Red Team Strategies for Helping Protect the Modern Workplace

大家好!

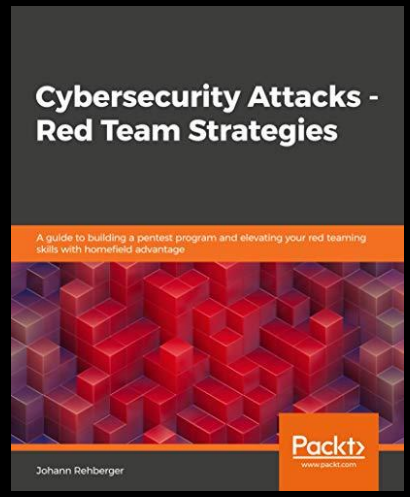
Johann Rehberger

WUNDERWUZZI, LLC
February 2021

Introduction - Johann Rehberger

Enjoy breaking things and help fixing them.

- Established and managed multiple offensive security teams throughout career
- Always learning and love teaching



Twitter: @wunderwuzzi23
Blog: https://embracethered.com

Uber

Agenda

- Modern Workplace
- How can the red team help?
- Zero Trust, Assume Breach and Homefield Advantage
- MITRE ATT&CK and ATT&CK for Mobile
- Survivorship bias and closing thoughts

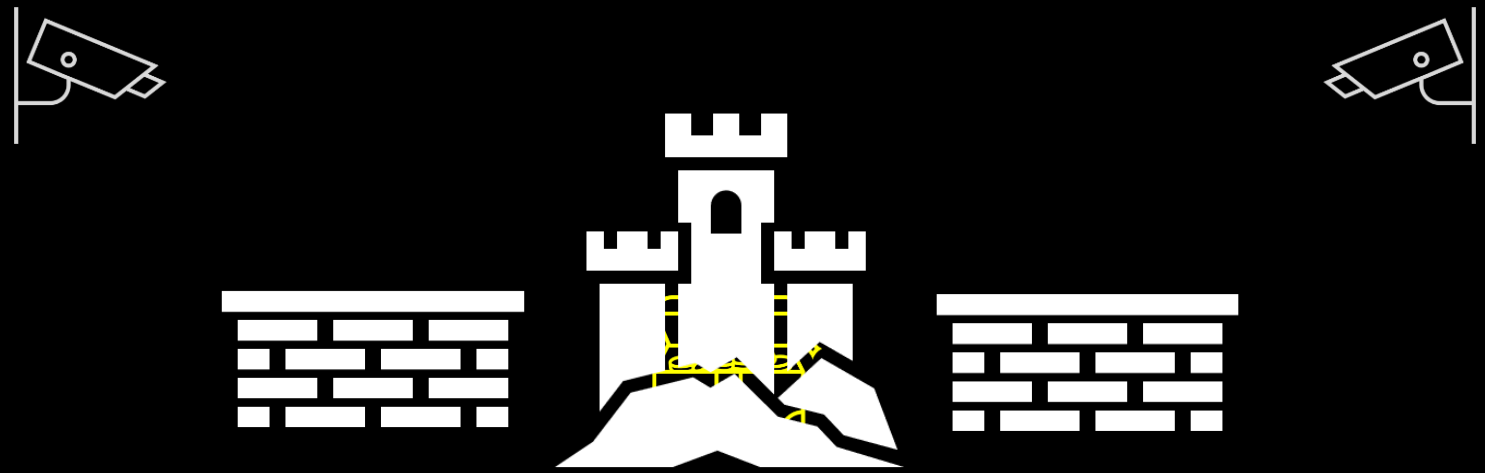
Modern workplace

Work from anywhere, any time on any device

Without losing control over your data

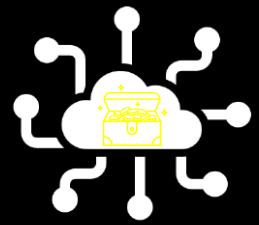
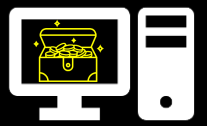
Security is about helping to enabling these scenarios for the business

Closed shop security and Full Trust



Location == Security

Perimeter-less security and Zero Trust

"Within a typical organisation today, 60% of the endpoints containing or accessing enterprise data are mobile." -- Zimperium, Inc.



Location by itself doesn't grant access

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 06, 2020

Alert Number
I-100620-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

A COVID 19-Driven Increase in Telework from Hotels Could Pose a Cyber Security Risk for Guests

