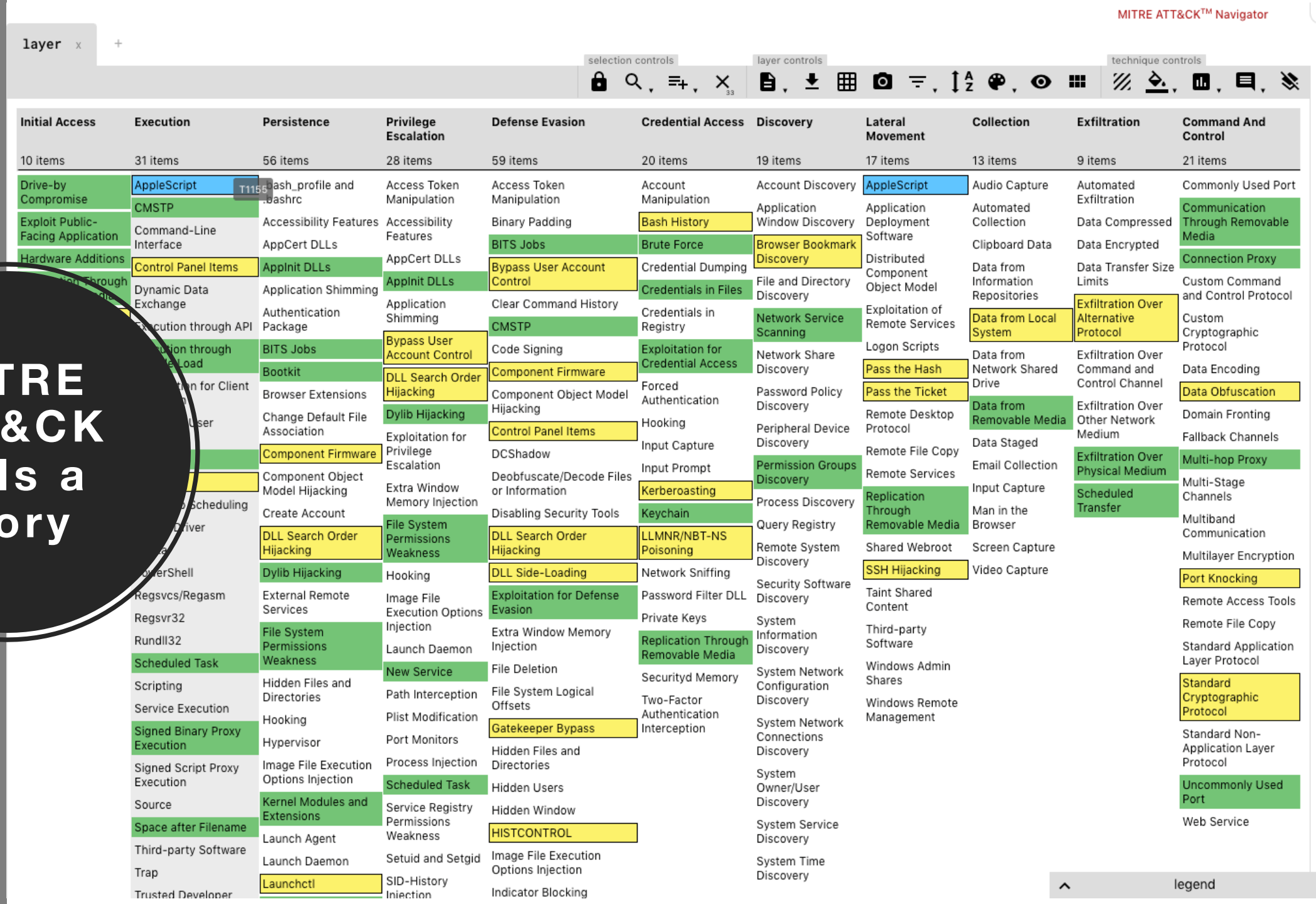
ANOMALI®

MITRE ATT&CK:
The Play at Home Edition

Nicholas Hayden

Global Head of Intelligence Operations
Anomali

MITRE ATT&CK Tells a Story



Since this is

MITRE ATT&CK:

The Play at Home Edition


What better way to tell a story then…

The Disney Way

Disney + Story = ?

