USING INDICATORS OF COMPROMISE (IOC) FOR INCIDENT RESPONSE

Agenda

Intro and Overview

- Course Description
- Learning Objectives
- Overview of IOCs

IOCs

- Use of IOCs
- Types of IOCs
- CHIRP Digital Forensic Video
- MITRE ATT&CK® Framework

Case Studies

- Numbered Panda
- Elfin
- Fancy Bear

Knowledge Check

Key Takeaways

Resources

Learning Objectives

Terminal Objective

Summarize the importance of indicators of compromise (IOCs) and how they are used during incident response

Enabling Objectives

- Define IOCs
- Explain why IOCs are important
- Identify types of IOCs and how they are used, with examples
- Describe the MITRE ATT&CK Framework for incident response and IOC analysis
- Identify Advanced Persistent Threat (APT) groups and recommended actions
- Provide example analysis of IOCs using the ATT&CK Framework

What are Indicators of Compromise (IOCs)?

An IOC is a clue that can be used to indicate an intrusion or compromise of a host in a network.

.sf-menu > li.current_page
.sf-menu > li.current-menu-
> ul > li > a:hover > .sf-
ul #search-btn a:hover span,
.sf-menu > li.current-menu-
hover .icon-salient-cart,.ascend
!important;color:#ffffff!impo
header#top nav>ul>li.butt
widget-area-toggle a i.
transparent

Overview: IOC vs. IOA

Indicator of Attack (**IOA**)	Indicator of Compromise (**IOC**)
Identified as the event or process is **active** and occurring. Focused upon attribution and intent of threat actors.	Provides Information about known adversaries **after** an event has occurred. **Reactive** incident response indicator used for detection of threats.

What does an IOC reveal?

IOC can reveal:

- Tactics, Techniques and Procedures (TTPs) used during a cyberattack
- Severity of the event
- Where to focus incident response and mitigation
- Who the threat actors are

Introducing IOCs

A car dashboard provides real-time performance measures and safety indicator signals.

Like mechanics, incident responders use **indicators** to diagnose potential problems and determine how or why they occurred.

IOC and Digital Forensics

As per **NIST 800-53**, IOCs are forensic artifacts from intrusions identified on organizational systems at the host or network level

- **Digital forensics** is the application of scientific investigatory techniques to digital crimes and attacks.
- The Locard Principle: *"Every contact leaves a trace"*
- An IOC is the **trace** of the threat actor

Uses for IOCs

IOCs are a key source for:

- Identification of an Advanced Persistent Threat (APT) actor or group
- Indicating something is wrong on the network
- Forensic identification of crime or attack
- Understanding how a compromise occurred
- Testing your system or network for vulnerabilities

Knowledge Check (1)

An IOC can reveal:

- ❑ Severity of an attack
- ❑ Where the attack occurred
- ❑ Who is responsible
- ❑ Tactics
- ❑ All of the above

Ask the Audience (1)

Who has heard of the CISA Hunt and Incident Response Program (CHIRP) tool?

CHIRP

- CISA Hunt and Incident Response Program (CHIRP)
  - Forensics collection tool
  - Developed by CISA
  - Helps network defenders find IOCs associated with activity detailed in:

