Distinguishing Threat Actors, Vectors, and Intelligence Sources

Module Overview

Actors and threats

Attributes of actors

Vectors

Threat intelligence sources

Research sources

Covered Topics

Actors and threats

- Advanced persistent threat (APT)
- Insider threats
- State actors
- Hacktivists
- Script kiddies
- Criminal syndicates
- Hackers
  - White hat
  - Black hat
  - Gray hat
- Shadow IT
- Competitors

Attributes of actors

- Internal/external
- Level of sophistication/capability
- Resources/funding
- Intent/motivation

Vectors

- Direct access
- Wireless
- Email
- Supply chain
- Social media
- Removable media
- Cloud

Threat intelligence sources

- Open source intelligence (OSINT)
- Closed/proprietary
- Vulnerability databases
- Public/private information sharing centers
- Dark web
- Indicators of compromise
- Automated indicator sharing (AIS)
- Structured threat information exchange (STIX)/Trusted automated exchange of indicator information (TAXII)
- Predictive analysis
- Threat maps
- File/code repositories

Research sources

- Vendor websites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for comments (RFC)
- Local industry groups
- Social media
- Threat feeds
- Adversary tactics, techniques, and procedures (TTP)

Types of Actors

Threat Actors can range from beginners probing around to highly-organized nation states

- Script Kiddies
- Hacktivists
- Organized Crime
- Nation States/APT
- Insiders
- Competitors

Script Kiddies

Hackers that are relatively new or unskilled

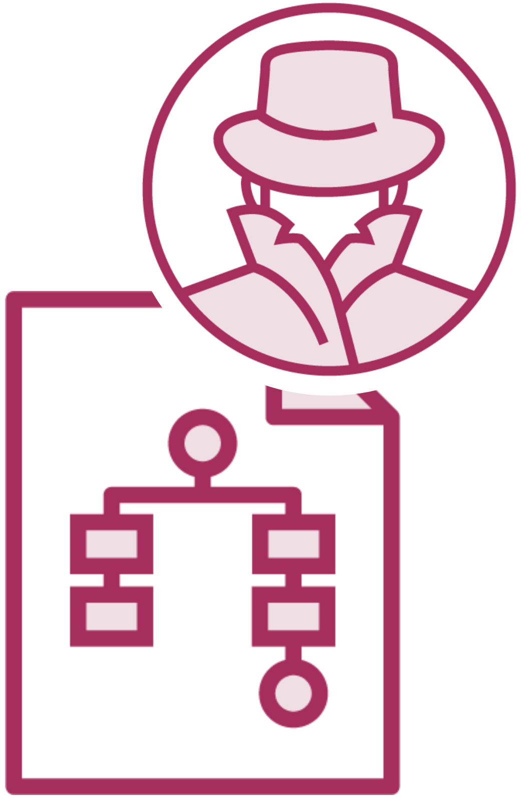
- Typically looking to see what they can get into
- The challenge is the attraction
- Not typically associated with any organized hacking groups
- Usually not well funded

Hacktivists

Hackers who are motivated by ideology or some social/political cause

- Can be well funded and skilled
- Usually deface websites
- Steal information
  - Personal information and credentials
- DDoS
- Not particularly patient or stealthy