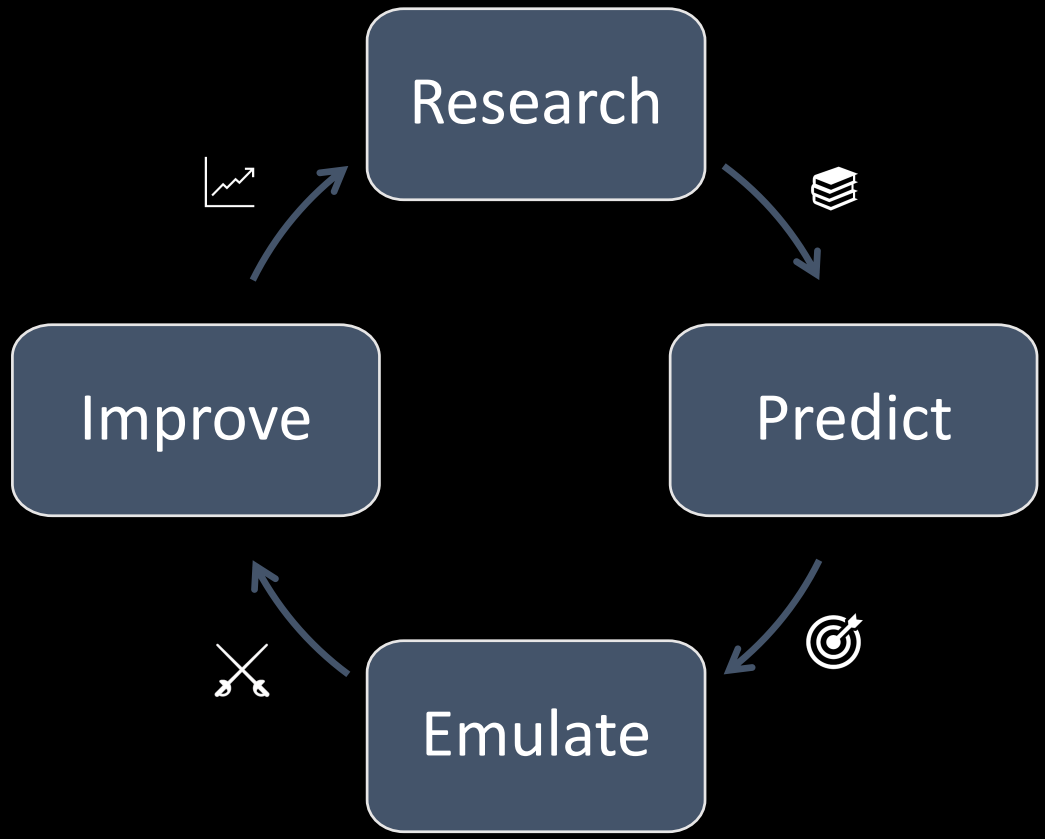
The Federal Bureau of Investigation is issuing this announcement to encourage Americans to exercise caution when using hotel wireless networks (Wi-Fi) for telework. FBI has observed a trend where individuals who were previously teleworking from home are beginning to telework from hotels. US hotels, predominantly in major cities, have begun to advertise daytime room reservations for guests seeking a quiet, distraction-free work environment. While this option may be appealing, accessing sensitive information from hotel Wi-Fi poses an increased security risk over home Wi-Fi networks. Malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests. Following good cyber security practices can minimize some of the risks associated with using hotel Wi-Fi for telework.

DANGERS OF USING HOTEL WI-FI

Remote Work and Mobile Devices

The adversary will come to your house!

How can a red team help?



Phase 1: Research

Who might attack and why?

Hacktivists

Financial gain

Research and learning

Espionage

Intelligence-gathering

Criminals

Demonstration of power

“Script Kiddies”

Political gain

Self-fulfillment

Nation-states

Opportunistic hacking

Phase 2: Predict

Planning a red team operation

Threat Informed Offense

Legal Implications and creation of safeguards
(esp. on telework environments)

Asset Inventory

Homefield Advantage

Decide on mode of operation:
Emulation, Simulation, Tabletop-exercise

Asset and Data Classification

Building risk models
(e.g. Monte Carlo Simulations)

What is MITRE ATT&CK®

MITRE is a not for profit, federally founded research and development centers to make the cyber world more secure.

ATT&CK

- Knowledgebase and Framework for adversarial behavior
- Tactics and Techniques and Common Knowledge

Matrices

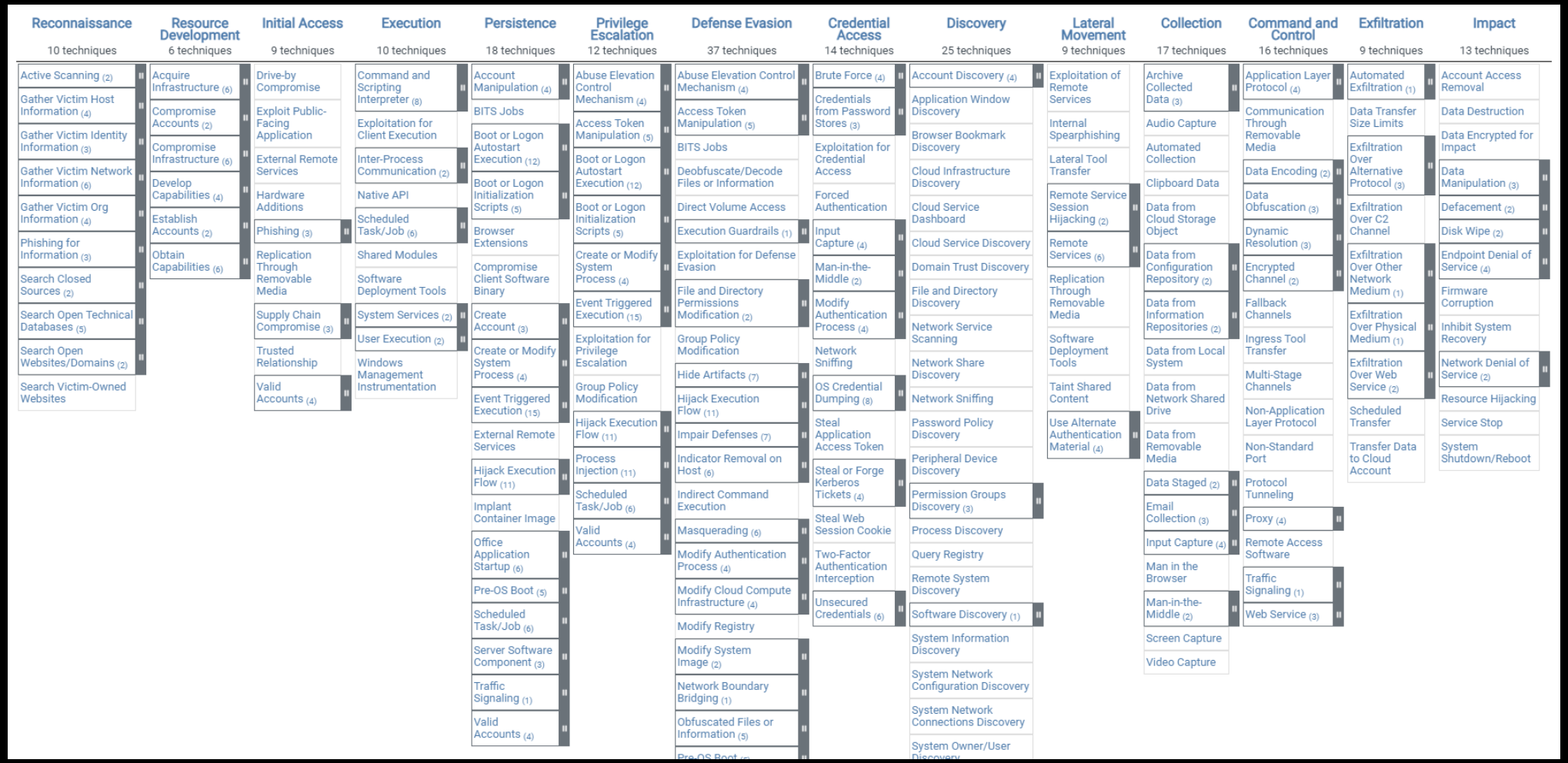
- ATT&CK for Enterprise, Mobile, Industrial Control Systems