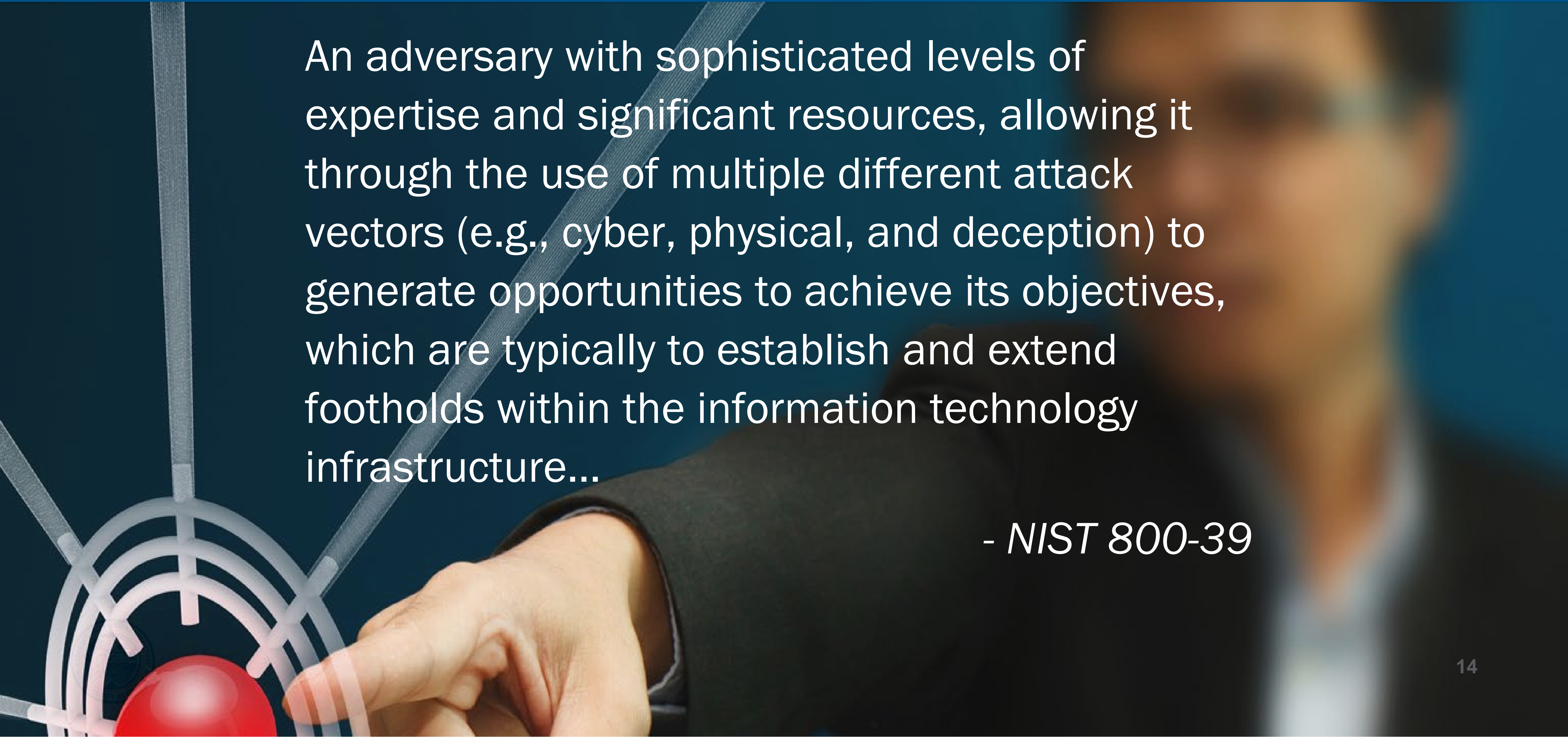
AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments

Similar to Sparrow—which scans for signs of APT compromise within an M365 or Azure environment—CHIRP scans for signs of APT compromise within an on-premises environment.

CISA HUNT AND INCIDENT RESPONSE PROGRAM (CHIRP)

What is an Advanced Persistent Threat (APT)?



An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure…

- NIST 800-39

Ask the Audience (2)

Who has experience with the MITRE ATT&CK Framework?

The MITRE ATT&CK® Framework

The MITRE ATT&CK Framework consists of adversarial techniques that can be correlated to the Tactics, Techniques, and Procedures (TTPs) employed by the APT groups.

- A collection of multiple IOC that allow analysts to identify which perpetrators may be involved
- IOCs correlate to **techniques** in the framework, which are mapped to **known APTs** based on the capabilities employed
- To strengthen security, organizations can use these techniques to simulate the threat actor and identify vulnerabilities in their network
- Based on IOC findings, defenders can create and apply signatures to their Intrusion Detection System (IDS) or Intrusion Prevention Systems (IPS) to identify or prevent future threat activity.

