RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAB1-R10

Fine-tuning Your Cyber Defense Technologies with the ATT&CK Framework

Lane Thames, PhD

Senior Security Researcher
Tripwire, Inc.
@Lane_Thames

Learning Lab Objectives

- Understanding the MITRE ATT&CK Framework and how it can be used
- Learning how to fine-tune cybersecurity technologies with ATT&CK
- Discovering how modern deception shifts the defender's odds for the better and how deception can be coupled with ATT&CK

Learning Lab Goals

- Let's learn together
- Highly Interactive
  - Group Discussions
  - Questions and Answers throughout
  - Hands-on exercises

Learning Lab Agenda

- MITRE ATT&CK Framework
  - General Overview, Definitions, Usage
- Fine Tuning Cybersecurity Technology with ATT&CK
- Shifting the Odds with Deception and ATT&CK

Exercise 1

- Meet your Neighbors

Exercise 2 – Group Discussion – Gathering Perspectives

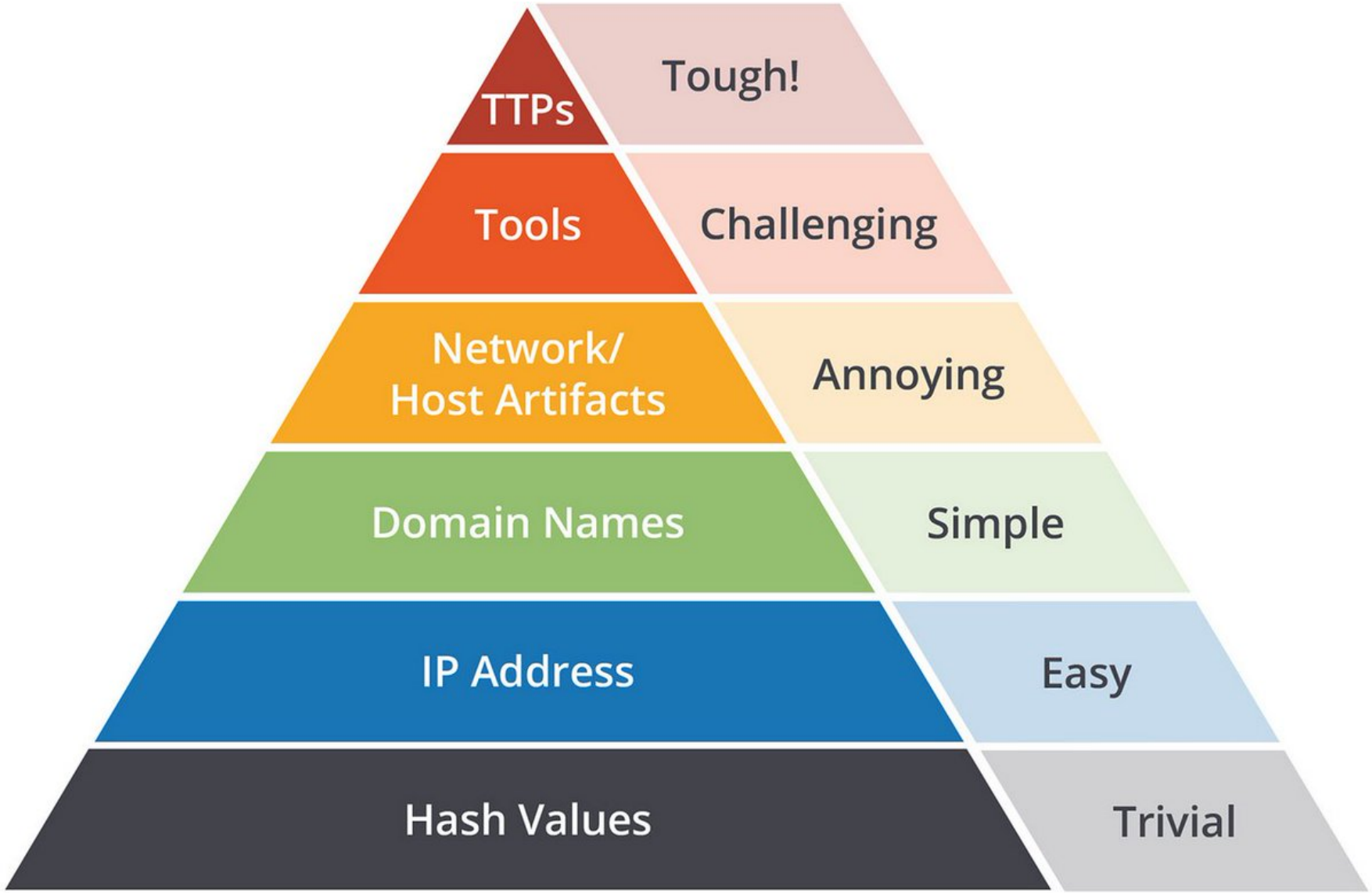
- As someone involved with cybersecurity (information security, network security, etc.), what type of security issues keep you up at night?
  - We'll come back to this question later!