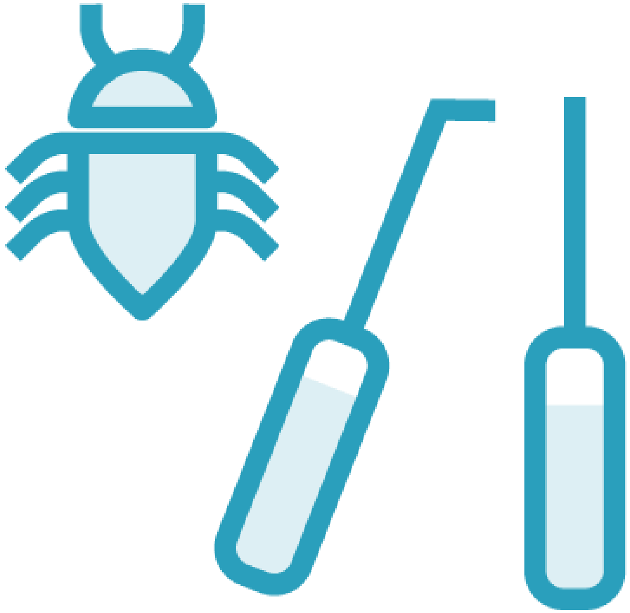
Organized Crime



Hackers who are motivated by financial gain

- Deliberate with high technical capability
- Well-funded
- Patient and persistent
- POS terminals, ATM machines, credit card numbers, etc
- Steal personal information for sale on the dark web

Nation States/APT



Highly skilled hackers whose main goal is to penetrate government or commercial systems

- Cyber espionage
- Data/IP theft
- Sabotage
- Cyber warfare

Very stealthy and persistent, well funded and connected

Insiders

Often motivated by financial gain

- CERT advises that over 70% of IP theft cases involve insiders
- Accidental exposure can occur from misuse or misconfigured systems
- Data theft includes IP and company secrets

Competitors

Motivated by financial gain

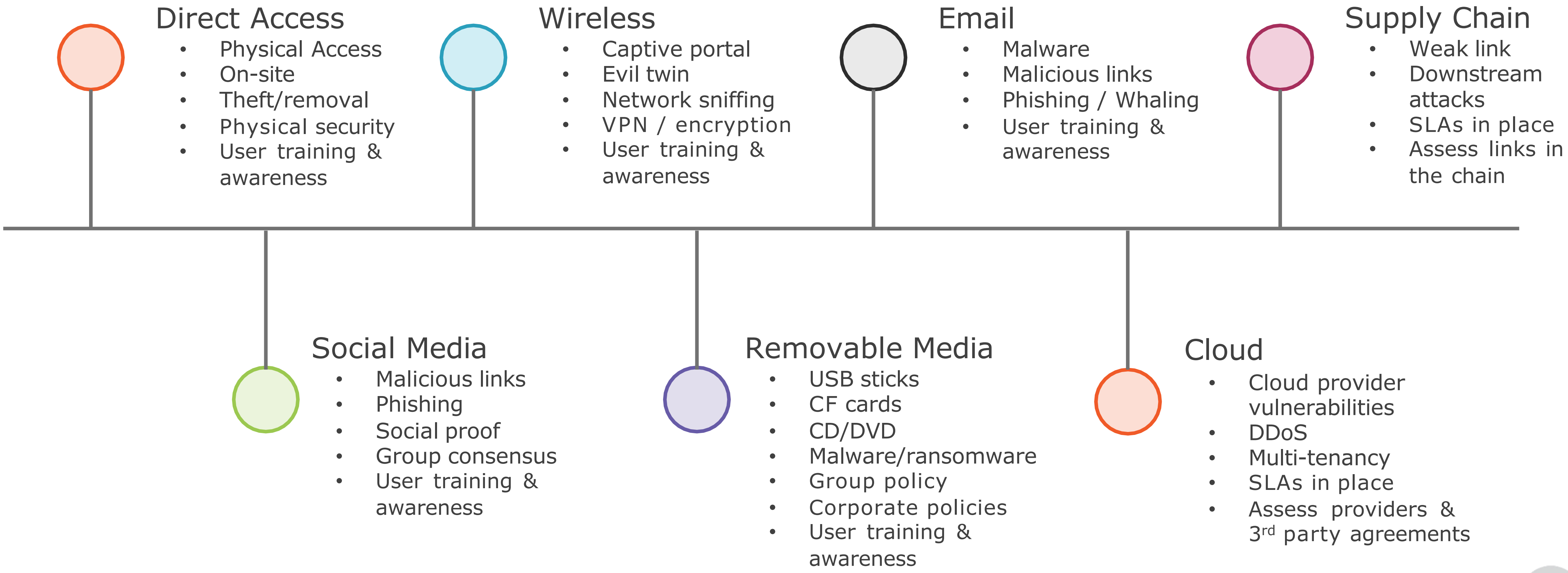
- Competitive advantage
- Theft of IP or company secrets
- Sabotage

