MOBIA |

Adversary Simulation Workshop

Spring 2021

Day 1:
Introduction to ATT&CK

Agenda

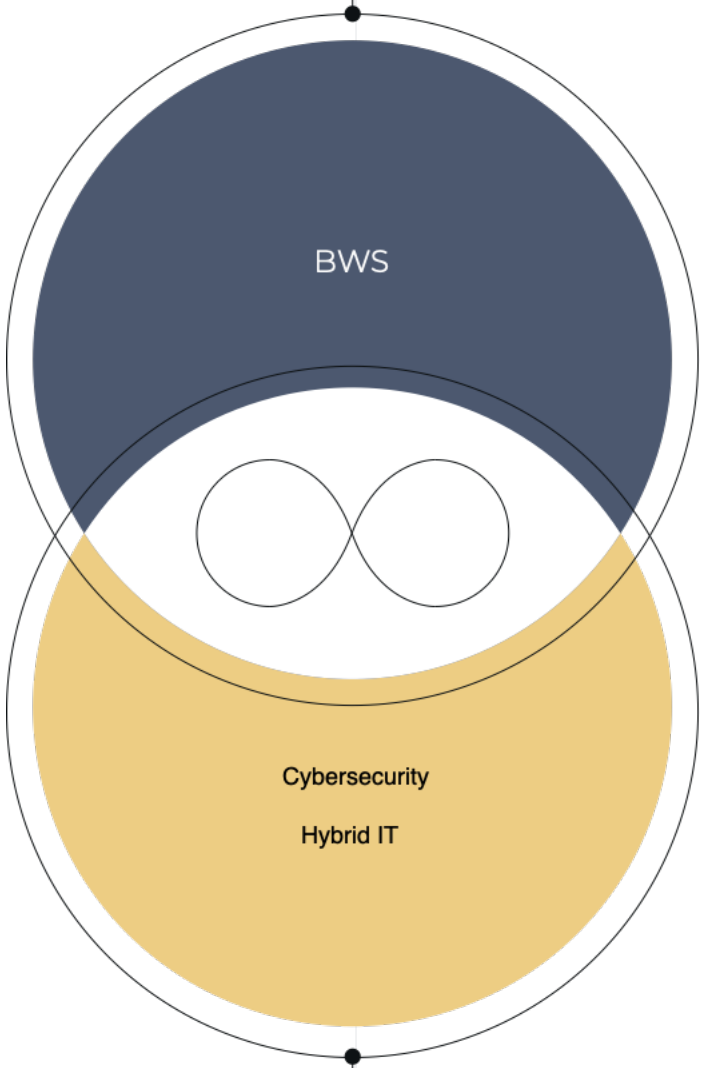
- Introduction
- The Challenge
- Prioritized Defense
- Mitre ATT&CK Framework
- Understand Your Adversary
- Testing Security Controls
- Labs!

Who we are…

We provide leading industry knowledge with an unmatched commitment to driving true business value through thoughtful technology solutions.

MOBIA is a 37yr. old business technology integrator with operations across Canada and the US. With nearly 500 employees, we serve our customers with a business first approach, diversely qualified technicians, incomparable agility and exceptional standards that set us above the rest.

Originating in telecommunications, MOBIA has expanded to become one of Canada's largest business technology integrators. Today MOBIA is a well-balanced marriage of broadband & wireless service and hybrid IT. Uniquely positioned to offer services and expertise beyond that of traditional IT.



whoami

> useradd -c “Jamie McMurray” –G “Security Services Innovation Lead”

