LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HPH-Sector Cyber Threat Actor Modeling with Mitre ATT&CK®

07/23/2020

Report #: 202007231030

Agenda

- Introduction
- Cyber Threat Modeling
- Overview of the Mitre ATT&CK® Framework
- Specific Cyber Threats to the HPH
- Threat Modeling with ATT&CK®
- Conclusion
- Reference Materials
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

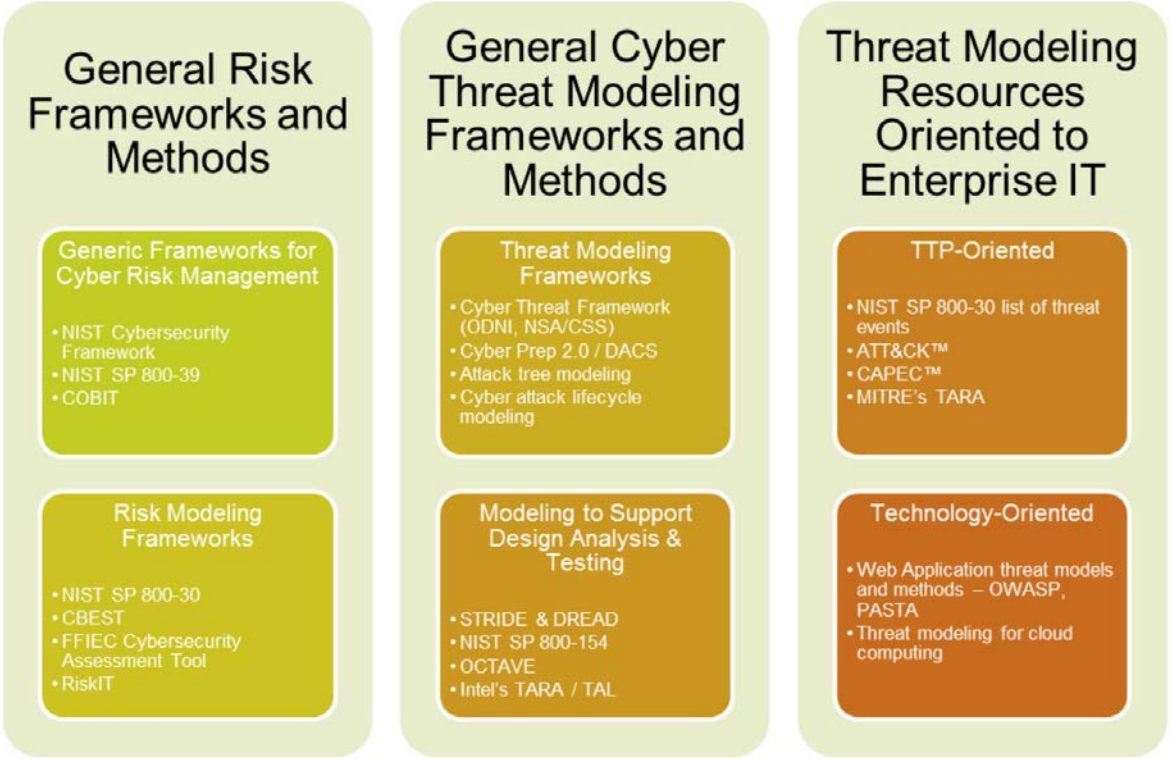
Introduction

Cyber Threat Modeling

According to the Homeland Security Systems Engineering & Development Institute:

- “Cyber threat modeling is the process of developing and applying a representation of adversarial threats (sources, scenarios, and specific events) in cyberspace.”

- Such threats can target or affect a:
  - Device
  - Application
  - System
  - Network
  - Mission
  - Business Function
  - Organization
  - Region
  - Critical infrastructure Sector



Cyber Threat Modeling (cont.)

Search

COVID Questions

Report Cyber Issue

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

About CISA > Infrastructure Security > Critical Infrastructure Sectors > Healthcare and Public Health Sector

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector

HEALTHCARE AND PUBLIC HEALTH SECTOR

Original release date: June 12, 2014 | Last revised: December 04, 2018

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure. Operating in all U.S. states, territories, and tribal areas, the sector plays a significant role in response and recovery across all other sectors in the event of a natural or manmade disaster. While healthcare tends to be delivered and managed locally, the public health component of the sector, focused primarily on population health, is managed across all levels of government: national, state, regional, local, tribal, and territorial.

The Healthcare and Public Health Sector is highly dependent on fellow sectors for continuity of operations and service delivery, including Communications, Emergency Services, Energy, Food and Agriculture, Information Technology, Transportation Systems, and Water and Wastewater Systems.

Expand All Sections

Source: CISA

Mitre ATT&CK® Framework

- MITRE ATT&CK® (Adversarial Tactics, Techniques & Common Knowledge) 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.

Version	Start Date	End Date	Data	Release Notes
ATT&CK v7 (current version)	July 8, 2020	n/a	v7.1 on MITRE/CTI	Updates — July 2020
ATT&CK v7-beta	March 31, 2020	July 7, 2020	v7.0-beta on MITRE/CTI	Updates — March 2020
ATT&CK v6	October 24, 2019	July 7, 2020	v6.3 on MITRE/CTI	Updates — October 2019
ATT&CK v5	July 31, 2019	October 23, 2019	v5.2 on MITRE/CTI	Updates — July 2019
ATT&CK v4	April 30, 2019	July 30, 2019	v4.0 on MITRE/CTI	Updates — April 2019
ATT&CK v3	October 23, 2018	April 29, 2019	v3.0 on MITRE/CTI	Updates — October 2018