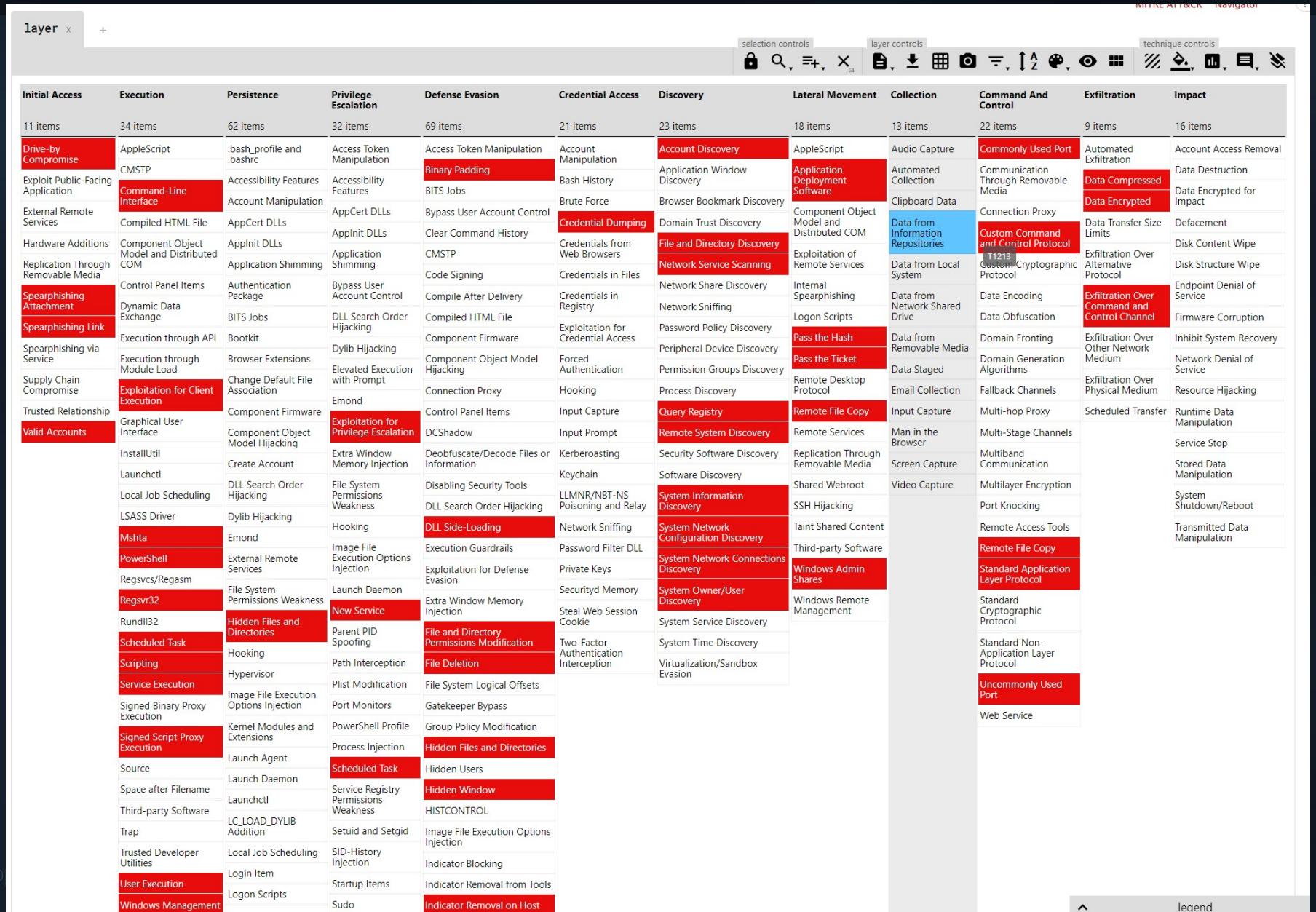

Once upon a time
In a kingdom