MITRE

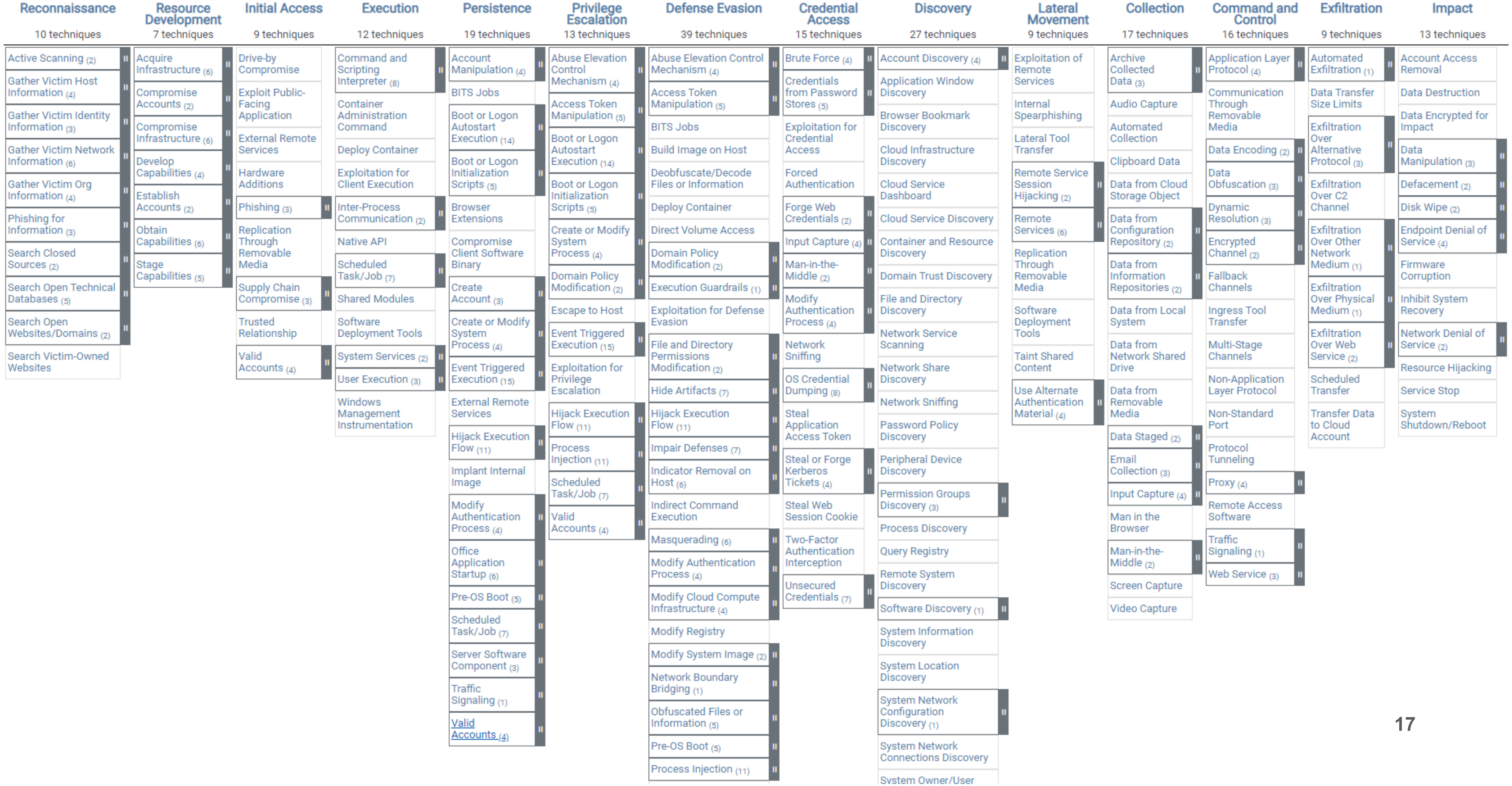
ATT&CK™

Adversarial Tactics, Techniques
& Common Knowledge

ATT&CK Matrix for Enterprise

TACTICS

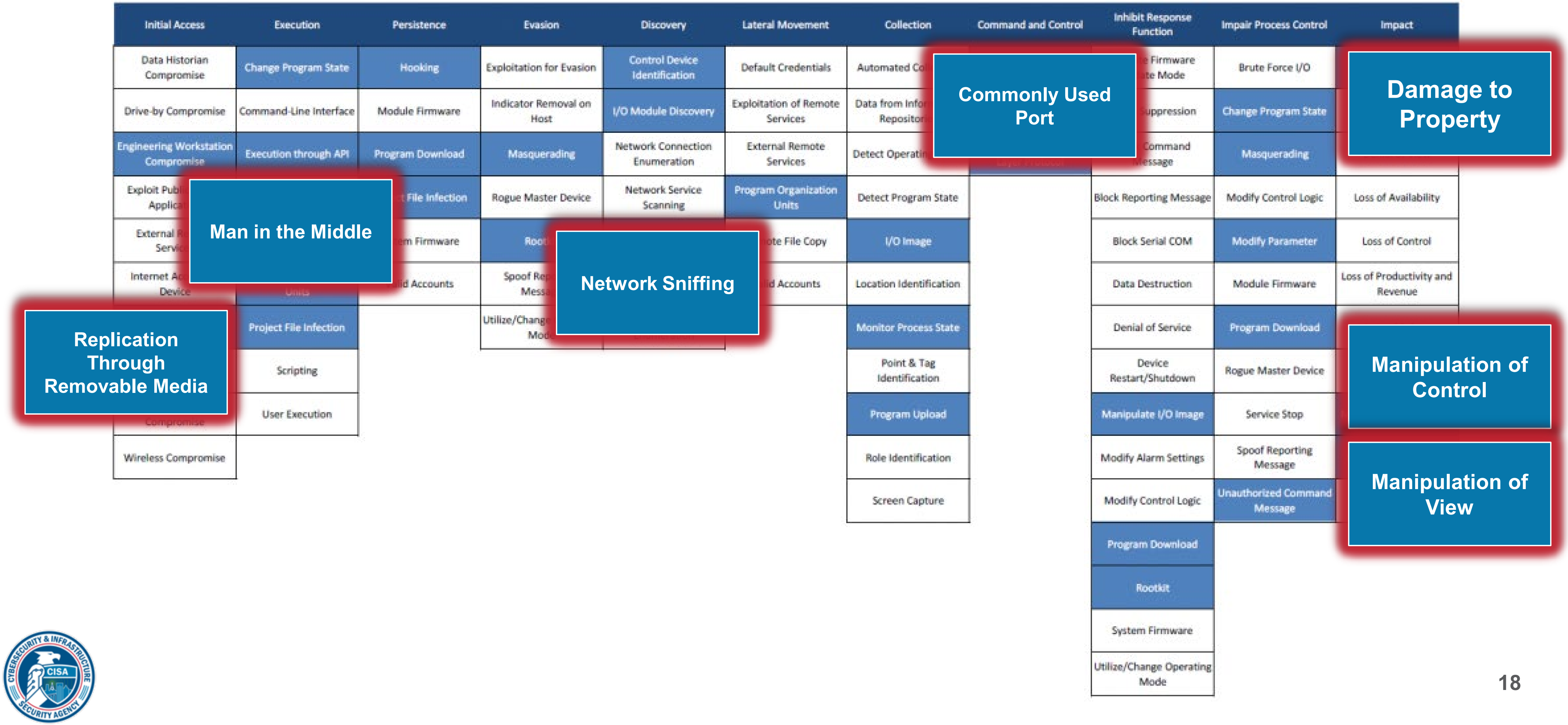
TECHNIQUES



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques
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)
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)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs
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
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
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)
				Office Application Startup (6)		Impair Defenses (7)
				Pre-OS Boot (5)		Indicator Removal on Host (6)
				Scheduled Task/Job (7)		Indirect Command Execution
				Server Software Component (3)		Masquerading (6)
				Traffic Signaling (1)		Modify Authentication Process (4)
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)
						Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (5)
						Pre-OS Boot (5)
						Process Injection (11)

Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)		
	Process Discovery		Screen Capture	Web Service (3)		
	Query Registry		Video Capture			
	Remote System Discovery					
	Software Discovery (1)					
	System Information Discovery					
	System Location Discovery					
	System Network Configuration Discovery (1)					
	System Network Connections Discovery					
	System Owner/User					