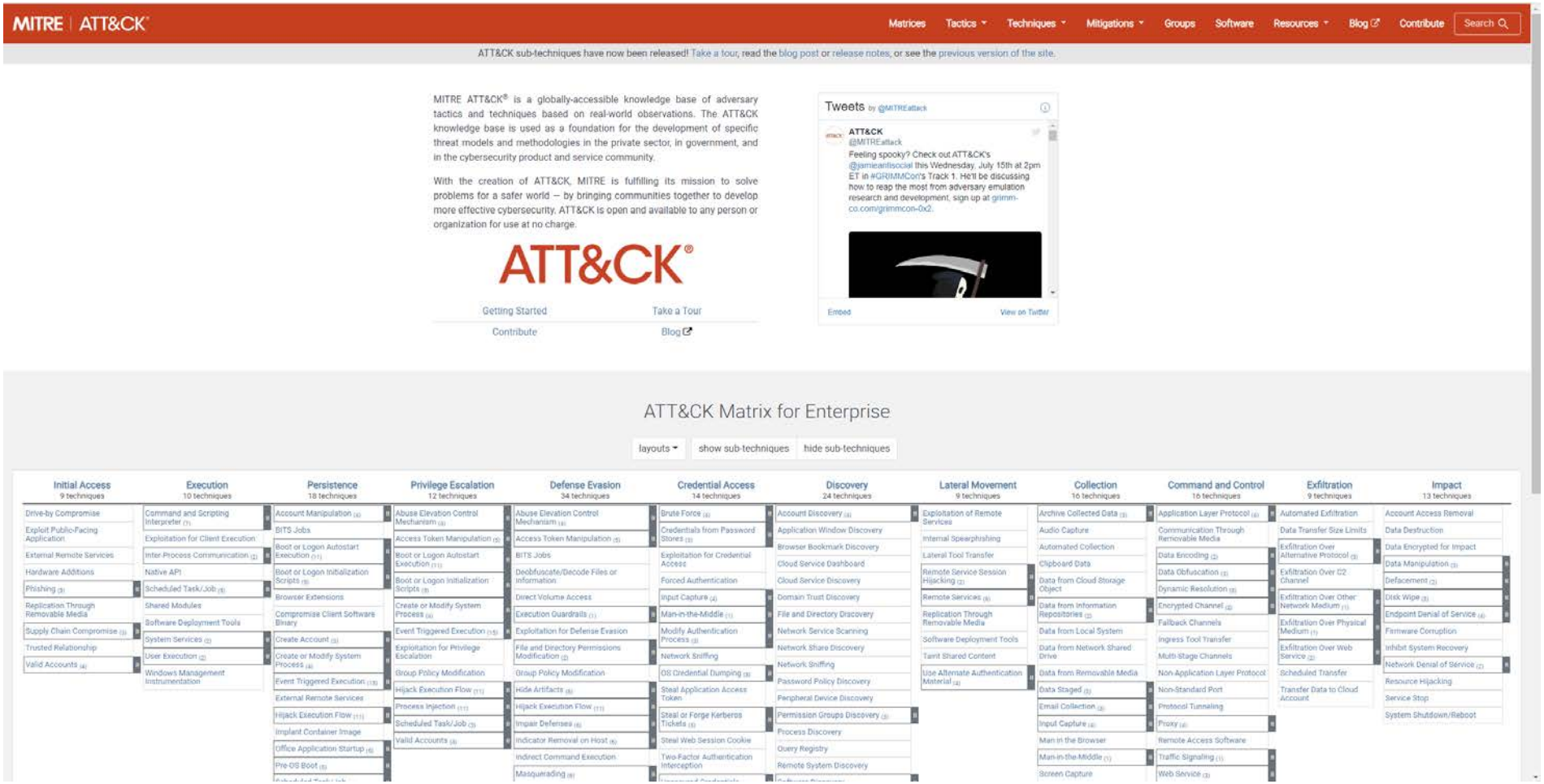
Versions from before the migration from MediaWiki are not preserved on this site:

ATT&CK v2	April 13, 2018	October 22, 2018	v2.0 on MITRE/CTI	Updates — April 2018
ATT&CK v1	January 16, 2018	April 12, 2018	v1.0 on MITRE/CTI	Updates — January 2018

Source: Mitre

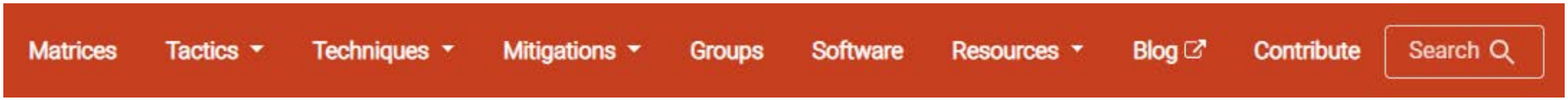
Mitre ATT&CK® Framework (cont.)

https://attack.mitre.org/



Source: Mitre

Mitre ATT&CK® Framework (cont.)



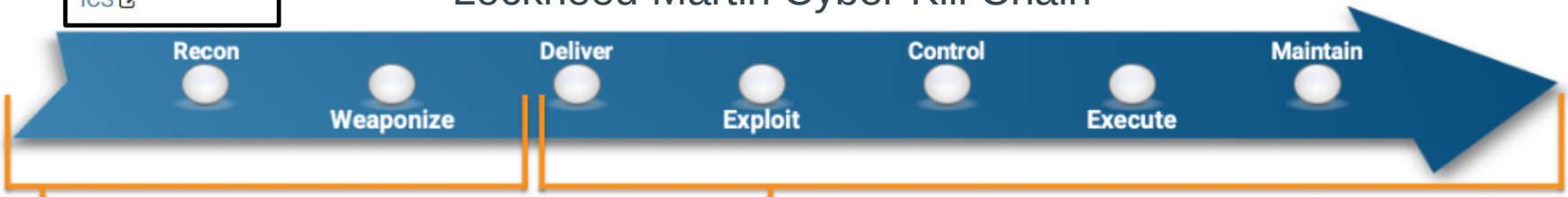
- **Matrices**
  - Detail adversary Tactics and Techniques
- **Tactics**
  - Threat actor's tactical objective for performing an action
- **Techniques**
  - How a threat actor achieves a tactical objective
- **Mitigations**
  - Actions taken to prevent successful execution of a technique
- **Groups**
  - Threat Actors
- **Software**
  - Software used by Threat Actors
- **Resources**
  - Miscellaneous information regarding the ATT&CK Framework
- **Blog**
  - Running blog by Mitre on the ATT&CK Framework
- **Contribute**
  - Ways to contribute to improving the ATT&CK Framework

Mitre ATT&CK® Framework (cont.)

MATRICES

- PRE-ATT&CK
- Enterprise
- Mobile
- ICS

Lockheed Martin Cyber Kill Chain®



PRE-ATT&CK

- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

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

Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Tactics – 12

Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Techniques – 156
  - Sub-Techniques – 272

Enterprise Techniques

Techniques: 156
Sub-techniques: 272

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may perform shell escapes or exploit vulnerabilities in an application with the setsuid or setgid bits to get code running in a different user's context. On Linux or macOS, when the setuid or setgid bits are set for an application, the application will run with the privileges of the owning user or group respectively. . Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn't need the elevated privileges.
.002	Bypass User Access Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
.003	Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the suoders file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.
.004	Elevated Execution with Prompt	Adversaries may leverage the `AuthorizationExecuteWithPrivileges` API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.
T1134	Access Token Manipulation	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.
.001	Token Impersonation/Theft	Adversaries may duplicate then impersonate another user's token to escalate privileges and bypass access controls. An adversary can create a new access token that duplicates an existing token using `DuplicateToken(Ex)`. The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.
.002	Create Process with Token	Adversaries may create a new process with a duplicated token to escalate privileges and bypass access controls. An adversary can duplicate a desired access token with `DuplicateToken(Ex)` and use it with `CreateProcessWithTokenW` to create a new process running under the security context of the impersonated user. This is useful for creating a new process under the security context of a different user.
.003	Make and Impersonate Token	Adversaries may make and impersonate tokens to escalate privileges and bypass access controls. If an adversary has a username and password but the user is not logged onto the system, the adversary can then create a logon session for the user using the `LogonUser` function. The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.
.004	Parent PID Spoofing	Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the `CreateProcess` API call, which supports a parameter that defines the PPID to use. This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via `svchost.exe` or `consent.exe`) rather than the current user context.
.005	SID-History Injection	Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. An account can hold additional SIDs in the SID-History Active Directory attribute , allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Mitigations – 41

Enterprise Mitigations

Mitigations: 41

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.
M1013	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M1040	Behavior Prevention on Endpoint	Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.
M1046	Boot Integrity	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.
M1045	Code Signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.
M1043	Credential Access Protection	Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.
M1053	Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.
M1042	Disable or Remove Feature or Program	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
M1055	Do Not Mitigate	This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.
M1041	Encrypt Sensitive Information	Protect sensitive information with strong encryption.

Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Groups – 107

Groups

Groups: 107

Name	Associated Groups	Description
admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
APT-C-36	Blind Eagle	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.
APT1	Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
APT12	IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.
APT16		APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.
APT17	Deputy Dog	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.
APT18	TG-0416, Dynamite Panda, Threat Group-0416	APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.
APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.
APT28	SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.
APT29	YTTRIUM, The Dukes, Cozy Bear, CozyDuke	APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015.
APT3	Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110	APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. MITRE has also developed an APT3 Adversary Emulation Plan.
APT30		APT30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.

Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Software – 477

Software

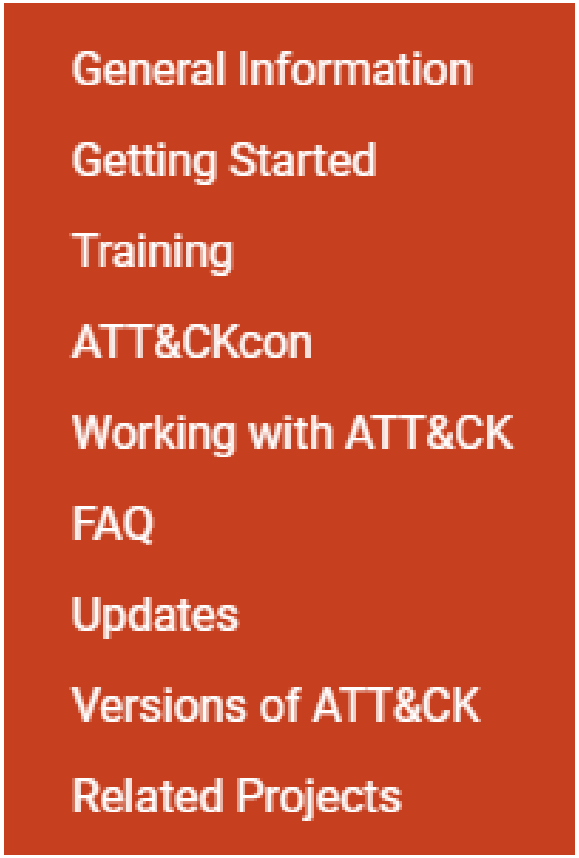
Software: 477

Name	Associated Software	Description
3PARA RAT		3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
4H RAT		4H RAT is malware that has been used by Putter Panda since at least 2007.
ABK		ABK is a downloader that has been used by BRONZE BUTLER since at least 2019.
adbupd		adbupd is a backdoor used by PLATINUM that is similar to Dipsind.
Adups		Adups is software that was pre-installed onto Android devices, including those made by BLU Products. The software was reportedly designed to help a Chinese phone manufacturer monitor user behavior, transferring sensitive data to a Chinese server.
ADVSTORESHELL	AZZY, EVILTOSS, NETUI, Sedreco	ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase.
Agent Smith		Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 Agent Smith had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States.
Agent Tesla		Agent Tesla is a spyware Trojan written for the .NET framework that has been observed since at least 2014.
Agent.btz		Agent.btz is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008.
Allwinner		Allwinner is a company that supplies processors used in Android tablets and other devices. A Linux kernel distributed by Allwinner for use on these devices reportedly contained a backdoor.
Android/Chuli.A		Android/Chuli.A is Android malware that was delivered to activist groups via a spearphishing email with an attachment.
ANDROIDOS_ANSERVER.A		ANDROIDOS_ANSERVER.A is Android malware that is unique because it uses encrypted content within a blog site for command and control.
AndroRAT		AndroRAT is malware that allows a third party to control the device and collect information.
Anubis		Anubis is Android malware that was originally used for cyber espionage, and has been retooled as a banking trojan.
Aria-body		Aria-body is a custom backdoor that has been used by Naikon.
Arp	arp.exe	Arp displays information about a system's Address Resolution Protocol (ARP) cache.
ASPXSpy	ASPXTool	ASPXSpy is a Web shell. It has been modified by Threat Group-3390 actors to create the ASPXTool version.

Source: Mitre

Mitre ATT&CK® Framework (cont.)

