain Controller's machine account and extract credentials

- steps in exploiting zero logon vulnerability

    - client sends NetServerReqChallenge to Domain Controller
        - DC
        - target (which is also DC)
        - nonce (16 bytes of zero)
    - server receives and generates its own nonce called server challenge and send it back
    - client computes netlogon credentials with server challenge using NetServerAuthenticate3
    - server validates authentication request
    - if calculation matches, responds with required info
        - repeated till it works (1/256 chance)