RSAConference2019

The ATT&CK Framework

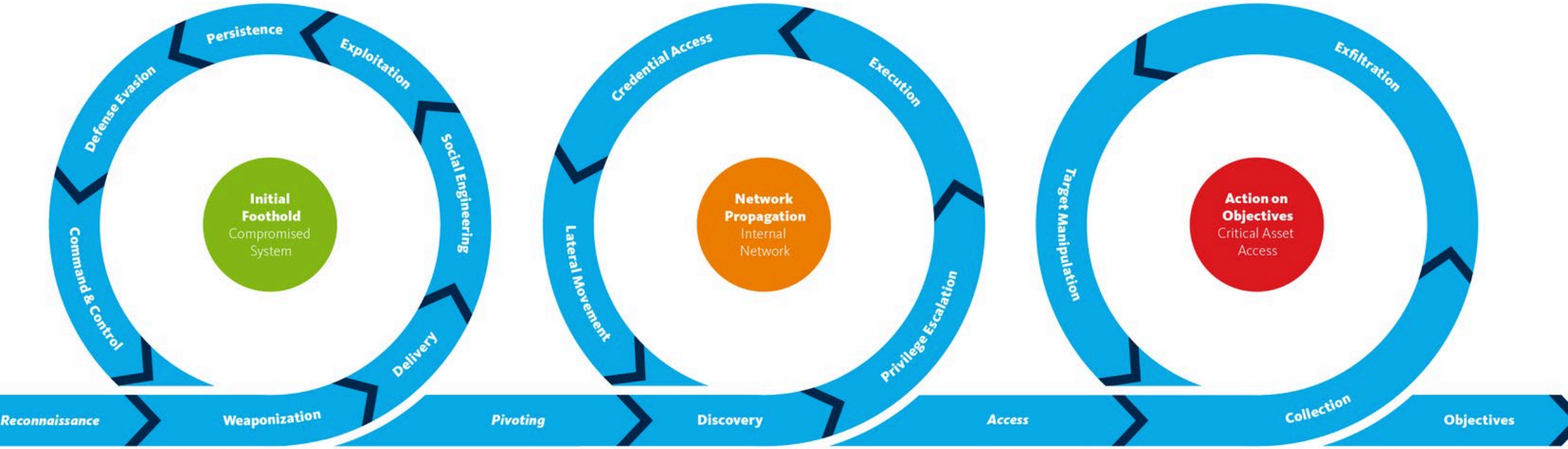
Introduction

David Bianco's Pyramid of Pain



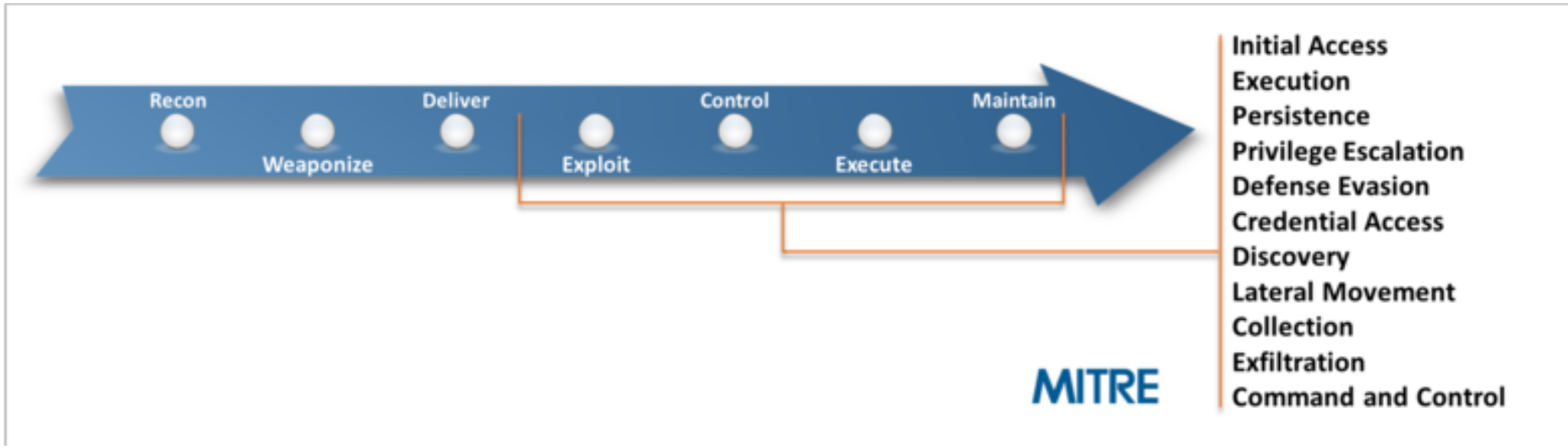
Phases of the Intrusion Kill Chain

Source: By U.S. Senate Committee on Commerce, Science, and Transportation - http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf, Public Domain, https://commons.wikimedia.org/w/index.php?curid=49822676



Source: By Fox-IT - https://blog.fox-it.com/, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=73793339

ATT&CK



MITRE has developed a curated knowledge base and framework known as ***Adversarial Tactics***, ***Techniques***, and ***Common Knowledge*** (ATT&CK). ATT&CK provides knowledge describing behaviors, actions, and processes that a cyber adversary might utilize once **initial access has been gained** within an organization's network.