> cd / Background in Development

> cd ../../../ Professional Services Engineer for Endpoint Security

> cd ../../ Security Consultant

> cd ../ Security Operations Lead

> cd . Splunk Certified Consultant

> while false; do echo “I’ve driven a NASCAR”; done

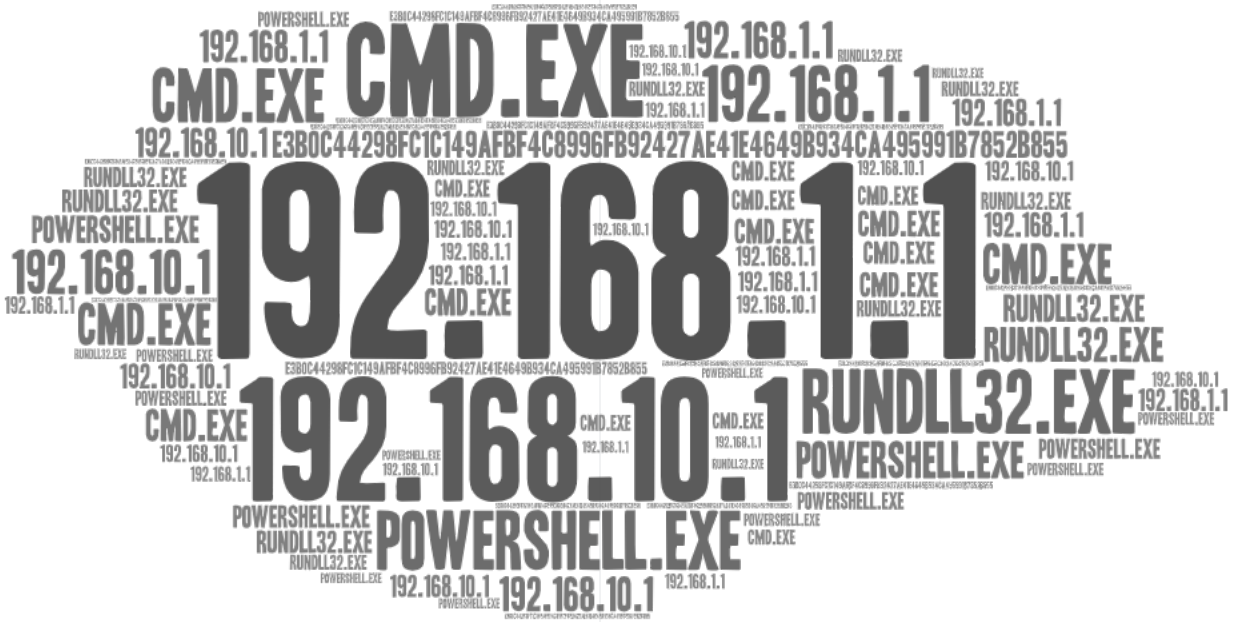
Our Approach | Security

- **Security Tools** are only successful when there is an understanding of the linkage between initial deployment and on-going operations.
- **Automation**, repeatable process and tools with focus on low-footprint operations.
- **Eliminating Gaps** in operational process is a key contributor to reduced attack surface.
- **Visibility** is key to understanding where you are today and what steps to take next.

MOBIA TECHNOLOGY INNOVATIONS

The Challenge

- **Dynamic Adversary** using Modern Tools
- **Traditional Indicators** are Static (e.g. Hash, IP, DNS)
- **Communicating** Current State and Risk can be difficult
- **Need Measure** Security Control Efficacy
- **Configuration Drift**