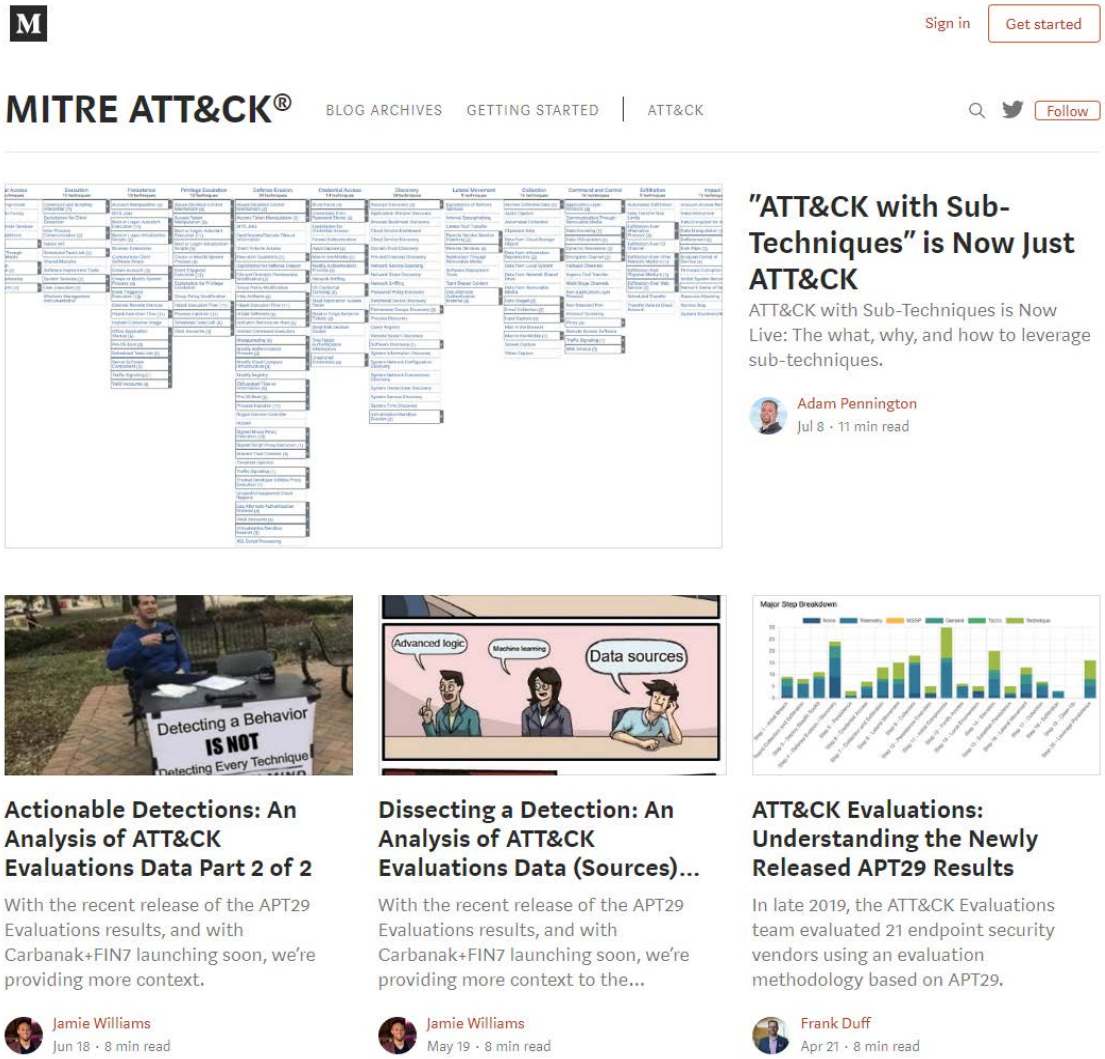
- Resources



Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Blog



Source: Mitre

Mitre ATT&CK® Framework (cont.)

- Contribute

New Technique Example

(Sub-)Technique Name: COM, ROM, & BE GONE **Tactic:** Persistence

Platform: Windows **Required Permissions:** User

Sub-techniques: This is a sub-technique of T1XXX, or this would have T1XXX as a sub-technique

Data Sources: Windows API, Process monitoring, or other sources that can be used to detect this activity

Description: Component Object Model (COM) servers associated with Graphics Interchange Format (JIF) image viewers can be abused to corrupt arbitrary memory banks. Adversaries may leverage this opportunity to modify, mux, and maliciously annoy (MMA) read-only memory (ROM) regularly accessed during normal system operations.

Detection: Monitor the JIF viewers for muxing and malicious annoyance. Use event ID 423420 and 234222 to detect changes.

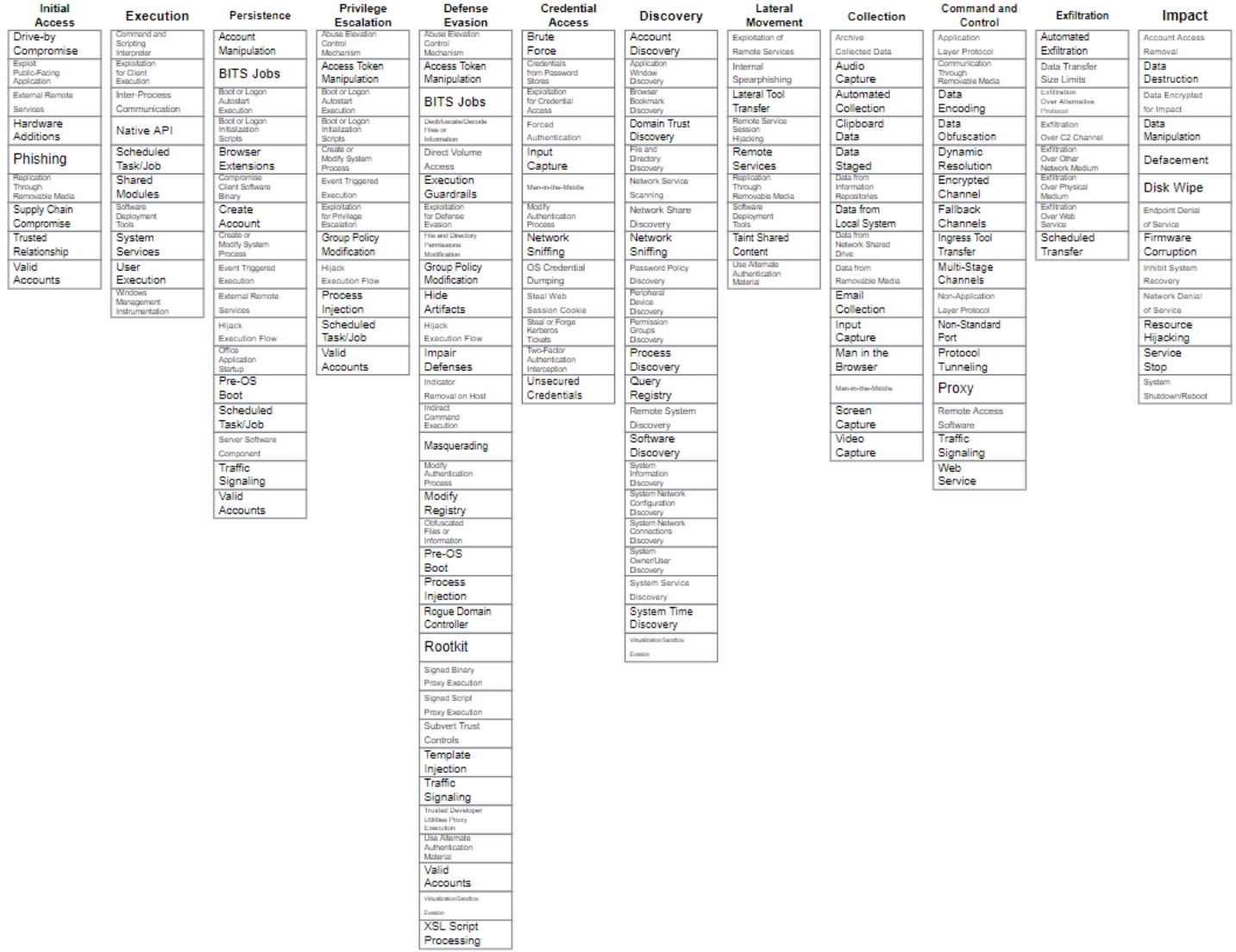
Mitigation: Configure the Registry key HKLM\SYSTEM\ControlSet\001\Control\WindowsJIFControl\ to 0 to disable MMA access if not needed within the environment.

Adversary Use: Here is a publicly-available reference about FUZZYSNUGGLYDUCK using this technique: (www[.]awesomeThreatReports[.]org/FUZZYSNUGGLYDUCK_NOMS _ON_ROM_VIA_COM). Additionally, our red team uses this in our operations.