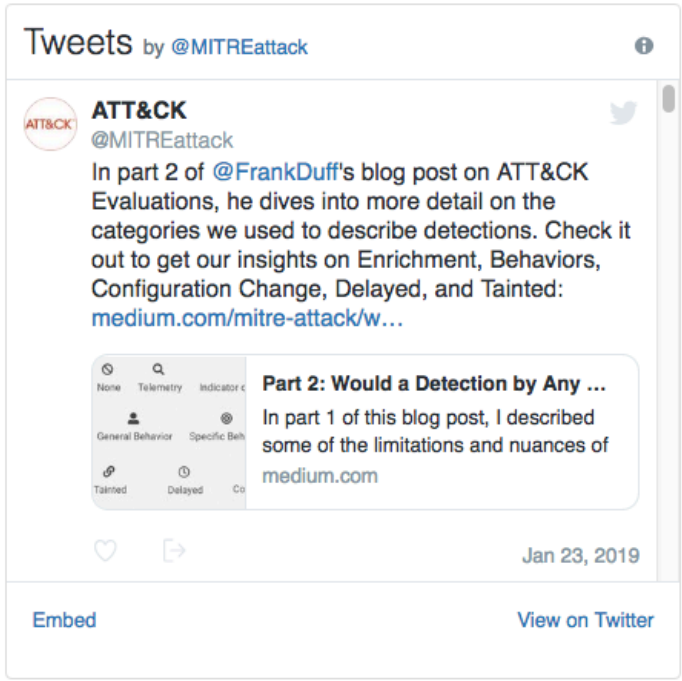
Source: https://attack.mitre.org

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

Get Started » | Contribute » | Check out our Blog



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Scheduled Task			Binary Padding	Credentials in Registry	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Physical Medium	Remote Access Tools
Trusted Relationship	LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access	Network Share Discovery	Distributed Component Object Model	Video Capture	Exfiltration Over Command and Control Channel	Port Knocking
Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation		Forced Authentication	Peripheral Device Discovery	Remote File Copy	Audio Capture		Multi-hop Proxy
Spearphishing Attachment	Trap		Bypass User Account Control		Hooking	File and Directory Discovery	Pass the Ticket	Automated Collection		Domain Fronting
Exploit Public-Facing Application	Launchctl		Process Injection		Password Filter DLL	Permission Groups Discovery	Replication Through Removable Media	Clipboard Data	Data Encrypted	Data Encoding
Replication Through Removable Media	Signed Binary Proxy Execution	Image File Execution Options Injection			LLMNR/NBT-NS Poisoning	Process Discovery	Windows Admin Shares	Email Collection	Automated Exfiltration	Remote File Copy
Spearphishing via Service	User Execution	Plist Modification			Private Keys	System Network Connections Discovery	Pass the Hash	Screen Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Spearphishing Link	Exploitation for Client Execution	Valid Accounts			Keychain	System Owner/User Discovery	Third-party Software	Data Staged	Exfiltration Over Alternative Protocol	Web Service
Drive-by Compromise	CMSTP	DLL Search Order Hijacking		Signed Script Proxy Execution	Input Prompt	System Network Configuration Discovery	Shared Webroot	Input Capture	Data Transfer Size Limits	Standard Non-Application Layer Protocol
Valid Accounts	Dynamic Data Exchange	AppCert DLLs		DCShadow	Bash History	Application Window Discovery	Logon Scripts	Data from Network Shared Drive	Data Compressed	Connection Proxy
	Mshta	Hooking		Port Knocking	Two-Factor Authentication Interception	Password Policy Discovery	Windows Remote Management	Data from Local System	Scheduled Transfer	Multilayer Encryption
	AppleScript	Startup Items		Indirect Command Execution		System Time Discovery	Application Deployment Software	Man in the Browser		Standard Application Layer Protocol
	Source	Launch Daemon		BITS Jobs	Replication Through Removable Media	Account Discovery	SSH Hijacking	Data from Removable Media		Commonly Used Port
	Space after Filename	Dylib Hijacking		Control Panel Items	Input Capture	System Information Discovery	AppleScript			Standard Cryptographic Protocol
	Execution through Module Load	Application Shimming		CMSTP	Network Sniffing	Security Software Discovery	Taint Shared Content			Custom Cryptographic Protocol
	Regsvcs/Regasm	AppInit DLLs		Process Doppelgänging	Credential Dumping	Network Service Scanning	Remote Desktop Protocol			Data Obfuscation
	InstallUtil	Web Shell		Mshta	Kerberoasting	Remote System Discovery	Remote Services			Custom Command and Control Protocol
	Regsvr32	Service Registry Permissions Weakness		Hidden Files and Directories	Securityd Memory	Query Registry				Communication Through Removable Media
	Execution through API	New Service		Space after Filename	Brute Force	System Service Discovery				Multiband Communication
	PowerShell	File System Permissions Weakness		LC_MAIN Hijacking	Account Manipulation					Fallback Channels
	Rundll32	Path Interception	Sudo Caching	HISTCONTROL	Credentials in Files					Uncommonly Used Port
	Third-party Software	Accessibility Features	SID-History Injection	Hidden Users						
	Scripting	Port Monitors	Sudo	Clear Command History						
	Graphical User Interface	Kernel Modules and Extensions	Setuid and Setgid	Gatekeeper Bypass						
	Command-Line Interface	Port Knocking	Exploitation for Privilege Escalation	Hidden Window						
	Service Execution	SIP and Trust Provider Hijacking		Deobfuscate/Decode Files or Information						
	Windows Remote Management	Screensaver		Trusted Developer Utilities						
	Signed Script Proxy Execution	Browser Extensions		Component Object Model Hijacking						
	Control Panel Items	Re-opened Applications		InstallUtil						
	Trusted Developer Utilities	Rc.common		Regsvr32						
	Windows Management Instrumentation	Login Item		Code Signing						
		LC_LOAD_DYLIB Addition		Modify Registry						
		Hidden Files and Directories		Component Firmware						
		Office Application Startup		Redundant Access						
		External Remote Services		File Deletion						
		Netsh Helper DLL		Web Service						
		Component Object Model Hijacking		Timestomp						
		Redundant Access		NTFS File Attributes						
		Security Support Provider		Process Hollowing						
		Bootkit		Disabling Security Tools						
		Hypervisor		Rundll32						
		Registry Run Keys / Start Folder		DLL Side-Loading						
		Logon Scripts		Indicator Removal on Host						
		Modify Existing Service		Scripting						
		Shortcut Modification		Indicator Blocking						
		System Firmware		Software Packing						
		Winlogon Helper DLL		Masquerading						
		Time Providers		Obfuscated Files or Information						
		BITS Jobs		Signed Binary Proxy Execution						
		Launch Agent		Exploitation for Defense Evasion						
		.bash_profile and .bashrc		SIP and Trust Provider Hijacking						
		Create Account		Launchctl						
		Authentication Package		Install Root Certificate						
		Component Firmware		Network Share Connection Removal						
		Windows Management Instrumentation Event Subscription		Regsvcs/Regasm						
		Change Default File Association		Indicator Removal from Tools						
				Rootkit						

THE MITRE ATT&CK™ ENTERPRISE FRAMEWORK

ATTACK.MITRE.ORG

ATT&CK™

MITRE

tripwire

RSAConference2019

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Hardware Additions	Scheduled Task			Binary Padding	Credentials in Registry	Browser Bookmark Discovery
Trusted Relationship	LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access	
Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation			Network Share Discovery
	Trap		Bypass User Account Control		Forced Authentication	
Spearphishing Attachment	Launchctl		Process Injection		Hooking	Peripheral Device Discovery
	Signed Binary Proxy Execution	Image File Execution Options Injection			Password Filter DLL	
Exploit Public-Facing Application		Plist Modification			LLMNR/NBT-NS Poisoning	File and Directory Discovery
	User Execution	Valid Accounts				
Replication Through Removable Media	Exploitation for Client Execution	DLL Search Order Hijacking			Private Keys	Permission Groups Discovery
		AppCert DLLs		Signed Script Proxy Execution	Keychain	
Spearphishing via Service	CMSTP	Hooking			Input Prompt	Process Discovery
	Dynamic Data Exchange	Startup Items		DCShadow	Bash History	System Network Connections Discovery
Spearphishing Link	Mshta	Launch Daemon		Port Knocking	Two-Factor Authentication Interception	
Drive-by Compromise	AppleScript	Dylib Hijacking		Indirect Command Execution		System Owner/User Discovery
Valid Accounts	Source	Application Shimming				
	Space after Filename	AppInit DLLs		BITS Jobs	Replication Through Removable Media	System Network Configuration Discovery
	Execution through Module Load	Web Shell		Control Panel Items		
		Service Registry Permissions Weakness		CMSTP	Input Capture	Application Window Discovery
	Regsvcs/Regasm	New Service		Process Doppelgänging	Network Sniffing	

MITRE Enterprise ATT&CK Framework - Tactics

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

MITRE Enterprise ATT&CK Framework - Tactics

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

Tactic: Discovery
Technique: Remote System Discovery

Remote System Discovery

Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used.