far far away

Or…

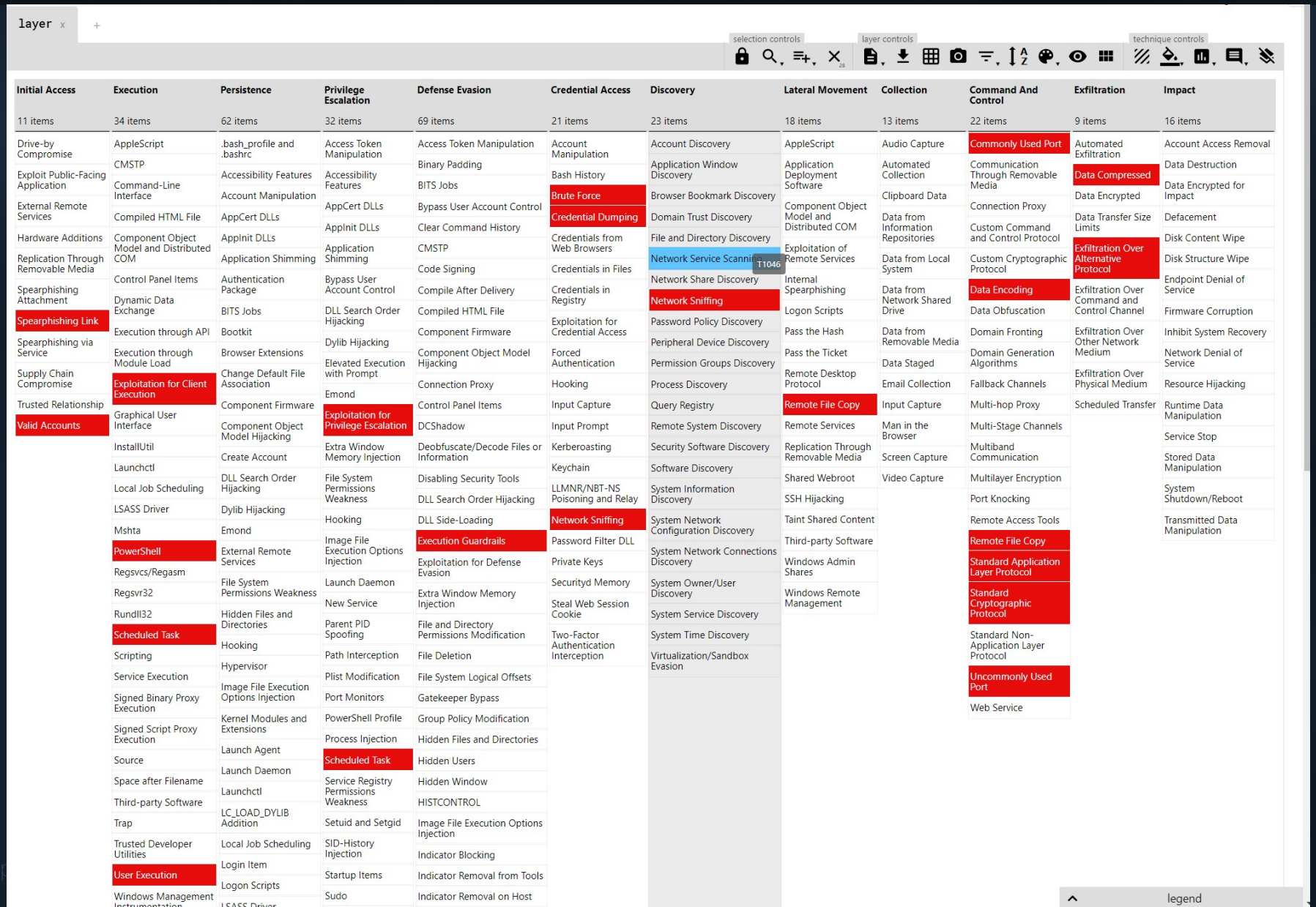
Disney + Star Wars = ?