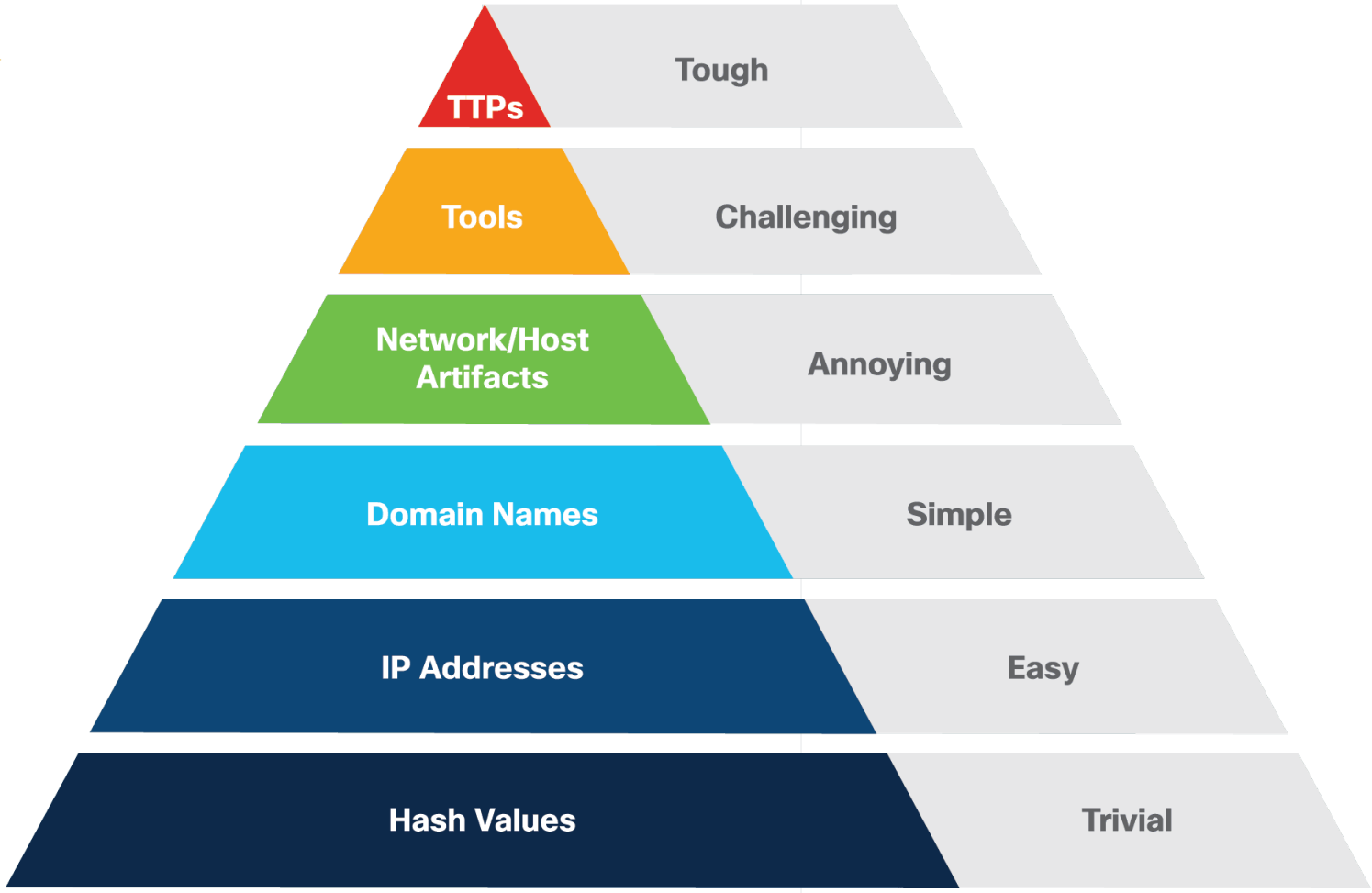
Our Goals

- Our goal is to **Embiggen our Blue Team**
- Be more **Proactive**
- **Grow Red and Purple Team** Capabilities
- Be **Better at Communicating** Our Progress

Prioritized Defense

- Adversary Focused Detection
- Make it harder for Attacker
- Understanding Adversary Goals
- Detect/Block Attacker

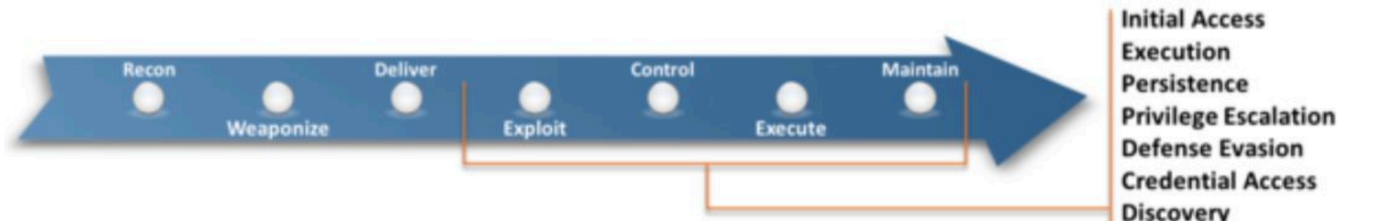
  Tactics Tools and Procedures (TTP)