Contents [hide]

1 Windows
2 Mac
3 Linux
4 Examples
5 Mitigation
6 Detection
7 References

Remote System Discovery
Technique

ID	T1018
Tactic	Discovery
Platform	Linux, macOS, Windows
Permissions Required	User, Administrator, SYSTEM
Data Sources	Network protocol analysis, Process command-line parameters, Process monitoring, Process use of network

Windows

Examples of tools and commands that acquire this information include "ping" or "net view" using Net.

Mac

Specific to Mac, the `bonjour` protocol to discover additional Mac-based systems within the same broadcast domain. Utilities such as "ping" and others can be used to gather information about remote systems.

Linux

Utilities such as "ping" and others can be used to gather information about remote systems.

RSAConference2019

Tactic: Discovery
Technique: Remote System Discovery

Examples

- APT3 has a tool that can detect the existence of remote systems.[1][2]
- BRONZE BUTLER typically use `ping` and Net to enumerate systems.[3]
- FIN5 has used the open source tool Essential NetTools to map the network and build a list of targets.[4]
- FIN6 used publicly available tools (including Microsoft's built-in SQL querying tool, osql.exe) to map the internal network and conduct reconnaissance against Active Directory, Structured Query Language (SQL) servers, and NetBIOS.[5]
- FIN8 uses dsquery and other Active Directory utilities to enumerate hosts.[6]
- Turla surveys a system upon check-in to discover remote systems on a local network using the `net view` and `net view /DOMAIN` commands.[7]
- menuPass uses scripts to enumerate IP ranges on the victim network.[8] menuPass has also issued the command `net view /domain` to a PlugX implant to gather information about remote systems on the network.[9]
- Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network.[10]
- MURKYTOP has the capability to identify remote hosts on connected networks.[11]
- Commands such as `net view` can be used in Net to gather information about available remote systems.[12]
- OSInfo performs a connection test to discover remote systems in the network [1]
- Ping can be used to identify remote systems within a network.[13]
- Remsec can ping or traceroute a remote host.[14]
- SHOTPUT has a command to list all servers in the domain, as well as one to locate domain controllers on a domain.[15]
- Shamoon scans the C-class subnet of the IPs on the victim's interfaces.[16]
- Sykipot may use `net view /domain` to display hostnames of available systems on a network.[17]

Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting[18] tools, like AppLocker,[19][20] or Software Restriction Policies[21] where appropriate.[22]

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

References

1. ^ a b ↑ Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.
2. ^ ↑ Chen, X., Scott, M., Caselden, D.. (2014, April 26). New Zero-Day Exploit targeting Internet
12. ^ ↑ Savill, J. (1999, March 4). Net.exe reference. Retrieved September 22, 2015.
13. ^ ↑ Microsoft. (n.d.). Ping. Retrieved April 8, 2016.
14. ^ ↑ Kaspersky Lab's Global Research & Analysis Team. (2016, August 9). The ProjectSauron APT.

tripwire
RSAConference2019

ATT&CK: Use Cases

- Training and Learning

- Engineering
  - R&D for new technology
  - Innovating existing Technology
  - Gap Analysis WRT current security posture

ATT&CK: Use Cases

- Threat Intelligence
  - Threat Hunting
  - Indicator of Compromise (IoC) Capture & Sharing

- Security Operations
  - Adversary Emulation
    - Red-Blue (Purple) Teaming
  - High-fidelity Detection
  - Risk Prioritization

MITRE | ATT&CK

Matrices Tactics Techniques Groups Software Resources Blog Conta

Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

Home > Resources

ATT&CK Domain Overviews

- ATT&CK for Enterprise
- PRE-ATT&CK
- ATT&CK for Mobile

Papers

- The Design and Philosophy of ATT&CK
- Finding Cyber Threats with ATT&CK-Based Analytics

Presentations

- ATT&CKing the Status Quo: Improving Threat Intel and Cyber Defense with MITRE ATT&CK
- ATT&CKing with Threat Intelligence

Other Resources

- ATT&CKcon 2018 Presentations
- Contribute to ATT&CK
- Adversary Emulation Plans
- ATT&CK Update Log
- Interfaces for Working with ATT&CK
- Related Standardization Efforts
- MITRE ATT&CK Matrix Poster

Exercise 3 – ATT&CK Use Case – Gap Analysis

- Evaluating your controls and resources – People, Process, and Technology – with respect to the ATT&CK Matrix

RSAConference2019

Fine-tuning with ATT&CK

ATT&CK Fine-tuning – People, Process, Technology

- The Matrix has you!
  - ATT&CK knowledge store is vast.
- Use it to Implement Internal Training Programs
  - Onboarding new hires
  - Professional development for existing staff

ATT&CK Fine-tuning – People, Process, Technology

- Threat Hunting

admin@338

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. [1]

ID: G0018
Aliases: admin@338
Version: 1.0

Alias Descriptions

Name	Description
admin@338	[1]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: `net user >> %temp%\download` `net user /domain >> %temp%\download` [1]
Enterprise	T1059	Command-Line Interface	Following exploitation with LOWBALL malware, admin@338 actors created a file containing a list of commands to be executed on the compromised computer.[1]
Enterprise	T1083	File and Directory Discovery	admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about files and directories: `dir c:\ >> %temp%\download` `dir "c:\Documents and Settings" >> %temp%\download` `dir "c:\Program Files\" >> %temp%\download` `dir d:\ >> %temp%\download` [1]
Enterprise	T1036	Masquerading	admin@338 actors used the following command to rename one of their tools to a benign file name: `ren "%temp%\upload" audiodg.exe` [1]
Enterprise	T1069	Permission	admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to list local groups: `net`

Software

ID	Name	Techniques
S0043	BUBBLEWRAP	Standard Application Layer Protocol, Standard Non-Application Layer Protocol, System Information Discovery
S0100	ipconfig	System Network Configuration Discovery
S0042	LOWBALL	Commonly Used Port, Remote File Copy, Standard Application Layer Protocol, Web Service
S0039	Net	Account Discovery, Create Account, Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery, Remote System Discovery, Service Execution, System Network Connections Discovery, System Service Discovery, System Time Discovery, Windows Admin Shares
S0104	netstat	System Network Connections Discovery
S0012	PoisonIvy	Application Window Discovery, Command-Line Interface, Data from Local System, Data Staged, Input Capture, Modify Existing Service, Modify Registry, New Service, Obfuscated Files or Information, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Rootkit, Standard Cryptographic Protocol, Uncommonly Used Port
S0096	Systeminfo	System Information Discovery

References

1. FireEye Threat Intelligence. (2015, December 1). China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets. Retrieved December 4, 2015.