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

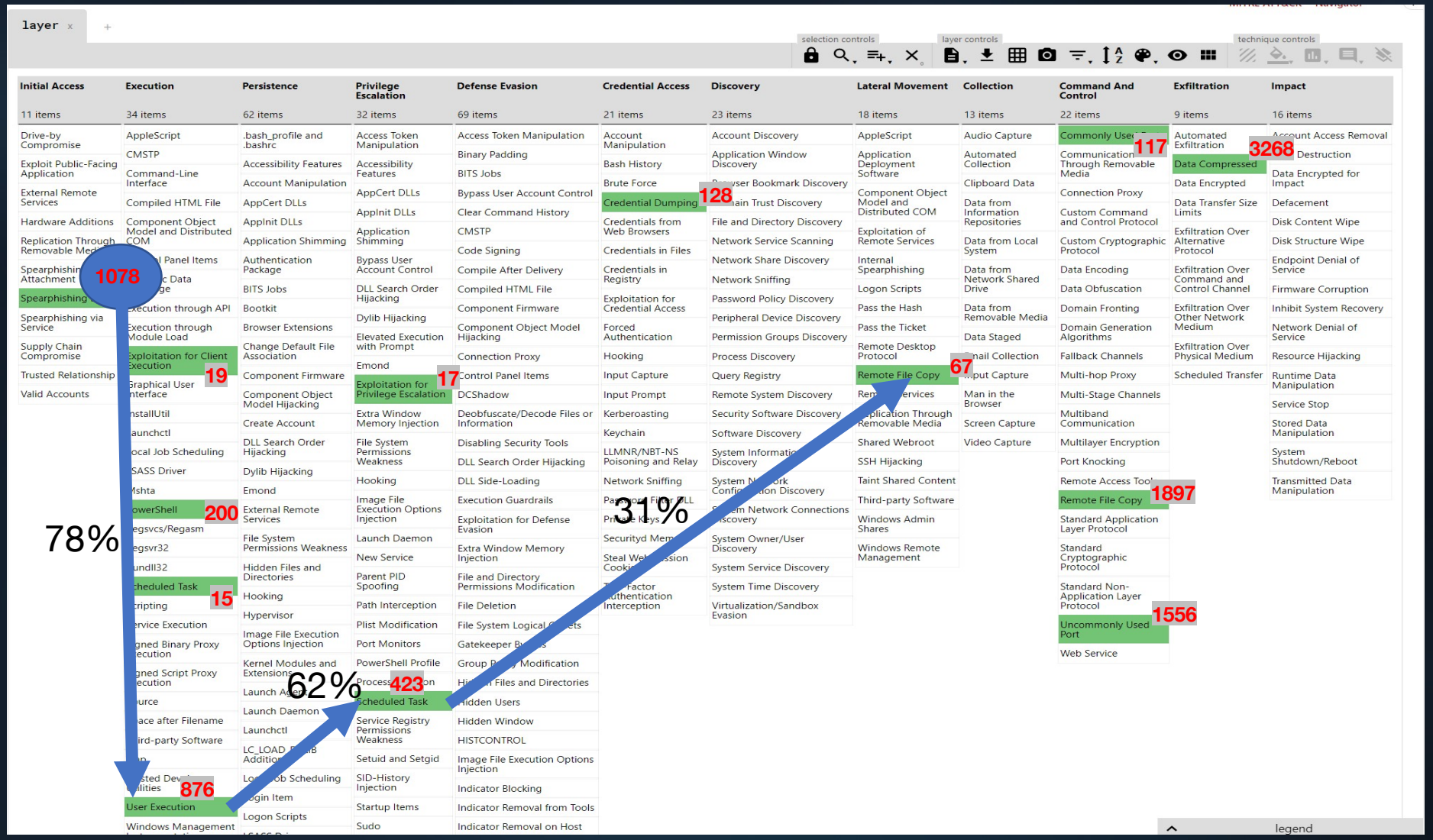
APT 32


layer x
selection controls
layer controls
technique controls
Initial Access
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
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
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
62 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
Emond
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
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection
Startup Items
Sudo
Defense Evasion
69 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
Connection Proxy
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 and Directory Permissions Modification
File Deletion
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
Indicator Removal on Host
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
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
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
23 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
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
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
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
T1213
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
16 items
Account Access Removal
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
System Shutdown/Reboot
Transmitted Data Manipulation
legend