Can be well funded and range from low to high skill

Threat Actor Attributes

Actor Type	Internal / External	Level of Sophistication	Resources / Funding	Intent / Motivation
Script Kiddies	External	Low	Low	Curiousity
Hacktivist	External	Medium to High	Medium to High	Ideological
Organized Crime	External	High	High	Financial Gain
Nation States / APT	External	High	High	Espionage
Insiders	Internal	Low to High	Low to High	Financial Gain
Competitors	External	Low to High	Low to High	Competitive Advantage, Financial Gain

Attack Vectors



Direct Access

- Physical Access
- On-site
- Theft/removal
- Physical security
- User training & awareness

Social Media

- Malicious links
- Phishing
- Social proof
- Group consensus
- User training & awareness

Wireless

- Captive portal
- Evil twin
- Network sniffing
- VPN / encryption
- User training & awareness

Removable Media

- USB sticks
- CF cards
- CD/DVD
- Malware/ransomware
- Group policy
- Corporate policies
- User training & awareness

Email

- Malware
- Malicious links
- Phishing / Whaling
- User training & awareness

Cloud

- Cloud provider vulnerabilities
- DDoS
- Multi-tenancy
- SLAs in place
- Assess providers & 3rd party agreements

Supply Chain

- Weak link
- Downstream attacks
- SLAs in place
- Assess links in the chain

Use of Open Source Intelligence

There are numerous tools and websites available for intelligence gathering and reconnaissance. Open Source Intelligence (OSINT) tools exist as stand-alone applications, browser plugins and websites and can be passive or active in nature.

- Maltego
- Metagoofil
- Shodan
- Google Hacking Database (GHDB)
- FOCA
- EXIF Data Viewers
- BackTrack Linux
- Buscador Linux
- Kali Linux
- Social Engineer Toolkit
- PeekYou
- Lullar
- Wayback Machine
- YouGetSignal
- Browser Plugins
- Metasploit
- Spokeo

Closed / Proprietary Intelligence

Commercial sources

- Typically not available to the public at large
- Part of a software package and/or service
- Often has SIEM integration SOAR capabilities built-in

Vulnerability Databases

Google Hacking Database (GHDB)

- www.exploit-db.com

VirusTotal

- www.virustotal.com

NVD (National Vulnerability Database)

- nvd.nist.gov

MITRE CVE database

- cve.mitre.org

Public and Private Information Sharing

Cybersecurity Act of 2015

- Provided a framework for sharing of information between pubic and private sectors
- Goal of sharing information across both sectors to help strengthen defense and quicken response times

Information Sharing and Analysis Centers (ISACs)

National Cybersecurity and Communications Integration Center (NCCIC)

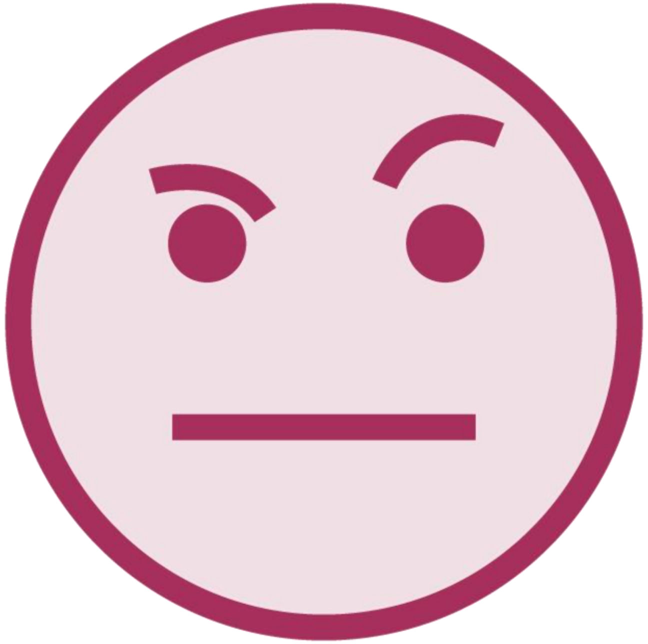
Dark Web

The "Dark Web" is an area of the internet not accessible via normal web browsers

Requires special software or applications:

- TOR (The Onion Router)
- TOR gateway (tor2web)
- I2P (Invisible Internet Project)

Indicators of Compromise (IOC)



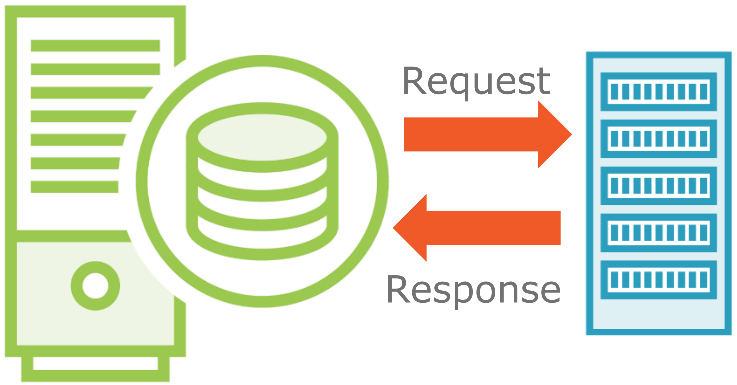
Pieces of data (breadcrumbs) that can identify potential malicious activity

- Common IOCs
  - Unusual outbound traffic
  - Unusual privileged account activity
  - Geographical anomalies
  - Suspicious registry or system file changes
  - Mismatched port-application traffic

Automated Indicator Sharing (AIS)

- Department of Homeland Security (DHS) free sharing service
  - Shares indicators between the federal government and private sector at machine speed
  - Participants connect to DHS managed systems at NCCIC
- All systems must be able to communicate using STIX and TAXII specifications