Others

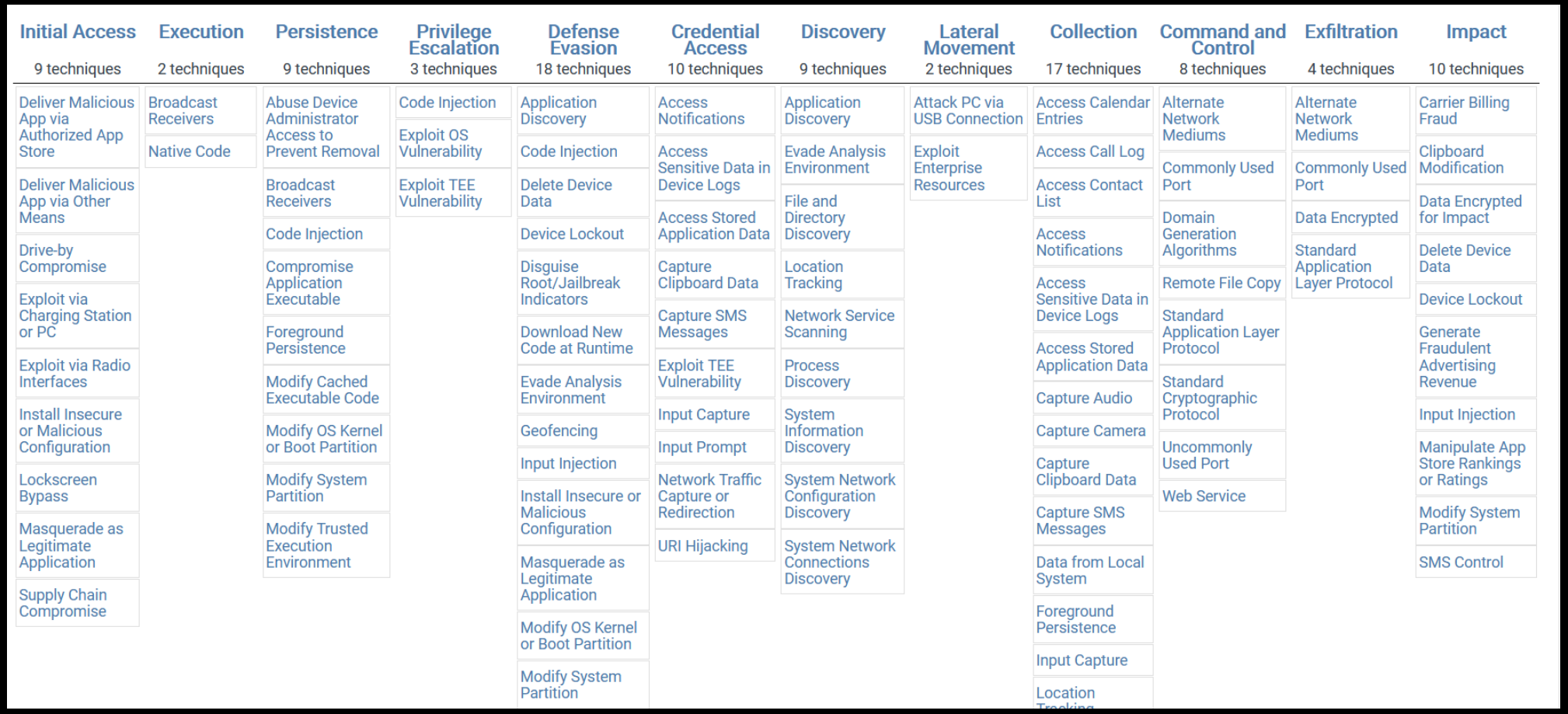
- ATT&CK for AI, Kubernetes,…

ATT&CK focuses on public threat intelligence.

