

ANOMALI®

MITRE ATT&CK:  
The Play at Home Edition



**Nicholas Hayden**

Global Head of Intelligence Operations  
Anomali





# Since this is MITRE ATT&CK: The Play at Home Edition



An open book lies on a rustic wooden surface. From the center of the open pages, a brilliant, ethereal light bursts forth, accompanied by a shower of sparkling stars and wispy, smoke-like clouds. This magical light fills the upper portion of the frame. The background is a deep, dark blue, decorated with several large, semi-transparent hexagonal shapes that overlap each other. The overall composition evokes a sense of wonder, magic, and the power of storytelling.

What better way to tell a story then...





The Disney  
Way

Disney + Story = ?

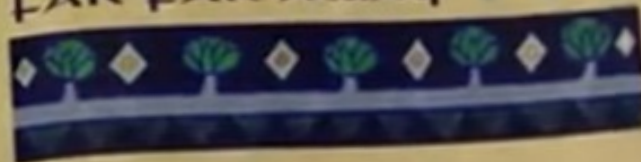




ONCE  
UPON A TIME



IN A KINGDOM  
FAR FAR AWAY



Or...



Disney + Star Wars = ?

A long time ago in a galaxy far,  
far away....



# APT 32

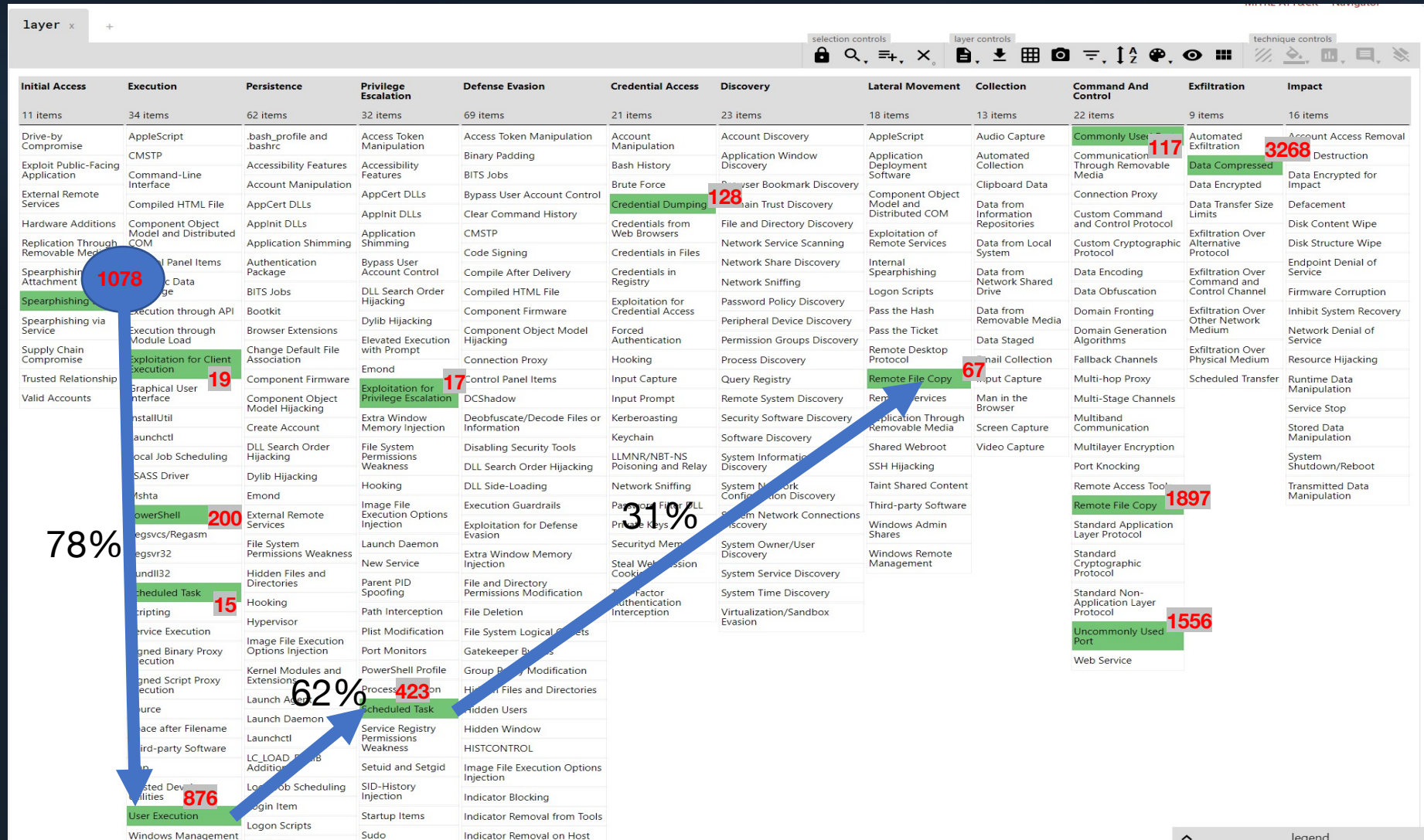
layer x +											
selection controls layer controls technique controls											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimmming	Application Shimmming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Share Discovery	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Logon Scripts	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	Bootkit	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Pass the Hash	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Browser Extensions	Elevated Execution with Prompt	Component Firmware	Hooking	Peripheral Device Discovery	Pass the Ticket	Email Collection	Domain Generation Algorithms	Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Change Default File Association	Emond	Component Object Model Hijacking	Input Capture	Process Discovery	Remote Desktop Protocol	Input Capture	Fallback Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Query Registry	Remote File Copy	Man in the Browser	Multi-hop Proxy	Service Stop	Resource Hijacking
	InstallUtil	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Remote Services	Screen Capture	Multi-Stage Channels	Runtime Data Manipulation	Service Stop
	Launchctl	Create Account	Extra Window Memory Injection	Disabling Security Tools	Keychain	Security Software Discovery	Replication Through Removable Media	Video Capture	Multiband Communication	Stored Data Manipulation	System Shutdown/Reboot
	Local Job Scheduling	DLL Search Order Hijacking	File System Permissions Weakness	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	Shared Webroot		Port Knocking	Transmitted Data Manipulation	
	LSASS Driver	Dylib Hijacking	Hooking	DLL Side-Loading	Network Sniffing	System Information Discovery	SSH Hijacking		Remote Access Tools		
	Mshta	Emond	Image File Execution Options Injection	Execution Guardrails	Password Filter DLL	System Network Configuration Discovery	Taint Shared Content		Remote File Copy		
	PowerShell	External Remote Services	Image File Execution Options Injection	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Third-party Software		Standard Application Layer Protocol		
	Regsvcs/Regasm	File System Permissions Weakness	Launch Daemon	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery	Windows Admin Shares		Standard Cryptographic Protocol		
	Regsvr32	Hidden Files and Directories	New Service	Steal Web Session Cookie	System Service Discovery	System Time Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		
	Rundll32	Hooking	Parent PID Spoofing	Two-Factor Authentication Interception					Uncommonly Used Port		
	Scheduled Task	Hypervisor	Path Interception	File Deletion					Web Service		
	Scripting	Plist Modification	File System Logical Offsets								
	Service Execution	Port Monitors	Gatekeeper Bypass								
	Signed Binary Proxy Execution	PowerShell Profile	Group Policy Modification								
	Signed Script Proxy Execution	Process Injection	Hidden Files and Directories								
	Source	Launch Agent	Scheduled Task								
	Space after Filename	Launch Daemon	Hidden Users								
	Third-party Software	Launchctl	Hidden Window								
	Trap	LC_LOAD_DYLIB Addition	HISTCONTROL								
	Trusted Developer Utilities	Setuid and Setgid	Image File Execution Options Injection								
	User Execution	SID-History Injection	Indicator Blocking								
	Windows Management	Startup Items	Indicator Removal from Tools								
		Logon Scripts	Indicator Removal on Host								
		Sudo									

# APT 33

layer x +											
selection controls											
layer controls											
technique controls											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Service Scanning	Network Share Discovery	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication	Bypass User Account Control	Compile After Delivery	Credentials in Registry	Network Sniffing	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Password Policy Discovery	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Other Network Medium	Inhibit System Recovery
Spearphishing via Service	Execution through Module Load	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Network Denial of Service
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	Email Collection	Fallback Channels	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	Change Default File Association	Emond	Emond	Connection Proxy	Input Capture	Process Discovery	Remote File Copy	Input Capture	Scheduled Transfer	Exfiltration Over Physical Medium	Resource Hijacking
Valid Accounts	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Query Registry	Remote Services	Man in the Browser	Multi-hop Proxy	Scheduled Transfer	Runtime Data Manipulation
	InstallUtil	Component Object Model Hijacking	DCShadow	DCShadow	Kerberoasting	Remote System Discovery	Remote Services	Man in the Browser	Multi-Stage Channels	Scheduled Transfer	Runtime Data Manipulation
	Launchctl	Create Account	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Keychain	Security Software Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication	Scheduled Transfer	Runtime Data Manipulation
	Local Job Scheduling	DLL Search Order Hijacking	File System Permissions Weakness	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	Shared Webroot	Video Capture	Multilayer Encryption	Scheduled Transfer	Runtime Data Manipulation
	LSASS Driver	Dylib Hijacking	File System Permissions Weakness	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	System Information Discovery	SSH Hijacking		Port Knocking	Scheduled Transfer	Runtime Data Manipulation
	Mshta	Emond	Hooking	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Taint Shared Content		Remote Access Tools	Scheduled Transfer	Runtime Data Manipulation
	PowerShell	External Remote Services	Image File Execution Options Injection	Execution Guardrails	Password Filter DLL	System Network Connections Discovery	Third-party Software		Remote File Copy	Scheduled Transfer	Runtime Data Manipulation
	Regsvcs/Regasm	Launch Daemon	Launch Daemon	Exploitation for Defense Evasion	Private Keys	System Owner/User Discovery	Windows Admin Shares		Standard Application Layer Protocol	Scheduled Transfer	Runtime Data Manipulation
	Regsvr32	File System Permissions Weakness	New Service	Extra Window Memory Injection	Securityd Memory	System Service Discovery	Windows Remote Management		Standard Cryptographic Protocol	Scheduled Transfer	Runtime Data Manipulation
	Rundll32	Hidden Files and Directories	Parent PID Spoofing	File and Directory Permissions Modification	Steal Web Session Cookie	System Time Discovery			Standard Non-Application Layer Protocol	Scheduled Transfer	Runtime Data Manipulation
	Scheduled Task	Hooking	Path Interception	File Deletion	Two-Factor Authentication Interception	Virtualization/Sandbox Evasion			Uncommonly Used Port	Scheduled Transfer	Runtime Data Manipulation
	Scripting	Hypervisor	Plist Modification	File System Logical Offsets					Web Service	Scheduled Transfer	Runtime Data Manipulation
	Service Execution	Image File Execution Options Injection	Port Monitors	Gatekeeper Bypass						Scheduled Transfer	Runtime Data Manipulation
	Signed Binary Proxy Execution	Kernel Modules and Extensions	PowerShell Profile	Group Policy Modification						Scheduled Transfer	Runtime Data Manipulation
	Signed Script Proxy Execution	Launch Agent	Process Injection	Hidden Files and Directories						Scheduled Transfer	Runtime Data Manipulation
	Source	Launch Daemon	Scheduled Task	Hidden Users						Scheduled Transfer	Runtime Data Manipulation
	Space after Filename	Launchctl	Service Registry Permissions Weakness	Hidden Window						Scheduled Transfer	Runtime Data Manipulation
	Third-party Software	LC_LOAD_DYLIB Addition	HISTCONTROL	HISTCONTROL						Scheduled Transfer	Runtime Data Manipulation
	Trap	Setuid and Setgid	Image File Execution Options Injection	Indicator Blocking						Scheduled Transfer	Runtime Data Manipulation
	Trusted Developer Utilities	Local Job Scheduling	Sudo	Indicator Removal from Tools						Scheduled Transfer	Runtime Data Manipulation
	User Execution	Login Item	Startup Items	Indicator Removal on Host						Scheduled Transfer	Runtime Data Manipulation
	Windows Management Instrumentation	Logon Scripts								Scheduled Transfer	Runtime Data Manipulation
		LSASS Driver								Scheduled Transfer	Runtime Data Manipulation



# Do the Groups Matter?



# Key Takeaways

- Statistical based historical knowledge (Cyber Threat Data) of advisory's tactics will tell a story
- Everyone in the community needs help contribute to the story by associating tactics and techniques to current events
- We need to start using threat intel data to actually produce intelligence

ANOMALI PRODUCTS COMMUNITY APP STORE ISACs RESOURCES COMPANY REQUEST DEMO

WEEKLY THREAT BRIEFING

## Weekly Threat Briefing: Malicious Campaign Targets South Korean Users with Backdoor-Laced Torrents

July 9, 2019 | Anomali Labs

f t g+ in

Top 100 Threat Types

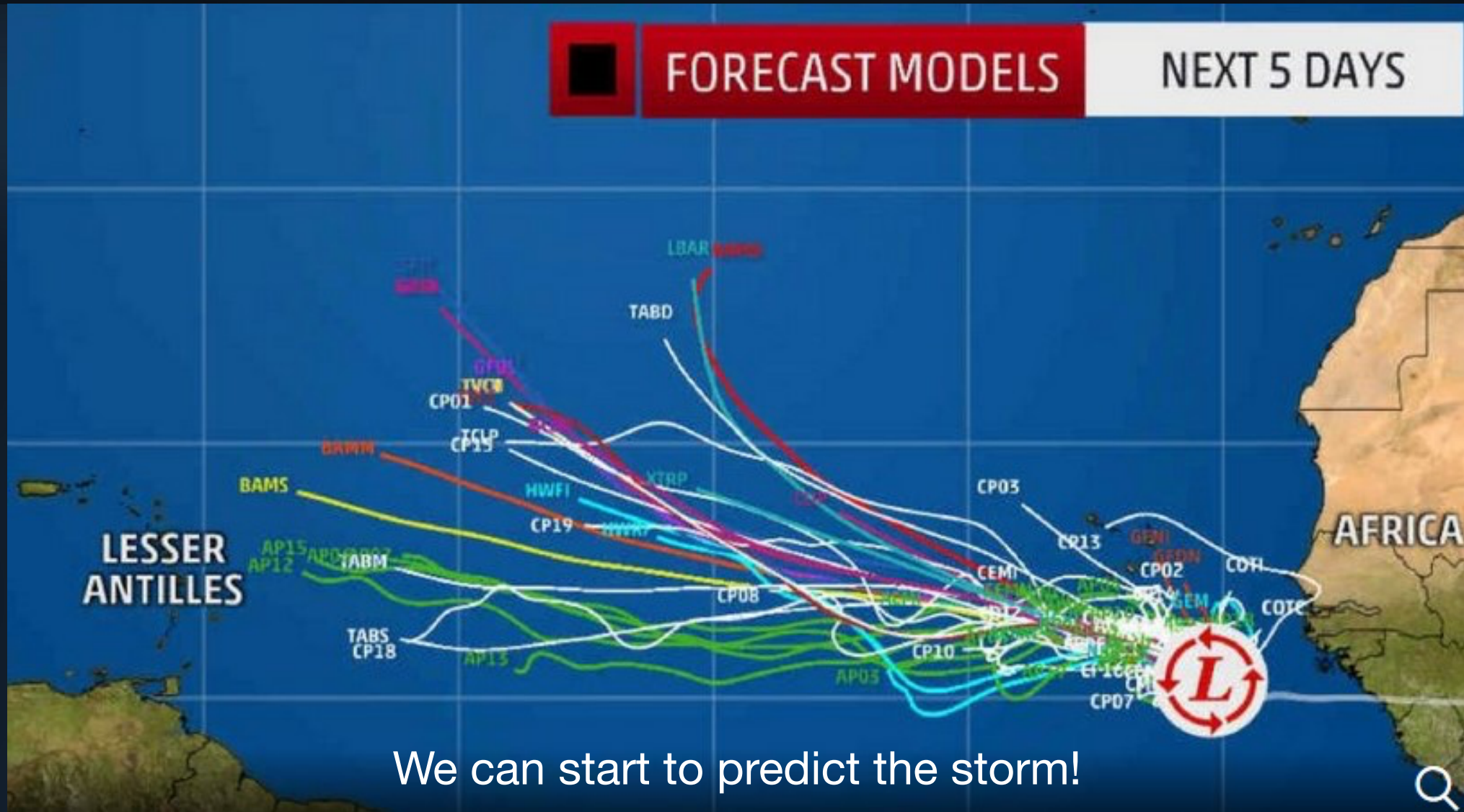
Top 100 Threat Types

MITRE ATT&CK™ Tactics, Techniques, and Procedures

This section listed below contains summaries on various threat intelligence stories that occurred during the past week. The intelligence in this week's iteration discuss the



# Once We Understand the Story



# How Does a Good Disney Story End?







Questions?