APT 33

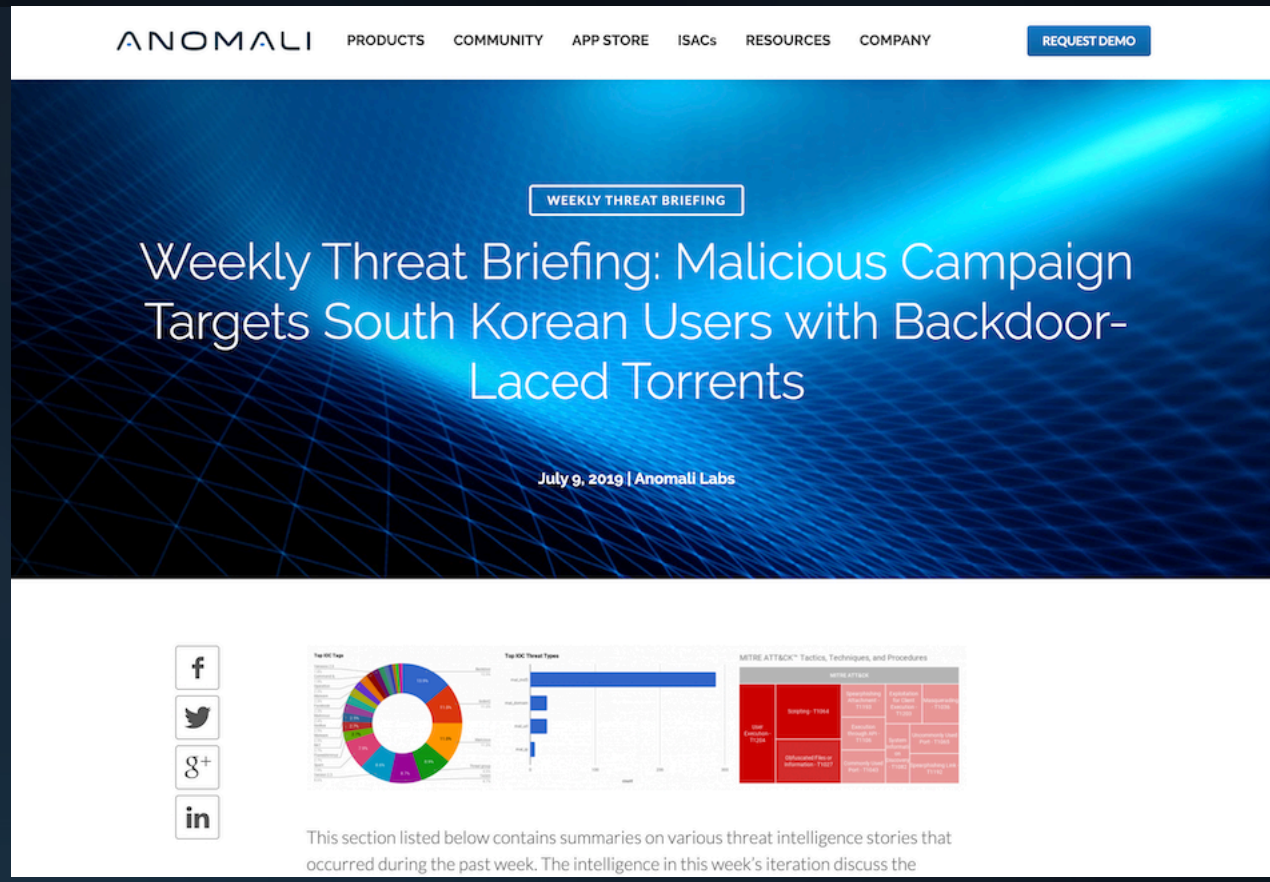

layer
selection controls
layer controls
technique controls
Initial Access
11 items
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
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
62 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
Emond
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
LSASS Driver
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection
Startup Items
Sudo
Defense Evasion
69 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
Connection Proxy
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 and Directory Permissions Modification
File Deletion
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
Indicator Removal on Host
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
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
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
T1046
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
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
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
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
16 items
Account Access Removal
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
System Shutdown/Reboot
Transmitted Data Manipulation
legend

Do the Groups Matter?