TAXII Layout



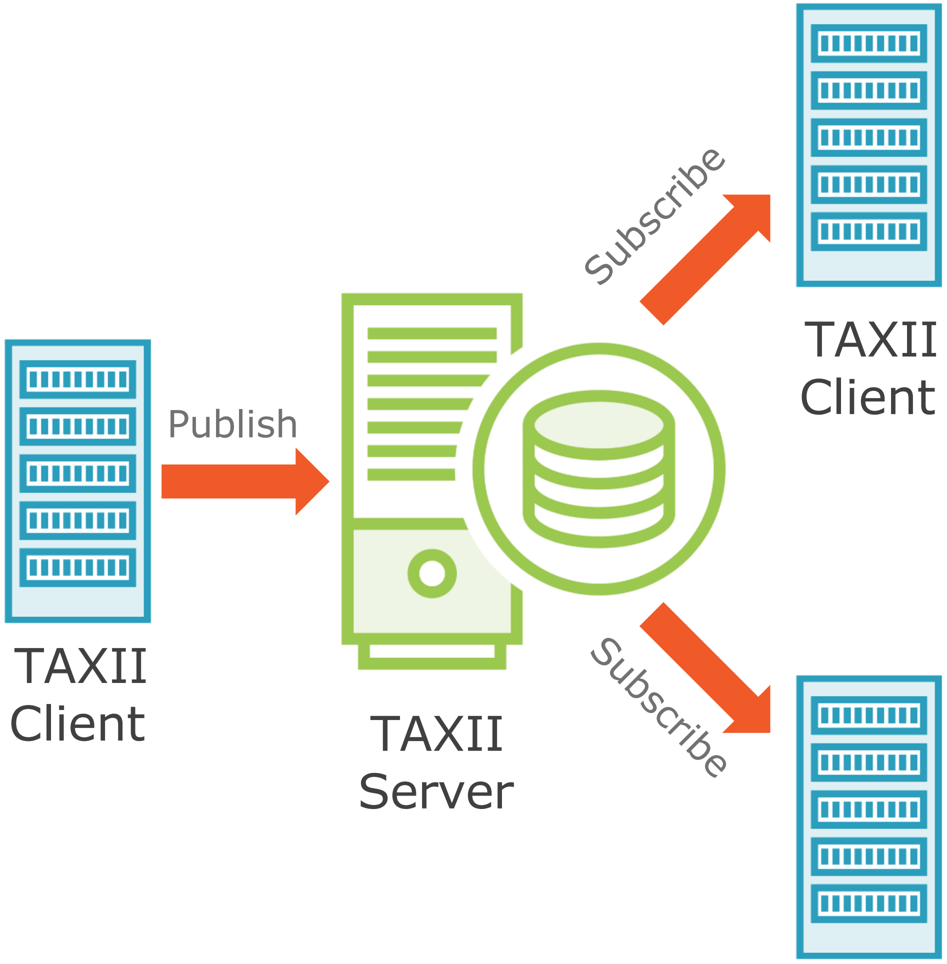
Request

Response

TAXII Server

TAXII Client

Collections



Publish

Subscribe

Subscribe

TAXII Client

TAXII Server

TAXII Client

TAXII Client

Channels

MITRE

MITRE is a not-for-profit organizations that manages federal funding for research projects across multiple agencies