Mapping of Stuxnet on the ATT&CK for ICS Matrix



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Co		e Firmware te Mode	Brute Force I/O	
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Infor Repositor		uppression	Change Program State	
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operati	Layer Protocol	Command essage	Masquerading	
Exploit Publ Applica		t File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External R Servic		em Firmware	Root		ote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Ac Device	Units	lid Accounts	Spoof Rep Messa		id Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
	Project File Infection		Utilize/Change Mod			Monitor Process State		Denial of Service	Program Download	
	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	
Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	
						Screen Capture		Modify Control Logic	Unauthorized Command Message	
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Commonly Used Port

Damage to Property

Man in the Middle

Network Sniffing

Replication Through Removable Media

Manipulation of Control

Manipulation of View

Knowledge Check (2)

The MITRE ATT&CK Framework consists of techniques employed by:

- ❑ Domestic Terrorists
- ❑ Script Kiddies
- ❑ Environmental Hacktivists
- ❑ APT Groups

APT Case Studies

The following section provides case studies of MITRE ATT&CK identified APT groups:

China (APT 12)

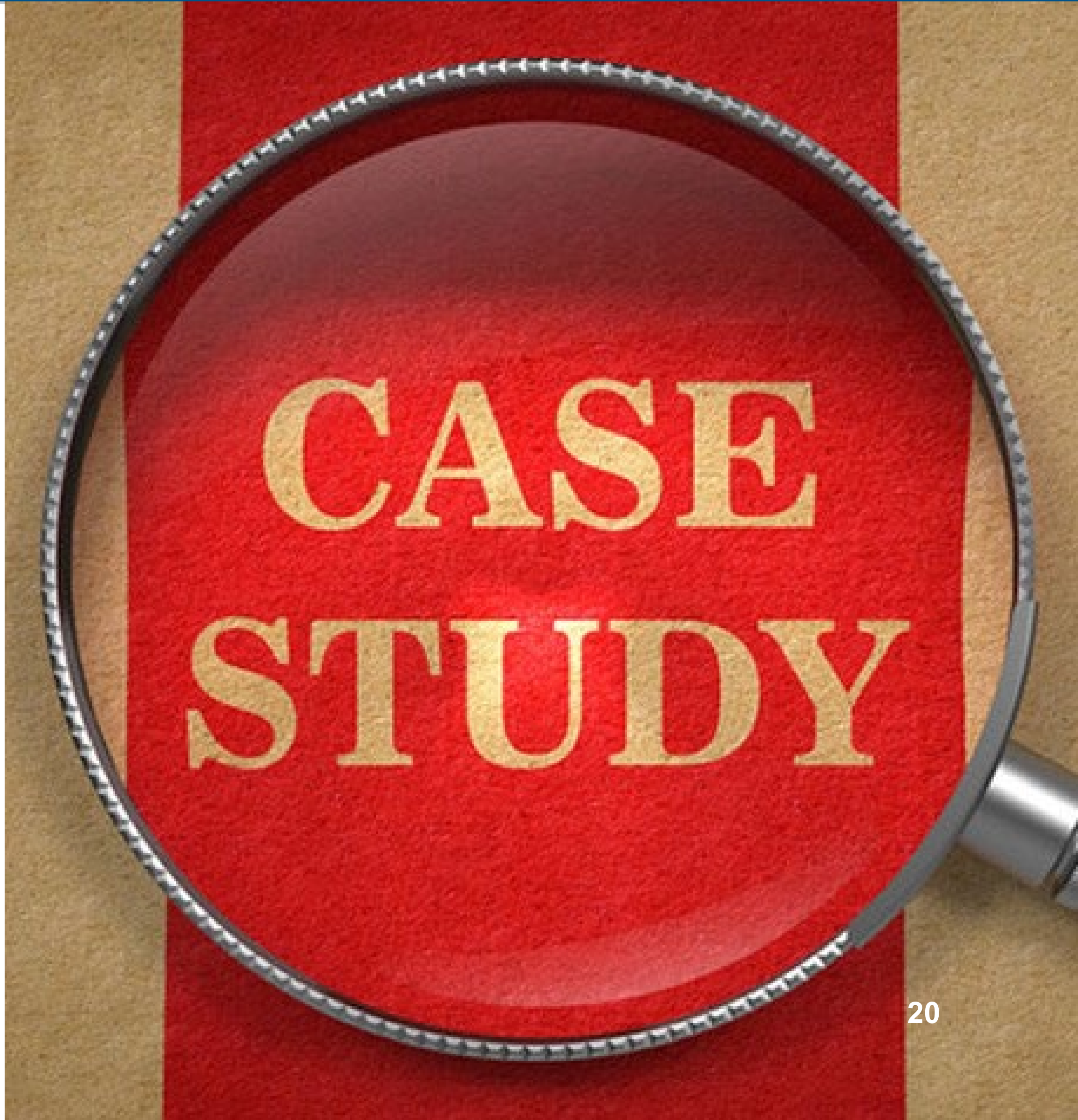
- “Numbered Panda”

