

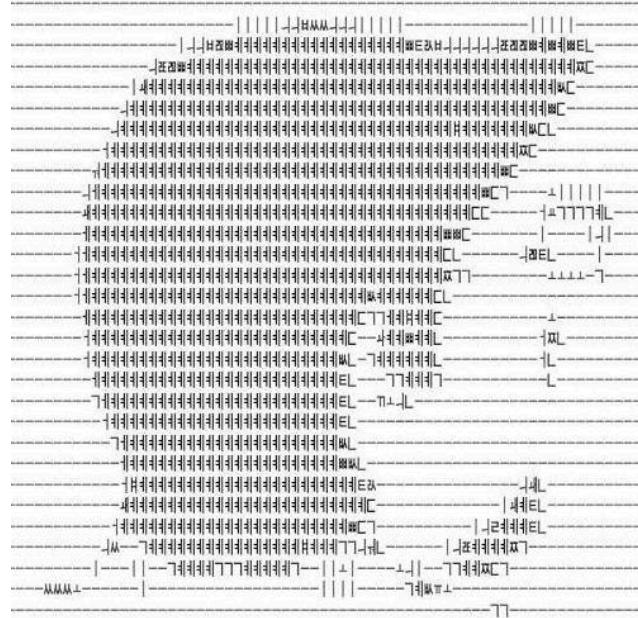
# Hunting the quick version

Ryan Kovar | Security Strategists @ Splunk

splunk >

# whoami

## Ryan Kovar: CISSP, MSc(Dist)



Staff Security Strategist  
Minster of the OODAloopers

@meansec

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

# # whoami

> **Dave Herrald** [@daveherrald](mailto:dherrald@splunk.com)

- Senior Security Architect at Splunk
- 20+ years in IT and security
  - Information security officer, security analyst/engineer/architect, pen tester, consultant, SE, sysadmin, network engineer
- GIAC GSE #79, former SANS Mentor
- Maintainer of Splunk Sysmon add-on
- Co-creator of Splunk Boss of the SOC



**IMHO**

# Why?

splunk > listen to your data

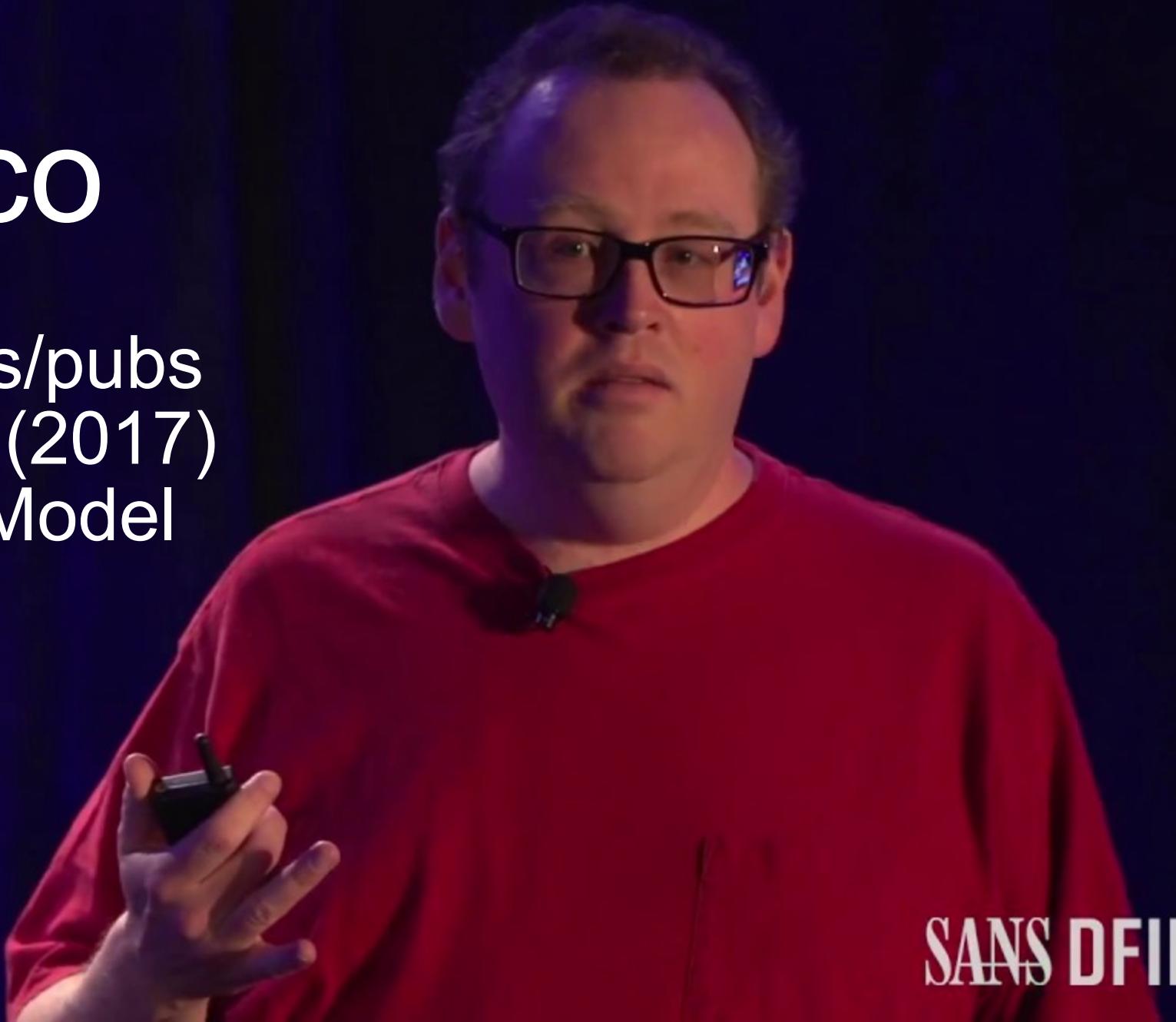
A close-up photograph of a person's hands. The person is wearing a dark suit jacket, a white shirt, and a blue striped tie. They are holding a blue credit card with both hands, presenting it towards the camera. The card has a world map graphic, the text 'Credit Card' at the top right, and 'Card' at the bottom right. It also features a card number (1234 5678 9012 3456), expiration dates (08/13 and 08/17), and a signature line that says 'CURRENT NAME'.

But first...

Let's give credit

# David Bianco

- Pyramid of Pain
- MANY SANS talks/pubs
- Blackhat speaker (2017)
- Hunting Maturity Model