ATT&CK Fine-tuning – People, Process, Technology

- Mapping ATT&CK to CIS Controls
  - See Handouts

ATT&CK Fine-tuning – People, Process, Technology

The CIS Critical Security Controls for Effective Cyber Defense

The **Center for Internet Security Critical Security Controls for Effective Cyber Defense** is a publication of best practice guidelines for computer security. The project was initiated early in 2008 as a response to extreme data losses experienced by organizations in the US defense industrial base and recently.[1] The publication was initially developed by the SANS Institute, ownership was transferred to the Council on Cyber Security (CCS) in 2013 and then transferred to Center for Internet Security (CIS) in 2015. It was earlier known as the Consensus Audit Guidelines and it is also known as the CIS CSC, CIS 20, CCS CSC, SANS Top 20 or CAG 20.

ATT&CK Fine-tuning – People, Process, Technology

Controls

Version 3.0 was released on April 13, 2011. Version 5.0 was released on February 2, 2014 by the Council on Cyber Security (CCS).[5]Version 6.0 was released on October 15, 2015 and consists of the security controls below. Version 6.1 was released on August 31, 2016 and has the same priorization as version 6. Version 7 has been released March 19 2018.[6] Compared to version 5, version 6/6.1 has re-prioritized the controls and changed these two controls:

- 'Secure Network Engineering' was CSC 19 in version 5 but has been deleted in version 6/6.1.
- 'CSC 7: Email and Web Browser Protections' has been added in version 6/6.1.

```
CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations,
and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises
```

ATT&CK Fine-tuning – People, Process, Technology

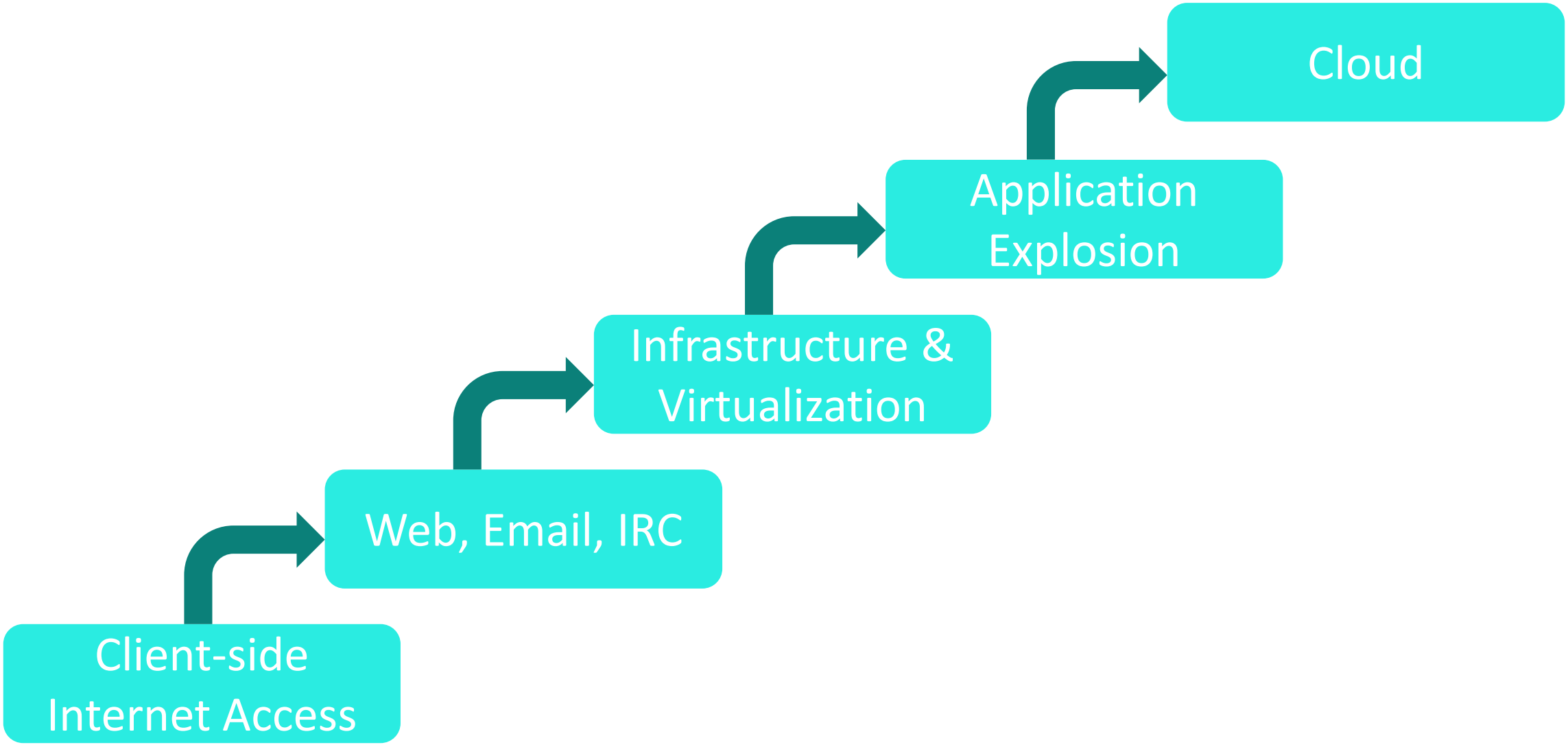
Initial Access	Execution	Persistence	Privilege Escalation
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert Dlls
Replication Through Removable Media	Contgrol Panel Items	AppInit DLLs	AppInit DLLs
Spearphishing Attachmentz	Dynamic Data Exchange	Application Shimming	Application Shimming
Spearphishing Link	Execution through API	Authentication Package	Authentication Package
Spearphishing via Servie	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking
Trusted Relatioznship	Graphical User Interface	Browser Extensions	Exploitation of Vulnerability
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection
	LSASS Driver	Component Firmware	File System Permissions Weakness
	Launchctl	Component Object Model Hijacking	Hooking
		Create Account	
	Local Job Scheduling	DLL Search Order Hijacking	Image File Execution Options Injection
	Mshta	Dylib Hijacking	Launch Daemon
	PowerShell	External Remote Services	New Service
	Regsvcs/Regasm	File System Permissions Weakness	Path Interception
	Regsvr32	Hidden Files and Directories	Plist Modification
	Rundll32	Hooking	Port Monitors
	Scheduled Task	Hypervisor	Process Injection
	Scripting	Image File Execution Options Injection	SID-History Injection
	Service Execution	Kernel Modules and Extensions	Scheduled Task
	Signed Binary Proxy Execution	LC_LOAD_DYLIB Addition	Service Registry Permissions Weakness
	Signed Script Proxy Execution	LSASS Driver	Setuid and Setgid
	Source	Launch Agent	Startup Items
	Space after Filename	Launch Daemon	Sudo
	Third-party Software	Launchctl	Sudo Caching
	Trap	Local Job Scheduling	Valid Accounts
	Trusted Developer Utilities	Login Item	Web Shell
	User Execution	Logon Scripts	
	Windows Management Instrumentation	Modify Existing Service	
	Windows Remote Management	Netsh Helper DLL	
		New Service	

Critical Security Control 2
Mapped to ATT&CK

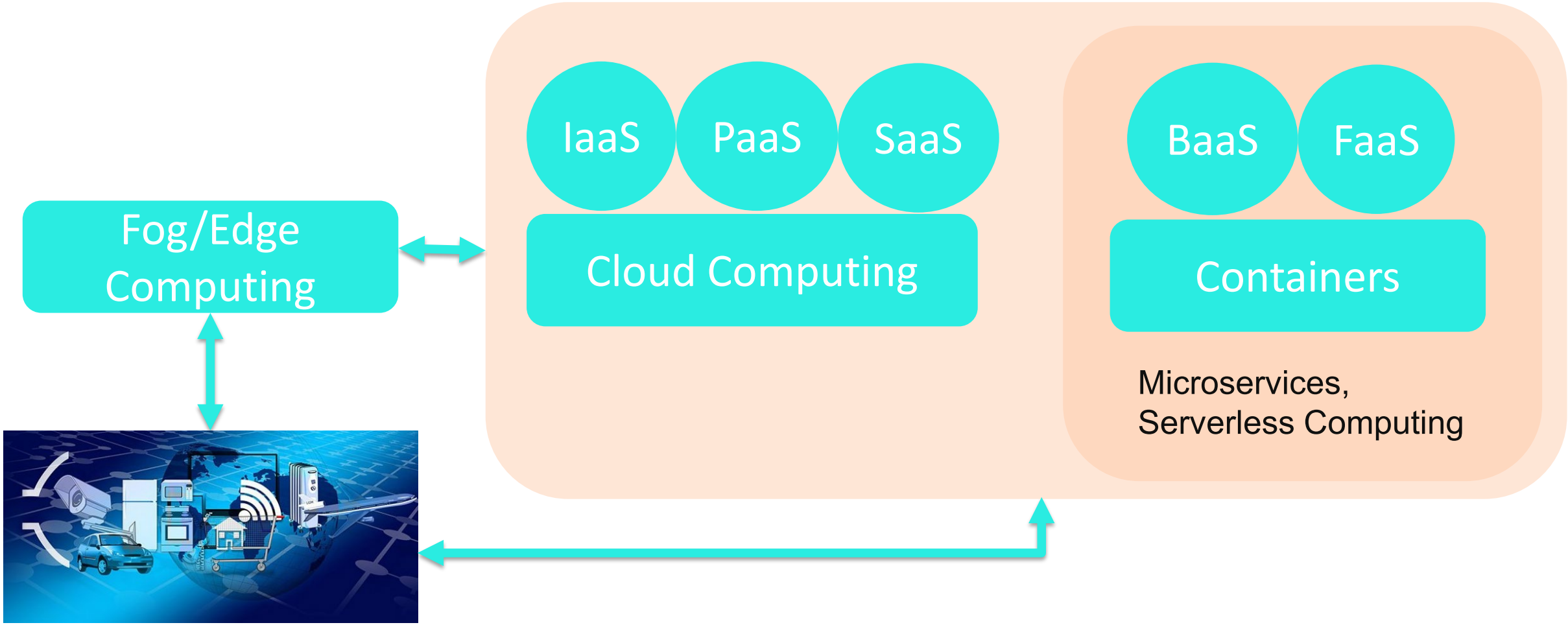
RSAConference2019

Deception

Computing Evolution

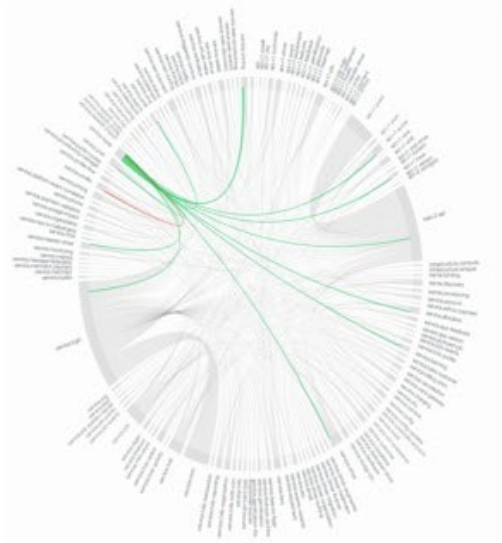


It's a Brave New World



Complexity and Chaos

450 microservices

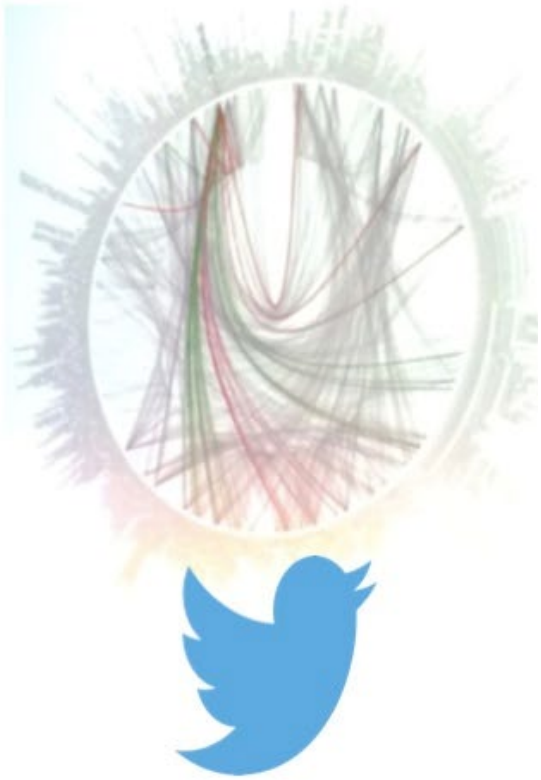


HAIL O

500+ microservices

NETFLIX

500+ microservices



Source:
Netflix: http://www.slideshare.net/BruceWong3/the-case-for-chaos
Twitter: https://twitter.com/adrianco/status/441883572618948608
Hail-o: https://sudo.hailoapp.com/services/2015/03/09/journey-into-a-microservice-world-part-3/

Deception – It's making a comeback

de·ceive

/dəˈsēv/

verb

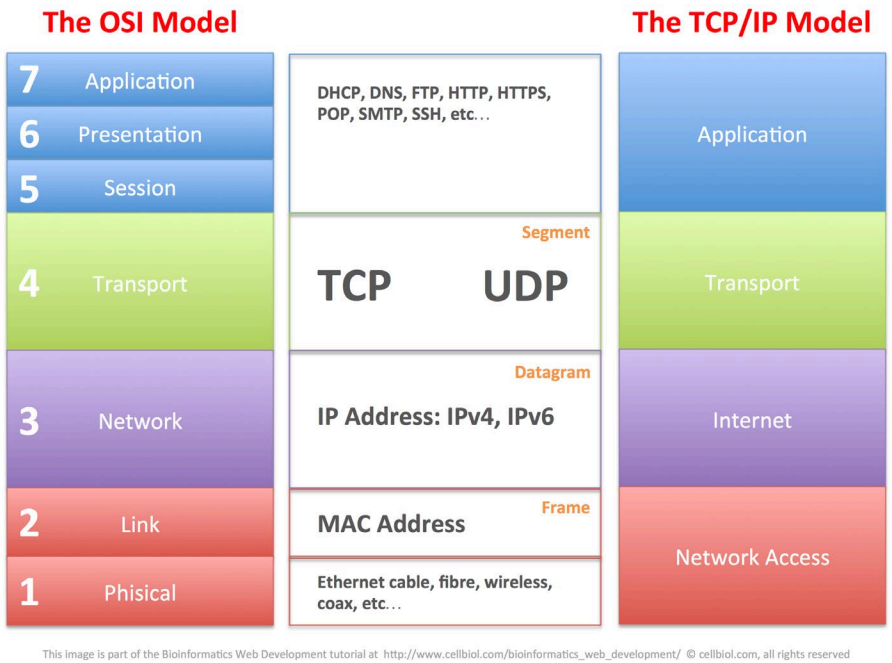
(of a person) cause (someone) to believe something that is not true, typically in order to gain some personal advantage.
"I didn't intend to **deceive** people **into** thinking it was French champagne"
synonyms: swindle, defraud, cheat, trick, hoodwink, hoax, dupe, take in, mislead, delude, fool, outwit, lead on, inveigle, beguile, double-cross, gull; More

- (of a thing) give a mistaken impression.
  "the area may seem to offer nothing of interest, but don't be deceived"
- fail to admit to oneself that something is true.
  "enabling the rulers to deceive themselves about the nature of their own rule"

Deception – My Dynamic Deception Open Source Project

https://github.com/jlthames2/thddt

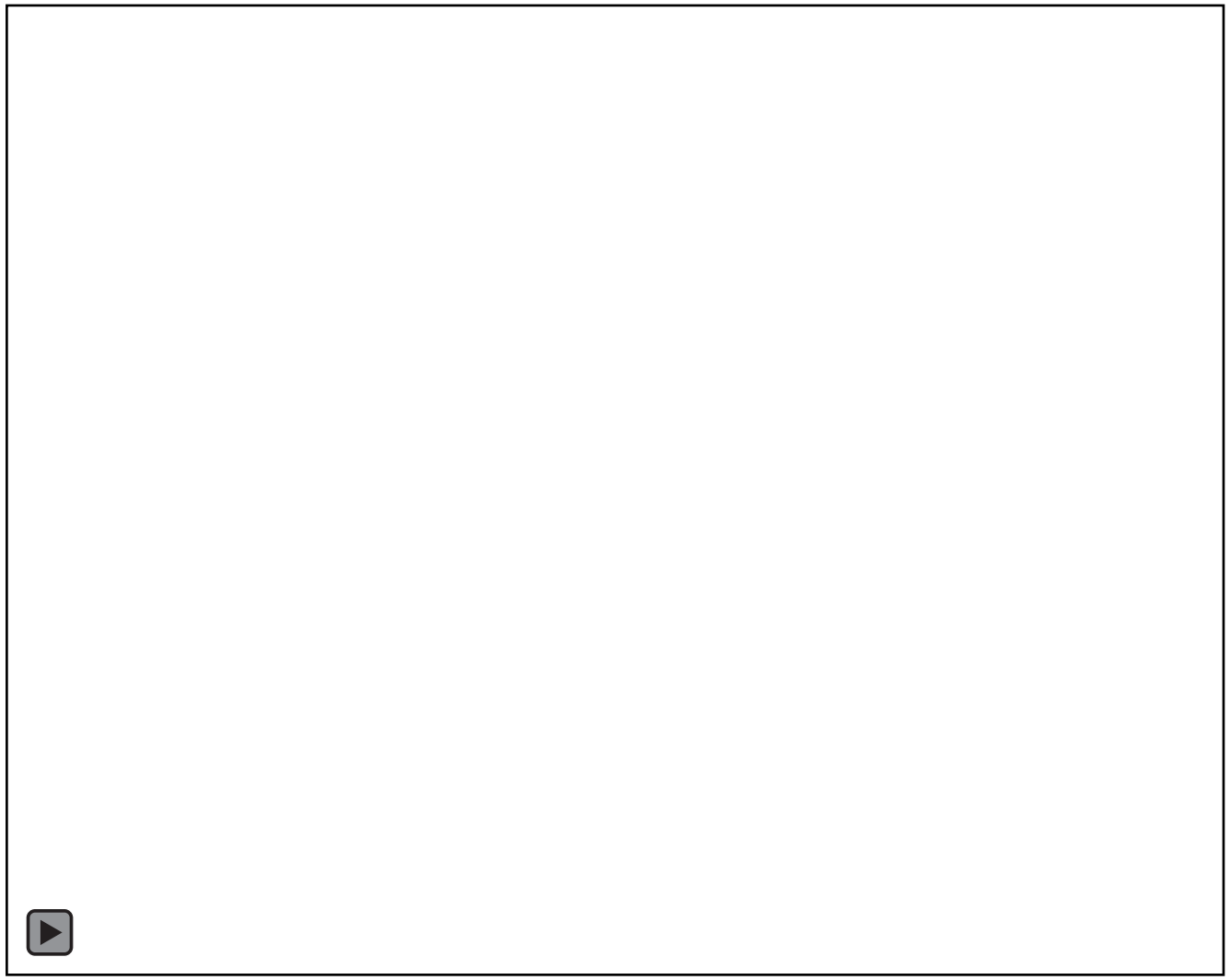
Network Dynamics



20 lines (13 sloc) | 500 Bytes

```
1   FROM python:2.7-slim
2
3   # Set the working directory to /app
4   WORKDIR /app
5
6   # Copy the current directory contents into the container at /app
7   ADD . /app
8
9   # Install Dependencies
10  RUN apt-get update && apt-get install -y gcc
11
12  # Install any needed packages specified in requirements.txt
13  RUN pip install --trusted-host pypi.python.org -r requirements.txt
14
15  # Make port 80 available to the world outside this container
16  EXPOSE 80
17
18  # Run twisted-web.py when the container launches
19  CMD ["python", "twisted-web.py"]
```

Dynamic Deception



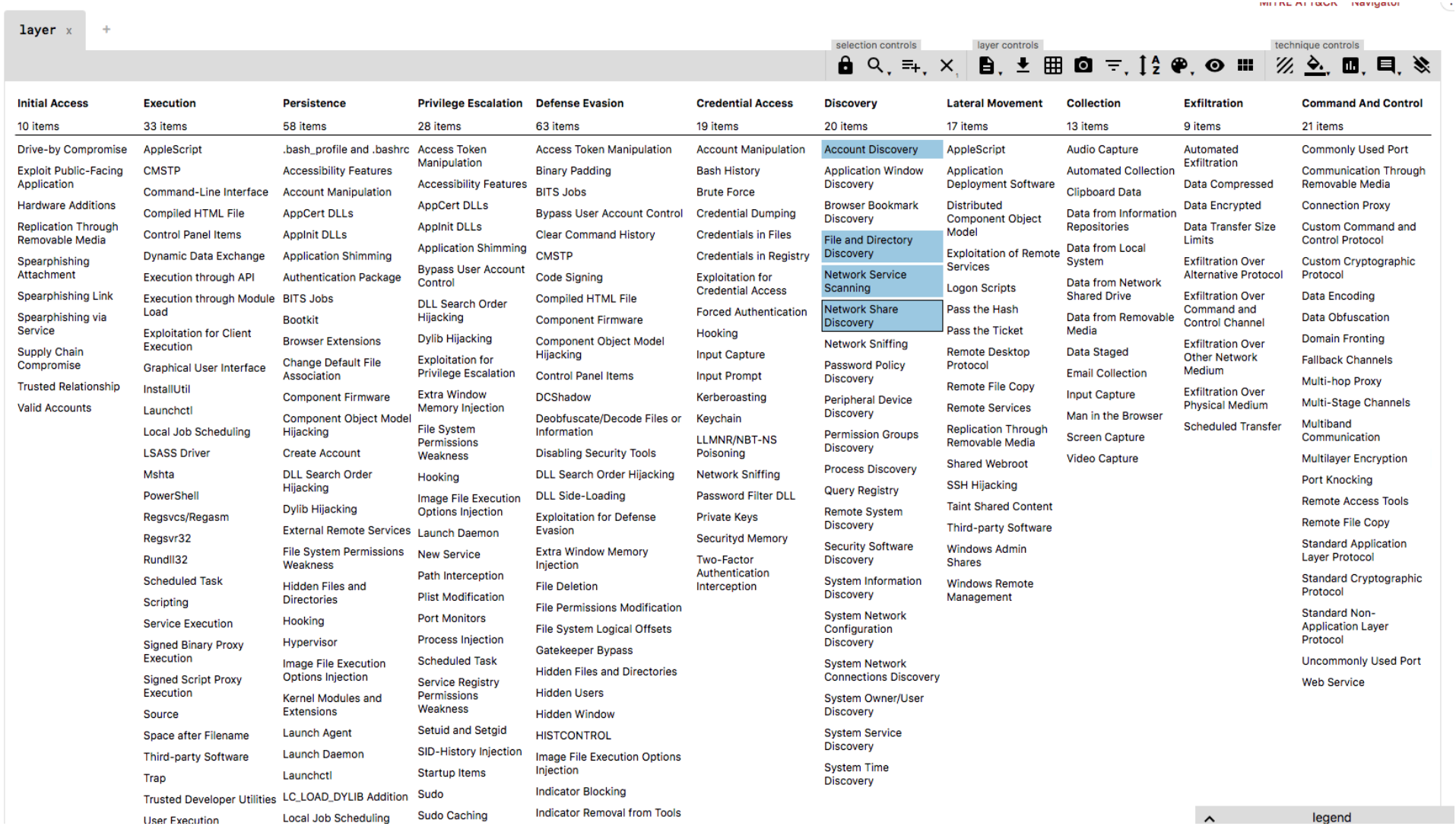
Exercise 4 – Group Discussion

- Why would we want to use deception nowadays?
  - Consider this with respect to the goals of ATT&CK.

Exercise 5 – ATT&CK and Deception

- Using the ATT&CK Matrix in your handout and what we've discussed for deception, let's map techniques that are suitable targets for deception technologies.

Exercise 5 – ATT&CK and Deception – Navigator Tool



RSAConference2019

Final Thoughts

- Did you observe any patterns or trends here in our discussions today? What do things like the ATT&CK Framework, Threat Hunting, System Complexity, etc. imply to you?

Final Thoughts

- Answer:
  - Embracing System Compromise

Final Thoughts

- Traditional Thinking
  - Defend list of assets
  - Manage incidents
  - View pentest results as report card
  - Think about stopping attacks
- Newer Thinking
  - Defend graph of assets
  - Manage adversaries
  - View pentest results as input
  - Think about increasing attacker requirements

Summary – What did we accomplish today?

- Learned about the MITRE ATT&CK Framework
- Learned how to Fine Tune Cybersecurity Technology with ATT&CK
- Learned how Deception and ATT&CK Can Work Together

Applying What You Have Learned

- Next week you should:
  - Introduce your security staff and stakeholders to ATT&CK as a learning resource
- In the first three months following this presentation you should:
  - Perform a gap analysis using ATT&CK with respect to your people, processes, and technologies
- Within six months you should:
  - Formulate and execute a roadmap for filling in any relevant gaps

Thanks for your Attendance!