ATT&CK for Enterprise



ATT&CK for Mobile

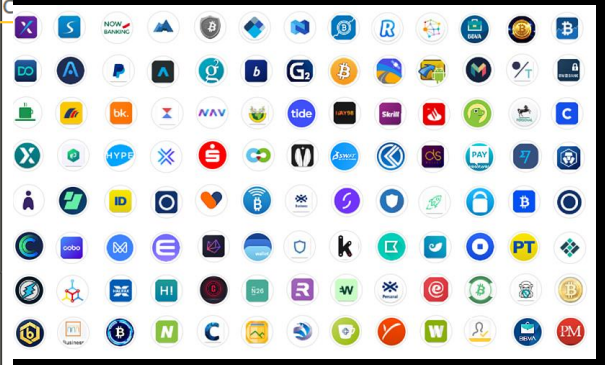


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	2 techniques	9 techniques	3 techniques	18 techniques	10 techniques	9 techniques	2 techniques	17 techniques	8 techniques	4 techniques	10 techniques
Deliver Malicious App via Authorized App Store	Broadcast Receivers	Abuse Device Administrator Access to Prevent Removal	Code Injection	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Carrier Billing Fraud
Deliver Malicious App via Other Means	Native Code	Broadcast Receivers	Exploit OS Vulnerability	Code Injection	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Access Call Log	Commonly Used Port	Commonly Used Port	Clipboard Modification
Drive-by Compromise		Code Injection	Exploit TEE Vulnerability	Delete Device Data	Access Stored Application Data	File and Directory Discovery		Access Contact List	Domain Generation Algorithms	Data Encrypted	Data Encrypted for Impact
Exploit via Charging Station or PC		Compromise Application Executable		Device Lockout	Capture Clipboard Data	Location Tracking		Access Notifications	Remote File Copy	Standard Application Layer Protocol	Delete Device Data
Exploit via Radio Interfaces		Foreground Persistence		Disguise Root/Jailbreak Indicators	Capture SMS Messages	Network Service Scanning		Access Sensitive Data in Device Logs	Standard Application Layer Protocol		Device Lockout
Install Insecure or Malicious Configuration		Modify Cached Executable Code		Download New Code at Runtime	Exploit TEE Vulnerability	Process Discovery		Access Stored Application Data	Standard Cryptographic Protocol		Generate Fraudulent Advertising Revenue
Lockscreen Bypass		Modify OS Kernel or Boot Partition		Evade Analysis Environment	Input Capture	System Information Discovery		Capture Audio	Uncommonly Used Port		Input Injection
Masquerade as Legitimate Application		Modify System Partition		Geofencing	Input Prompt	System Network Configuration Discovery		Capture Camera	Web Service		Manipulate App Store Rankings or Ratings
Supply Chain Compromise		Modify Trusted Execution Environment		Input Injection	Network Traffic Capture or Redirection	System Network Connections Discovery		Capture Clipboard Data			Modify System Partition
				Install Insecure or Malicious Configuration	URI Hijacking			Capture SMS Messages			SMS Control
				Masquerade as Legitimate Application				Data from Local System			
				Modify OS Kernel or Boot Partition				Foreground Persistence			
				Modify System Partition				Input Capture			
								Location Tracking			

Android

- First identi
- Targets ove
- Leverages A
- Collects pe nking information
- Can read S

Initial Access	Persistence	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	C2
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Masquerade as Legitimate Application	Capture SMS Messages	Application Discovery	Input capture	Data Encrypted	Standard Cryptographic Protocol
Lockscreen Bypass		Suppress Application Icon	Input Capture	System Information Discovery	Access Sensitive Data in Device Logs	Standard Application Layer Protocol	
		Download New Code at Runtime			Access Stored Application Data		
		Input Injection					



NOCTURNUS Threa
https://www.cybere orn
https://www.cybereason.com/hubfs/Threat%20Alert%20EventBot.pdf

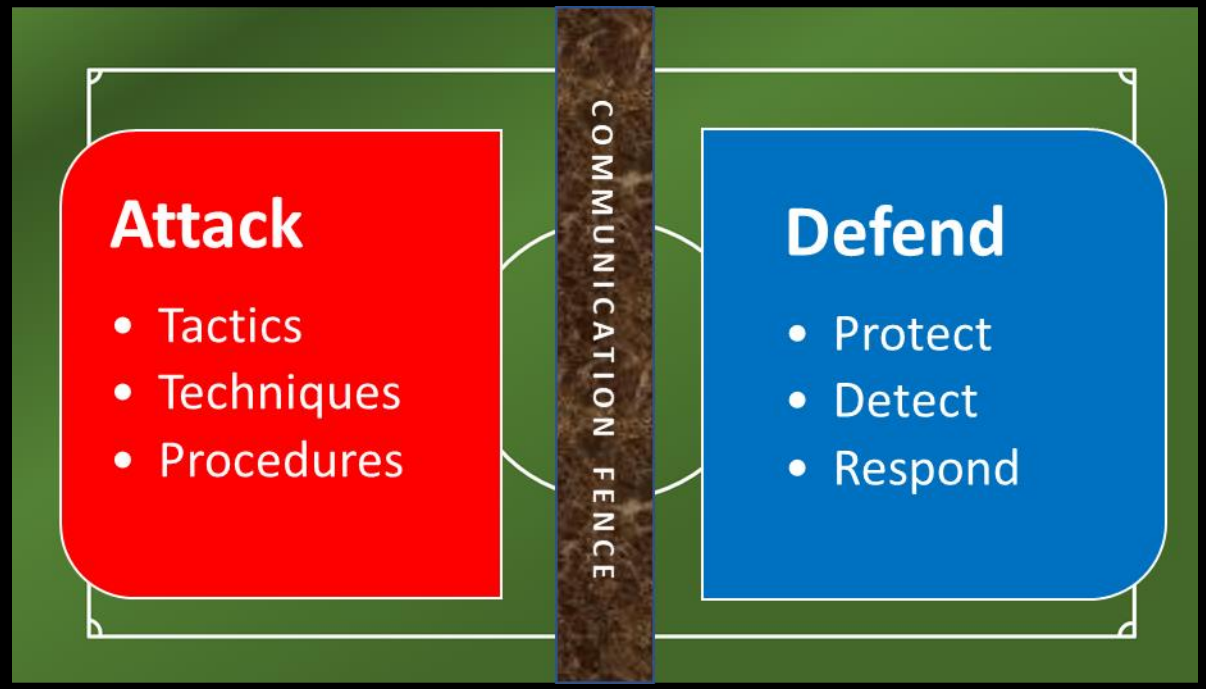
Phase 3: Emulate

Execute operation

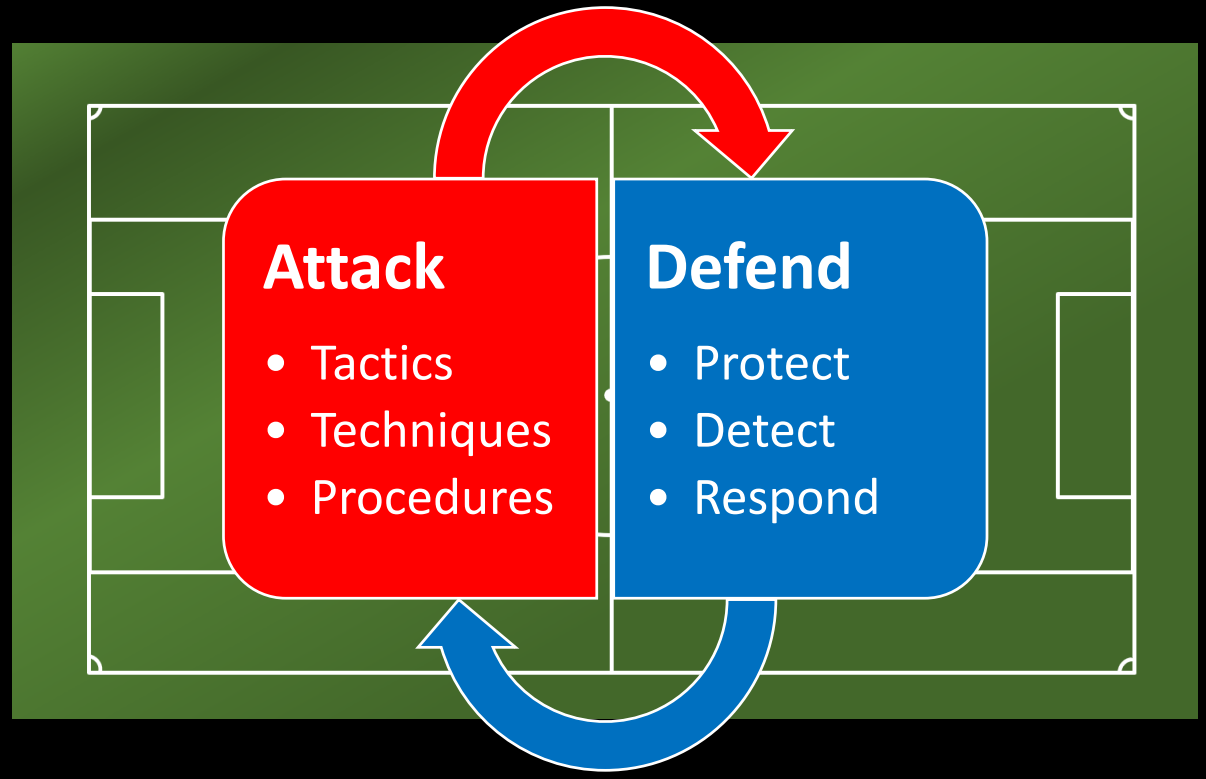
- Test Automation vs Purple Teaming vs Red Teaming
- Automation and Tooling (e.g. Caldera, Atomic from Red Canary,..)

- Threat Hunting
- Leveraging Homefield Advantage

Communication fence limits progress



Leveraging Homefield Advantage



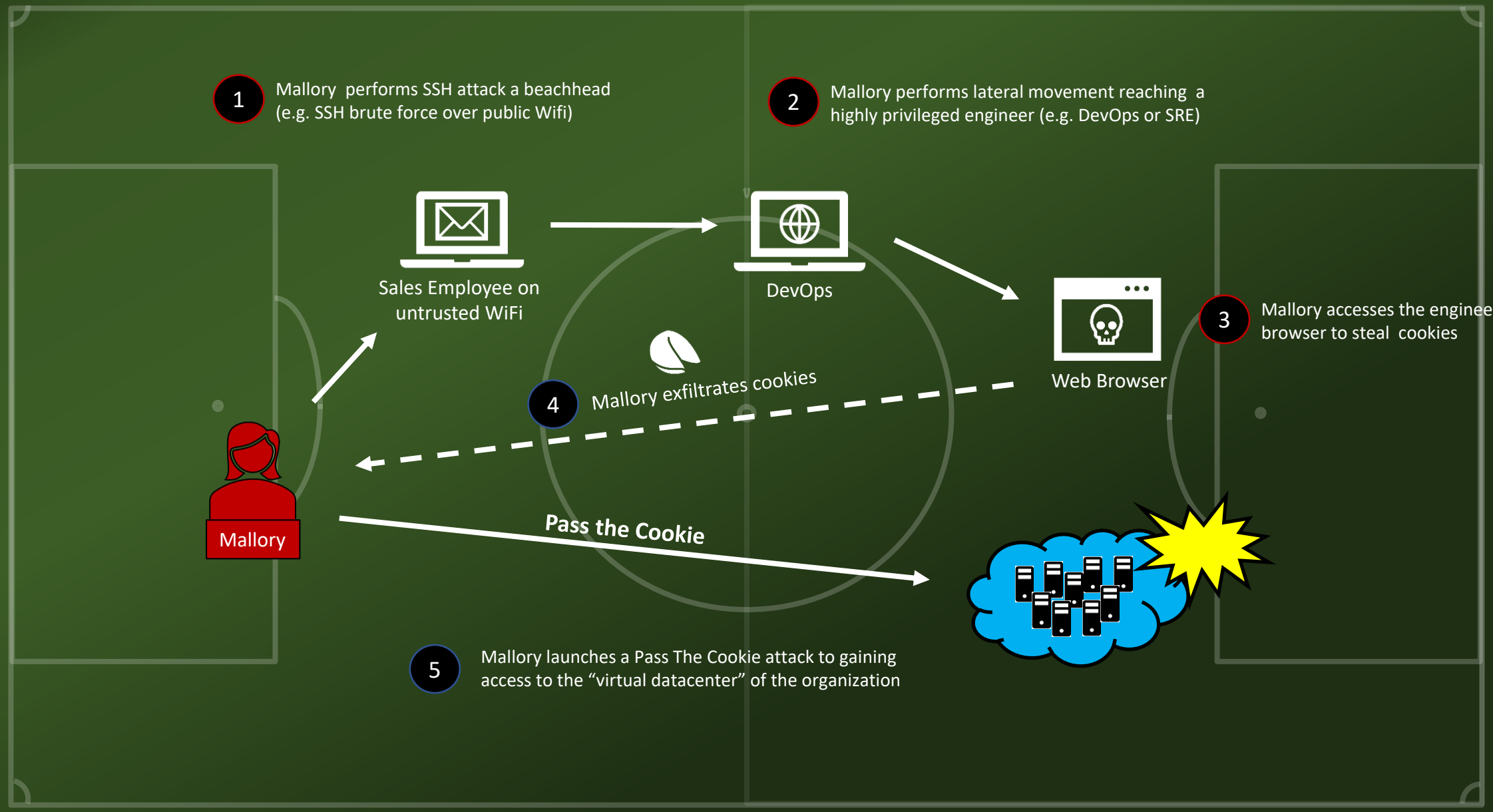
Phase 4: Improve

Implement Mitigations

- Implement mitigations and improve security posture
- Refine attack graphs and risk models

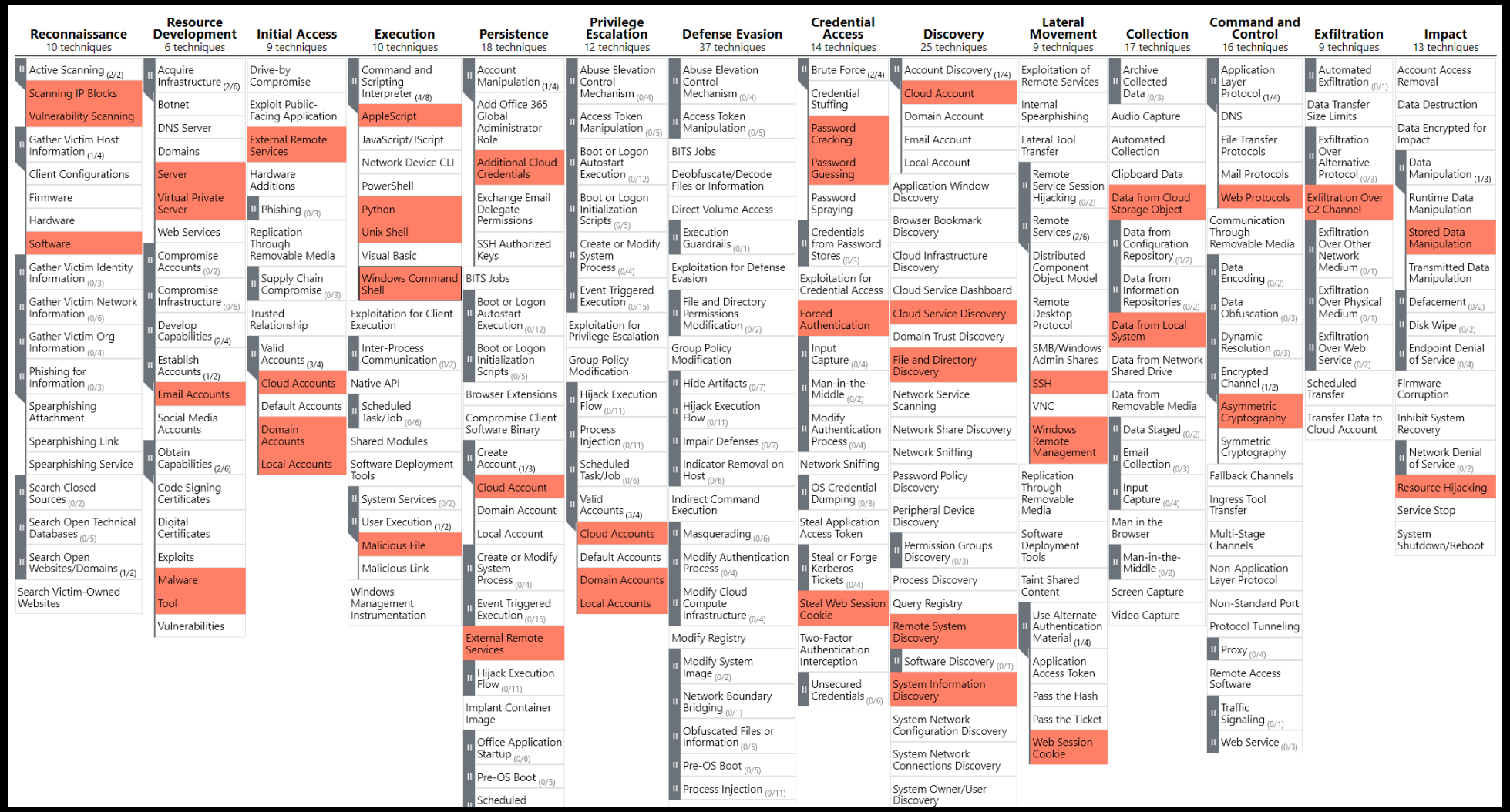
- The Blue Team is not only the security organization
  - Include engineers and others who build/use the systems
  - “Management by walking around”

- Education and sharing outcomes of operations with the organization



MITRE ATT&CK Navigator

ATT&CK Bingo!



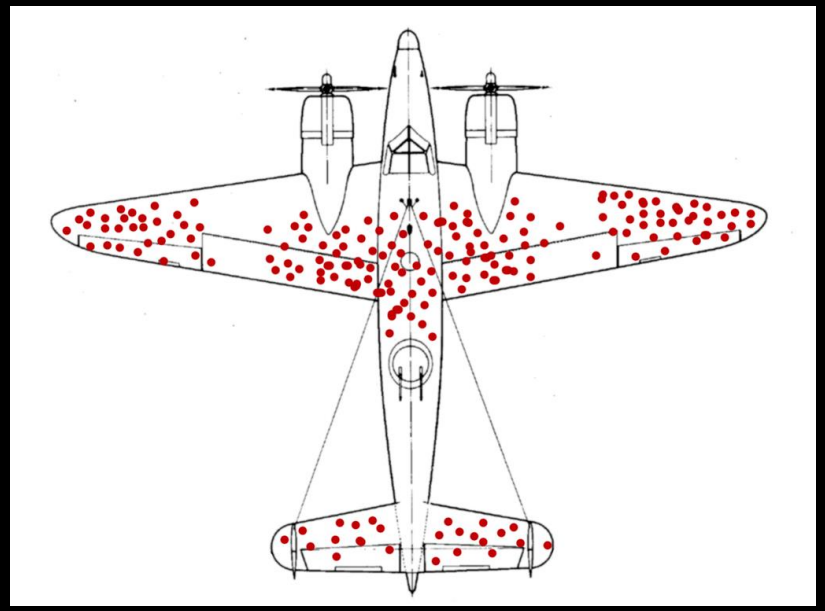
Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2/2)	Acquire Infrastructure (2/6)	Drive-by Compromise	Command and Scripting Interpreter (4/8)	Account Manipulation (1/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (2/4)	Account Discovery (1/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Scanning IP Blocks	Botnet	Exploit Public-Facing Application	AppleScript	Add Office 365 Global Administrator Role	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credential Stuffing	Cloud Account	Internal Spearphishing	Audio Capture	DNS	Data Transfer Size Limits	Data Destruction
Vulnerability Scanning	DNS Server	External Remote Services	JavaScript/JScript	Additional Cloud Credentials	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Password Cracking	Domain Account	Lateral Tool Transfer	Automated Collection	File Transfer Protocols	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Host Information (1/4)	Domains	Hardware Additions	Network Device CLI	Exchange Email Delegate Permissions	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Password Guessing	Email Account	Remote Service Session Hijacking (0/2)	Clipboard Data	Mail Protocols	Exfiltration Over C2 Channel	Data Manipulation (1/3)
Client Configurations	Server	Phishing (0/3)	PowerShell	SSH Authorized Keys	Create or Modify System Process (0/4)	Direct Volume Access	Password Spraying	Local Account	Remote Services (2/6)	Data from Cloud Storage Object	Web Protocols	Exfiltration Over Other Network Medium (0/1)	Runtime Data Manipulation
Firmware	Virtual Private Server	Replication Through Removable Media	Python	BITS Jobs	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Credentials from Password Stores (0/3)	Application Window Discovery	Distributed Component Object Model	Data from Configuration Repository (0/2)	Communication Through Removable Media	Exfiltration Over Physical Medium (0/1)	Stored Data Manipulation
Hardware	Web Services	Supply Chain Compromise (0/3)	Unix Shell	Boot or Logon Autostart Execution (0/12)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Desktop Protocol	Data from Information Repositories (0/2)	Data Encoding (0/2)	Exfiltration Over Web Service (0/2)	Transmitted Data Manipulation
Software	Compromise Accounts (0/2)	Trusted Relationship	Visual Basic	Boot or Logon Initialization Scripts (0/5)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Forced Authentication	Cloud Infrastructure Discovery	SMB/Windows Admin Shares	Data from Local System	Data Obfuscation (0/3)	Scheduled Transfer	Defacement (0/2)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	Valid Accounts (3/4)	Windows Command Shell	Browser Extensions	Hijack Execution Flow (0/11)	Group Policy Modification	Input Capture (0/4)	Cloud Service Dashboard	SSH	Data from Network Shared Drive	Dynamic Resolution (0/3)	Transfer Data to Cloud Account	Disk Wipe (0/2)
Gather Victim Network Information (0/6)	Develop Capabilities (2/4)	Cloud Accounts	Exploitation for Client Execution	Compromise Client Software Binary	Process Injection (0/11)	Hide Artifacts (0/7)	Man-in-the-Middle (0/2)	Cloud Service Discovery	VNC	Data from Removable Media	Encrypted Channel (1/2)		Endpoint Denial of Service (0/4)
Gather Victim Org Information (0/4)	Establish Accounts (1/2)	Default Accounts	Inter-Process Communication (0/2)	Create Account (1/3)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Modify Authentication Process (0/4)	Domain Trust Discovery	Windows Remote Management	Data Staged (0/2)	Asymmetric Cryptography		Firmware Corruption
Phishing for Information (0/3)	Email Accounts	Domain Accounts	Native API	Cloud Account	Valid Accounts (3/4)	Impair Defenses (0/7)	Network Sniffing	File and Directory Discovery	Replication Through Removable Media	Email Collection (0/3)	Symmetric Cryptography		Inhibit System Recovery
Spearphishing Attachment	Social Media Accounts	Local Accounts	Scheduled Task/Job (0/6)	Domain Account	Cloud Accounts	Indicator Removal on Host (0/6)	OS Credential Dumping (0/8)	Network Service Scanning	Software Deployment Tools	Input Capture (0/4)	Fallback Channels		Network Denial of Service (0/2)
Spearphishing Link	Obtain Capabilities (2/6)		Shared Modules	Local Account	Default Accounts	Indirect Command Execution	Steal Application Access Token	Network Share Discovery	Taint Shared Content	Man in the Browser	Ingress Tool Transfer		Resource Hijacking
Spearphishing Service	Code Signing Certificates		Software Deployment Tools	Create or Modify System Process (0/4)	Domain Accounts	Masquerading (0/6)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing	Use Alternate Authentication Material (1/4)	Man-in-the-Middle (0/2)	Multi-Stage Channels		Service Stop
Search Closed Sources (0/2)	Digital Certificates		System Services (0/2)	Event Triggered Execution (0/15)	Local Accounts	Modify Authentication Process (0/4)	Steal Web Session Cookie	Password Policy Discovery	Application Access Token	Screen Capture	Non-Application Layer Protocol		System Shutdown/Reboot
Search Open Technical Databases (0/5)	Exploits		User Execution (1/2)	External Remote Services		Modify Cloud Compute Infrastructure (0/4)	Two-Factor Authentication Interception	Peripheral Device Discovery	Pass the Hash	Video Capture	Non-Standard Port		
Search Open Websites/Domains (1/2)	Malware		Malicious File	Hijack Execution Flow (0/11)		Modify Registry	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)	Pass the Ticket		Protocol Tunneling		
Search Victim-Owned Websites	Tool		Malicious Link	Implant Container Image		Modify System Image (0/2)		Process Discovery	Web Session Cookie		Proxy (0/4)		
	Vulnerabilities		Windows Management Instrumentation	Office Application Startup (0/6)		Network Boundary Bridging (0/1)		Query Registry			Remote Access Software		
				Pre-OS Boot (0/5)		Obfuscated Files or Information (0/5)		Remote System Discovery			Traffic Signaling (0/1)		
				Scheduled		Pre-OS Boot (0/5)		Software Discovery (0/1)			Web Service (0/3)		
						Process Injection (0/11)		System Information Discovery					
								System Network Configuration Discovery					
								System Network Connections Discovery					
								System Owner/User Discovery					