SANS DFIR





We've  
seen and heard  
it all



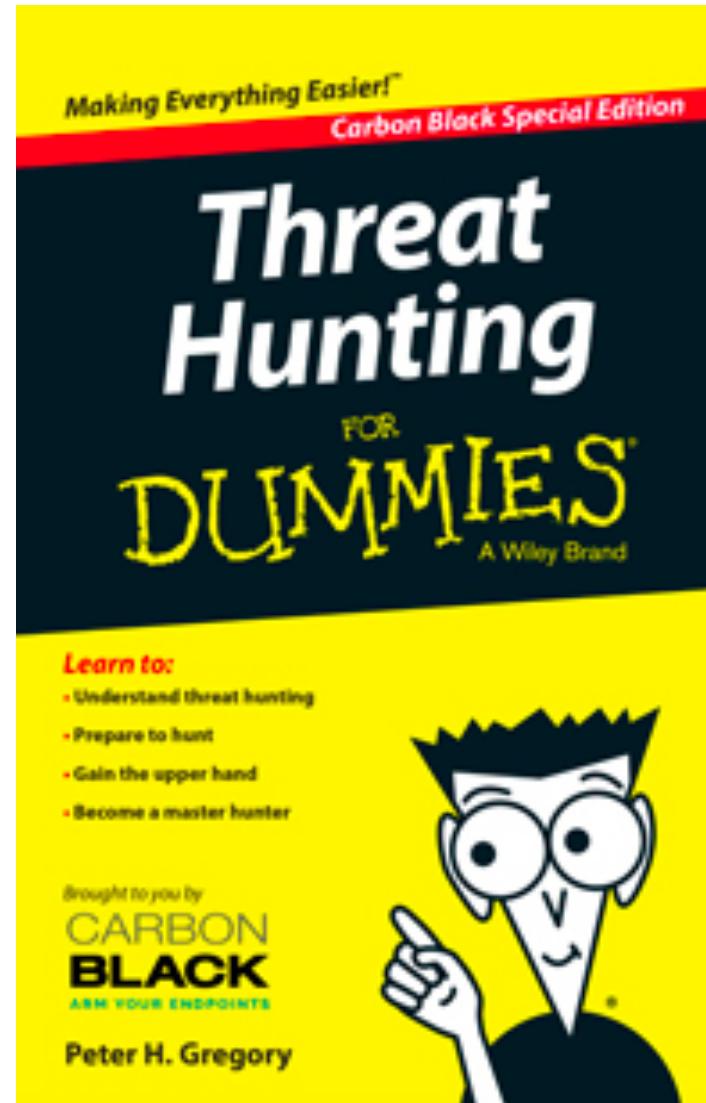
THE GOOD THE BAD AND THE UGLY

130,60,4 ~ [07/Jan 18:10:57:153] "GET /c  
128,241,220,82 ~ [07/Jan 18:10:57:123]  
1, 317,27,160,0,0 ~ [07/Jan 18:10:56:155]  
litemId=EST-16&product\_id=RP-L1-02 "o-  
://buttercup.shopping.com/n/  
to?action=purchase&t=  
opping.com/can...  
/buttercup...  
10,2  
sten to your data®

# What do I think hunting is?

splunk > listen to your data

# So many different “definitions” (vendors aren’t exactly helping)



splunk>listen to your data®

# If you are hunting Wooly Mammoth...



splunk > listen to your data®



Don't bring a 22  
caliber bullet





**“Hunting is creating a hypothesis about a threat or vulnerability and using the scientific method against your data to determine if the threat/vulnerability is relevant and present in your organization. Then... finding it”**

**- Ryan Kovar** (created for this slide)

© 2017 SPLUNK INC.

# So how do I (Ryan) hunt?

splunk > listen to your data

# SCIENTIFIC METHOD

## PURPOSE

State the problem.

## RESEARCH

Find out about the topic.

## HYPOTHESIS

Predict the outcome to the problem.

## EXPERIMENT

Develop a procedure to test the hypothesis.

## ANALYSIS

Record the results of the experiment.

## CONCLUSION

Compare the hypothesis to the experiment's conclusion.

# Know the battleground

splunk > listen to your data



# Know thy Enemy



Duck Call Demonstrations - Mallard, Pintail, Wigeon, and Blue/Green Winged Teal

pdog44450

Up next



Autoplay

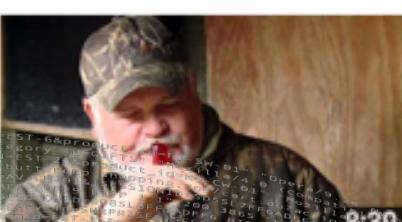
**Duck Sounds - Curious ducks talking**  
Denisa TV  
126,921 views



**Duck Commanders Teach Conan To Make Duck Calls - CONAN on TBS**  
Team Coco  
2,180,618 views

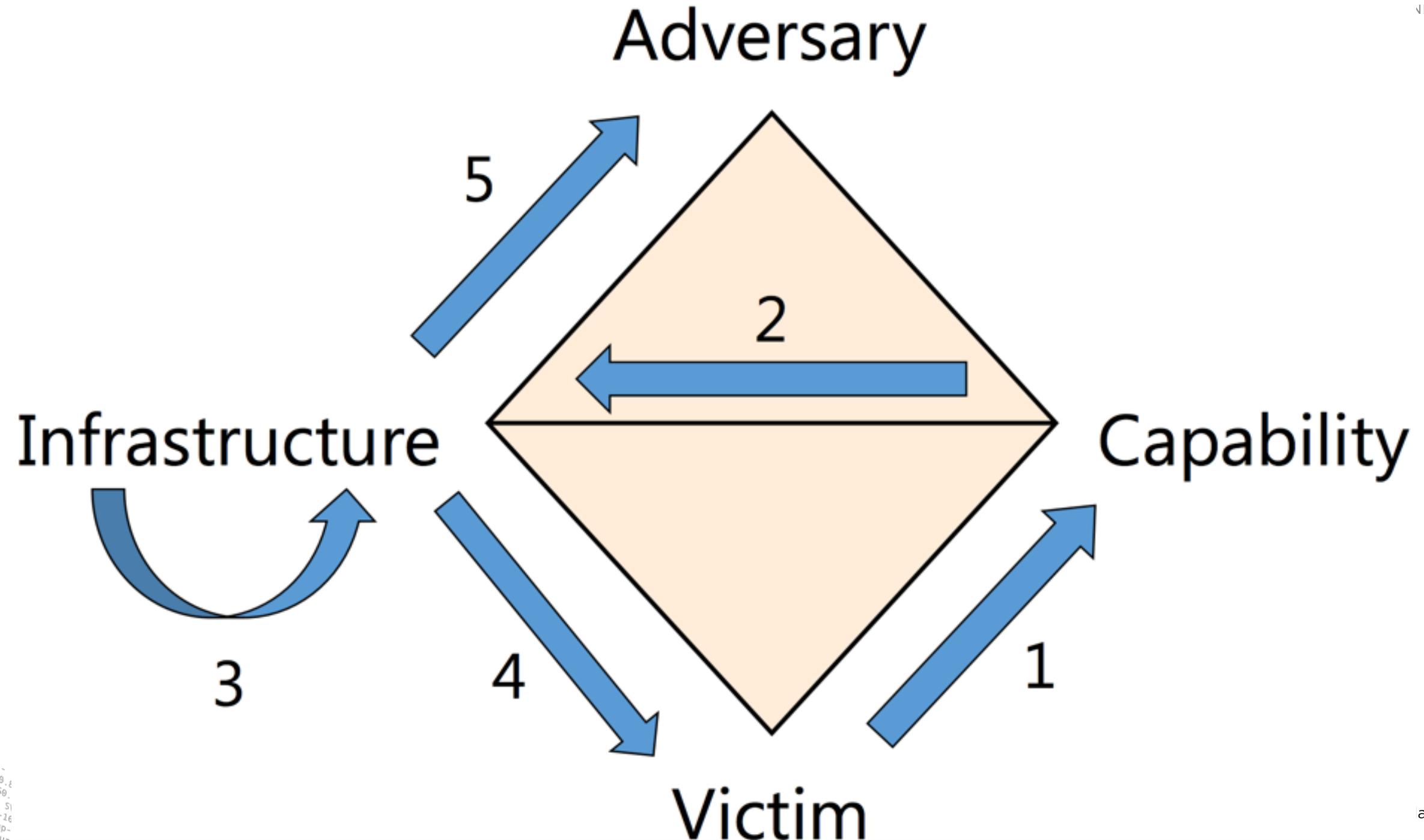


**How To Silence A Recurve Bow**  
Survival Lilly  
Recommended for you **NEW**



**Duck calling tips for beginners. Making it hum.**  
KYAfield  
splunk> listen to your data





1

## SOCIO-POLITICAL AXIS

To further strategic Chinese foreign policy objectives in the South China Sea

## CAPABILITIES



- Families of Unique Custom Malware
- Specific Post-Infection, Second-Stage Tools & Utilities
- Use of an Exploit Kit Leveraged by Asian Hackers

2

## TECHNICAL AXIS



CVE-2012-015



Spear Phishing



Right-to-Left Character Override



Self-Extracting Executables



## ADVERSARY

- People's Liberation Army Chengdu Military Region
- Second Technical Reconnaissance Bureau Military Unit Cover Designator 78020
- Ge Xing aka GreenSky27



## INFRASTRUCTURE

- Global Command & Control Infrastructure
- Chinese Dynamic DNS Infrastructure Providers
- Attacker-Registered Domains