- Common Vulnerabilities and Exposures (CVE) database
- Common Weakness Enumeration (CWE) database

MITRE ATT&CK Framework

Trusted Automated Exchange of Intelligence Information (TAXII™)

- Transport protocol that allows sharing of threat intelligence information over HTTPS using APIs

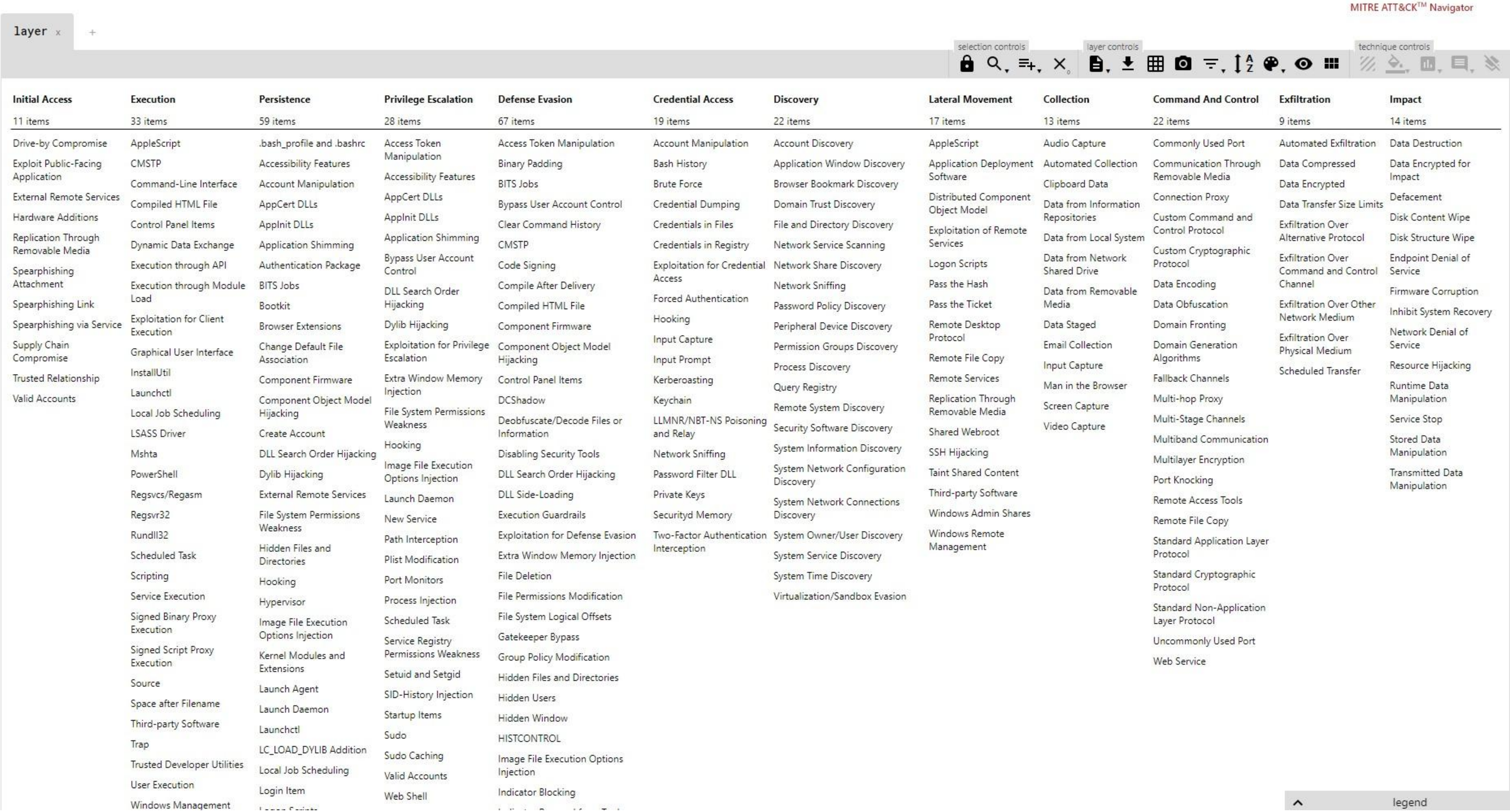
Structured Threat Information eXpression (STIX™)

- Standardized format for presenting threat intelligence information

MITRE ATT&CK™
Adversarial Tactics, Techniques and Common Knowledge

Tactic Categories (314 Tactics)

1. Initial access (11)
2. Execution (33)
3. Persistence (59)
4. Privilege escalation (28)
5. Defense evasion (67)
6. Credential access (19)
7. Discovery (22)
8. Lateral movement (17)
9. Collection (13)
10. Command and Control (22)
11. Exfiltration (9)
12. Impact (14)



Initial Access
11 items

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
33 items

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management

Persistence
59 items

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts

Privilege Escalation
28 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Plist Modification
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion
67 items

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools

Credential Access
19 items

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery
22 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
17 items

- AppleScript
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
22 items

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
9 items

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
14 items

- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

Predictive Analysis

AI and machine learning

- Provides proactive analysis to detect breaches before they occur
- Learning algorithms constantly monitor, learn and evolve to detect new and emerging threats

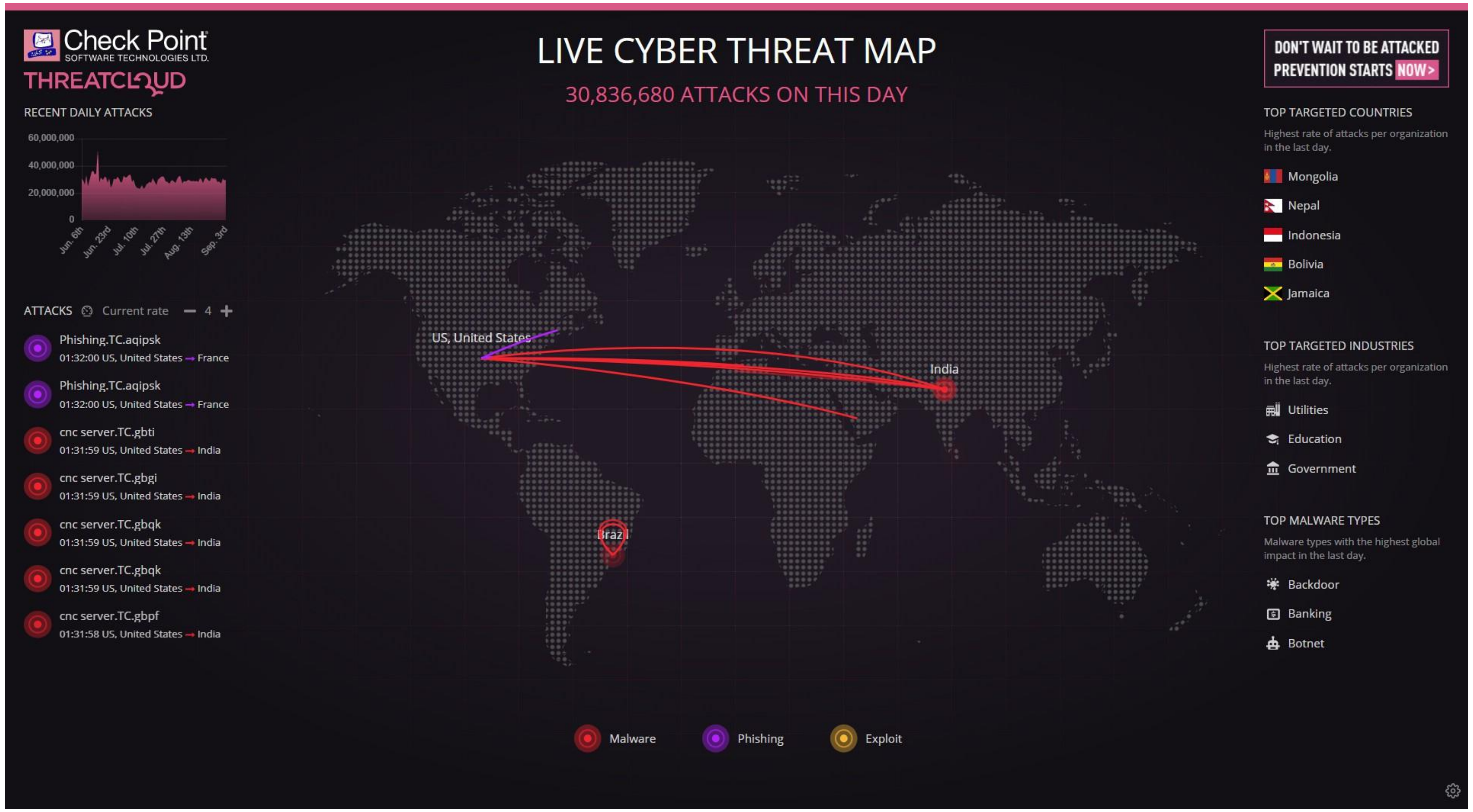
Threat Maps

Provide real-time monitoring of threats

- Type
- Origin / destination
- Threat level

Can be enriched with additional threat feeds / data

Localized for a specific company or industry, or global showing attacks worldwide



Check Point SOFTWARE TECHNOLOGIES LTD.

THREATCLOUD

LIVE CYBER THREAT MAP

30,836,680 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate − 4 +

Phishing.TC.aqipsk
01:32:00 US, United States → France

Phishing.TC.aqipsk
01:32:00 US, United States → France

cnc server.TC.gbti
01:31:59 US, United States → India

cnc server.TC.gbgi
01:31:59 US, United States → India

cnc server.TC.gbqk
01:31:59 US, United States → India

cnc server.TC.gbqk
01:31:59 US, United States → India

cnc server.TC.gbpf
01:31:58 US, United States → India

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Indonesia
- Bolivia
- Jamaica

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Utilities
- Education
- Government

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Backdoor
- Banking
- Botnet

● Malware ● Phishing ● Exploit

File/Code Repositories

GitHub is the most common

- Users/developers use GitHub as a repository for code version control
- Numerous GitHub repositories are not secured properly, leaking sensitive information

Bitbucket has similar offerings, more geared toward enterprise customers

Research Sources

- Vendor websites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for comments (RFC)
- Local industry groups
- Social media
- Threat feeds
  - Recorded Future
- Adversary tactics, techniques, and procedures (TTP)
  - MITRE ATT&CK

Module Review

Actors and threats

Attributes of actors

Vectors

Threat intelligence sources

Research sources