Zero Trust

Assume Breach

Homefield Advantage

Survivorship Bias



Red Teaming, ATT&CK TTPs and threat intel feeds

- **ATT&CK focuses on known tactics, techniques and procedures**
  It is based on only on open-source intel – by design.

- **Insider Threats are not explicitly captured** – compensate for that in operations
- **ATT&CK is great.**
  Use it to your advantage to identify weak spots, communicate progress and so forth.

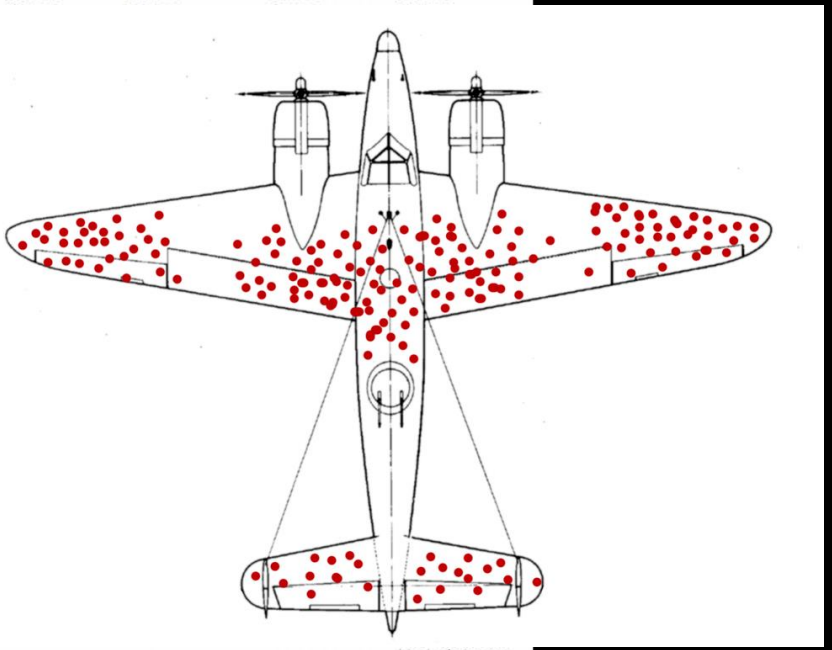
- **MITRE's CAPEC** (Common Attack Pattern Enumeration) that can be very useful for documenting and planning operations also

MITRE ATT&CK™ Navigator

Operation Homefield Advantage | Blue Team View | layer by operation

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	33 items	59 items	28 items	67 items	19 items	22 items	17 items				
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript		Remote Access Tools		Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software		Remote File Copy		
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model		Standard Application Layer Protocol		
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Servi		Standard Cryptographic Protocol		
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts				
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash				
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticke				
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Deskt Protocol				
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File C				
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Servi				
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable M				
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webro				
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking				
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content				
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software				
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares				
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management				
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery					
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery					
	Scheduled Task			Extra Window Memory Injection		System Service Discovery					
	Scripting			File Deletion		System Time Discovery					
	Service Execution			File Permissions Modification		Virtualization/Sandbox					
	Signed Binary Proxy			File System Logical Offsets							



Call to action

- Perform an Assume Breach exercise from mobile devices and telework devices
- Review the Mobile ATT&CK matrix for more insights

- Do an exercise for the Blue Team infrastructure
  => one central system to rule all hosts via endpoint agents

- Lock down machines
  - ✓Review remote management exposure
  - ✓Check your laptop right now, does it have SMB, WinRM, RDP or SSH exposed?
  - ✓How many administrator accounts are on your machine right now?

- Remember that the company's adversary will now come to your house.

謝謝你!

Johann Rehberger
johann@wunderwuzzi.net
Twitter: @wunderwuzzi23
embracethered.com

References

- https://blog.zimperium.com/zimperiums-state-of-enterprise-mobile-security-report-says-every-enterprise-has-mobile-security-threats-and-attacks/)
- “67% of the malicious app installs researchers identified came from the Google Play Store” (https://arxiv.org/pdf/2010.10088.pdf)
- https://www.rsaconference.com/industry-topics/blog/the-battle-to-address-mobile-threats-in-the-endpoint-security-space
- EventBot (Allie Allen, Cybereason) https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born
- The last eight years every iPhone was vulnerable to RCE attacks through the iOS Mail app (https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/)
- https://github.com/mitre/caldera
- https://mobliciti.com/state-of-enterprise-mobile-security-whitepaper/
- Matt Snyder (VMWare) discussed survivorship bias during a monthly MITRE ATT&CK Power Hour