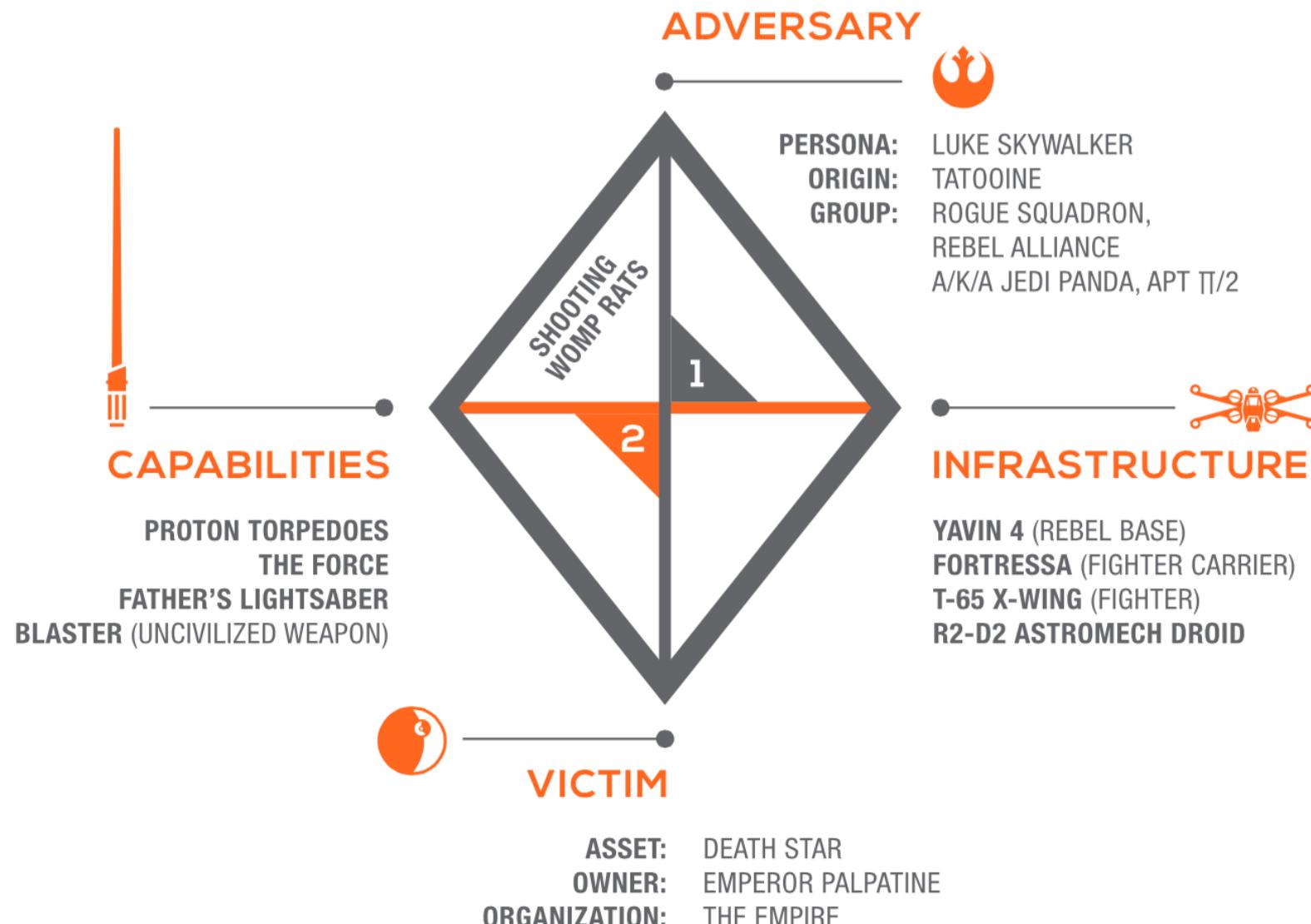


## VICTIMS

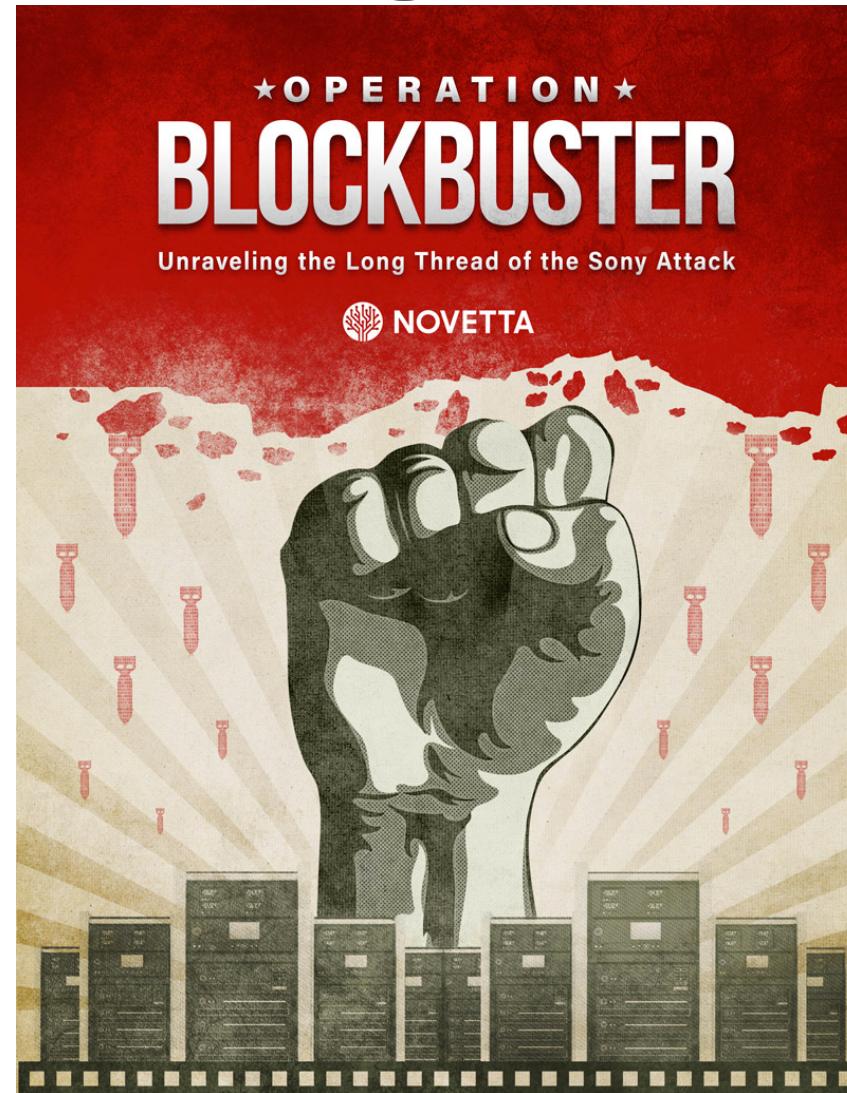
- Governments in Southeast Asia
- International organizations such as the Association of Southeast Asian Nations
- Public and private energy organizations

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

© 2017 SPLUNK INC.