Additional References: Here is a reference from the researcher who discovered this technique: (www[.]crazySmartResearcher[.]net/POC_DETECTIONS_&_MITIGATIONS_4_WHEN_COM_RAMS_ROM)

Source: Mitre

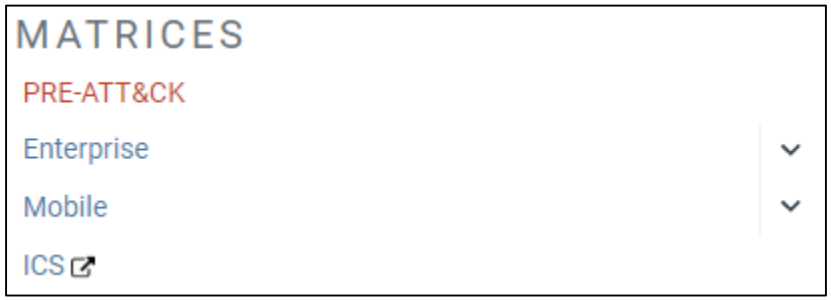
Mitre ATT&CK® Framework (cont.)

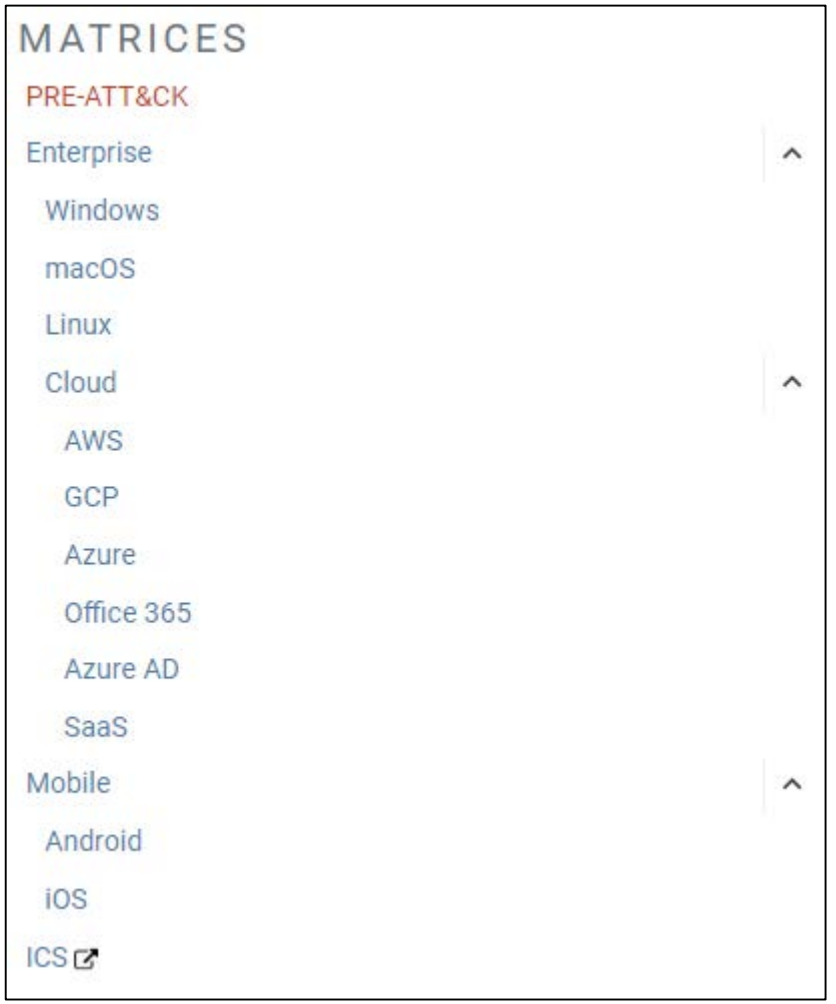


Source: Mitre

Mitre ATT&CK® Framework (cont.)

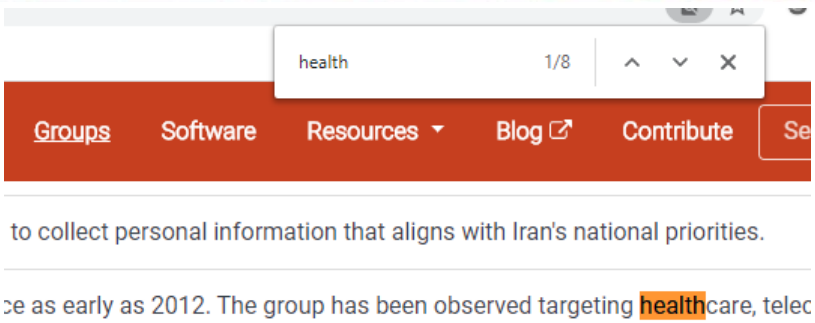
Mitre ATT&CK® Framework (cont.)





Specific Threats to the HPH

- Navigate to “Groups”
- Ctrl+F
- Search for “health”
- Seven Groups are identified
- Four Groups with US HPH focus



Name	Associated Groups	Description
APT41		APT41 is a group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity. APT41 has been active since as early as 2012. The group has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries.
Deep Panda	Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine	Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. The intrusion into healthcare company Anthem has been attributed to Deep Panda. This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same.
FIN4		FIN4 is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013. FIN4 is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.
menuPass	Stone Panda, APT10, Red Apollo, CVNX, HOGFISH	menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university.
Orangeworm		Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.
Whitefly		Whitefly is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore’s largest public health organization, SingHealth.
Tropic Trooper	Pirate Panda, KeyBoy	Tropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.

Specific Threats to the HPH (cont.)

Deep Panda

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into healthcare company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. [4] Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same. [5]

Associated Group Descriptions

Name
Shell Crew
WebMasters
KungFu Kittens
PinkPanther
Black Vine

ID: G0009

Associated Groups: Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine

Contributors: Andrew Smith, @jakx_

Version: 1.2

Created: 31 May 2017

Last Modified: 17 April 2020

References

1. Alperovitch, D. (2014, July 7). Deep in Thought: Chinese Targeting of National Security Think Tanks. Retrieved November 12, 2014.
2. ThreatConnect Research Team. (2015, February 27). The Anthem Hack: All Roads Lead to China. Retrieved January 26, 2016.
3. RSA Incident Response. (2014, January). RSA Incident Response Emerging Threat Profile: Shell Crew. Retrieved January 14, 2016.
4. DiMaggio, J.. (2015, August 6). The Black Vine cyberespionage group. Retrieved January 26, 2016.
5. Scott, J. and Spaniel, D. (2016, July 28). ICIT Brief - China's Espionage Dynasty: Economic Death by a Thousand Cuts. Retrieved June 7, 2018.
6. RYANJ. (2014, February 20). Mo' Shells Mo' Problems – Deep Panda Web Shells. Retrieved September 16, 2015.
7. Cylance SPEAR Team. (2017, February 9). Shell Crew Variants Continue to Fly Under Big AV's Radar. Retrieved February 15, 2017.

Specific Threats to the HPH (cont.)