Iran (APT 33)

- “Elfin”

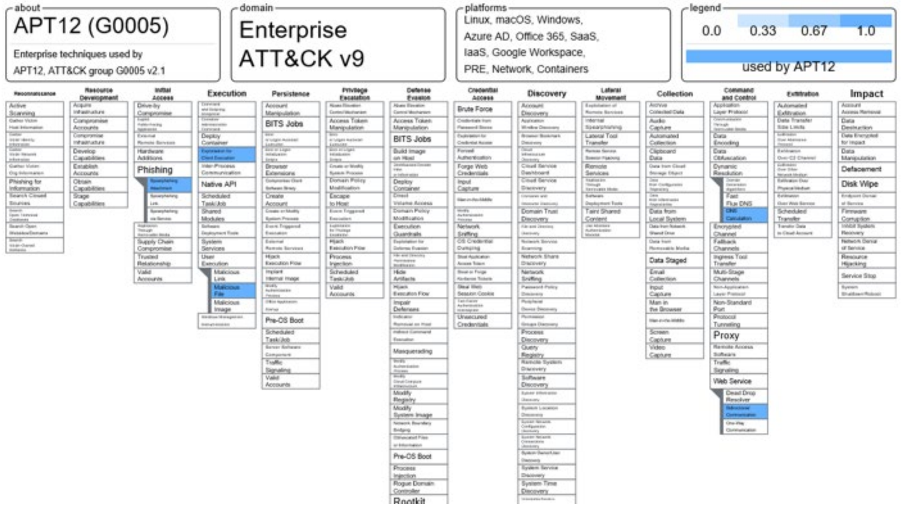
Russia (APT 28)

- “Fancy Bear”



APT 12 | China (Numbered Panda)

- MITRE ATT&CK® Framework TTPs
  - Initial Access
  - Execution
  - Command and Control
- APT 12 IOCs:
  - Current IOC profile denotes focus on the human element of the target enterprise, gaining access with social engineering and obtaining command and control[1].
- [Group G0005 | MITRE ATT&CK®]



about
APT12 (G0005)
Enterprise techniques used by
APT12, ATT&CK group G0005 v2.1

domain
Enterprise
ATT&CK v9

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

legend
0.0 0.33 0.67 1.0
used by APT12

[1] These are the highlighted knowns for this threat actor but does not define the entire TTP executed by threat actor.

APT 12 | China (Numbered Panda), cont

Description

- A China-attributed threat group that targets media outlets, tech companies and multiple governments
- Believed to be operating since 2009
- Though this group typically targeted East Asia, in 2012 they are believed to have breached the New York Times

Tools and Techniques

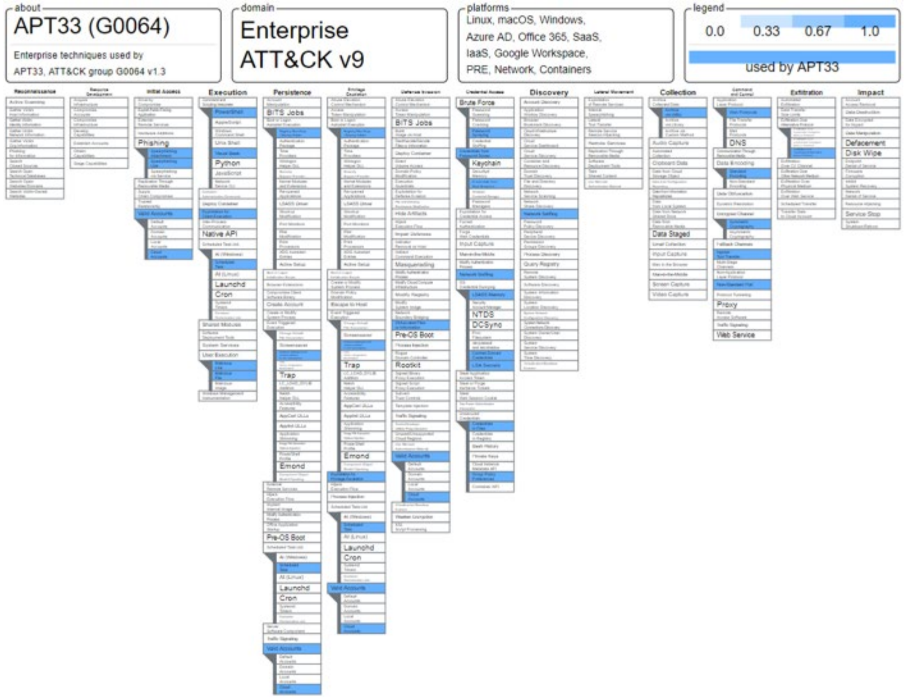
- DNS Calculation: multiplying the first two octets of an IP address and adding the third octet to that value in order to get a resulting command and control port.
- Phishing: sending emails with malicious Microsoft Office documents and PDFs attached.
- User execution/ malicious file: get victims to open malicious Word and PDF files sent via spearphishing
- Web Service Bidirectional Communication: used blogs and WordPress for C2 infrastructure

Associated Groups

- IXESHE, DynCalc, and DNSCALC

APT 33 | Iran (Elfin)

- MITRE ATT&CK® Framework TTPs
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Collection
  - Command and Control
  - Exfiltration
- APT 33 IOCs:
  - Current IOC profile denotes focus on the human element of the target enterprise, gaining access with social engineering and obtaining command and control moving laterally and escalating privileges as needed to eventually **exfil data**[1].
  - APT 33 known to use a multitude of tools with known IOCs, which may indicate either lack of novel sophistication OR the **use of obfuscation** to cover true objectives/intent; they're patient and tend to linger once they are in.
- Group G0064 | MITRE ATT&CK®



about
APT33 (G0064)
Enterprise techniques used by APT33, ATT&CK group G0064 v1.3

domain
Enterprise
ATT&CK v9

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

legend
0.0 0.33 0.67 1.0
used by APT33

[1] These are the highlighted knowns for this threat actor but does not define the entire TTP executed by threat actor.

APT 33 | Iran (Elfin), cont

Description

- A suspected Iranian threat group that targeted organizations across multiple industries in the US, Saudi Arabia, and South Korea, notably in the aviation and energy sectors
- This group is believed to be formed no later than 2013