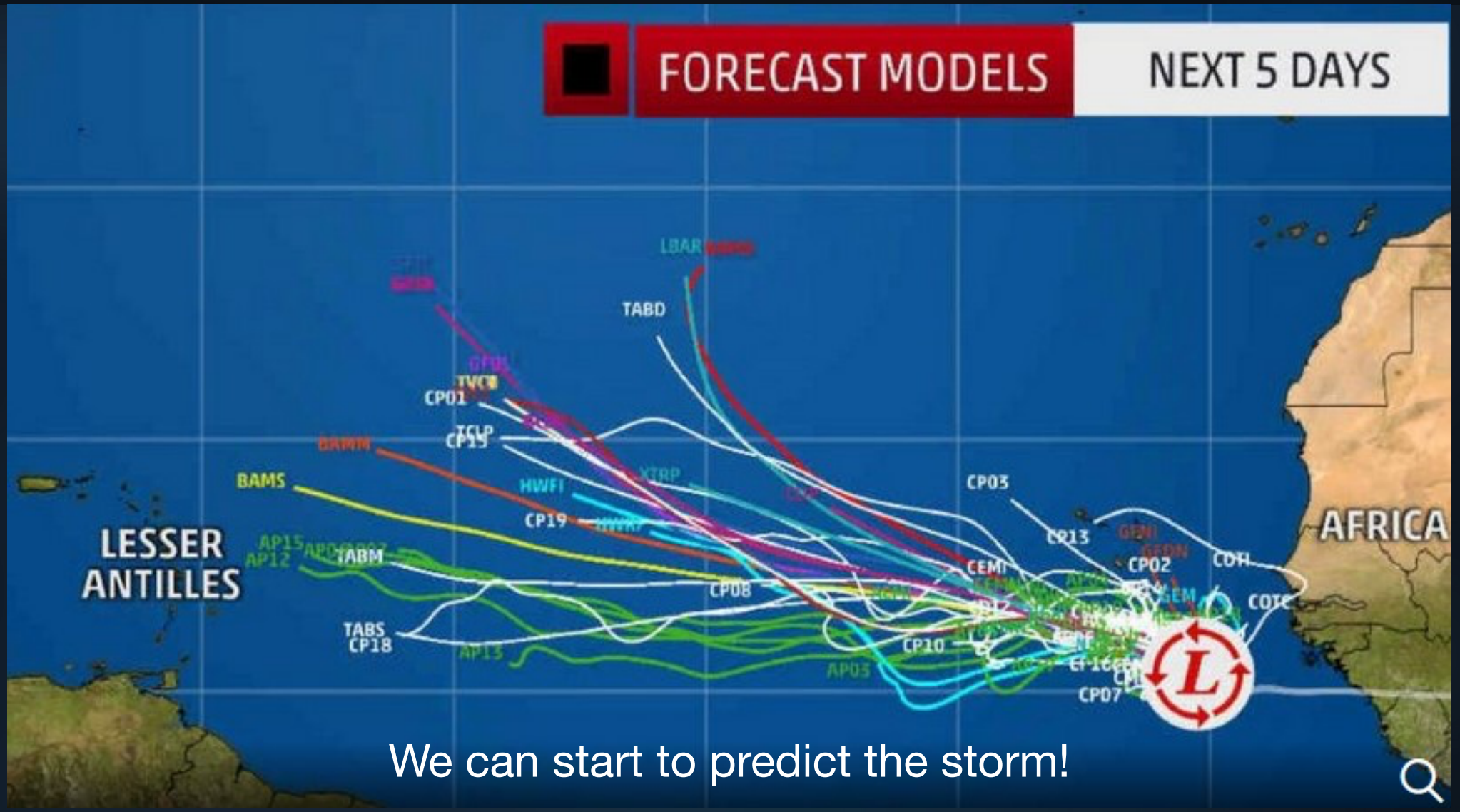


Key Takeaways

- 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



Once We Understand the Story



We can start to predict the storm!

How Does a Good Disney Story End?

Questions?