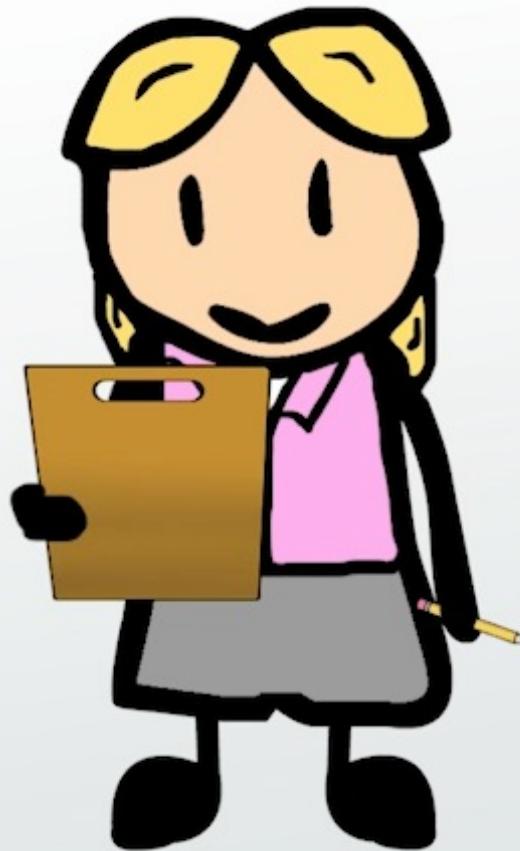


# Threat Intelligence Reports



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\_68&product\_id=F1-SW-01" "Operate 20 Compan 200  
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-ZL11a/4\_0\_Scompa 200  
1 317 27 160 0 0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST\_01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_26&product\_id=F1-ZL11a/4\_0\_Scompa 200  
0ws NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14 10  
kitemid=EST\_16&product\_id=RP-L1-02 "o-  
to?action=purchase&t  
opping.com/cart.d  
o?action=view&item  
l://buttercup-shoppin  
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\_68&product\_id=F1-SW-01" "Operate 20 Compan 200  
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-ZL11a/4\_0\_Scompa 200  
1 317 27 160 0 0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST\_01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_26&product\_id=F1-ZL11a/4\_0\_Scompa 200  
0ws NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14 10  
kitemid=EST\_16&product\_id=RP-L1-02 "o-  
to?action=purchase&t  
opping.com/cart.d  
o?action=view&item  
l://buttercup-shoppin

## ***A hypothesis should always:***



- ***explain what you expect to happen***
- ***be clear and understandable***
- ***be testible***
- ***be measurable***
- ***contain an independent and dependent variable***

# Group Hunting

---

# But first, where do I get these ideas for hunting from...

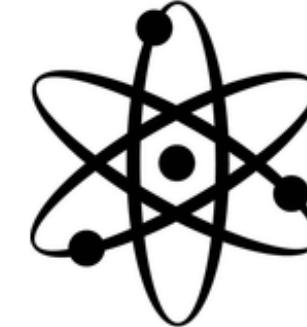




# HYPOTHESIS MONDAY.



138 69 4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=5D5SLAFT1WADFF1D HTTP/1.1" 494  
128 242 220 82 - - [07/Jan 18:10:57:153] "GET /product.screen?category\_id=GIFTS&JSESSIONID=5D5SL75EGADDF19 HTTP/1.1  
131 327 27 160 8:0 - - [07/Jan 18:10:57:153] "GET /oldlink?product\_id=FL-DSH-01&JSESSIONID=5D5SL75EGADDF19 HTTP/1.1" 200 131  
oys NT 5.1; SV1; .NET CLR 1.1.4322) 468 225 17 14 131  
kItemid=EST-16&product\_id=RP-LI-02" 404 131  
://buttercup-shopping.com/online-store/oldlink?item\_id=EST-26&JSESSIONID=5D5SL75EGADDF19 HTTP/1.1" 200 131  
dor?action=purchase&it  
ouping.com/cart  
g :  
138 69 4 - - [07/Jan 18:10:57:123] "GET /product.screen?category\_id=GIFTS&JSESSIONID=5D5SLAFT1WADFF1D HTTP/1.1" 494



**“I believe that there are  
TTPs from APT reports  
that maybe found in our  
own data”**

**KEEP  
CALM  
AND  
TEST YOUR  
HYPOTHESIS**

ThreatMiner.org | Data Mining | Ryan

Secure <https://www.threatminer.org/index.p...>

Analysis Sysadmin stuff Programming/script... Splunk SEAL capture.jpg 11 new message.... Other Bookmarks

 ThreatMiner  
Data Mining for Threat Intelligence

Search IOC Search APTNotes

Credit: This is driven by the APTNotes repository which is maintained by @kbandla, @beast\_fighter and @threatminer. All indicators are automatically extracted using a modified version of the IOCParse.

Nuclear

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017

## Search results for "Nuclear"

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

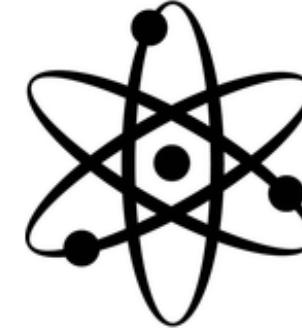
[Kaspersky\\_Lab\\_crouching\\_yeti\\_appendices\\_eng\\_final.pdf](#)

[kaspersky-the-net-traveler-part1-final.pdf](#)

[wp\\_luckycat\\_redux.pdf](#)

[Back to the top](#)

**“North Korea has been  
researching and attacking  
critical infrastructure. I  
believe that they are  
coming from their IP  
address space and  
attacking US Orgs”**



**KEEP  
CALM  
AND  
TEST YOUR  
HYPOTHESIS**

Your Friendly North Korean Net × Ryan

Secure https://nknetobserver.github.io

Analysis Sysadmin stuff Programming/script... Splunk SEAL capture.jpg 11 new message... Other Bookmarks

# ./ Your Friendly North Korean Network Observer

Packets don't care about borders

[View on GitHub](#)

---

## Introduction

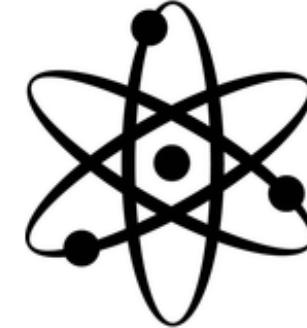
On 17 December 2011, Kim Jong Un became the leader of North Korea. Two days later, on 19 December 2011, I started my first scan of North Korean Internet space. I was curious to see if their new leader would result in change on their Internet. That was three years ago. I've been keeping an eye on that network now and again.

Ever been curious about what North Korea's Internet looks like? People seem to be interested in that country's use of computers on the Internet more these days for some reason...

Back up a second, how does North Korea get Internet, anyway?

North Korea's Internet access is as unique as many other things about the country are. The country is said to have a fairly large internal domestic internet disconnected from the world. However, there is evidence of external connections through various proxies and relay points. The screenshot shows a browser window displaying the "Your Friendly North Korean Network Observer" website, which includes a GitHub link and a "View on GitHub" button. The page content discusses the author's initial scan of the North Korean Internet in 2011 and their continued interest in monitoring it. It also poses the question of how North Korea gets Internet access. The bottom of the page features a dark background with white text containing a log of network traffic or logs, which is partially cut off at the bottom. The traffic log includes various HTTP requests and responses, such as "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" and "GET /product.screen?category\_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1". The overall theme is the exploration of North Korea's digital landscape and its connection to the outside world.

**“I believe when  
adversaries gain access to  
machines their tools leave  
artifacts on the box”**



**KEEP  
CALM  
AND  
TEST YOUR  
HYPOTHESIS**

Ryan

blog.jpcert.or.jp

Analysis Sysadmin stuff Programming/script... Splunk SEAL capture.jpg 11 new message.... Other Bookmarks

**JPCERT CC® Official Blog**  
Japan Computer Emergency Response Team Coordination Center

Jun 12, 2017

## Research Report Released: Detecting Lateral Movement through Tracking Event Logs

JPCERT/CC has been seeing a number of APT intrusions where attackers compromise a host with malware then moving laterally inside network in order to steal confidential information. For lateral movement, attackers use tools downloaded on infected hosts and Windows commands.

In incident investigation, traces of tool and command executions are examined through logs. For an effective incident investigation, a reference about logs recorded upon tool and command executions would be useful.

JPCERT/CC conducted a research on typical tools and commands that attackers use after intrusion, and traces that they leave on Windows when executed. The result of the research is available on the report below:

Detecting Lateral Movement through Tracking Event Logs

[https://www.jpcert.or.jp/english/pub/sr/ir\\_research.html](https://www.jpcert.or.jp/english/pub/sr/ir_research.html)

This entry will introduce the overview of the report.

### Intended Audience

This report is designed for technical staff including those responsible for initial investigation of incidents. Even without forensic software or knowledge in forensics, readers capable of examining event logs and registry entries can understand the contents.

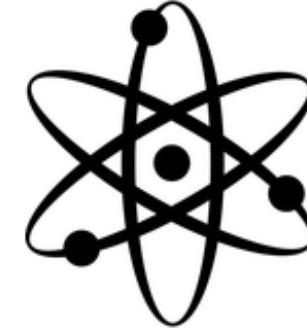
RECENT POSTS

- Research Report Released: Detecting Lateral Movement through Tracking Event Logs
- Fact-finding Report on the Establishment and Operation of CSIR in Japan
- Volatility Plugin for Detecting RedLine Malware
- RedLeaves - Malware Based on Open Source RAT
- Board game on Cyber Security for Awareness Raising
- Malware Clustering using impfuzzy & Network Analysis - impfuzzy for Nec
- Malware Leveraging PowerSploit
- PlugX + Poison Ivy = PlugIvy? - PlugX Integrating Poison Ivy's Code -
- ChChes - Malware that Communicate with C&C Servers Using Cookie Header
- Anti-analysis technique for PE Analy Tools -INT Spoofing-

CATEGORIES

- #APCERT #FIRST #Incident
- management #JPCERT new
- #Threats #Trends in Japan
- #Tsubame #Vulnerabilities Africa India

**“I believe that adversaries  
use breaking news  
headlines to lure victims”**



**KEEP  
CALM  
AND  
TEST YOUR  
HYPOTHESIS**

[Search](#)[Datasets](#)[Reports](#)[Alerts](#)[Dashboards](#)

## New Search

```
sourcetype=news_api_json  
| mvexpand articles{}.title  
| dedup articles{}.title  
| rename articles{}.title AS "Economist Headlines"  
| table "Economist Headlines"
```

10 events (before 6/19/17 8:37:00.000 PM)    [No Event Sampling](#) ▾

[Events](#)    [Patterns](#)    [Statistics \(10\)](#)    [Visualization](#)

[20 Per Page](#) ▾     [Format](#)    [Preview](#) ▾

Economist Headlines ▾

[Why May will have to compromise on Brexit](#)

[Donald Trump's need for flattery is trashing reputations](#)

[Emmanuel Macron wins a majority, though not a record one](#)

[Why Colombia's peace deal is taking so long to implement](#)

[New technology is eroding your right to tinker with things you own](#)

[The politics of a tragedy](#)

["Basic economy" class is winning over flyers](#)

[The siege of Qatar isn't working](#)

[An industry shudders as Amazon buys Whole Foods for \\$13.7bn](#)

[Italy is drifting back to its old fragmented politics](#)

330, 60, 4, ~, 1, 317, 27, 160, 0, ~, [07]Jan18:10:57:153] "GET /category.screen?categoryId=EST\_6&productId=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:156] "GET /product.screen?productId=EST-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_6&product.productId=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:56:156] "GET /oldlink?itemId=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=oldlink?itemId=EST-26&JSESSIONID=SD55L9FF1ADFF3" [07]Jan18:10:57:157] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:159] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:161] "GET /oldlink?itemId=EST-26&JSESSIONID=SD55L8FF2ADFF2 HTTP/1.1" 200 3851 "http://buttercup-shopping.com/cart.do?action=oldlink?itemId=EST-26&JSESSIONID=SD55L8FF2ADFF2" [07]Jan18:10:57:162] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:164] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:166] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07]Jan18:10:57:168] "GET /category.screen?categoryId=EST-6&productId=F1-SP-02" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

## Economist Headlines ▾

[Why May will have to compromise on Brexit](#)

[Donald Trump's need for flattery is trashing reputations](#)

[Emmanuel Macron wins a majority, though not a record one](#)

[Why Colombia's peace deal is taking so long to implement](#)

[New technology is eroding your right to tinker with things you own](#)

[The politics of a tragedy](#)

["Basic economy" class is winning over flyers](#)

[The siege of Qatar isn't working](#)

[An industry shudders as Amazon buys Whole Foods for \\$13.7bn](#)

[Italy is drifting back to its old fragmented politics](#)

## New Search

[Save As](#) [New Table](#) [Close](#)

```
index=* source="rest://newspi" | fields articles{}.title | rename articles{}.title AS text | mvexpand text | dedup text | eval news =split(text, " ") | eval news=lower(news) | mvexpand news | lookup common_words words AS news | fillnull value=NULL isTrue | search isTrue=NULL AND news!="" | stats count by news|
```

Last 24 hours



✓ 47 events (6/19/17 10:00:00.000 PM to 6/20/17 10:30:58.000 PM) No Event Sampling

Job ▾ II ■ ↗ 🔍 ⌂ ⌄ Smart Mode ▾

Events

Patterns

Statistics (46)

Visualization

20 Per Page ▾

&lt; Prev 1 2 3 Next &gt;

news

count

\$13.7bn

1

2016

1

awfully

1

bash

1

battles

1

brexit

2

britain's

1

chaotic

1

colombia's

1

displaced

1

drifting

1

economy"

1

emmanuel

1

# Now doing things

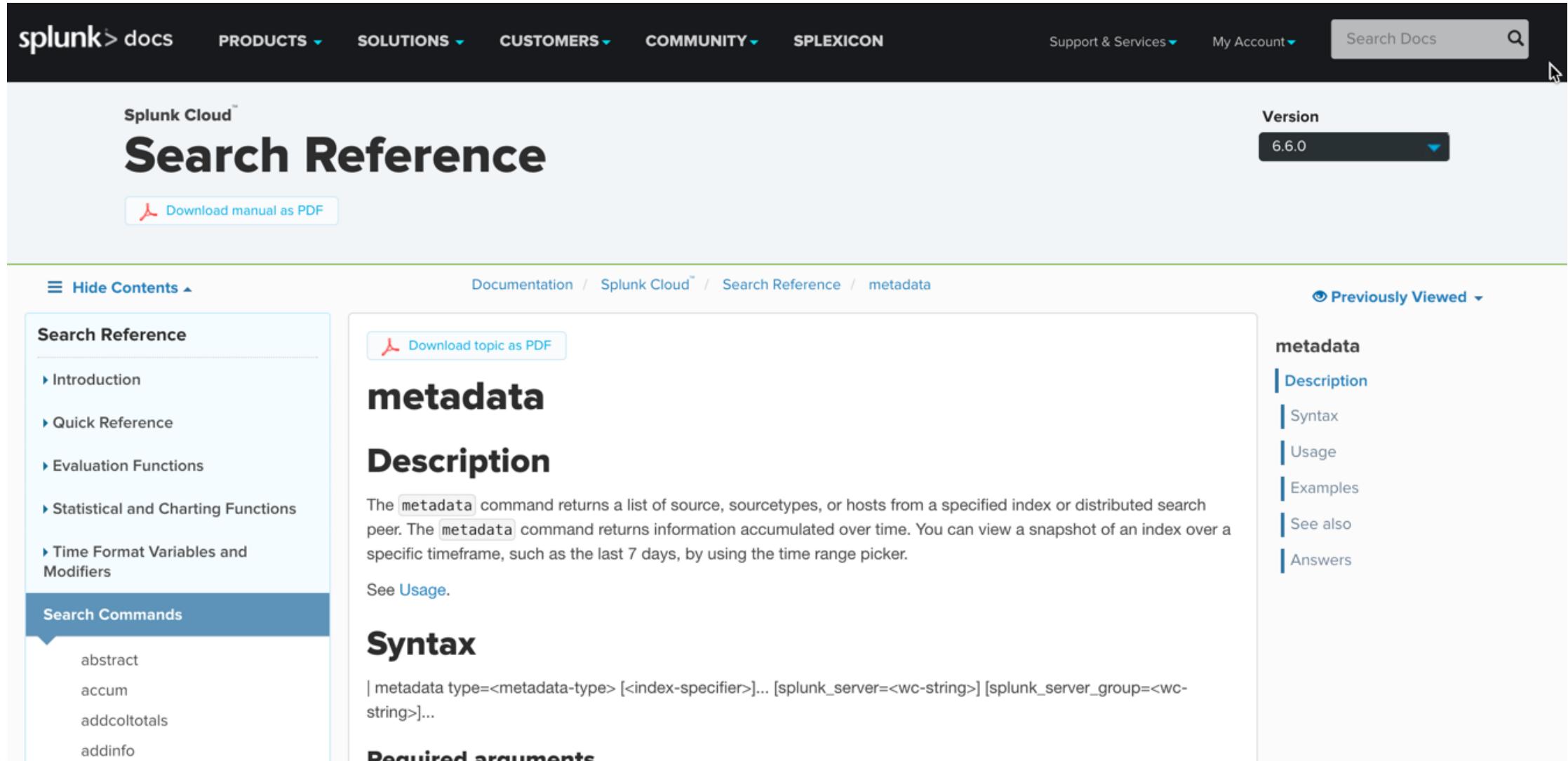
splunk > listen to your data

# Lets have a little hands on with Dave



```
138,60,4,- [07/Jan 18:10:57:153] "GET /category.screen?&category_id=5015LAFF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6Xproduct...  
128,241,220,82,- [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD55L7EEGADFF9 HTTP 1.1" 404 372 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_264&product...  
," 317,27,160,0,0,- [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L4AF4ADEF9 HTTP 1.1" 200 3118 "http://buttercup-shopping.com/cart.do?actio...  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 408 125,17 14,33  
&itemid=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
/product.purchase&itemId=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
pping.com/cart.do?action=purchase&itemId=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
10,36,- [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD48SLBF2ADF9 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
128,60,4,- [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD55L7EEGADFF9 HTTP 1.1" 404 372 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_264&product...  
," 317,27,160,0,0,- [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L4AF4ADEF9 HTTP 1.1" 200 3118 "http://buttercup-shopping.com/cart.do?actio...  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 408 125,17 14,33  
&itemid=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
/product.purchase&itemId=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
pping.com/cart.do?action=purchase&itemId=EST_16&product_id=RP-LI-02" "GET /product.screen?category_id=5015LAFF10ADF10 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio...  
10,36,- [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD48SLBF2ADF9 HTTP 1.1" 200 1080 "http://buttercup-shopping.com/cart.do?actio..."
```

# Figuring out what data you have



The screenshot shows the Splunk Cloud Search Reference page for the `metadata` command. The top navigation bar includes links for **splunk> docs**, **PRODUCTS**, **SOLUTIONS**, **CUSTOMERS**, **COMMUNITY**, **SPLEXICON**, **Support & Services**, **My Account**, and a search bar labeled **Search Docs**. A dropdown menu indicates the version is **6.6.0**.

The main content area has a sidebar titled **Search Reference** containing links for **Introduction**, **Quick Reference**, **Evaluation Functions**, **Statistical and Charting Functions**, and **Time Format Variables and Modifiers**. Below this is a section for **Search Commands** with links for `abstract`, `accum`, `addcoltotals`, and `addinfo`.

The main content area features the **metadata** command documentation. It includes a **Description** section stating that the `metadata` command returns a list of source, sourcetypes, or hosts from a specified index or distributed search peer. It also includes a **Syntax** section showing the command structure and required arguments.

A sidebar on the right is titled **metadata** and lists **Description**, **Syntax**, **Usage**, **Examples**, **See also**, and **Answers**. The bottom right corner features the **splunk>** logo with the tagline **listen to your data**.

# Filtering your data with eval and stats

splunk > docs    PRODUCTS ▾    SOLUTIONS ▾    CUSTOMERS ▾    COMMUNITY ▾    SPLEXICON    Support & Services ▾    My Account ▾    Search Docs 

Splunk Cloud™  
**Search Manual**

 Download manual as PDF

Version  
6.6.0 ▾

---

☰ Hide Contents ▾

Documentation / Splunk Cloud™ / Search Manual / Use stats with eval expressions and functions

 Download topic as PDF

## Use stats with eval expressions and functions

This topic discusses how to use eval expressions and functions within your stats calculation.

- For more information about the eval command and syntax, see the [eval command](#) in the [Search Reference](#).
- For the list of eval functions, see [Evaluation functions](#) in the [Search Reference](#).
- Also, you can read more about using the eval command to [evaluate and manipulate fields](#) in another section in this manual.

### Example 1: Distinct counts of matching events

This example counts the IP addresses where the errors originate. This is similar to a search for events that is filtered for a specific error code, and then used with the stats command to count the IP addresses.

status=404 | stats dc(ip)

Use stats with eval expressions and functions

Example 1: Distinct counts of matching events

Example 2: Categorizing and counting fields

splunk > listen to your data®

# Parsing the webz

The screenshot shows a web browser window displaying the URL Toolbox app page on Splunkbase. The title bar reads "URL Toolbox | Splunkbase". The address bar shows the URL "https://splunkbase.splunk.com/app/2734/". The page content includes a large image of the app's interface, which is a search results page for a query like "Events Before 12/1/19 3:34:55,000 PM". The search results table lists various URL components such as host, path, and query. Below the image, there are navigation arrows, a rating section with 5 stars and 5 ratings, and summary statistics: 711 installs and 2,890 downloads.

URL Toolbox | Splunkbase

Ryan

Splunk, Inc. [US] https://splunkbase.splunk.com/app/2734/

Analysis Sysadmin stuff Programming/script... Splunk SEAL capture.jpg 11 new message.... Disapproval Look Metro - Bus - Next... Other Bookmarks

Search App by keyword, technology...

My Account Support & Services

**URL Toolbox**

5 ratings

Overview Details

711 2,890

Installs Downloads

# Pivoting tastes goooooooood

Type	Site	TOCs	Description
IP/Domain/ Shared Domains on IP Address	<a href="http://www.Robtex.com">www.Robtex.com</a>	IPs, Domains	One of the best of breed tools to investigate Domains, IP addresses, and more.
IP/Domain Information	<a href="http://centralops.net">centralops.net</a>	IPs, Domains	Investigate Domains and IP addresses
Geolocate IPs/Domains	<a href="http://iplocation.net">iplocation.net</a>	IPs, Domains	Quick way to find the most up-to-date location of a IP from several different vendors
Geolocate Ps/Domains	<a href="http://Infosniper.net">Infosniper.net</a>	IPs, Domains	Shows location and provides a nice map
PassiveDNS, SSL Certificates, Shared Domains on	<a href="http://www.passivetotal.org">www.passivetotal.org</a>	IPs, Domains	Research Domains, IPs, passive DNS sources, SSL certs, and more. Sign up for a free license.

# Lets go to the cyber hunting range





# Incident #1



- ▶ Website defacement
  - ▶ Po1s0n1vy APT

**YOUR  
SITE  
HAS BEEN  
DEFACED**

P01s0n1vy was HERE

Deal with it, Admin



# Incident #2



► Ransomware

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-68&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:153] "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-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AUTOCUP-SHIRT SESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product\_id=F1-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AUTOCUP-SHIRT SESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-68&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product\_id=F1-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 4318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product\_id=F1-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 4318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AUTOCUP-SHIRT SESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-68&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468.125.17.14 - - [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-68&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:153] "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-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AUTOCUP-SHIRT SESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product\_id=F1-ZL11&category\_id=SURPRISES&JSESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AUTOCUP-SHIRT SESSIONID=SD59L4FFFAADEF7" HTTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-68&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"



Recycle Bin

# DECRYPT  
MY FILES #



EaseUS Todo  
Backup Free  
9.2



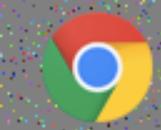
# DECRYPT  
MY FILES #



Google  
Chrome



oYYcfb-vFg...



# DECRYPT  
MY FILES #



# DECRYPT  
MY FILES #

Your documents, photos, databases and other important files  
have been encrypted!

If you understand all importance of the situation then we propose to you  
to go directly to your personal page where you will receive the complete  
instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

- 1. <http://cerberhyed5frqa.xmfir0.win/30EF-3C4E-A460-005E-93C9>
- 2. <http://cerberhyed5frqa.gkfit9.win/30EF-3C4E-A460-005E-93C9>
- 3. <http://cerberhyed5frqa.305iot.win/30EF-3C4E-A460-005E-93C9>
- 4. <http://cerberhyed5frqa.dkrti5.win/30EF-3C4E-A460-005E-93C9>
- 5. <http://cerberhyed5frqa.cneo59.win/30EF-3C4E-A460-005E-93C9>
- 6. [http://cerberhyed5frqa.onion/30EF-3C4E-A460-005E-93C9 \(TOR\)](http://cerberhyed5frqa.onion/30EF-3C4E-A460-005E-93C9 (TOR))



9:49 PM

8/26/2016

# Luckily Everything Is Captured In Splunk

Splunk > App: Search & Rep... frpcenk Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search Save As Close

index=main sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=2 TargetFilename=\*work\_stuff\*

10 events (before 9/19/16 9:21:47.000 PM) No Event Sampling Job II Smart Mode

Events (10) Patterns Statistics Visualization

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

List Format 20 Per Page

< Hide Fields	All Fields	i	Time	Event
Selected Fields		>	8/24/16 5:15:06.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><Event ID=2><EventID><Version>4</Version><Level>4</Level><Task>2</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T17:15:06.348391100Z'><EventRecordID>410002</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'></System><EventData><Data Name='UtcTime'>2016-08-24 17:15:06.348</Data><Data Name='ProcessGuid'>{0F2D76F0-D007-57BD-0000-0010D0C73500}</Data><Data Name='ProcessId'>3588</Data><Data Name='Image'>:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\{35ACA89F-933F-6A5D-2776-A3589FB99832}\os.exe</Data><Data Name='TargetFilename'>C:\Users\bob.smith.WAYNECORPINC\Desktop\work_stuff017017682.html</Data><Data Name='CreationUtcTime'>1602-05-15 14:07:01.334</Data><Data Name='PreviousCreationUtcTime'>2016-08-24 15:08:38.008</Data></EventData></Event>
Interesting Fields				host = we8105desk   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
a host 1				
a source 1				
a sourcetype 1				
a action 1				
a app 1				
a Computer 1				
a CreationUtcTime 1				
a direction 1				
a dvc 1				
a dvc_nt_host 1				
a EventChannel 1				
# EventCode 1				
a EventDescription 1				
Selected Fields		>	8/24/16 5:14:23.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><Event ID=2><EventID><Version>4</Version><Level>4</Level><Task>2</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T17:14:23.068837700Z'><EventRecordID>409661</EventRecordID><Correlation/><Execution ProcessID='1216'

splunk > listen to your data®

# Yes, Pretty Much Everything

Splunk search interface showing a search for sourcetypes:

```
|metadata type=sourcetypes index=* | sort -totalCount | fields sourcetype,totalCount | search sourcetype!="log2timeline"
```

The results table shows the following data:

sourcetype	totalCount
stream:amb	167894
suricata	151405
stream:tcp	86579
stream:ssl	80339
stream:ip	74720
fgt_traffic	58748
Wazuh Security	48114
stream:utm	45634
stream:imap	25395
stream:dnsmasq	12778
stream:ssh	9653
IIS	7025
stream:exif	5963
stream:application	852
stream:sip	750
stream:snmp	214
stog:peinfo	192
stog:clamav	98
stog:sntp	92
stog:vimis	75
stog:exif	50
stog:netback	38
stog:log	26
stog:peinfo	12
stog:clamav	8
stog:sntp	7
stog:vimis	3
stog:exif	3

Large green text overlay on the search results:

- Microsoft Sysmon
- Windows Events
- Windows Registry
- IIS
- Splunk Stream (wire data)
- Suricata
- Fortigate (NGFW)

# Two Different Splunk Servers

## 1. BOTS Scoring Server

splunk> App: Boss of the SOC ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Welcome Questions Top 10 Teams All Teams' Scores Boss of the SOC Activity Rules Help Credits Dashboards Search Boss of the SOC

**Welcome to the Boss of the SOC (BOTS) Competition**

BOTS is a Capture the Flag-esque competition where you play the part of a SOC analyst. You are presented with various questions about multiple security-related scenarios. Some are easy. Some are hard. You will use your Splunk Search Server, background information and external sources to answer the questions as quickly and accurately as you can.

Check out the following other pages

- **Questions:** You come here to submit answers and to see what you've already answered.
- **Top 10 Teams:** Look here to view the current top ten teams.
- **All Teams' Scores:** This shows the scores for all of the teams in the competition.
- **Boss of the SOC Activity:** You can view current activity like most active teams and question attempts.
- **Rules:** Take a look at the competition rules here if you haven't already.
- Help Menu: This is where you will see the scenarios and other resources that will help you during the competition.

\* If you ever need assistance, you can:

- Ask any on-site Splunk BOTS Personnel
- Email [bots@splunk.com](mailto:bots@splunk.com)
- Access the Slack channel that was setup for your event



About Support File a Bug Documentation Privacy Policy © 2005-2016 Splunk Inc. All rights reserved.

- ▶ Review the scenarios
- ▶ Get the questions
- ▶ Submit answers
- ▶ View team standings
- ▶ aka Q&A Server

# Questions

**splunk > App: Boss of the SOC**

Welcome Questions Scoring Analytics ▾ Rules Help ▾ Credits Dashboards Search **Boss of the SOC**

Questions Edit Export ...

Click a question below to submit an answer. Click ">" to see detail regarding the question.

#	Number	Question	Status	Base Points Avail.	Base Points Earned	Bonus Points Earned	Penalty Points	Hints Available	Hints Received
>	1	This is a simple question to get you familiar with submitting answers. What is the name of the software that you are using for this competition? Just a six-letter word with no punctuation.	Correct ✓	50	50	11	0	0	0
>	101	What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?	Unanswered ⚠	50	0	0	0	0	0
>	102	What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example "Microsoft" or "Oracle")	Incorrect ❌	50	0	0	10	0	0
>	103	What content management system is imreallynotbatman.com likely using?(Please do not include punctuation such as . , ! ? in your answer. We are looking for alpha characters only.)	Unanswered ⚠	50	0	0	0	0	0
>	104	What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with extension (For example "notepad.exe" or "favicon.ico")	Unanswered ⚠	250	0	0	0	0	0
>	105	This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?	Unanswered ⚠	250	0	0	0	0	0
>	106	What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?	Unanswered ⚠	500	0	0	0	0	0
>	107	Based on the data gathered from this attack and common open source intelligence sources for domain names, what is the email address that is most likely associated with Po1s0n1vy APT group?	Unanswered ⚠	100	0	0	0	0	0
>	108	What IP address is likely attempting a brute force password attack against imreallynotbatman.com?	Unanswered ⚠	50	0	0	0	0	0
>	109	What is the name of the executable uploaded by Po1s0n1vy? Please include file extension. (For example, "notepad.exe" or "favicon.ico")	Unanswered ⚠	50	0	0	0	0	0
>	110	What is the MD5 hash of the executable uploaded?	Unanswered ⚠	250	n	n	n	n	n

In the scoring app, click 'Questions' to get started.

# Two Different Splunk Servers

## 2. BOTS Search Server

The screenshot shows the Splunk Search & Reporting interface with a search bar containing the query `| metadata type=sourcetypes index=* | sort -| totalCount`. The results table displays 22 results, all of which are sourcetypes. The columns include firstTime, lastTime, recentTime, sourcetype, totalCount, and type. The results are as follows:

firstTime	lastTime	recentTime	sourcetype	totalCount	type
1470009600	1472428740	1473366071	WinEventLog:Security	14218920	sourcetypes
1470009602	1472428740	1473366112	fgt_traffic	7675023	sourcetypes
1470031200	1472450339	1473366092	suricata	5078376	sourcetypes
1470009600	1472428740	1473366082	stream:tcp	1754601	sourcetypes
1470009600	1472428740	1473366082	stream:ip	1435025	sourcetypes
1470009601	1472428740	1473366082	stream:dns	1369998	sourcetypes
1470009602	1472428739	1473366114	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	830389	sourcetypes
1470009600	1472428732	1473366082	stream:smb	448008	sourcetypes
1470009624	1472428706	1473366112	fgt_utm	257477	sourcetypes
1470009603	1472428718	1473366082	stream:idap	115625	sourcetypes
1472055742	1472063262	1472063262	WinRegistry	74720	sourcetypes
1470009613	1472428700	1473366112	fgt_event	53422	sourcetypes
1470009661	1472428498	1473366082	stream:http	39010	sourcetypes
1470863815	1472056633	1472056681	iis	22615	sourcetypes

- ▶ Just search!
- ▶ Core Splunk only
  - ☺ url toolbox
- ▶ index=main
- ▶ Shouldn't need wildcards

# KISS

splunk®

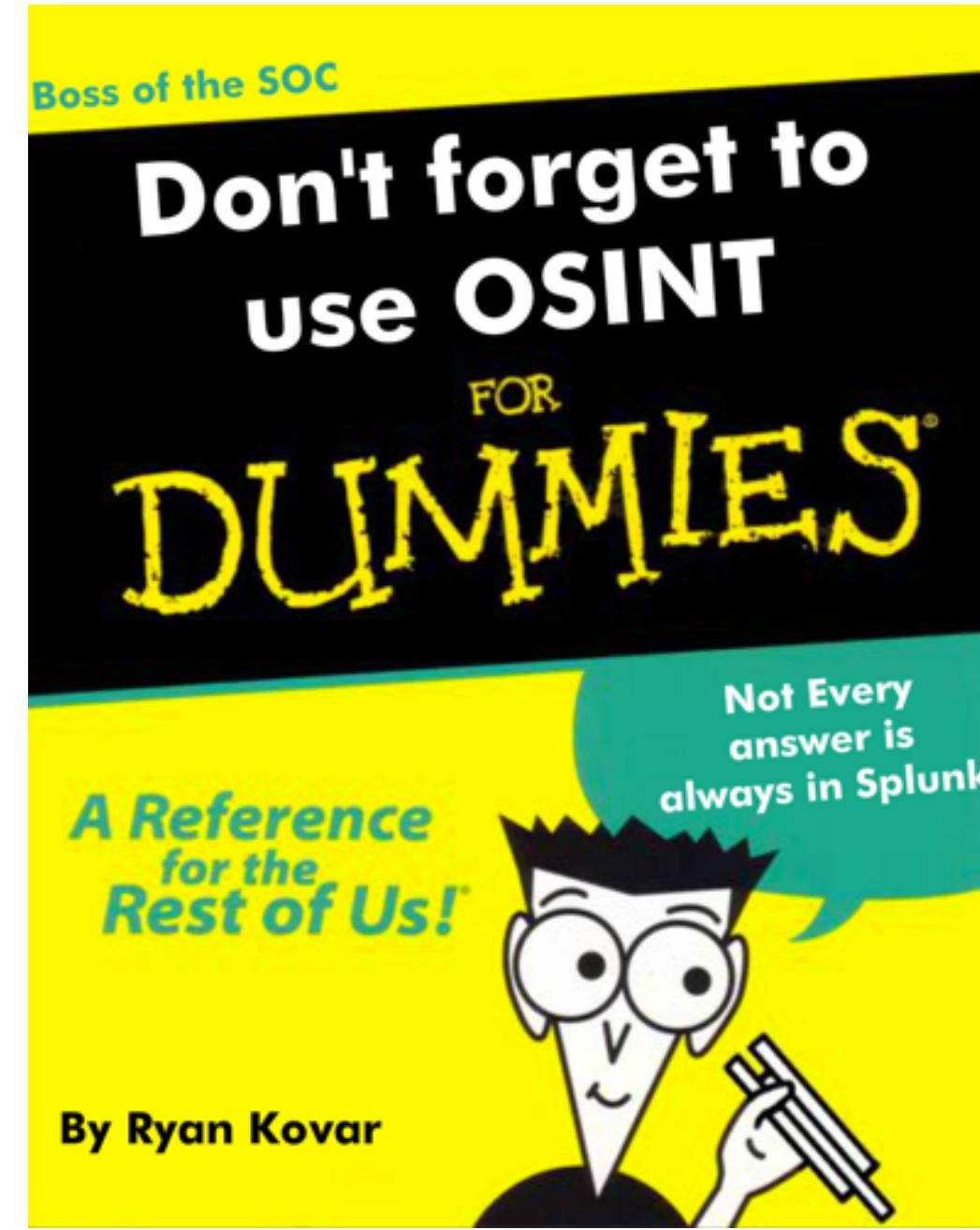


Just  
one  
more  
thing...

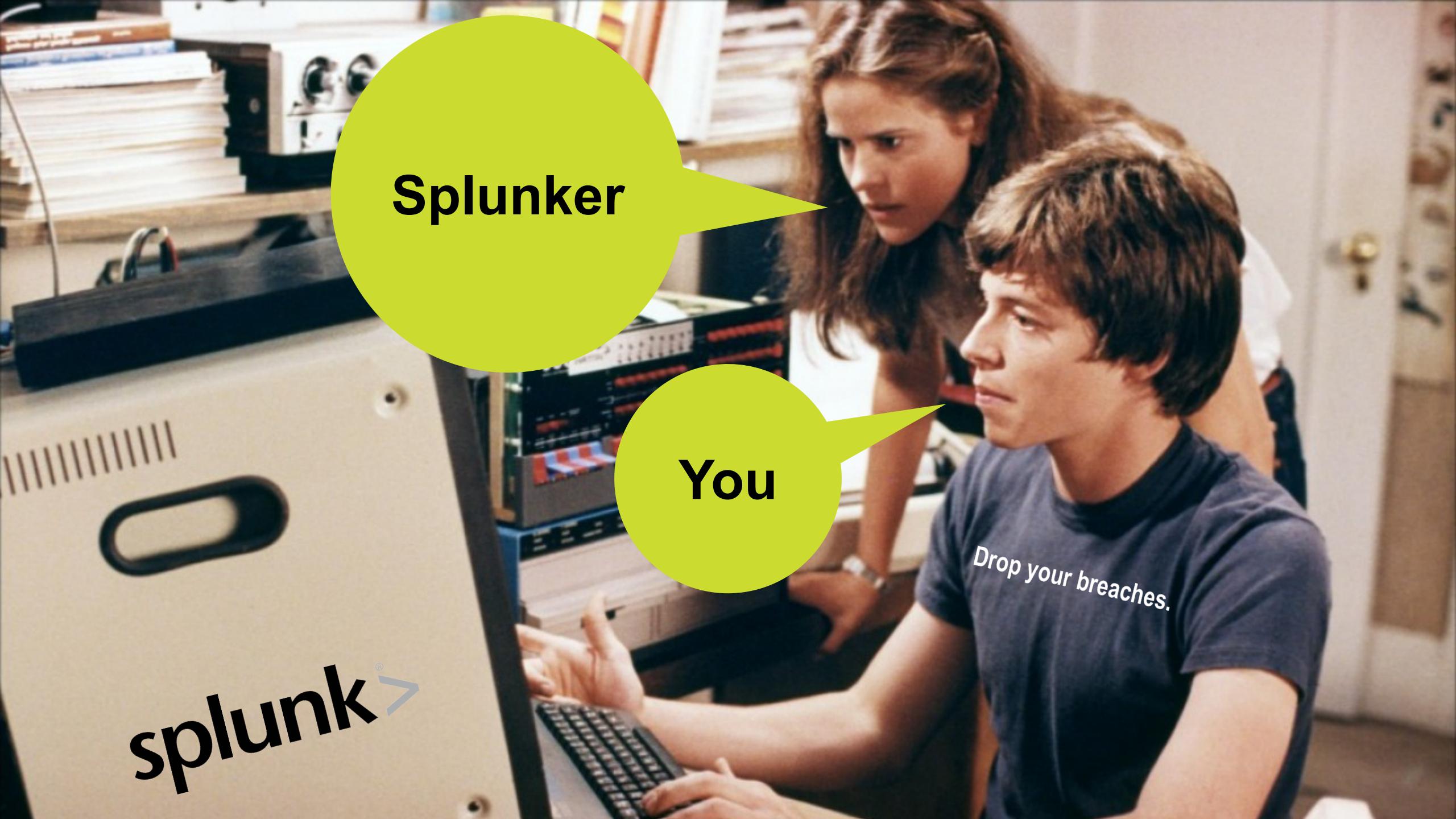


**None of the websites you will see are still alive...  
but on the internet nothing is forgotten**





splunk > listen to your data®



Splunker

You

*Drop your breaches.*

splunk®>

GAME OVER