Tools and Techniques

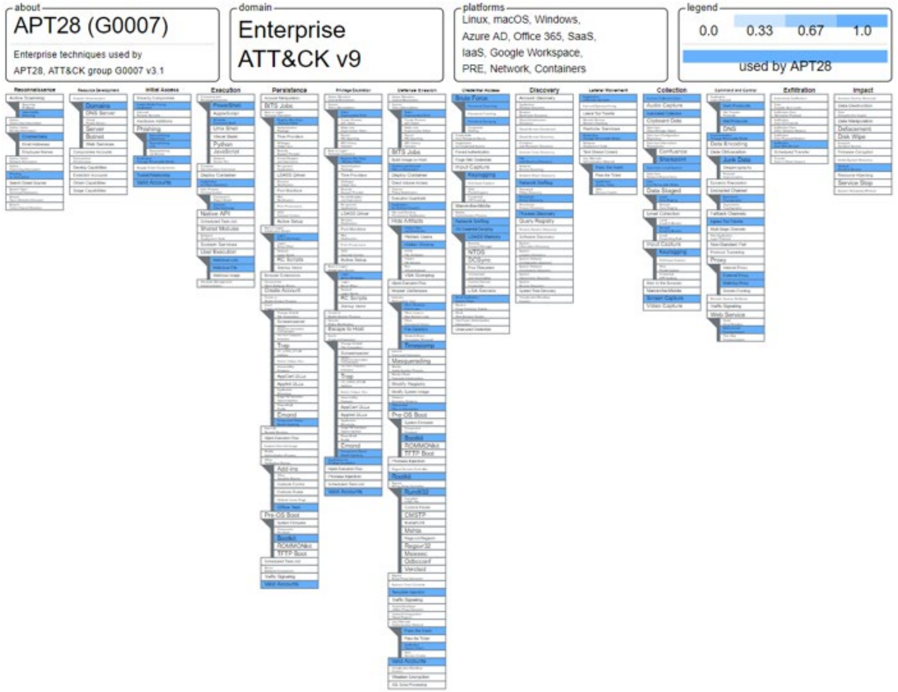
- A dropper program (written in Farsi) to deploy a wiper application that installs a backdoor
- Spearphishing emails loaded with malicious code to deliver the program to victims
- Impersonates commercial entities (i.e. Boeing and Northrop Grumman) through registered web domains

Associated Groups

- HOLMIUM

APT 28 | Russia (Fancy Bear)

- MITRE ATT&CK® Framework IOCs
  - **ALL** Enterprise Levels
- APT 28:
  - Current IOC profile denotes focus on the human element of the target enterprise to gain access but leverages a **multitude of TTPs** throughout the lifecycle to achieve intended objective(s)[1].
  - Indicates ability of a state backed organization to leverage a **wide array of resources.**
- Group G0007 | MITRE ATT&CK®



about: APT28 (G0007)
Enterprise techniques used by APT28, ATT&CK group G0007 v3.1

domain: Enterprise ATT&CK v9

platforms: Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers

legend: 0.0 0.33 0.67 1.0
used by APT28

[1] These are the highlighted knowns for this threat actor but does not define the entire TTP executed by threat actor.

APT 28 | Russia (Fancy Bear), cont

Description

- This Russia-attributed threat group targeted the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 to interfere with the U.S. presidential election.
- This group is believed to be operating since at least 2004.

Tools and Techniques

- Spearphishing emails with zero-day vulnerabilities were delivered to victims
- Fancy Bear has consistently been updating their malware since 2007
- They periodically wipe log events and rest timestamps to avoid forensic analysis of their hacks

Associated Groups

- SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, STRONTIUM, Tsar Team, Threat Group-4127, and TG-4127

Knowledge check

Knowledge Check (3)

This is the application of scientific investigatory techniques to cyber-related crimes:

❑ The Locard Principle

❑ Digital Forensics

❑ Bayesian Analysis

❑ Computer Engineering

Knowledge Check (4)

The forensics hunt and incident response tool developed by CISA is called:

□ SPARK

□ CHIRP

□ UASI

□ CyberTrace

Knowledge Check (4)

The APT group number 33 is affiliated with which country:

- □ China
- □ Russia
- □ Iran
- □ Brazil

Knowledge Check, extra credit

The APT group number 33 is affiliated with which country:

□ China

□ Russia

□ Iran

□ Brazil

Resources

- DHS Office of Cybersecurity and Communications- Federal Network Resiliency Division: High Value Asset Control Overlay- January 2021
  - https://www.cisa.gov/publication/high-value-asset-control-overlay
- CISA Insights: What Every Leader Needs to Know About the Ongoing APT Cyber Activity
  - https://www.cisa.gov/publication/what-every-leader-needs-know-about-ongoing-apt-cyber-activity
- MITRE | ATT&CK Matrix for Enterprise
  - https://attack.mitre.org
- US-CERT Indicator Alerts & Bulletins
  - https://us-cert.cisa.gov/ncas/alerts
  - https://us-cert.cisa.gov/ncas/bulletins
- Best Practices for MITRE ATT&CK Mapping
  - https://us-cert.cisa.gov/best-practices-mitre-attckr-mapping

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA