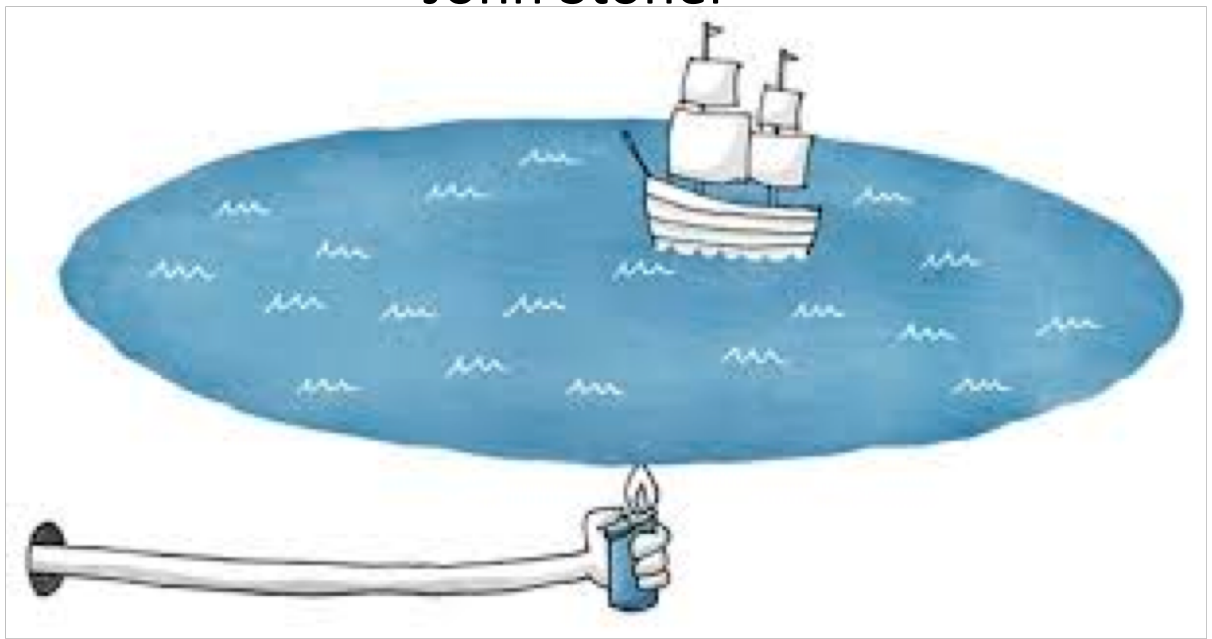
Don't Boil the Ocean: Using MITRE ATT&CK to Guide Threat Hunting Activities

BSidesSF – March 4 2019

John Stoner



Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a høliday in Sweden this yër? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON Including the majestik møøse A Møøse once bit my Marcus... No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møvies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Mølars of Horst Nordfink"... In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.

whoami > John Stoner

CISSP, GCIA, CISA, GCIH, GCTI

Principal Security Strategist @ Splunk

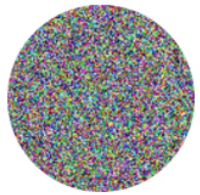
@stonerpsu

- 20+ years of cyber security experience
- Creator of SA-Investigator for Splunk
- Blogger on Hunting and SecOps
- Symantec→ArcSight→Splunk - I’ve Seen them all
- Loves The Smiths and all 80’s sadtimey music

Agenda

- Why/What Do We Hunt?
- MITRE ATT&CK
- Building Hypotheses
- Take Aways From Our Hunts