Mitre ATT&CK Framework

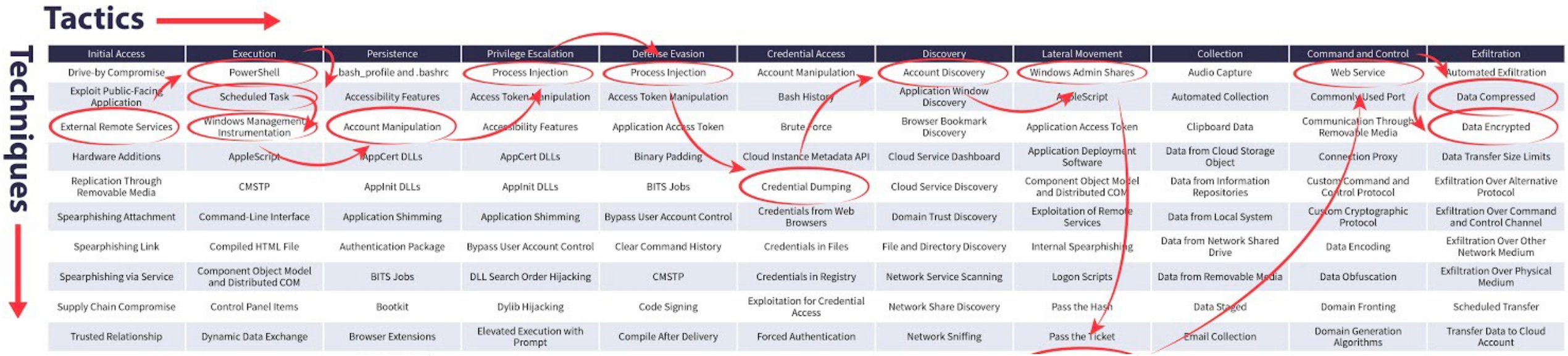
"A Framework for describing the behavior of cyber adversaries operating within enterprise networks."

- Comprehensive library of "what to look for"
- Threat model & framework



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

Mitre ATT&CK Framework



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	PowerShell	bash_profile and .bashrc	Process Injection	Process Injection	Account Manipulation	Account Discovery	Windows Admin Shares	Audio Capture	Web Service	Automated Exfiltration
Exploit Public-Facing Application	Scheduled Task	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Bash History	Application Window Discovery	AppleScript	Automated Collection	Commonly Used Port	Data Compressed
External Remote Services	Windows Management Instrumentation	Account Manipulation	Accessibility Features	Application Access Token	Brute Force	Browser Bookmark Discovery	Application Access Token	Clipboard Data	Communication Through Removable Media	Data Encrypted
Hardware Additions	AppleScript	AppCert DLLs	AppCert DLLs	Binary Padding	Cloud Instance Metadata API	Cloud Service Dashboard	Application Deployment Software	Data from Cloud Storage Object	Connection Proxy	Data Transfer Size Limits
Replication Through Removable Media	CMSTP	AppInit DLLs	AppInit DLLs	BITS Jobs	Credential Dumping	Cloud Service Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Command-Line Interface	Application Shimming	Application Shimming	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel
Spearphishing Link	Compiled HTML File	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	Exfiltration Over Other Network Medium
Spearphishing via Service	Component Object Model and Distributed COM	BITS Jobs	DLL Search Order Hijacking	CMSTP	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Removable Media	Data Obfuscation	Exfiltration Over Physical Medium
Supply Chain Compromise	Control Panel Items	Bootkit	Dylib Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data Staged	Domain Fronting	Scheduled Transfer
Trusted Relationship	Dynamic Data Exchange	Browser Extensions	Elevated Execution with Prompt	Compile After Delivery	Forced Authentication	Network Sniffing	Pass the Ticket	Email Collection	Domain Generation Algorithms	Transfer Data to Cloud Account

226 Unique Adversarial Techniques (Win, OSX, Linux, Cloud)

https://mitre-attack.github.io/attack-navigator/

Mitre ATT&CK Framework

Disclaimer:

This is not a magic bullet, tuning and investigation are still required to apply this framework effectively.

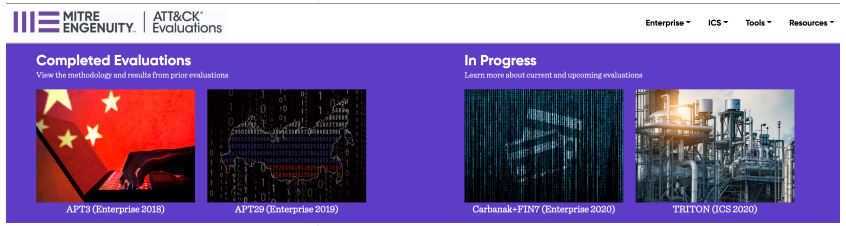
Understanding your Adversary

about
APT29
Evaluation Scope

domain
Enterprise
ATT&CK v8

filters
Windows

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	PowerShell	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Windows Command Shell	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Visual Basic	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Python	Browser Extensions	Create or Modify System Process	Direct Volume Access	Forge Web Credentials	File and Directory Discovery	Remote Services	Data from Information Repositories	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	JavaScript/JScript	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification	Input Capture	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Exploitation for Client Execution	Create Account	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Trusted Relationship	Inter-Process Communication	Create or Modify System Process	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts	Native API	Event Triggered Execution	Hijack Execution Flow	File and Directory Permissions Modification	Network Sniffing	Password Policy Discovery	Use Alternate Authentication Material	Data Staged	Multi-Stage Channels		Inhibit System Recovery
	Scheduled Task/Job	External Remote Services	Process Injection	Hide Artifacts	OS Credential Dumping	Peripheral Device Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
	Shared Modules	Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Input Capture	Non-Standard Port		Resource Hijacking
	Software Deployment Tools	Office Application Startup	Valid Accounts	Impair Defenses	Steal Web Session Cookie	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
	System Services	Pre-OS Boot		Indicator Removal on Host	Two-Factor Authentication Interception	Query Registry		Man-in-the-Middle	Proxy		System Shutdown/Reboot
	User Execution	Scheduled Task/Job		Indirect Command Execution	Unsecured Credentials	Remote System Discovery		Screen Capture	Remote Access Software		
	Windows Management Instrumentation	Server Software Component		Masquerading		Software Discovery		Video Capture	Traffic Signaling		
		Traffic Signaling		Modify Authentication Process		System Information Discovery			Web Service		
		Valid Accounts		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					



Understanding your Adversary

APT29

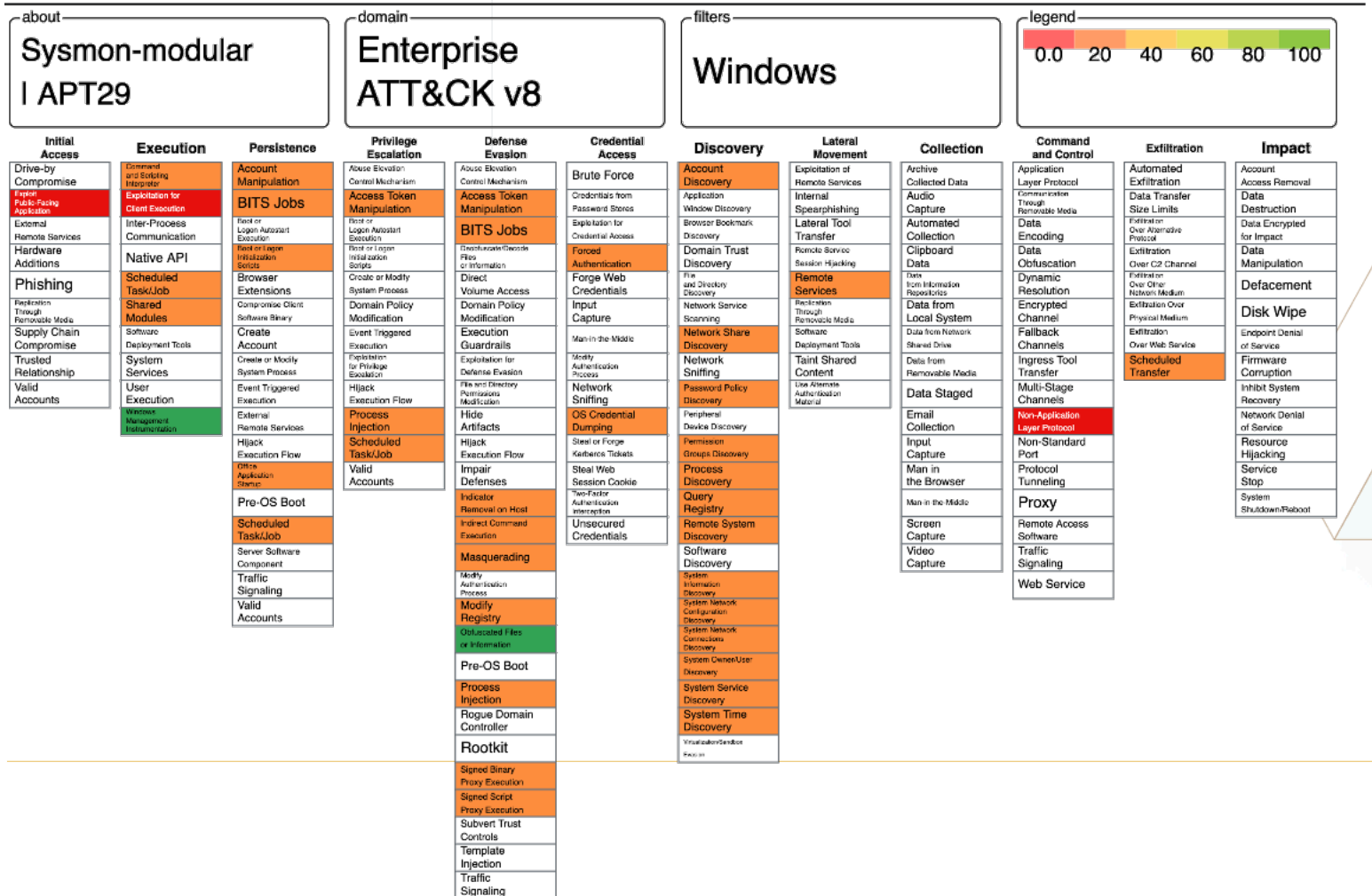
APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. [1] [2] This group reportedly compromised the Democratic National Committee starting in the summer of 2015. [3]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[7]
Enterprise	T1583	.006	Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERTOSS.[8]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT29 added Registry Run keys to establish persistence.[7]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution.[9]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell scripts to evade defenses.[10][7][9]
		.006	Command and Scripting Interpreter: Python	APT29 has developed malware variants written in Python.[5]
Enterprise	T1001	.002	Data Obfuscation: Steganography	APT29 has used steganography to hide C2 communications in images.[5]
Enterprise	T1587	.003	Develop Capabilities: Digital Certificates	APT29 has created self-signed digital certificates to enable mutual TLS authentication for malware.[11][12]
Enterprise	T1546	.008	Event Triggered Execution: Accessibility Features	APT29 used sticky-keys to obtain unauthenticated, privileged console access.[7][13]
		.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	APT29 has used WMI to establish persistence.[7][5]

Mapping Detection Capabilities



Open Source Testing Frameworks

- **Atomic Red Team** - Scripted Adversary Simulator
  https://github.com/redcanaryco/atomic-red-team
- **Caldera** – Mitre's tool for Adversary Simulation
  https://github.com/mitre/caldera
- **InfectionMonkey** – Chaos Engineering Simulation
  https://www.guardicore.com/infectionmonkey
- ***** **AdversarySimulation** – Plug-in for Splunk (Commercial)
  https://github.com/timfrazier1/AdversarySimulation

Commercial Testing Frameworks

- Mandiant Security Validation (MSV)
  https://www.fireeye.com/mandiant/security-validation.html
- AttackIQ
  https://attackiq.com
- Cymulate
  https://cymulate.com

MANDIANT®

ATTACKIQ®

Cymulate

LAB 1 – Mitre ATT&CK Navigator and ART (30 min)

LAB 2 – Install Atomic Redteam (30 mins)

LAB 3 – Import Atomic Redteam (30 mins)

LAB 4 – List Atomic Tests (30 mins)

LAB 5 – Check or Get Prereqs (30 mins)

Day 1 - Closing

- ATT&CK Navigator to Communicate and Plan
- Adversary Simulation to Validate Controls
- Day 2 – Labs, Labs and more Labs
  - Executing Tests
  - Custom Inputs
  - Cleanup
  - Chaining Multiple Tests
  - Simulating Lateral Movement