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.[1]
Enterprise	T1546	.008	Event Triggered Execution: Accessibility Features	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions.[3]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	Deep Panda has used `-w hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden. [1]
Enterprise	T1027	.005	Obfuscated Files or Information: Indicator Removal from Tools	Deep Panda has updated and modified its malware, resulting in different hash values that evade detection.[4]
Enterprise	T1057		Process Discovery	Deep Panda uses the Microsoft Tasklist utility to list processes running on systems.[1]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Deep Panda uses net.exe to connect to network shares using `net use` commands with compromised credentials.[1]
Enterprise	T1018		Remote System Discovery	Deep Panda has used ping to identify other machines of interest.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.[6]
Enterprise	T1218	.010	Signed Binary Proxy Execution: Regsvr32	Deep Panda has used regsvr32.exe to execute a server variant of Derusbi in victim networks.[3]
Enterprise	T1047		Windows Management Instrumentation	The Deep Panda group is known to utilize WMI for lateral movement.[1]

Software

ID	Name	References	Techniques
S0021	Derusbi	[2]	Audio Capture, Command and Scripting Interpreter: Unix Shell, Commonly Used Port, Encrypted Channel: Symmetric Cryptography, Fallback Channels, File and Directory Discovery, Indicator Removal on Host: Timestomp, Indicator Removal on Host: File Deletion, Input Capture: Keylogging, Non-Application Layer Protocol, Non-Standard Port, Process Discovery, Process Injection: Dynamic-link Library Injection, Query Registry, Screen Capture, Signed Binary Proxy Execution: Regsvr32, System Information Discovery, System Owner/User Discovery, Video Capture
S0080	Mivast	[4]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Ingress Tool Transfer, OS Credential Dumping: Security Account Manager
S0039	Net	[1]	Account Discovery: Local Account, Account Discovery: Domain Account, Create Account: Local Account, Create Account: Domain Account, Indicator Removal on Host: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery
S0097	Ping	[1]	Remote System Discovery
S0074	Sakula	[2]	Abuse Elevation Control Mechanism: Bypass User Access Control, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Encrypted Channel: Symmetric Cryptography, Hijack Execution Flow: DLL Side-Loading, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information, Signed Binary Proxy Execution: Rundll32
S0142	StreamEx	[7]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, File and Directory Discovery, Modify Registry, Obfuscated Files or Information, Process Discovery, Signed Binary Proxy Execution: Rundll32, Software Discovery: Security Software Discovery, System Information Discovery
S0057	Tasklist	[1]	Process Discovery, Software Discovery: Security Software Discovery, System Service Discovery

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the Tasklist utility via cmd or `Get-Process` via PowerShell. Information about processes can also be extracted from the output of Native API calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc.

Procedure Examples

Name	Description
4H RAT	4H RAT has the capability to obtain a listing of running processes (including loaded modules).[90]
ADVSTORESHELL	ADVSTORESHELL can list running processes.[49]
Agent Tesla	Agent Tesla can list the current running processes on the system.[57]
APT1	APT1 gathered a list of running processes on the system using `tasklist /v`.[138]
APT28	An APT28 loader Trojan will enumerate the victim's processes searching for explorer.exe if its current process does not have necessary permissions.[38]
APT3	APT3 has a tool that can list out currently running processes.[141][142]
APT37	APT37's Freenki malware lists running processes using the Microsoft Windows API.[136]
APT38	APT38 leveraged Sysmon to understand the processes, services in the organization.[139]
Aria-body	Aria-body has the ability to enumerate loaded modules for a process.[125]

ID: T1057
Sub-techniques: No sub-techniques
Tactic: Discovery
Platforms: Linux, Windows, macOS
System Requirements: Administrator, SYSTEM may provide better process ownership details
Permissions Required: Administrator, SYSTEM, User
Data Sources: API monitoring, Process command-line parameters, Process monitoring
CAPEC ID: CAPEC-573
Version: 1.2
Created: 31 May 2017
Last Modified: 26 March 2020

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events that look like process discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Threat Modeling with ATT&CK® (cont.)

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.[1]
Enterprise	T1546	.008	Event Triggered Execution: Accessibility Features	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions.[3]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	Deep Panda has used `-w hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden. [1]
Enterprise	T1027	.005	Obfuscated Files or Information: Indicator Removal from Tools	Deep Panda has updated and modified its malware, resulting in different hash values that evade detection.[4]
Enterprise	T1057		Process Discovery	Deep Panda uses the Microsoft Tasklist utility to list processes running on systems.[1]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Deep Panda uses net.exe to connect to network shares using `net use` commands with compromised credentials.[1]
Enterprise	T1018		Remote System Discovery	Deep Panda has used ping to identify other machines of interest.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.[6]
Enterprise	T1218	.010	Signed Binary Proxy Execution: Regsvr32	Deep Panda has used regsvr32.exe to execute a server variant of Derusbi in victim networks.[3]
Enterprise	T1047		Windows Management Instrumentation	The Deep Panda group is known to utilize WMI for lateral movement.[1]

Software

ID	Name	References	Techniques
S0021	Derusbi	[2]	Audio Capture, Command and Scripting Interpreter: Unix Shell, Commonly Used Port, Encrypted Channel: Symmetric Cryptography, Fallback Channels, File and Directory Discovery, Indicator Removal on Host: Timestomp, Indicator Removal on Host: File Deletion, Input Capture: Keylogging, Non-Application Layer Protocol, Non-Standard Port, Process Discovery, Process Injection: Dynamic-link Library Injection, Query Registry, Screen Capture, Signed Binary Proxy Execution: Regsvr32, System Information Discovery, System Owner/User Discovery, Video Capture
S0080	Mivast	[4]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Ingress Tool Transfer, OS Credential Dumping: Security Account Manager
S0039	Net	[1]	Account Discovery: Local Account, Account Discovery: Domain Account, Create Account: Local Account, Create Account: Domain Account, Indicator Removal on Host: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery
S0097	Ping	[1]	Remote System Discovery
S0074	Sakula	[2]	Abuse Elevation Control Mechanism: Bypass User Access Control, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Encrypted Channel: Symmetric Cryptography, Hijack Execution Flow: DLL Side-Loading, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information, Signed Binary Proxy Execution: Rundll32
S0142	StreamEx	[7]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, File and Directory Discovery, Modify Registry, Obfuscated Files or Information, Process Discovery, Signed Binary Proxy Execution: Rundll32, Software Discovery: Security Software Discovery, System Information Discovery
S0057	Tasklist	[1]	Process Discovery, Software Discovery: Security Software Discovery, System Service Discovery

Threat Modeling with ATT&CK® (cont.)