Tweet

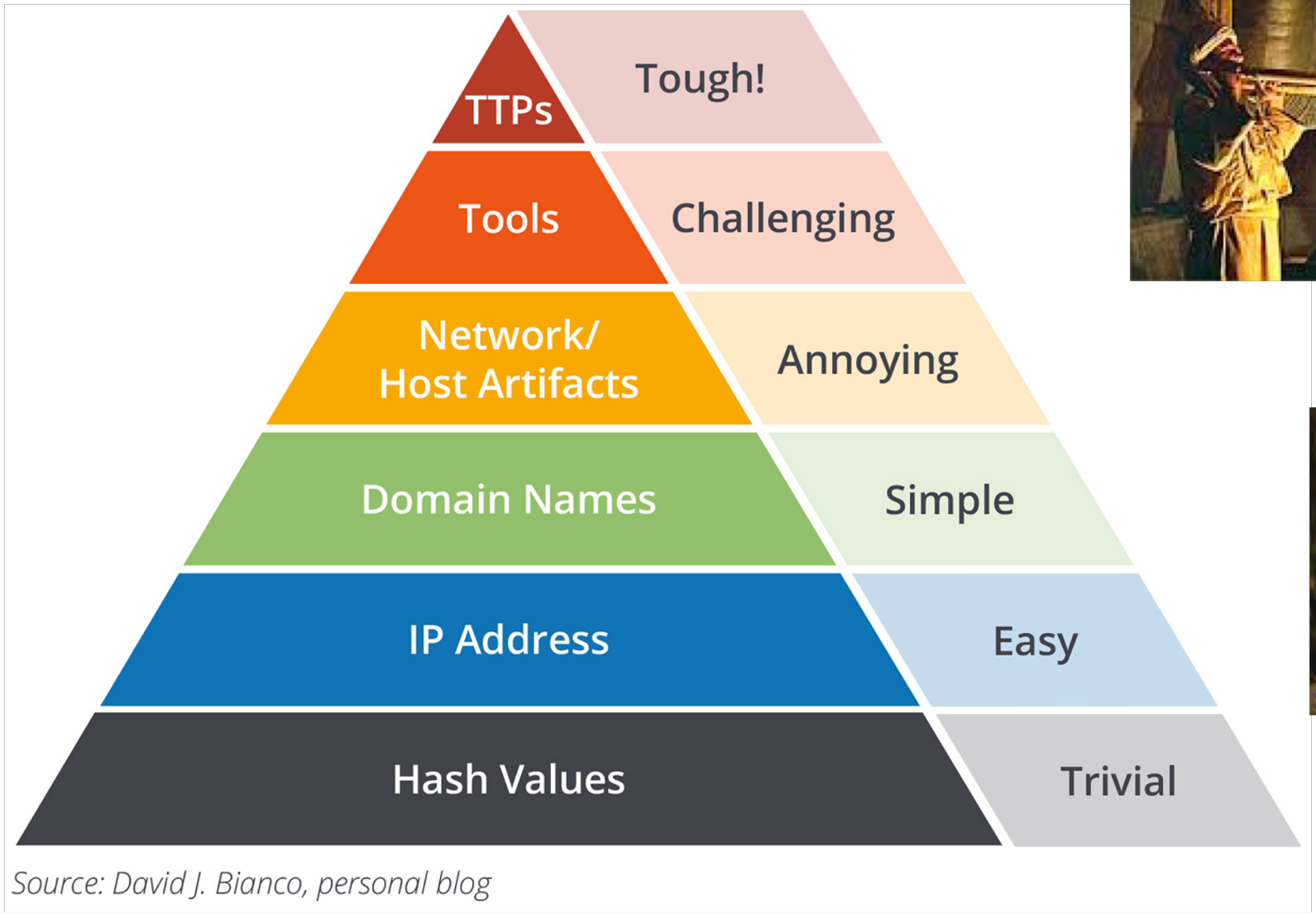


Matt Graeber
@mattifestation

Incident responder: "The machine was infected with crimeware. We just had IT rebuild the system. End of story."
Nation-state attacker: "We got our foothold and only lost a single host in the process."

2/18/18, 10:36 AM

What To Hunt For?

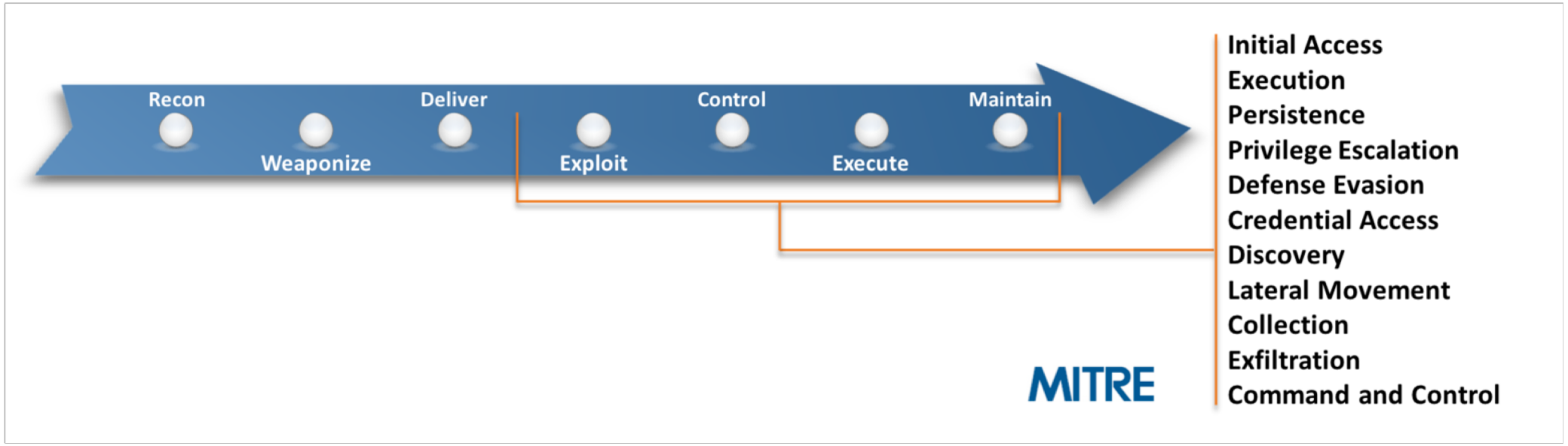


Source: David J. Bianco, personal blog

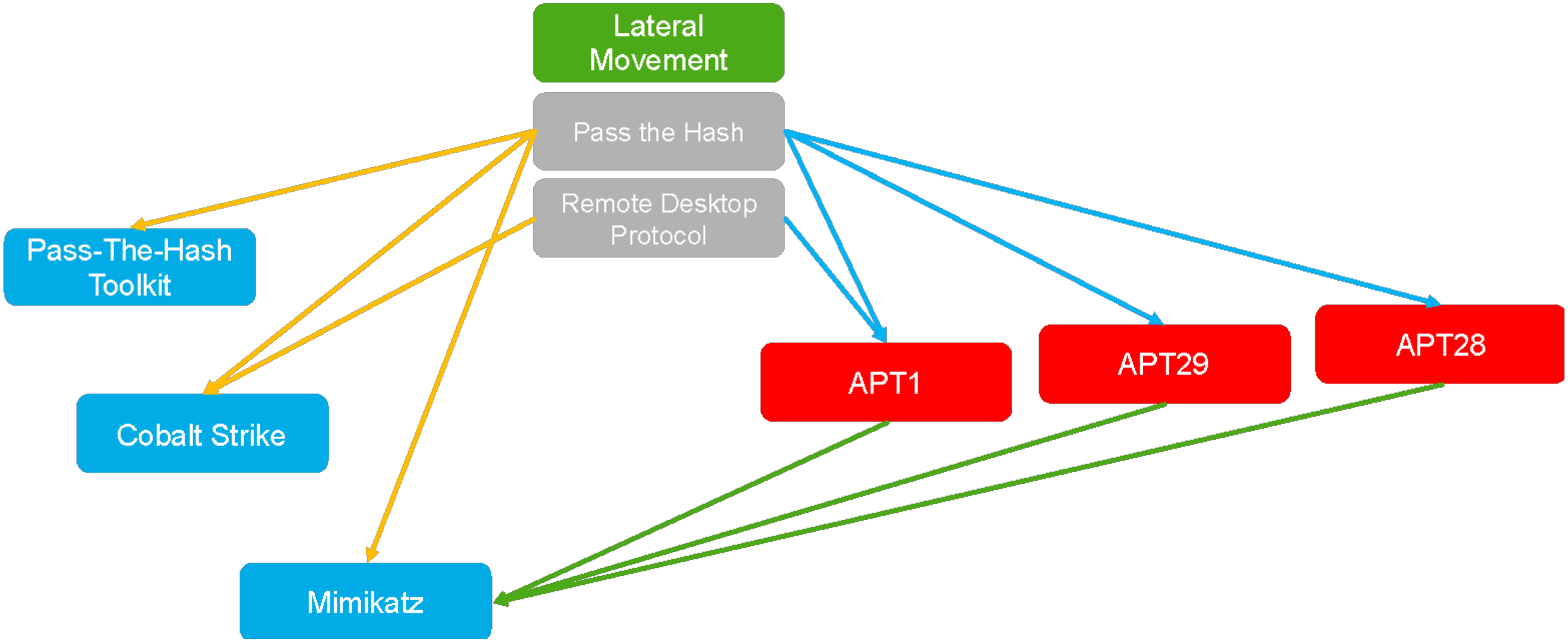

YOU MUST CHOOSE
...BUT CHOOSE WISELY

MITRE ATT&CK

- Adversarial Tactics, Techniques, and Common Knowledge
- Builds on Lockheed Martin's Kill Chain but focuses on tactics and techniques that occur during exploit and activity occurring post exploit



Tactic, Techniques, Adversaries and Software



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 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		Remote File Copy
Spearphishing via Service	User Execution	Plist Modification			Private Keys	System Network Connections Discovery	Pass the Hash	Screen Capture		Multi-Stage Channels
Spearphishing Link	Exploitation for Client Execution	Valid Accounts			Keychain	System Owner/User Discovery	Third-party Software	Data Staged		Web Service
Drive-by Compromise	CMSTP	DLL Search Order Hijacking		Signed Script Proxy Execution	Input Prompt	System Network Configuration Discovery	Shared Webroot	Input Capture		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		Connection Proxy
	Mshta	Hooking		Port Knocking	Two-Factor Authentication Interception	Password Policy Discovery	Windows Remote Management	Data from Local System		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

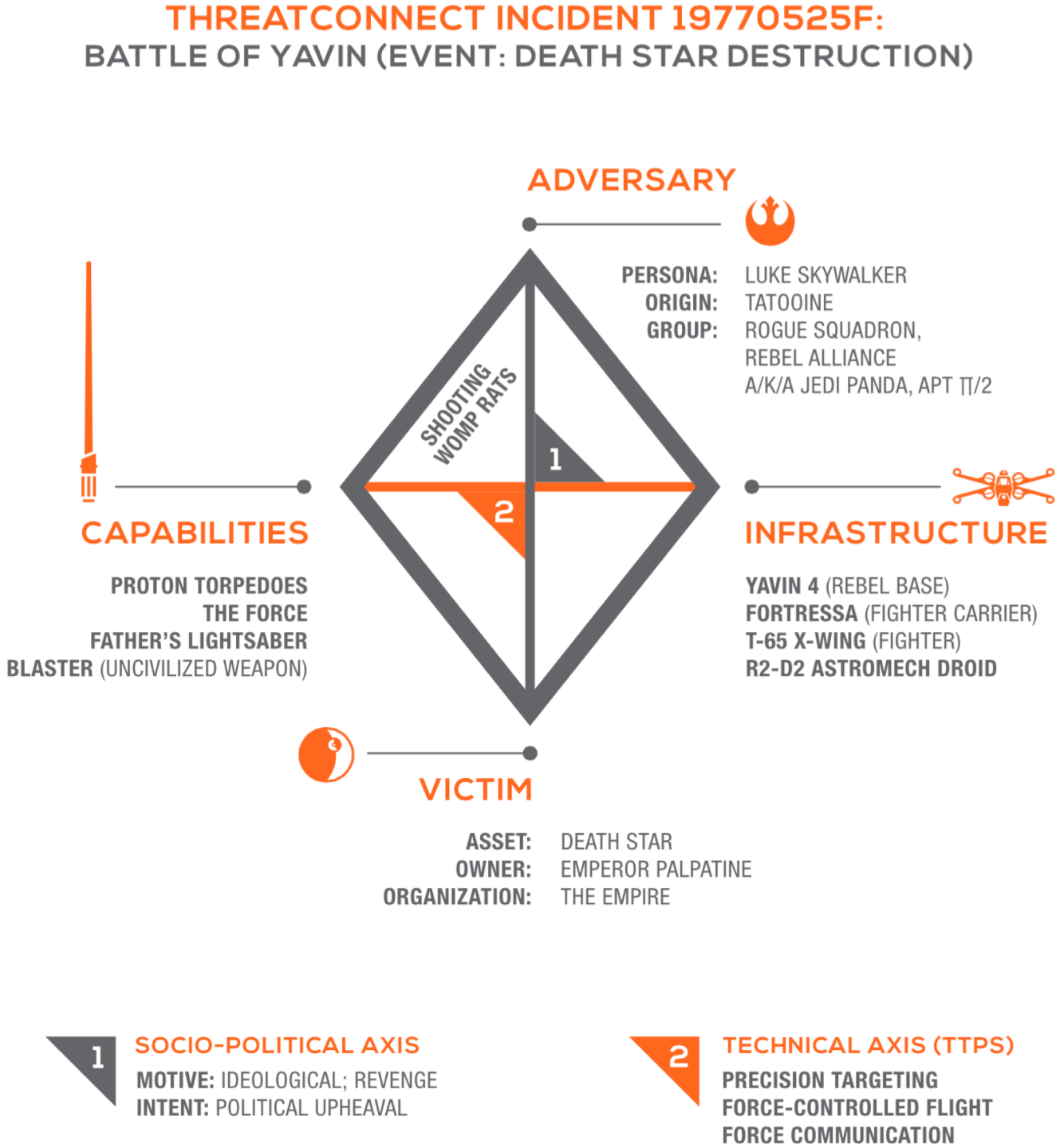
ATTACK.MITRE.ORG

ATT&CK™

MITRE

Diamond Model

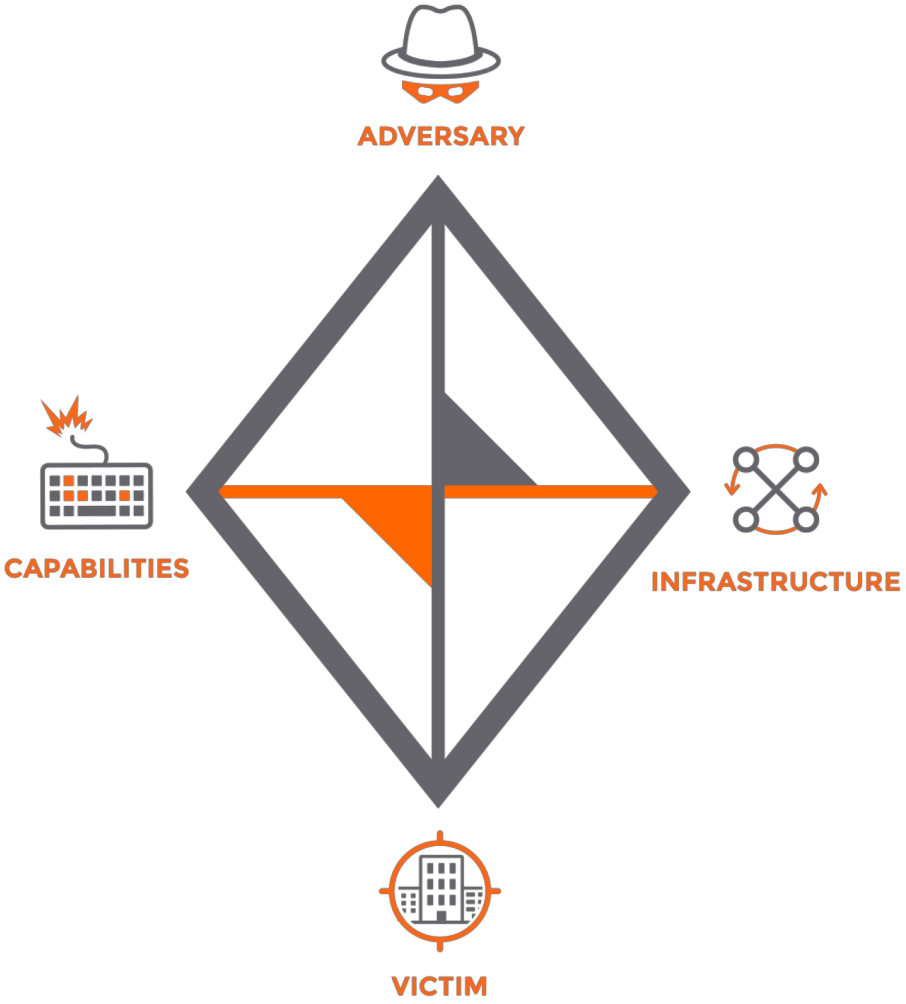
- More often used within Threat Intelligence, but has a place as part of Threat Hunting
- Used for contextualizing threat intelligence that is found during hunting
- Sergio Caltagirone, Andrew Pendergast, Christopher Betz
  - http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf
  - https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/



How Are You Going To Hunt?

- Four Vertices to the Diamond Model
- Focus your hunt on any one of them to start

- Victim and Capability are generally best places to start



http://www.activeresponse.org/building-threat-hunting-strategy-with-the-diamond-model/

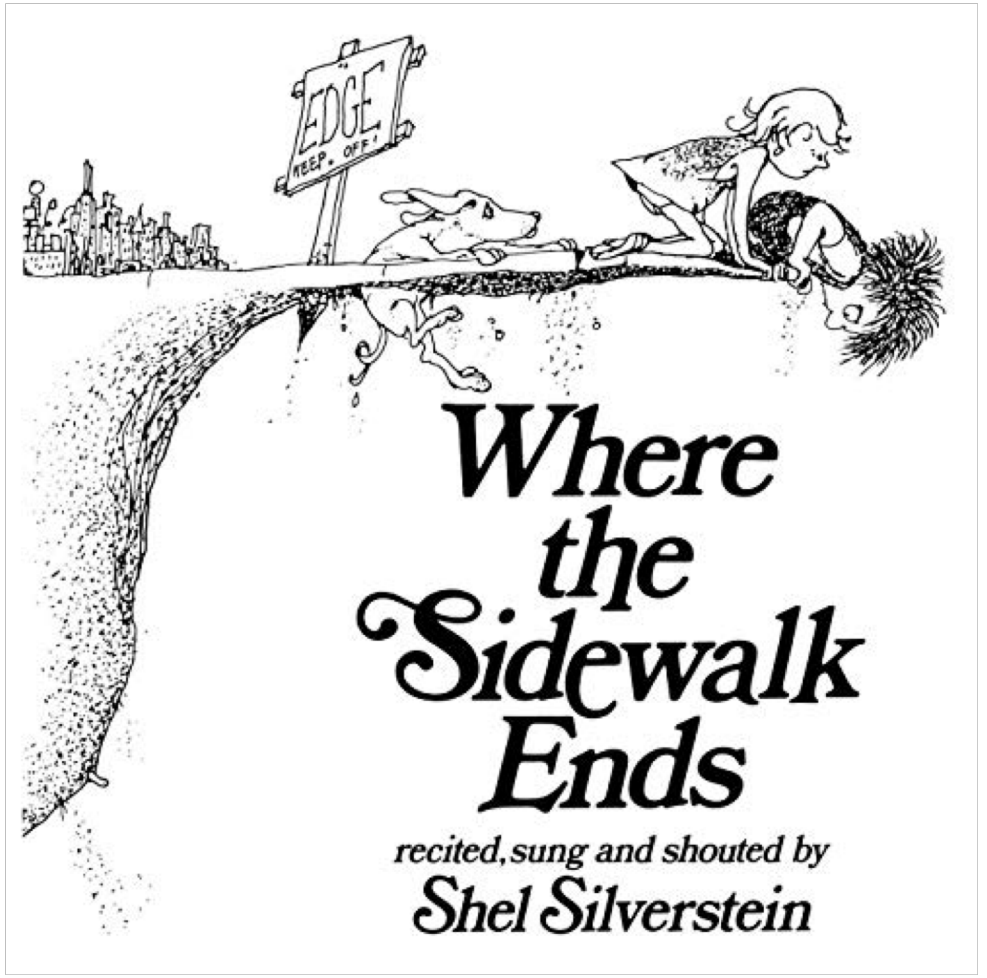

Threat Hunting
ATT&CK™
Threat Intelligence
Security Operations

Time Is A Crucial Factor

- Don’t Get Myopic on Your Hunt
- Start broadly and narrow so you don’t miss events
- Much of your data is time series data

Uncovering Unexpected Things

- Hunting against a hypothesis
  - Can take you in many directions
  - Note those turns so you can retrace your steps
  - Start new hunts when you reach a dead end



Hunts Do Not Exist in a Silo

- Techniques will cross paths with other techniques
  - Use them as guardrails
- Example: Hunting for PowerShell could yield the use of data encoding
  - Both are adversary techniques
  - Could we hunt just for data encoding?
  - Identifying the combination of specific techniques may help inform about a specific adversary or tool

Using ATT&CK Techniques To Build Our Hypothesis - PowerShell

ID: T1086

Tactic: Execution

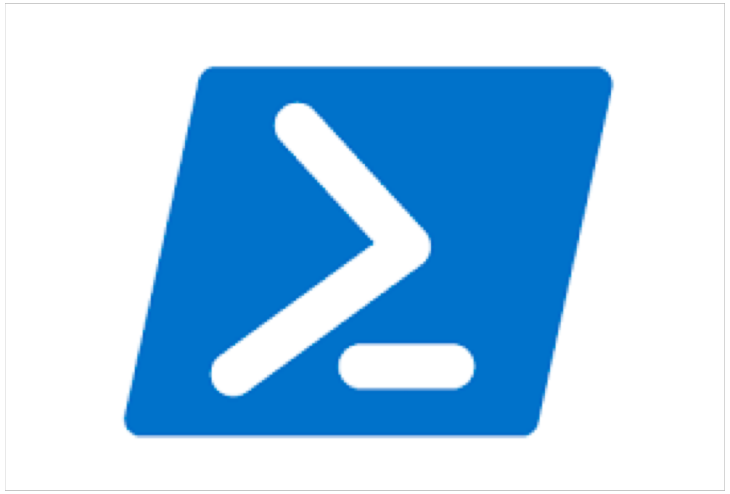
Platform: Windows

Permissions Required: User, Administrator

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Version: 1.0



https://attack.mitre.org/wiki/Technique/T1086

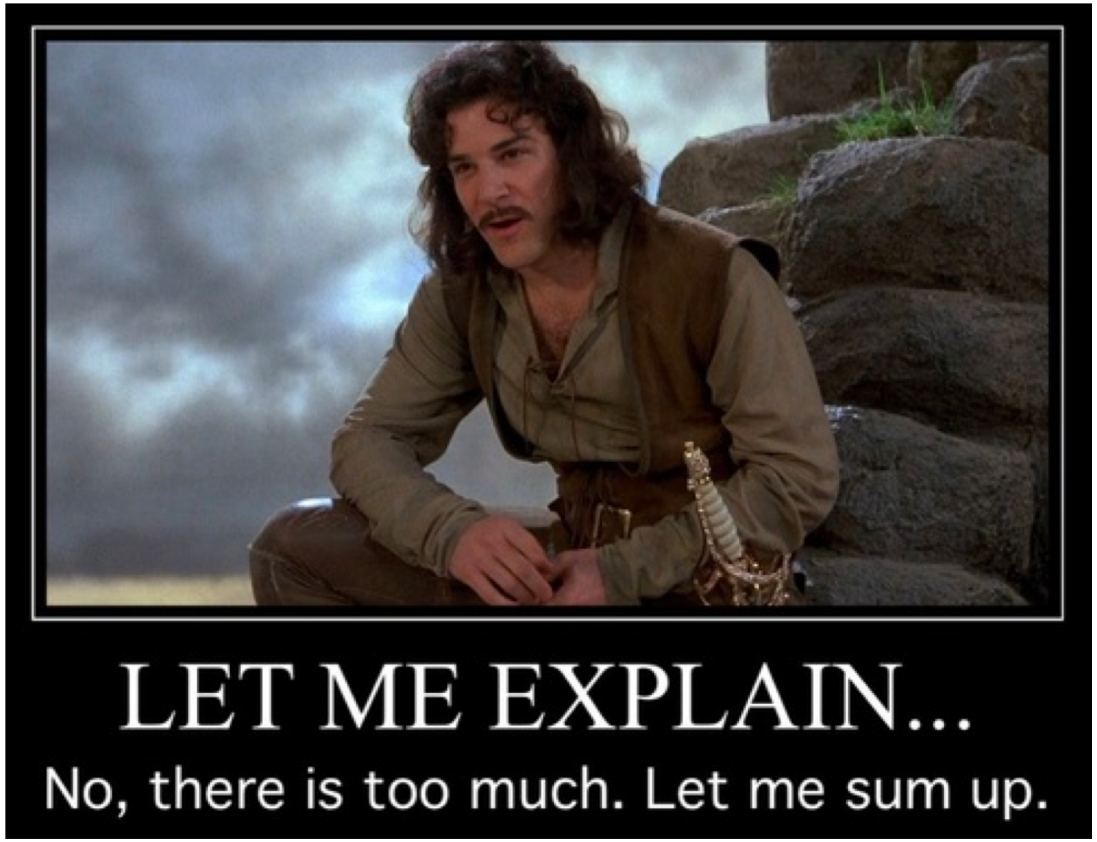
Adversaries will use PowerShell Empire to establish a foothold and carry out attacks

How Might We Confirm or Refute Our Hypothesis?

- What is PowerShell?
- Where can I learn more about PowerShell Empire?
- Does PowerShell Empire have default settings that I could hunt for?
- What do data flows look like between sources and destinations?
- What ports are being used?
- What user accounts are being used?
- When did events occur?
- Are we able to view the contents of scripts that PowerShell is running to gain greater insight?

As We Conclude A Hunt…

- Were we able to confirm or refute our hypothesis?
- What have we learned?
- What does our attack picture look like?
- How do our findings map to the diamond model?
- What other techniques were referenced?
- What should we operationalize?
- Where are our gaps?



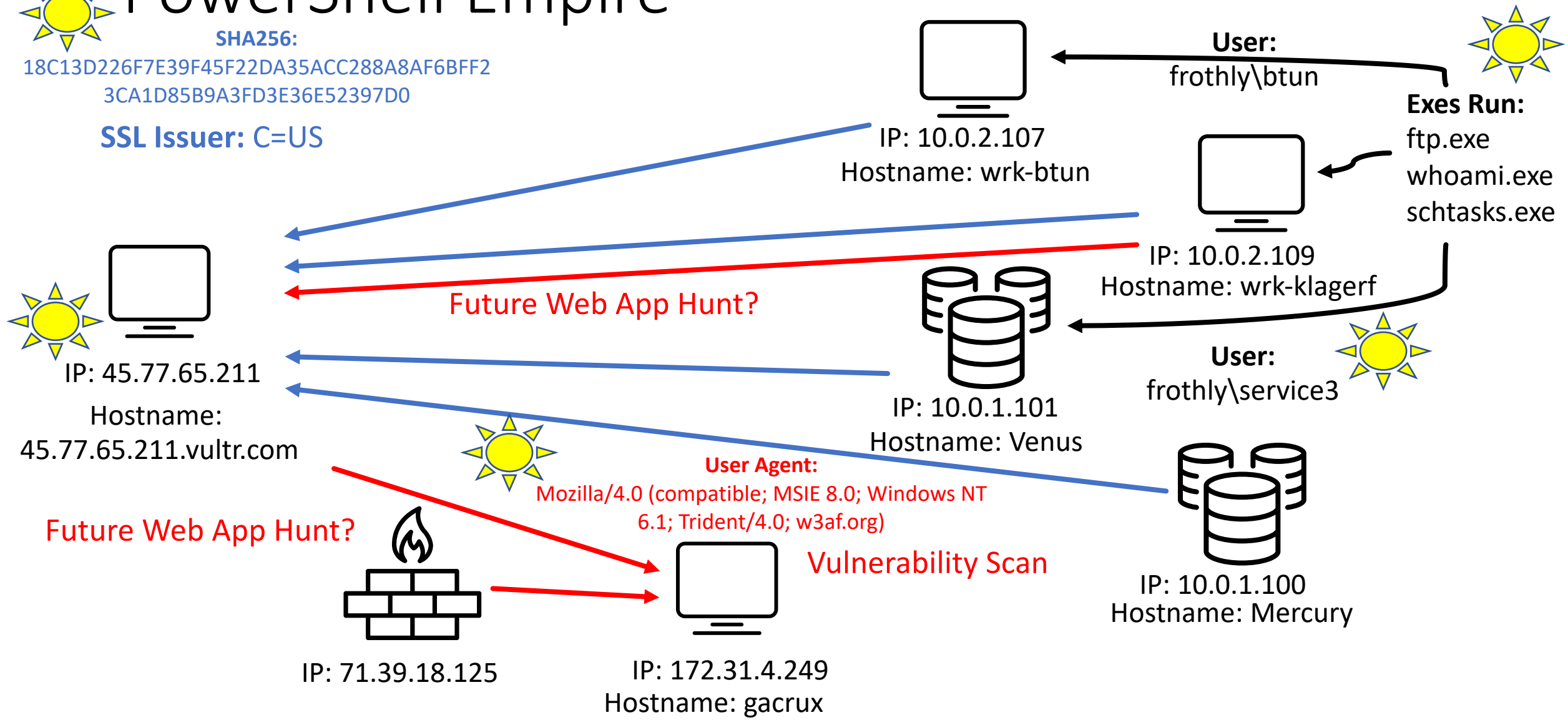
What Have We Learned?

- The default SSL Issuer value?
- Communication using this SSL Certificate exists between which systems?
- Is there outbound communication?
  - Between what systems?
  - Large or small percentage of overall traffic
  - What accounts are they associated with?
- Are specific processes running on systems?
  - Are they running under specific accounts?
  - Are they running in a specific order?
  - Are they all running encoded PowerShell?
  - Does anyone else see similar behavior by some variance?
- What other commands are being spawned?
- Can any of these nuggets found be found more broadly on the internet?

PowerShell Empire

SHA256:
18C13D226F7E39F45F22DA35ACC288A8AF6BFF2
3CA1D85B9A3FD3E36E52397D0

SSL Issuer: C=US

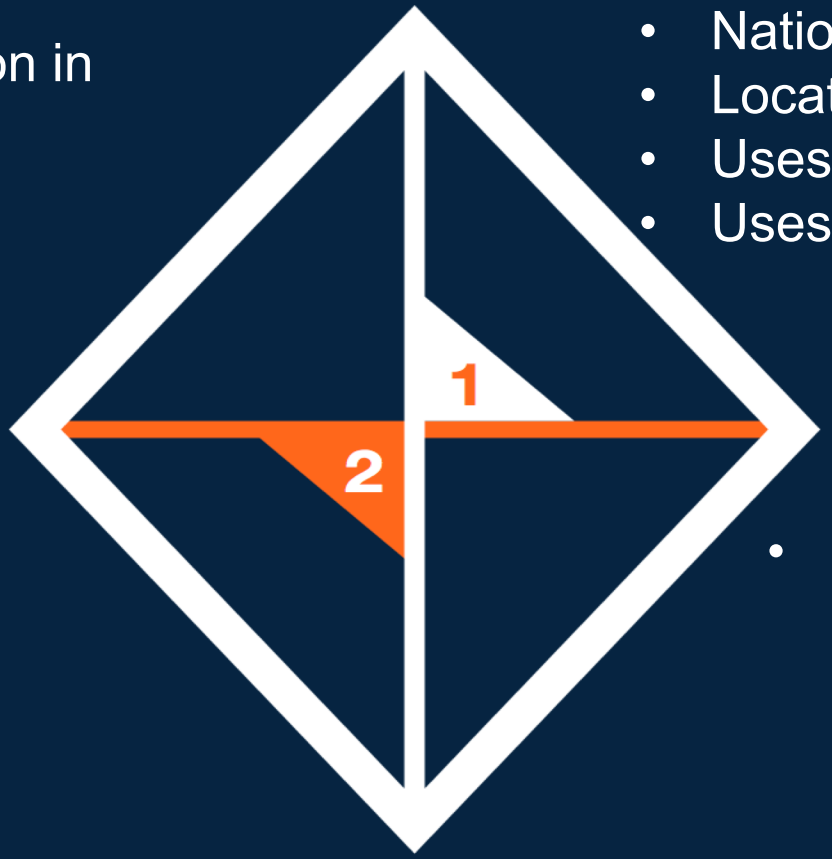


1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nationstate sponsored adversary
- Located (+8.5 timezone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office



CAPABILITIES

- PowerShell Empire
- Spearphishing

INFRASTRUCTURE

- European VPS servers

2 TECHNICAL AXIS

- WMI lateral movement
- Self signed SSL/TLS certificates
- FTP/DNS Exfiltration
- Documents with .hwp suffix
- Korean fonts for English
- User svcvnc for Persistence
- Schtasks.exe for reboot persistence
- Naenara useragent string
- YMLP
- +8.5 hour time zone
- Korean text google translated to English

VICTIMS

Western innovative Brewers and Home Brewing companies

THREATCONNECT

Thanks ThreatConnect!

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	27 items	42 items	21 items	53 items	15 items	20 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multiband Communication
	PowerShell	Create Account	New Service	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Admin Shares			Remote Access Tools
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Remote File Copy
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion		System Network Configuration Discovery				Standard Application Layer Protocol
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection		System Network Connections Discovery				Standard Cryptographic Protocol
	Scripting	Hooking	Service Registry Permissions Weakness	File Deletion		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Service Execution	Hypervisor	SID-History Injection	File Permissions Modification		System Service Discovery				Uncommonly Used Port
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File System Logical Offsets		System Time Discovery				Web Service
	Signed Script Proxy Execution	Logon Scripts	Web Shell	Hidden Files and Directories						
	Third-party Software	LSASS Driver		Image File Execution Options Injection						
	Trusted Developer Utilities	Modify Existing Service		Indicator Blocking						
	User Execution	Netsh Helper DLL		Indicator Removal from Tools						
	Windows Management Instrumentation	New Service		Indicator Removal on Host						
	Windows Remote Management	Office Application Startup		Indirect Command Execution						
				Install Root Certificate						

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

Operationalize Your Findings

- Create Feedback Loop from Hunting to Incident Response

- “End goal of hunting should be a change in policy or procedure - operationalization, don’t do the same thing over and over again”
  - Threat Hunting Webshells with Splunk, James Bower

What Could We Operationalize?

- Alert on encoded Powershell
- Alert when we see specific executables running in sequence
- Alert on SSL Issuer
- Detect new accounts created
  - Have a ticket to reference it being made to validate
- Blacklist IP Address
- Monitor User Agent String Usage
- Monitor for URIs
- Monitor and alert on firewall being disabled

```
<Image condition="image" name="technique_id=T1070,technique_name=Indicator Removal on Host">wevtutil.exe</Image>
```

```
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">RemoveDefinitions</CommandLine>
```

```
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell.exe</ParentImage>
```

https://github.com/olafhartong/sysmon-modular

```
sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" RuleName=* powershell.exe ParentImage=* | table Image ParentImage RuleName
```

Last 24 hours

✓ 29 events (2/14/19 10:00:00.000 PM to 2/15/19 10:14:43.000 PM) No Event Sampling Job Smart Mode

Events Patterns **Statistics (29)** Visualization

20 Per Page Format Preview

< Prev 1 2 Next >

Image	ParentImage	RuleName
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\whoami.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1033,technique_name=System Owner/User Discovery
C:\Windows\System32\ftp.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\netsh.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1063,technique_name=Security Software Discovery
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\eventvwr.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\eventvwr.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\eventvwr.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1086,technique_name=PowerShell
C:\Windows\System32\whoami.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1033,technique_name=System Owner/User Discovery
C:\Windows\System32\whoami.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	technique_id=T1033,technique_name=System Owner/User Discovery
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wbem\WmiPrvSE.exe	technique_id=T1086,technique_name=PowerShell

MITRE ATT&CK

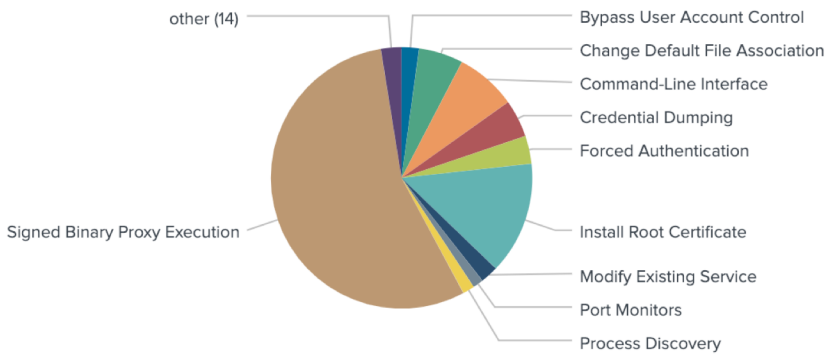
Edit | Export | ...

Sysmon Events associated with MITRE ATT&CK Techniques

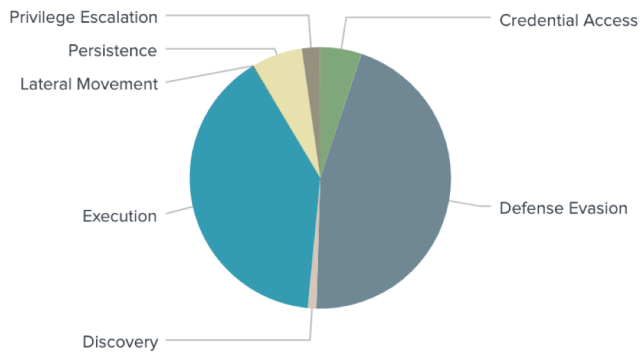
src | dest | user | tactic | technique | Time Range

All × | All × | Last 24 hours | Submit | Hide Filters

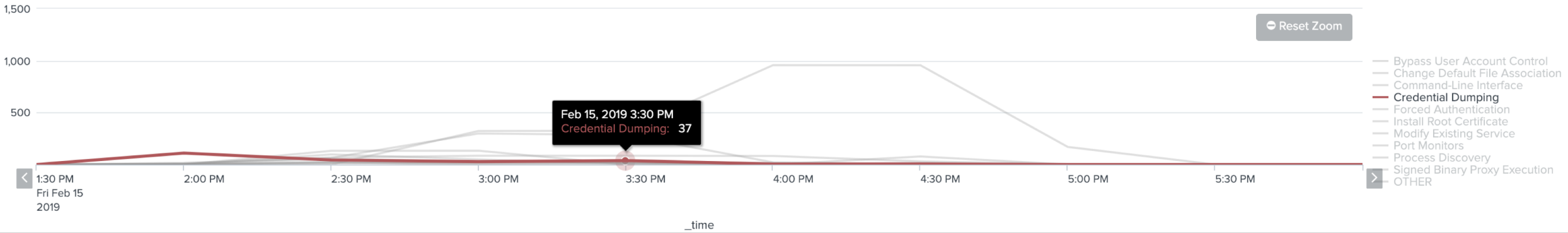
Technique



Tactic



Time Chart



MITRE ATT&CK

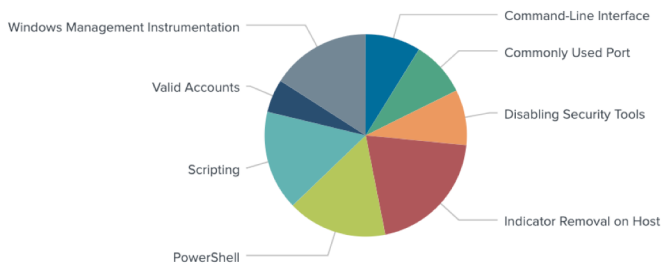
Edit | Export | ...

Notables associated with MITRE ATT&CK Techniques - Can be one notable to many techniques

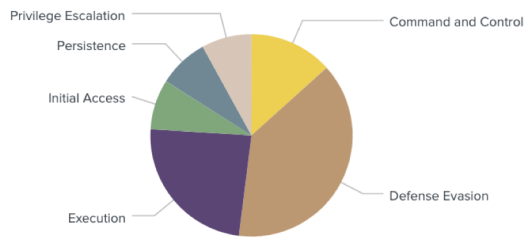
src | dest | user | tactic | technique | notable status | Time Range

All | All | All | Last 24 hours | Submit | Hide Filters

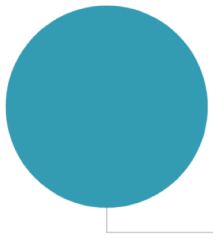
Technique



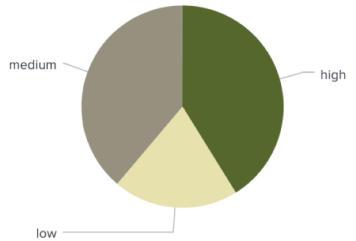
Tactic



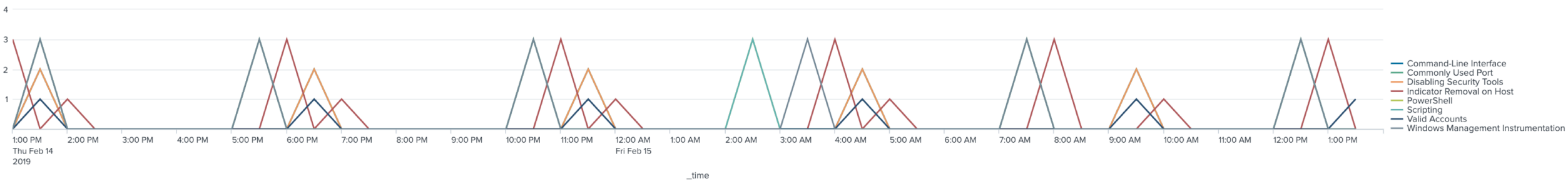
Status



Urgency



Time Chart



Where Are Our Gaps?

- Credential Access is most glaring
  - Do we have logging to provide insight into this?
- Privilege Escalation is light
- Not a lot of Discovery seen to date

- Do we have data to address these gaps?

- These could be additional hunts

Additional Resources

- Hunting with Splunk Blog Series
  - https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html
- Looking for Data Sets to Practice Against
  - Curated
    - https://www.splunk.com/blog/2018/05/03/introducing-the-security-datasets-project.html
    - http://live.splunk.com/splunk-security-dataset-project
  - DIY
    - https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html
    - http://explore.splunk.com/BOTS_1_0_datasets
    - https://splunkbase.splunk.com/app/3985/
  - Version 2 of Our Dataset Will Be Available Later in March

More on MITRE ATT&CK

- https://attack.mitre.org/
  - https://medium.com/mitre-attack

- https://www.splunk.com/blog/2019/01/15/att-ck-ing-the-adversary-episode-1-a-new-hope.html
- https://www.splunk.com/blog/2019/02/04/att-ck-ing-the-adversary-episode-2-hunting-with-att-ck-in-splunk.html
- https://www.splunk.com/blog/2019/02/08/att-ck-ing-the-adversary-episode-3-operationalizing-att-ck-with-splunk.html

Thank You!

John Stoner

@stonerpsu