Sakula

Sakula is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015. [1]

ID: S0074
Associated Software: Sakurel, VIPER
Type: MALWARE
Platforms: Windows
Version: 1.1
Created: 31 May 2017
Last Modified: 30 March 2020

Techniques Used

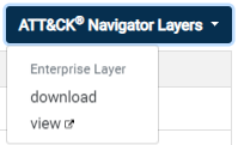
ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Access Control	Sakula contains UAC bypass code for both 32- and 64-bit systems.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Sakula uses HTTP for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Most Sakula samples maintain persistence by setting the Registry Run key `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\` in the HKLM or HKCU hive, with the Registry value and file name varying by sample.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Sakula calls cmd.exe to run various DLL files via rundll32 and also to perform file cleanup. Sakula also has the capability to invoke a reverse shell.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Some Sakula samples install themselves as services for persistence by calling WinExec with the `net start` argument.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Sakula encodes C2 traffic with single-byte XOR keys.[1]
Enterprise	T1574	.002	Hijack Execution Flow: DLL Side-Loading	Sakula uses DLL side-loading, typically using a digitally signed sample of Kaspersky Anti-Virus (AV) 6.0 for Windows Workstations or McAfee's Outlook Scan About Box to load malicious DLL files.[1]
Enterprise	T1070	.004	Indicator Removal on Host: File Deletion	Some Sakula samples use cmd.exe to delete temporary files.[1]
Enterprise	T1105		Ingress Tool Transfer	Sakula has the capability to download files.[1]
Enterprise	T1027		Obfuscated Files or Information	Sakula uses single-byte XOR obfuscation to obfuscate many of its files.[1]
Enterprise	T1218	.011	Signed Binary Proxy Execution: Rundll32	Sakula calls cmd.exe to run various DLL files via rundll32.[1]

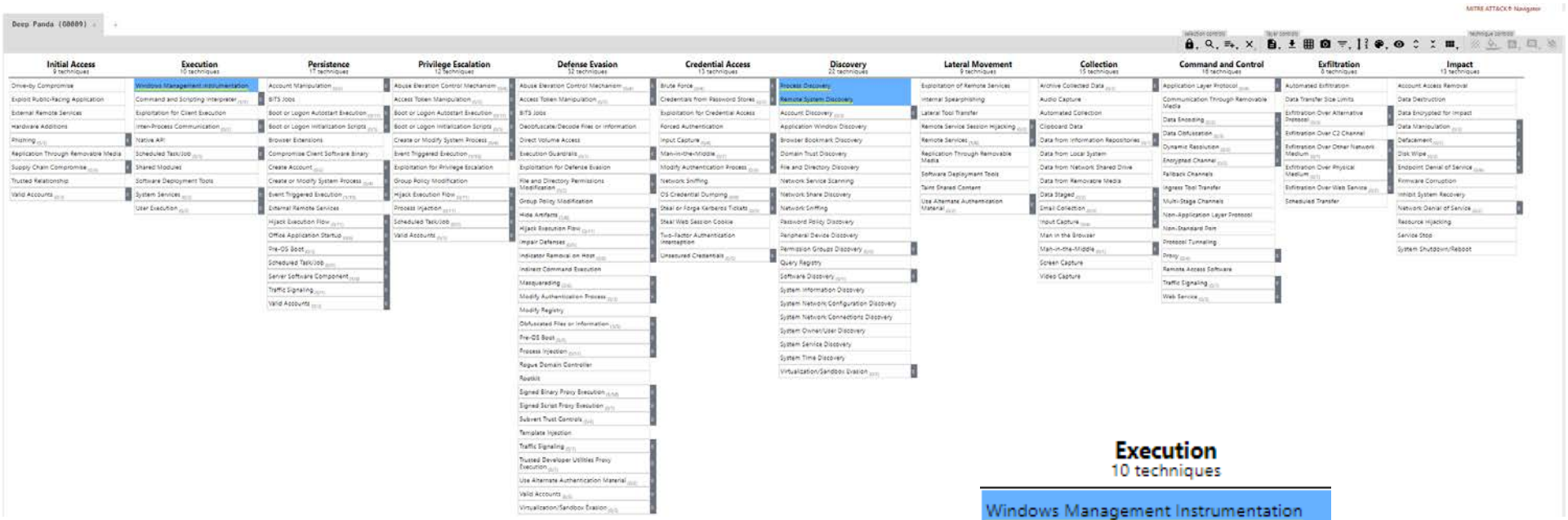
Groups That Use This Software

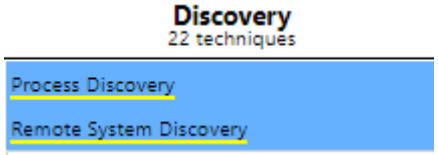
ID	Name
G0009	Deep Panda

Threat Modeling with ATT&CK® (cont.)

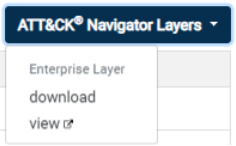


3 Techniques Listed

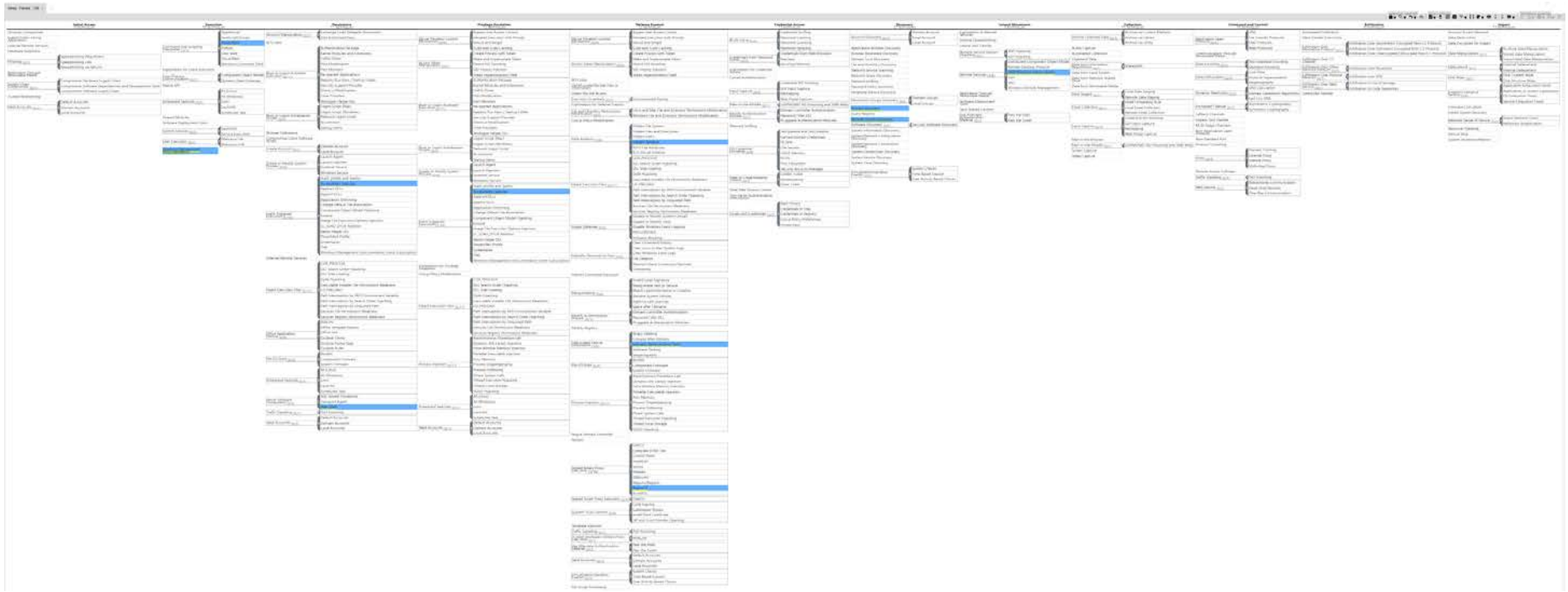




Threat Modeling with ATT&CK® (cont.)

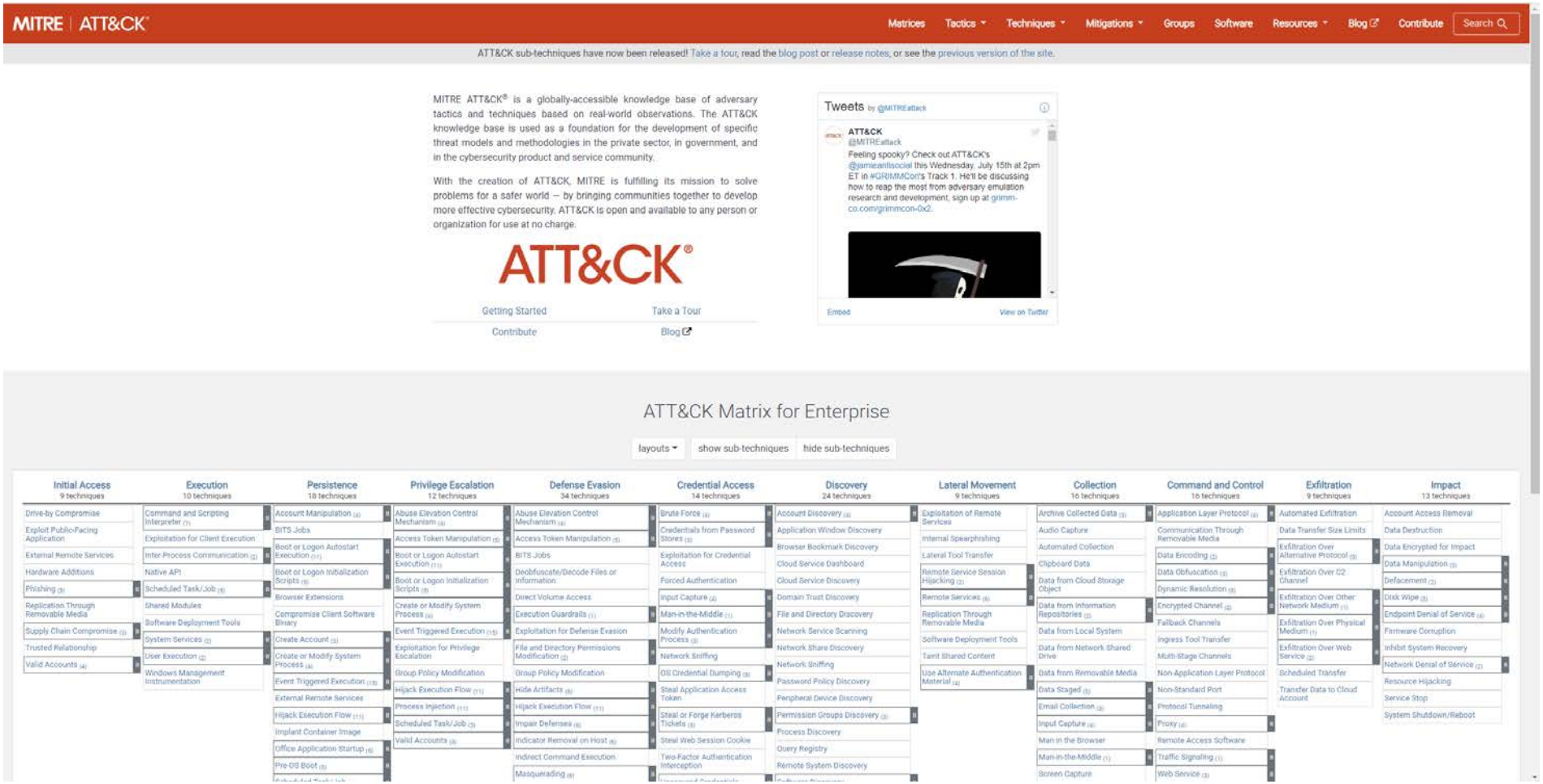


3 Techniques Listed



Introduction to ATT&CK Navigator

Conclusion


MITRE | ATT&CK
Matrices
Tactics
Techniques
Mitigations
Groups
Software
Resources
Blog
Contribute
Search
ATT&CK sub-techniques have now been released! Take a tour, read the blog post or release notes, or see the previous version of the site.
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®
Getting Started
Take a Tour
Contribute
Blog
Tweets by @MITREattack
ATT&CK
@MITREattack
Feeling spooky? Check out ATT&CK's @jamieantisocial this Wednesday, July 15th at 2pm ET in #GRIMMCon's Track 1. He'll be discussing how to reap the most from adversary emulation research and development, sign up at grimm-co.com/grimmcon-0x2.
Embed
View on Twitter
ATT&CK Matrix for Enterprise
layouts
show sub-techniques
hide sub-techniques
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
10 techniques
Command and Scripting Interpreter
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Container Image
Office Application Startup
Pre-OS Boot
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Event Triggered Execution
Exploitation for Privilege Escalation
Group Policy Modification
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
34 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Group Policy Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal on Host
Indirect Command Execution
Masquerading
Credential Access
14 techniques
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Input Capture
Man-in-the-Middle
Modify Authentication Process
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
24 techniques
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Service Dashboard
Cloud Service 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
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
16 techniques
Archive Collected Data
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
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
Man-in-the-Middle
Screen Capture
Command and Control
16 techniques
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service
Exfiltration
9 techniques
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

Reference Materials

References

- Mitre ATT&CK
  - https://attack.mitre.org/
- Cyber Threat Modeling: Survey, Assessment, and Representative Framework
  - https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf
- Mitre ATT&CK Blog
  - https://medium.com/mitre-attack
- Introduction to ATT&CK Navigator
  - https://www.youtube.com/watch?v=pcclNdwG8Vs&feature=youtu.be
- Critical Infrastructure Sectors – Healthcare and Public Health Sector
  - https://www.cisa.gov/healthcare-and-public-health-sector

Questions

Questions

Upcoming Briefs

- Cybercrime and the Healthcare Industry (7/30)
- Cybersecurity Maturity Models (8/6)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV