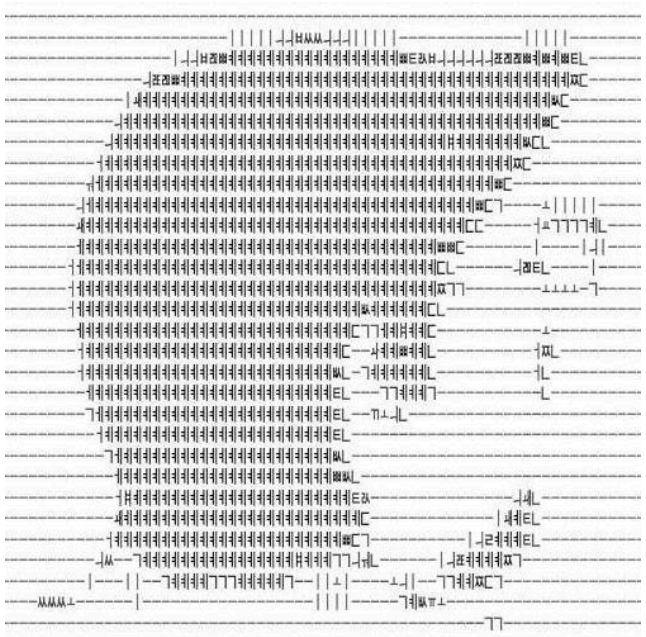
Hunting the quick version

Ryan Kovar | Security Strategists @ Splunk

whoami

Ryan Kovar: CISSP, MSc(Dist)



- 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 ಠ_ಠ

Staff Security Strategist

Minster of the OODAloopers

@meansec

whoami

> **Dave Herrald** dherrald@splunk.com|@daveherrald

- 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?


But first…
Let’s give credit
Credit Card
1234 5678 9012 3456
08/13 VALID DATES 08/17
RRENT NAME
Card

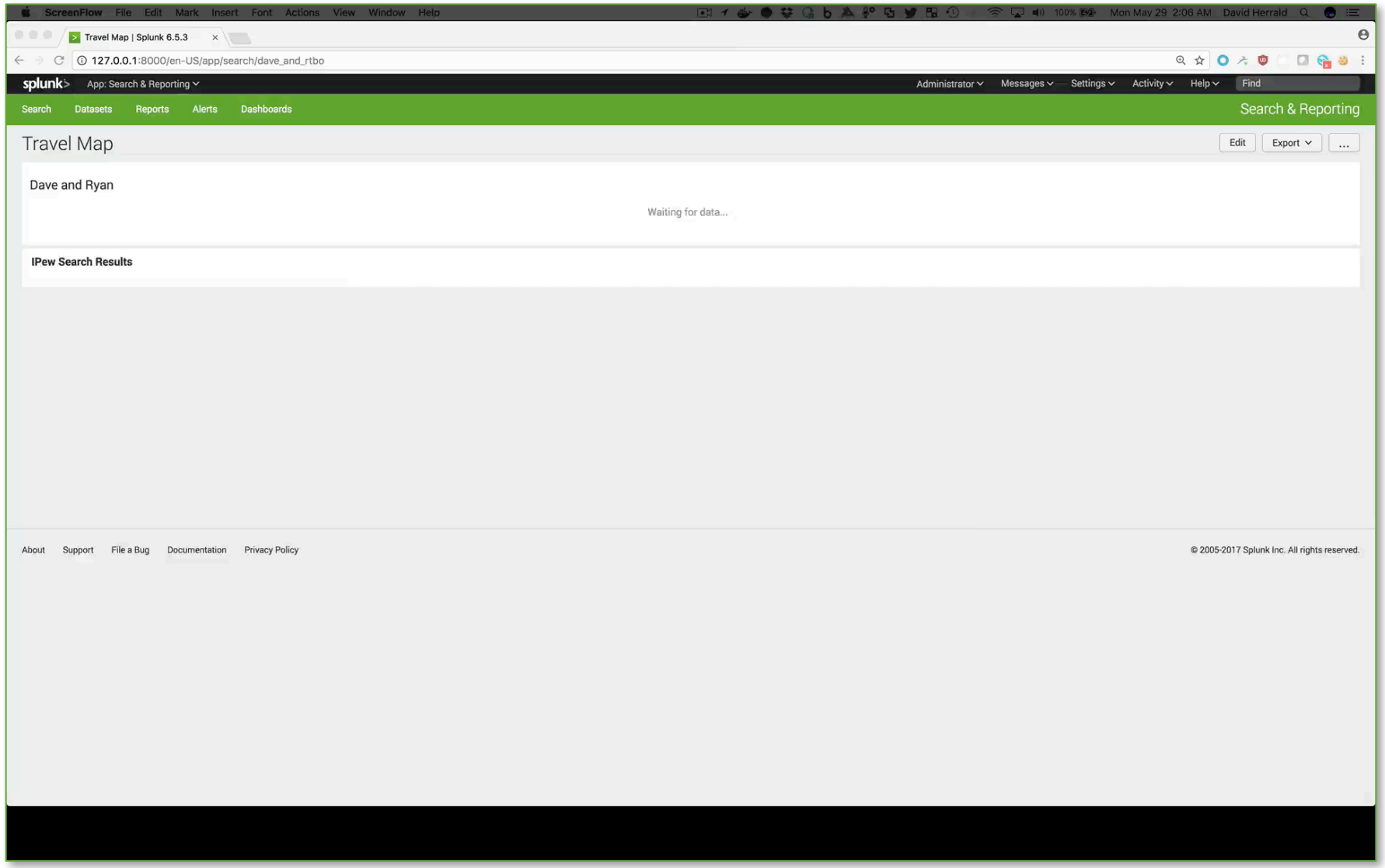
David Bianco

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

SANS DFIR

Hunting…

But We've been all over



We've seen and heard it all

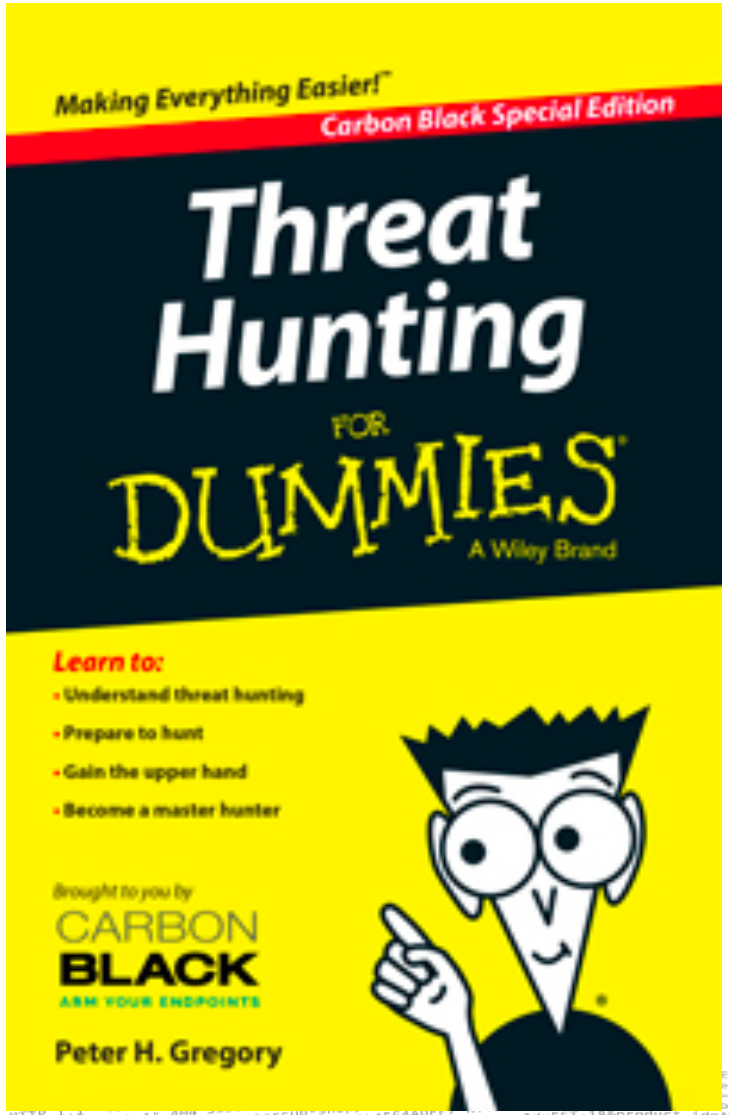
I've got Bro, Splunk, FireEye. I do OSINT, collect ALL the Logs, and even drink beer at work.

Sure I'm secure. I have a Firewall!

We don't need a SOC. We have a guy named Dave. He is friends with the boss and is great at computers

What do I think hunting is?

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



If you are hunting Wooly Mammoth…

splunk> listen to your data

Don’t bring a 22 caliber bullet

If you are trying to catch smelt…

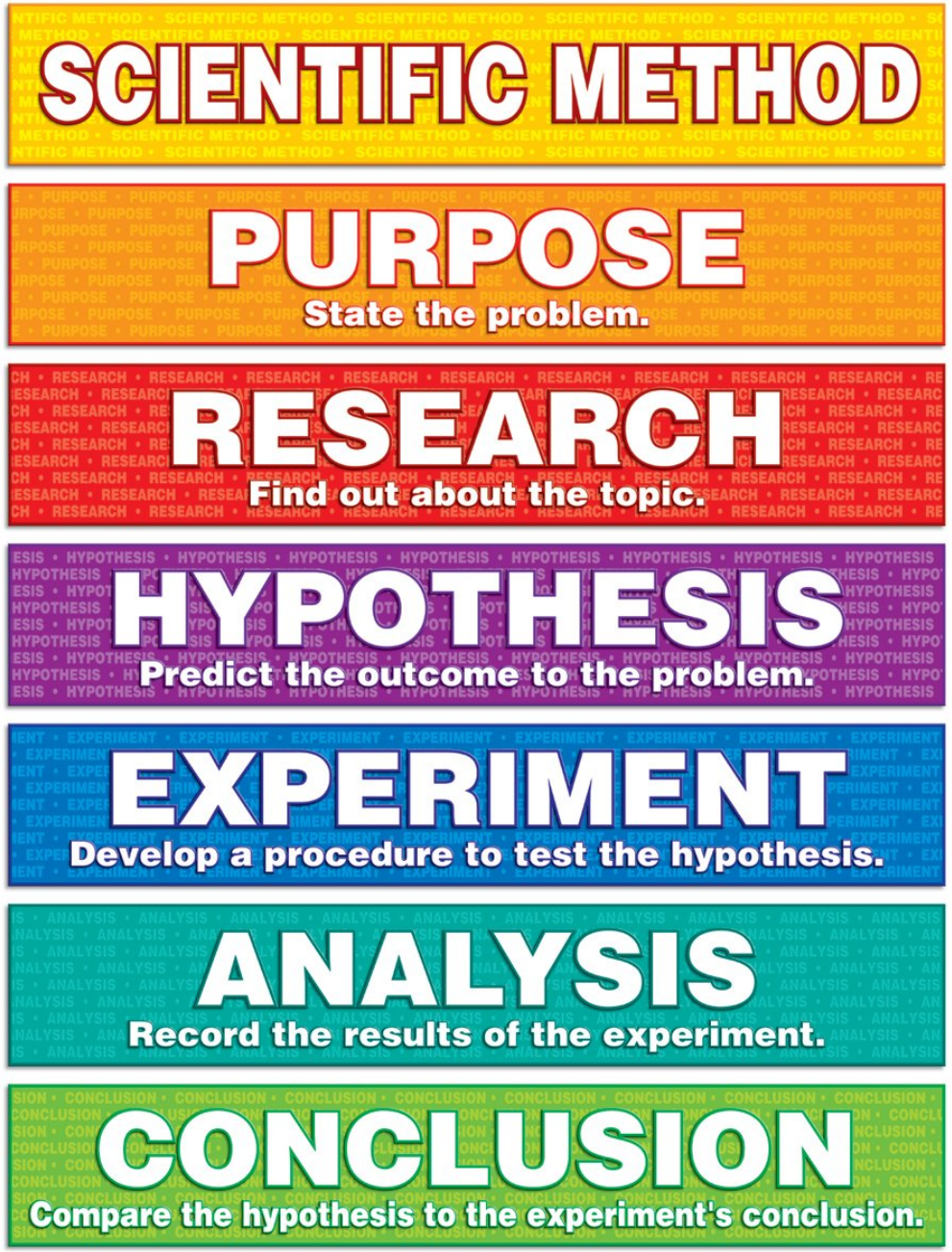
splunk> listen to your data

You might not use a big hook

“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)

So how do I (Ryan) hunt?



Know the battleground

splunk> listen to your data®

|metadata

New Search

Save As Close

```
| metadata type=sourcetypes index=main
```

Last 7 days

✓ 128 results (5/13/17 10:00:00.000 PM to 5/20/17 10:38:15.000 PM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (128) Visualization

20 Per Page Format Preview

< Prev 1 2 3 4 5 6 7 Next >

firstTime	lastTime	recentTime	sourcetype	totalCount	type
1494604265	1495317672	1495317709	FireEye_CEF	5162	sourcetypes
1494604017	1495319835	1495319893	Linux:SELinuxConfig	356780	sourcetypes
1494603971	1495319805	1495319893	Linux:Service	356780	sourcetypes
1494603990	1495319879	1495319893	Linux:Update	356785	sourcetypes
1494604045	1495319855	1495319893	Linux:VSFTPDConfig	356780	sourcetypes
1494604566	1495317673	1495317724	MonitorWare:Security	11940	sourcetypes
1494604564	1495317672	1495317724	NTSyslog:Security	5970	sourcetypes
1494603969	1495319834	1495319893	OSX:Service	356780	sourcetypes
1494603998	1495319847	1495319893	OSX:Update	356785	sourcetypes

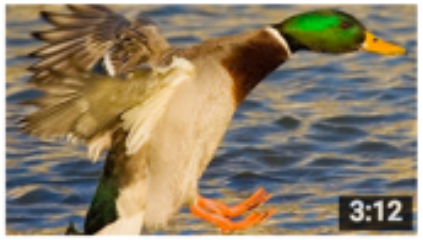
Know thy Enemy

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

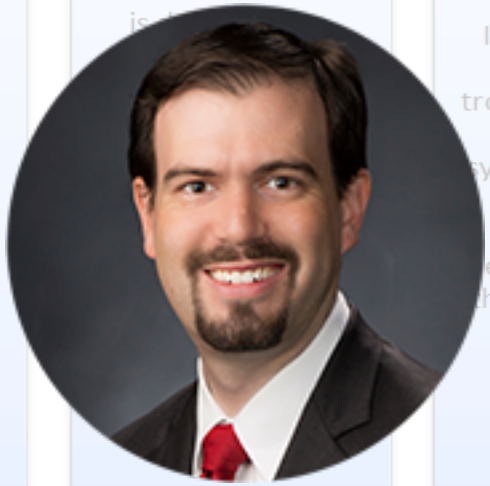
Duck Commanders Teach Conan To Make Duck Calls - CONAN on TBS
Team Coco
2,180,618 views

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

Duck calling tips for beginners. Making it hum.
KYAfield

"The Cyber Kill Chain"™

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control (C2)	Actions on Objectives
Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.	After the weapon is	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.



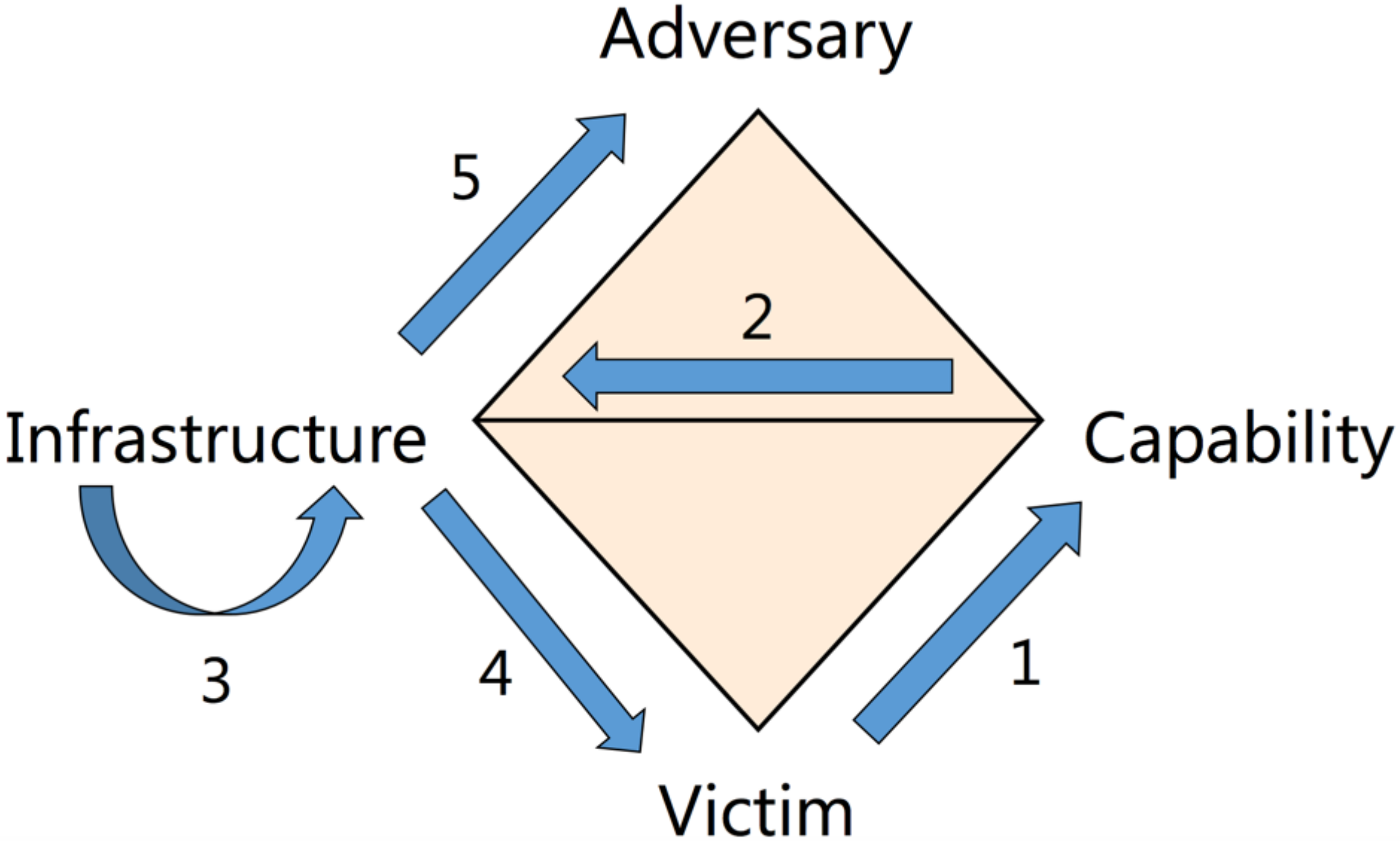
Detect, Deny Disrupt Degrade Deceive Destroy

Leverage, discover, analyze

Atomic, computed and behavior indicators

Campaign Analysis – Tools and Techniques

splunk> listen to your data



1 SOCIO-POLITICAL AXIS

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

ADVERSARY

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

CAPABILITIES

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

INFRASTRUCTURE

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

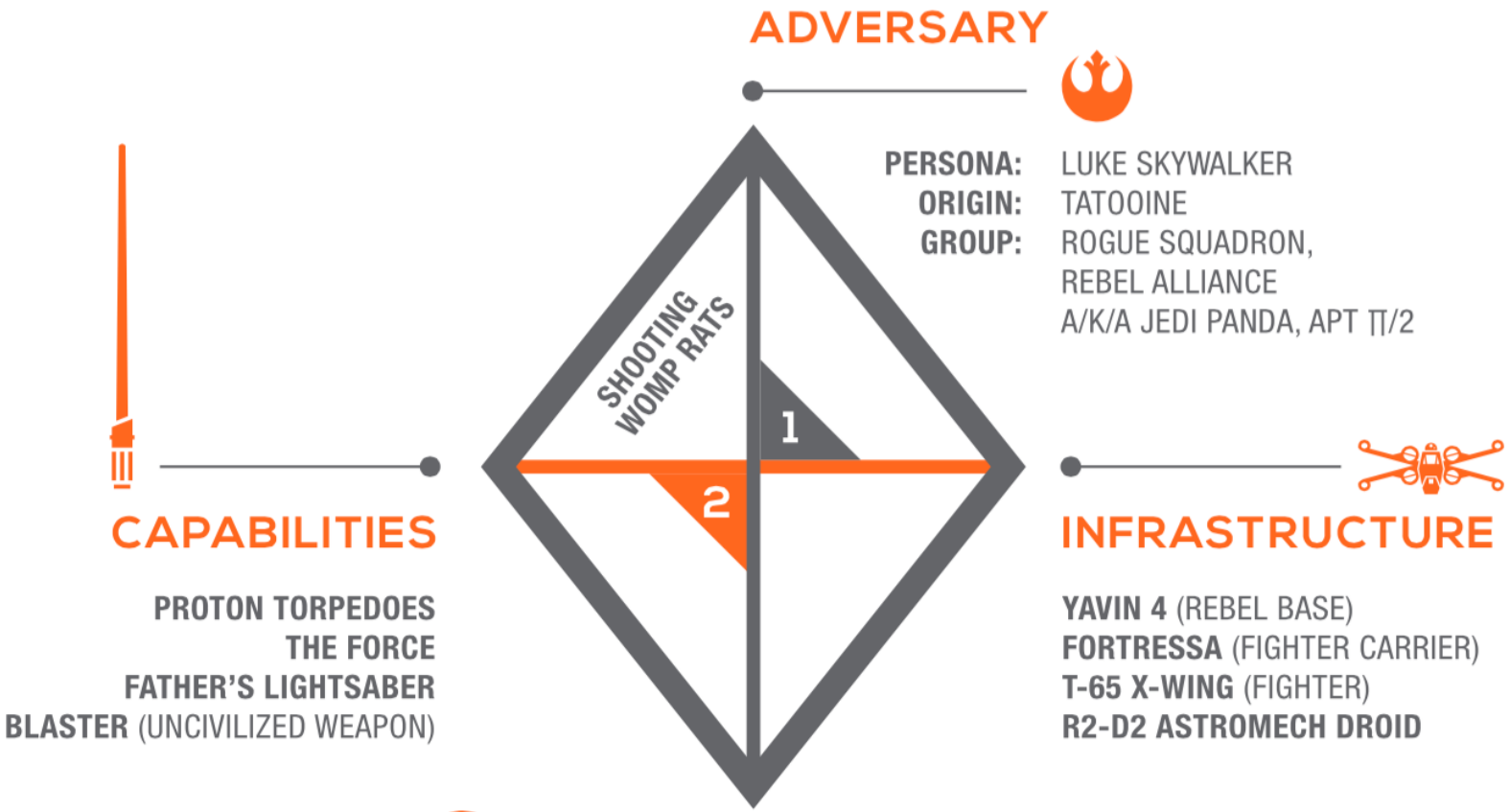
2 TECHNICAL AXIS

- CVE-2012-015
- Spear Phishing
- Right-to-Left Character Override
- Self-Extracting Executables

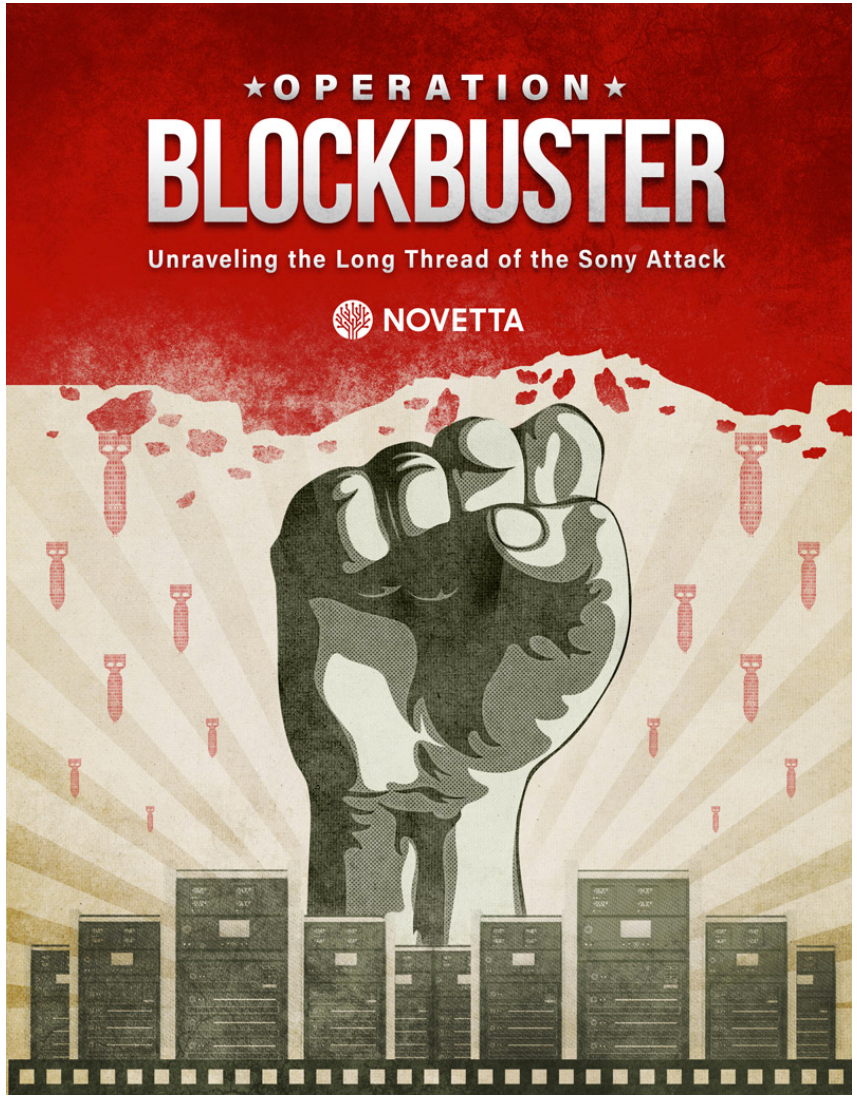
VICTIMS

- 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)



Threat Intelligence Reports



THE PURPOSE OF A HYPOTHESIS

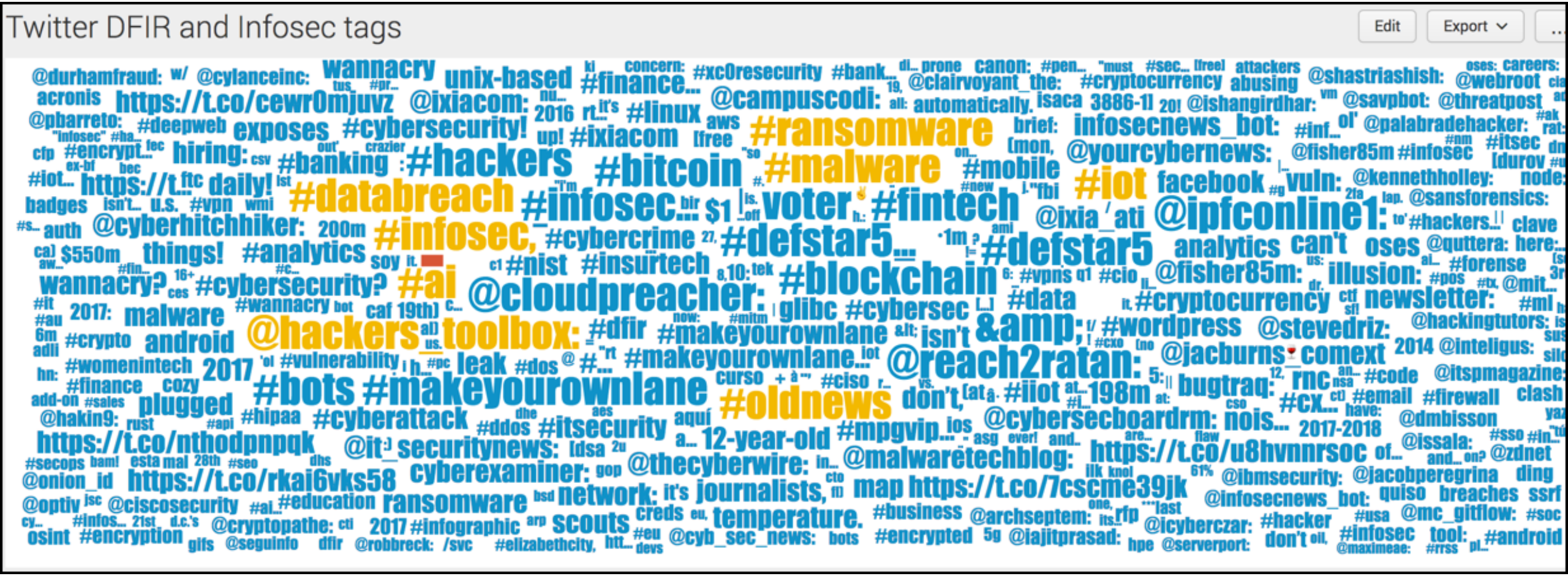
A hypothesis should always:

- 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…

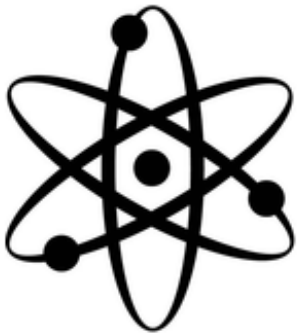
Obviously Word Clouds



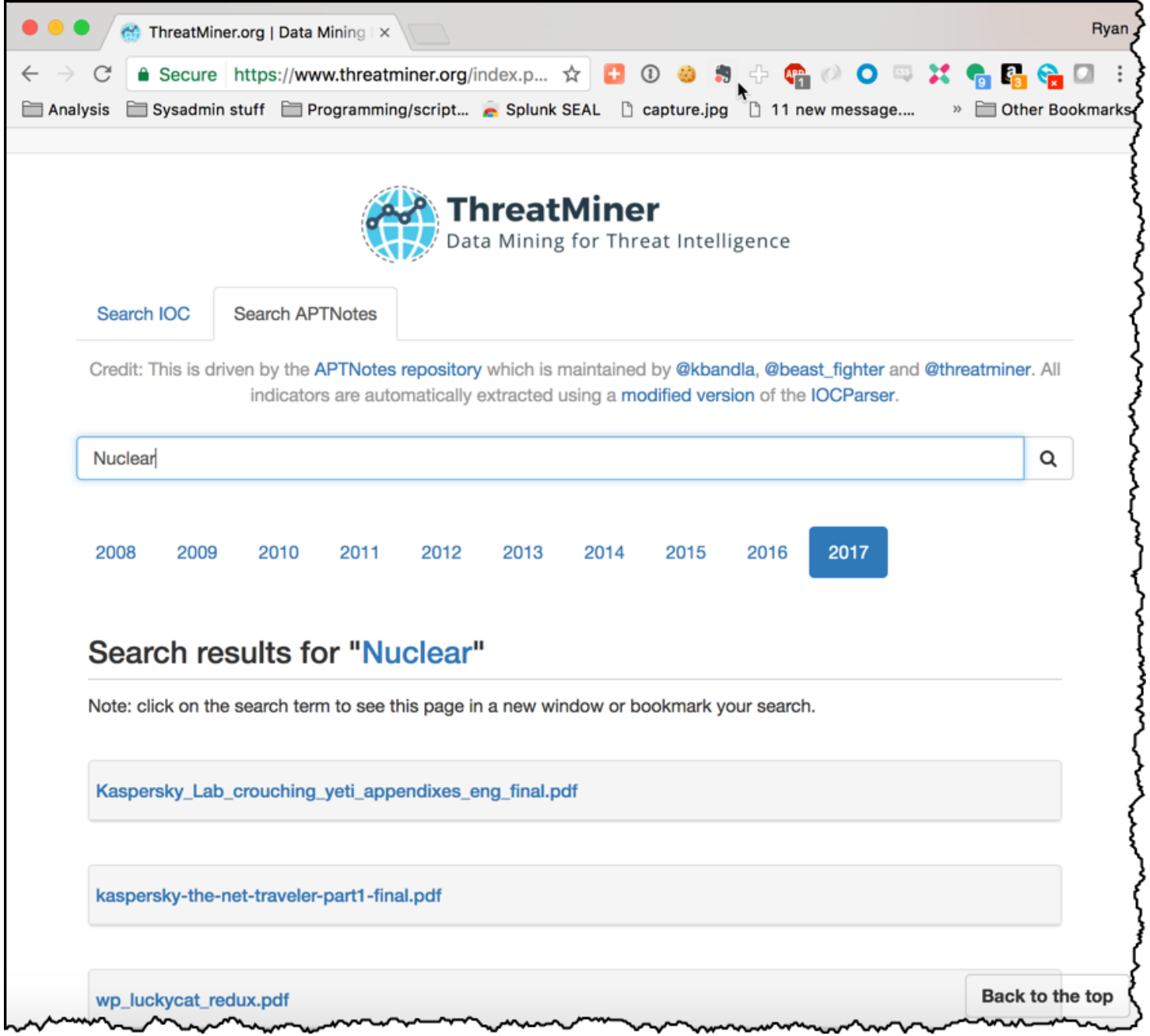
splunk> listen to your data®

HYPOTHESIS MONDAY.

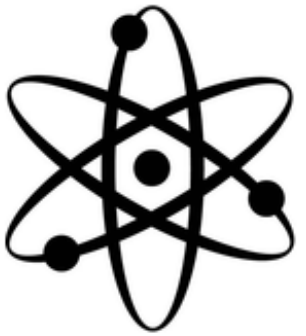
“I believe that there are TTPs from APT reports that maybe found in our own data”



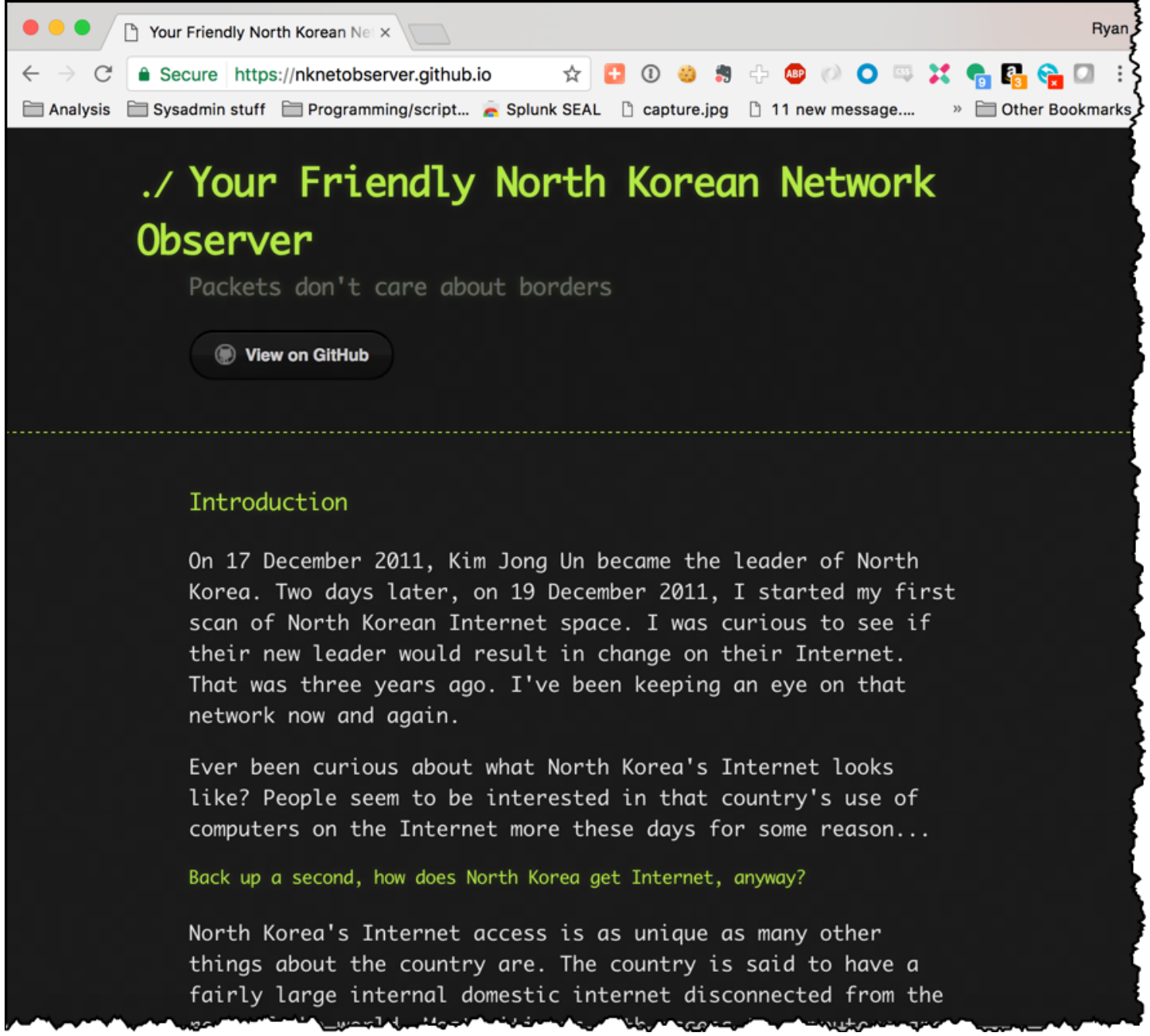
KEEP
CALM
AND
TEST YOUR
HYPOTHESIS



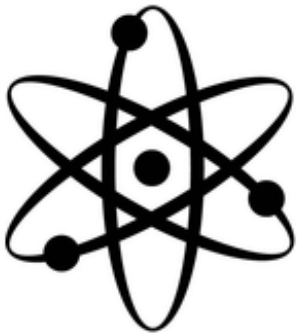
“North Korea has been researching and attacking critical infrastructure. I believe that they are coming from their IP address space and attacking US Orgs”



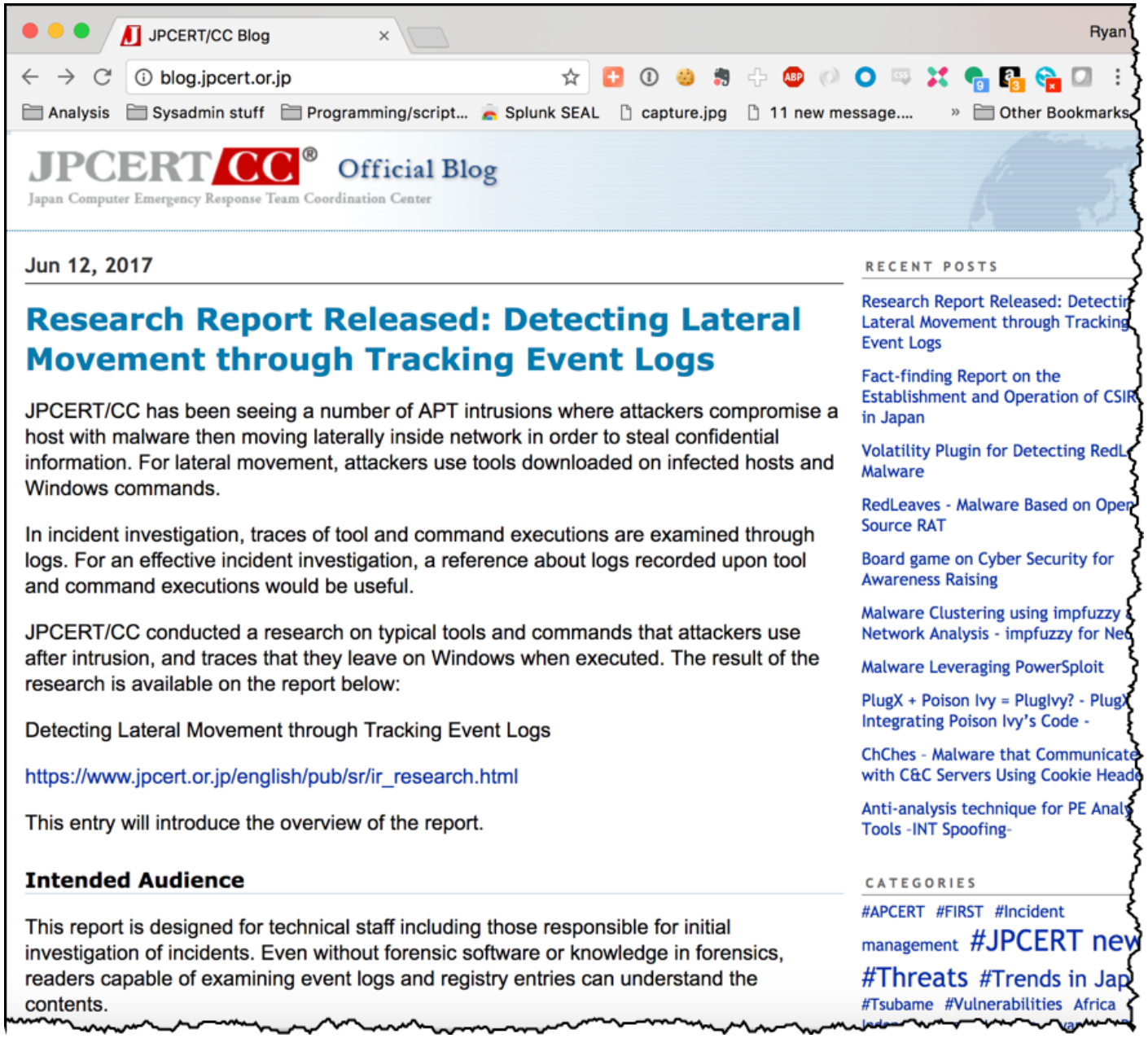
KEEP CALM AND TEST YOUR HYPOTHESIS



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



KEEP CALM AND TEST YOUR HYPOTHESIS



JPCERT/CC Blog

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

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: Detecti Lateral Movement through Tracking Event Logs

Fact-finding Report on the Establishment and Operation of CSIR in Japan

Volatility Plugin for Detecting RedL Malware

RedLeaves - Malware Based on Oper Source RAT

Board game on Cyber Security for Awareness Raising

Malware Clustering using impfuzzy Network Analysis - impfuzzy for Ne

Malware Leveraging PowerSploit

PlugX + Poison Ivy = PlugIvy? - Plug Integrating Poison Ivy's Code -

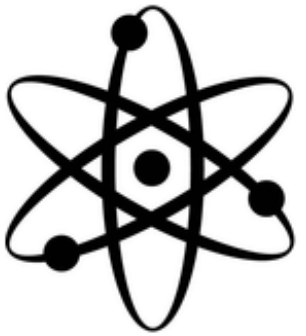
ChChes - Malware that Communicate with C&C Servers Using Cookie Head

Anti-analysis technique for PE Anal Tools -INT Spoofing-

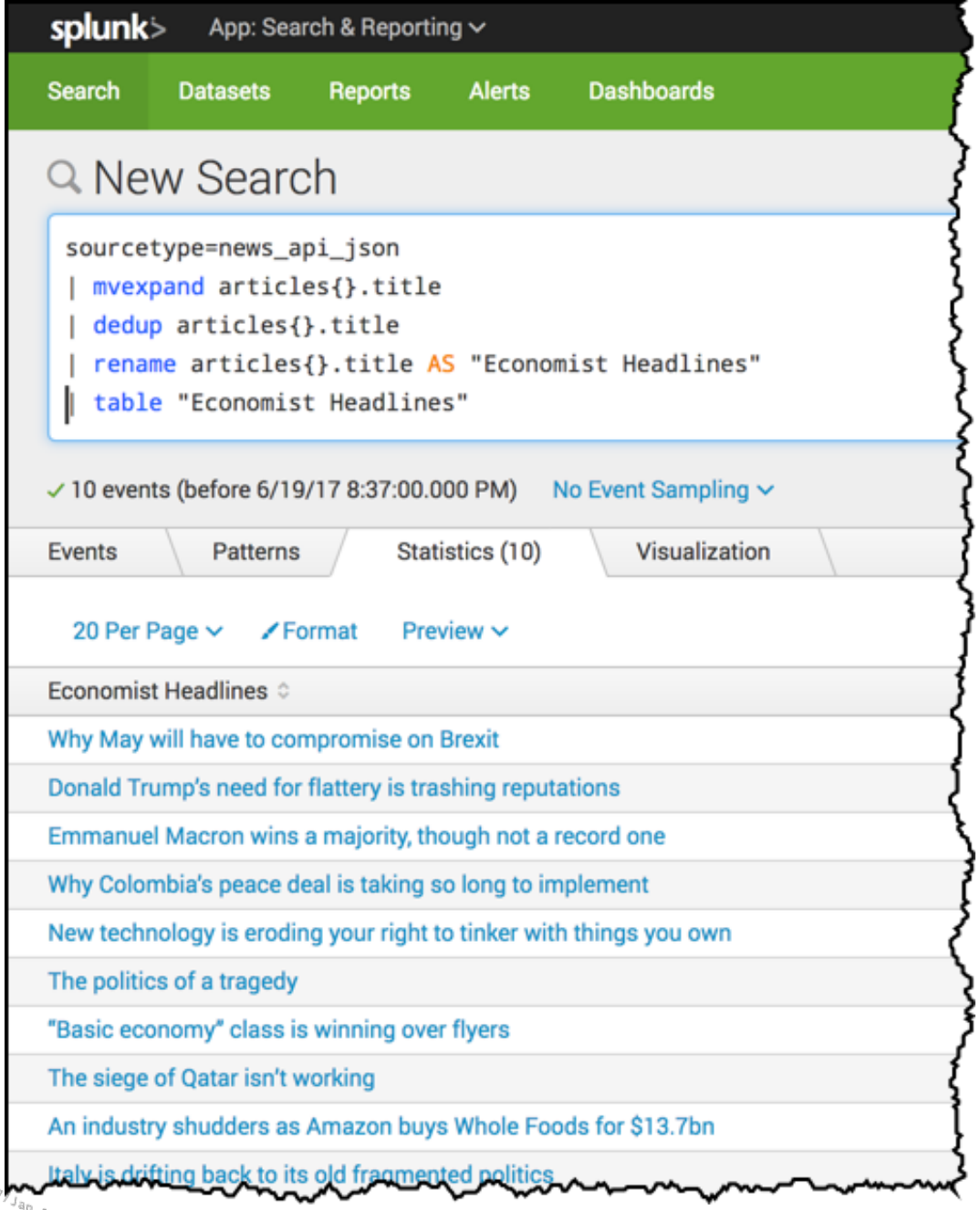
CATEGORIES

#APCERT #FIRST #Incident management #JPCERT new #Threats #Trends in Jap #Tsubame #Vulnerabilities Africa

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



KEEP
CALM
AND
TEST YOUR
HYPOTHESIS



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 | Smart Mode

Events | Patterns | Statistics (46) | Visualization

20 Per Page | Format | Preview

< Prev 1 2 3 Next >

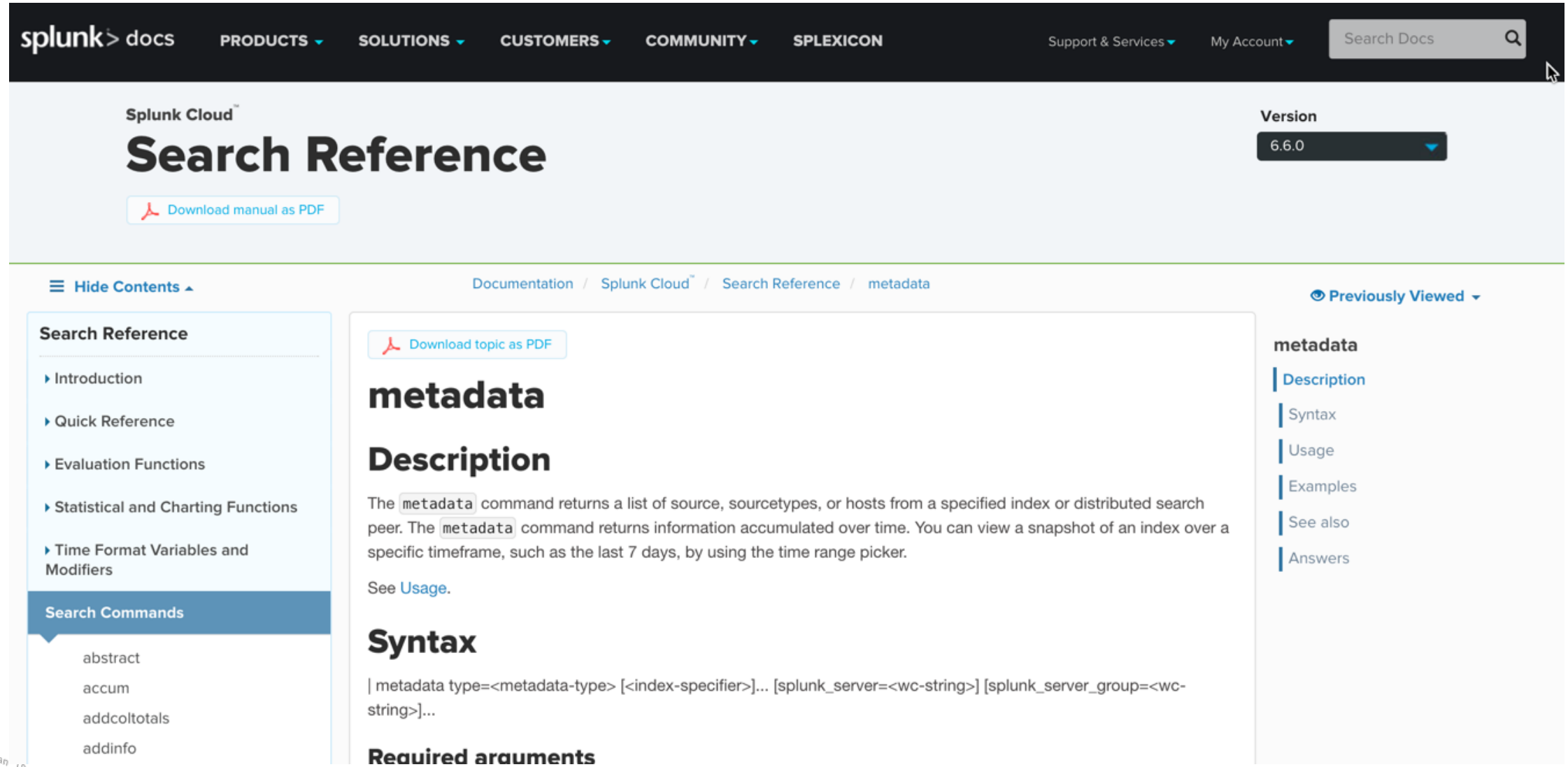
news	count
$13.7bn	1
2016	1
awfully	1
bash	1
battles	1
brexit	2
britain's	1
chaotic	1
colombia's	1
displaced	1
drifting	1
economy"	1
emmanuel	1

Now doing things

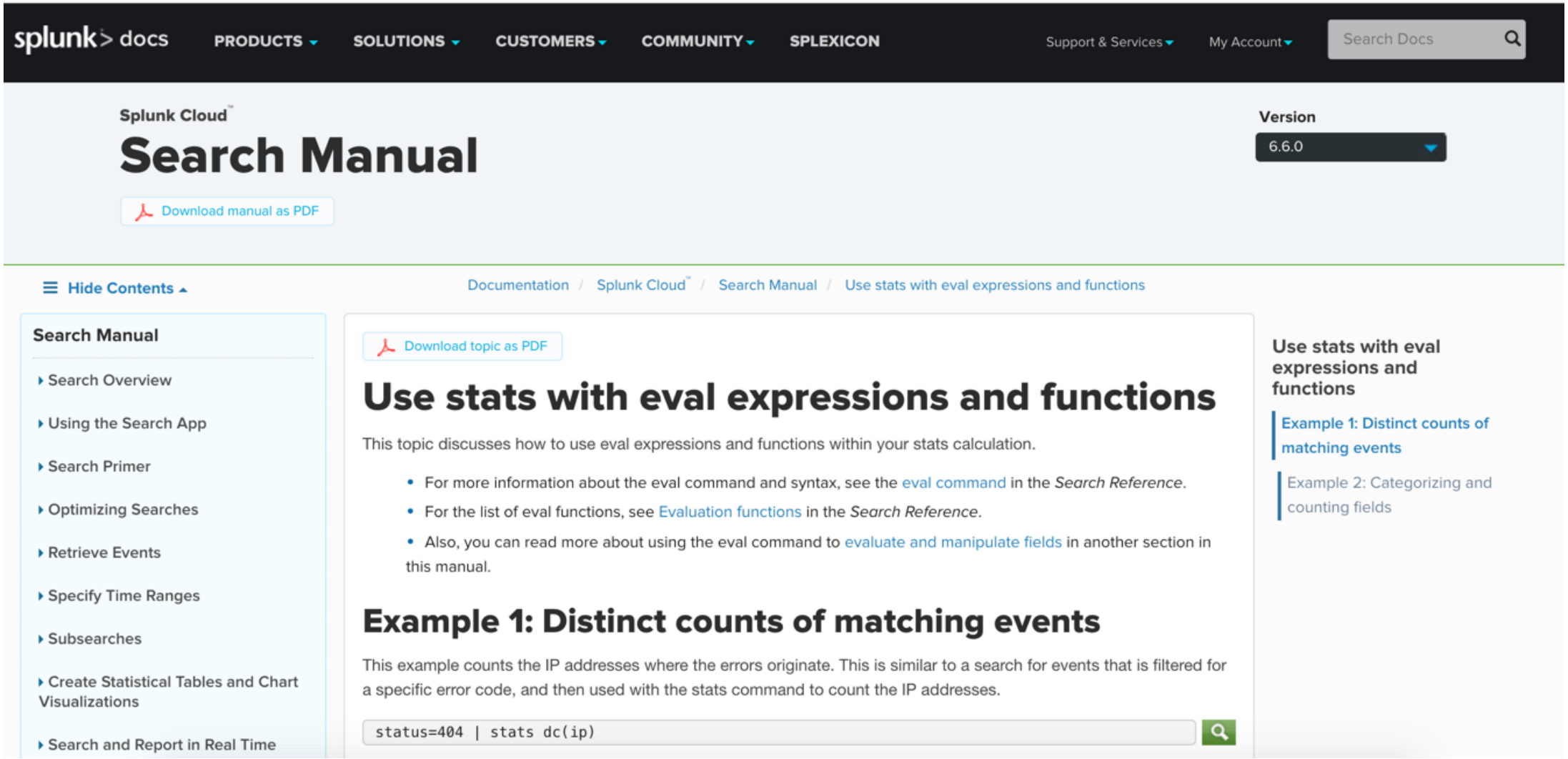
Lets have a little hands on with Dave

splunk> listen to your data

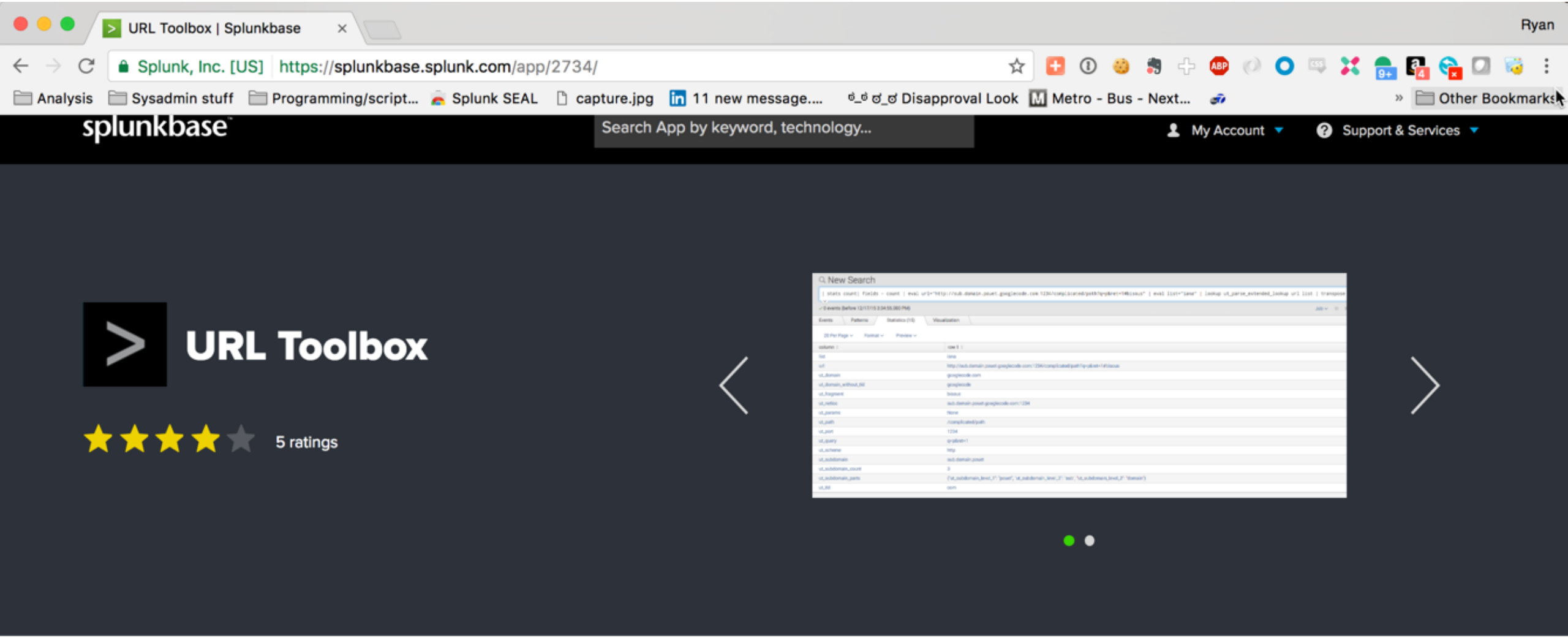
Figuring out what data you have



Filtering your data with eval and stats



Parsing the webz



Overview Details

711 Installs

2,890 Downloads

Pivoting tastes goooooooood

Type	Site	IOCs	Description
IP/Domain/ Shared Domains on IP Address	www.Robtex.com	IPs, Domains	One of the best of breed tools to investigate Domains, IP addresses, and more.
IP/Domain nformation	centralops.net	IPs, Domains	Investigate Domains and IP addresses
Geolocate IPs/Domains	iplocation.net	IPs, Domains	Quick way to find the most up-to-dat location of a IP from several differen vendors
Geolocate Ps/Domains	Infosniper.net	IPs, Domains	Shows location and provides a nice map
PassiveDNS, SSL Certificates, Shared Domains on	www.passivetotal.org	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

WAYNE

ENTERPRISES

Incident #1

- Website defacement
- Po1s0n1vy APT

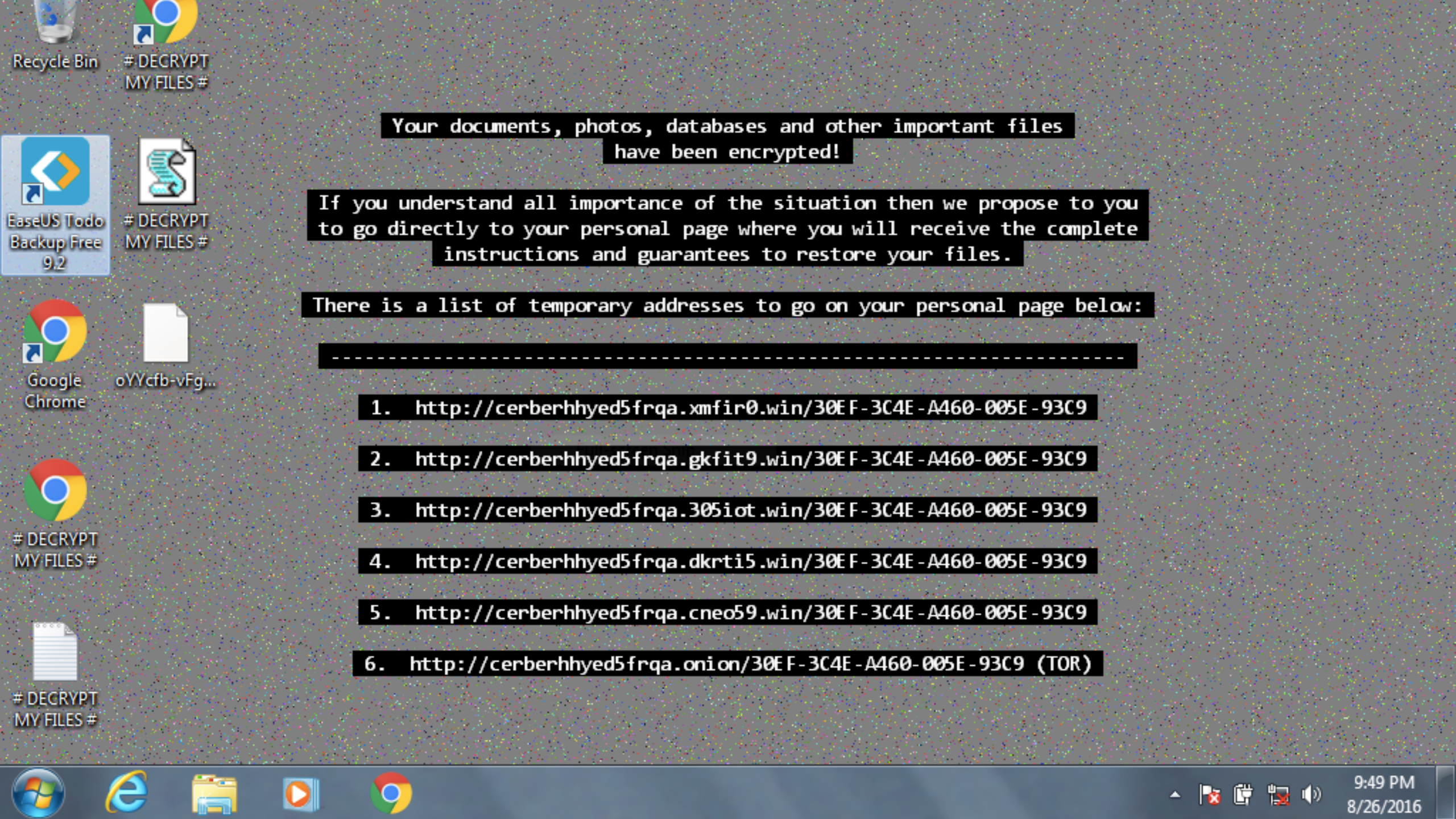
YOUR SITE HAS BEEN DEFACED

P01s0n1vy was HERE

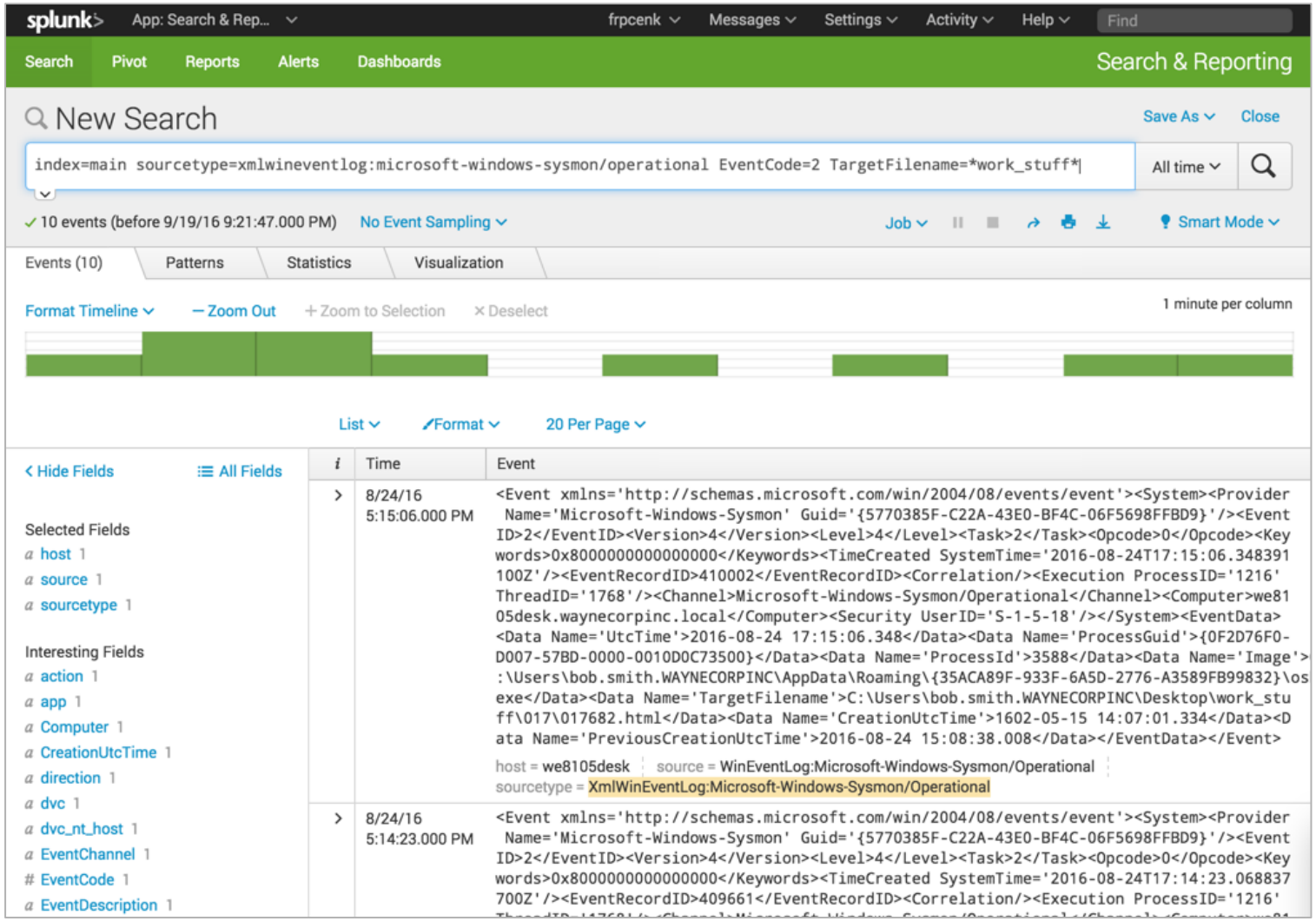
Deal with it, Admin

Incident #2

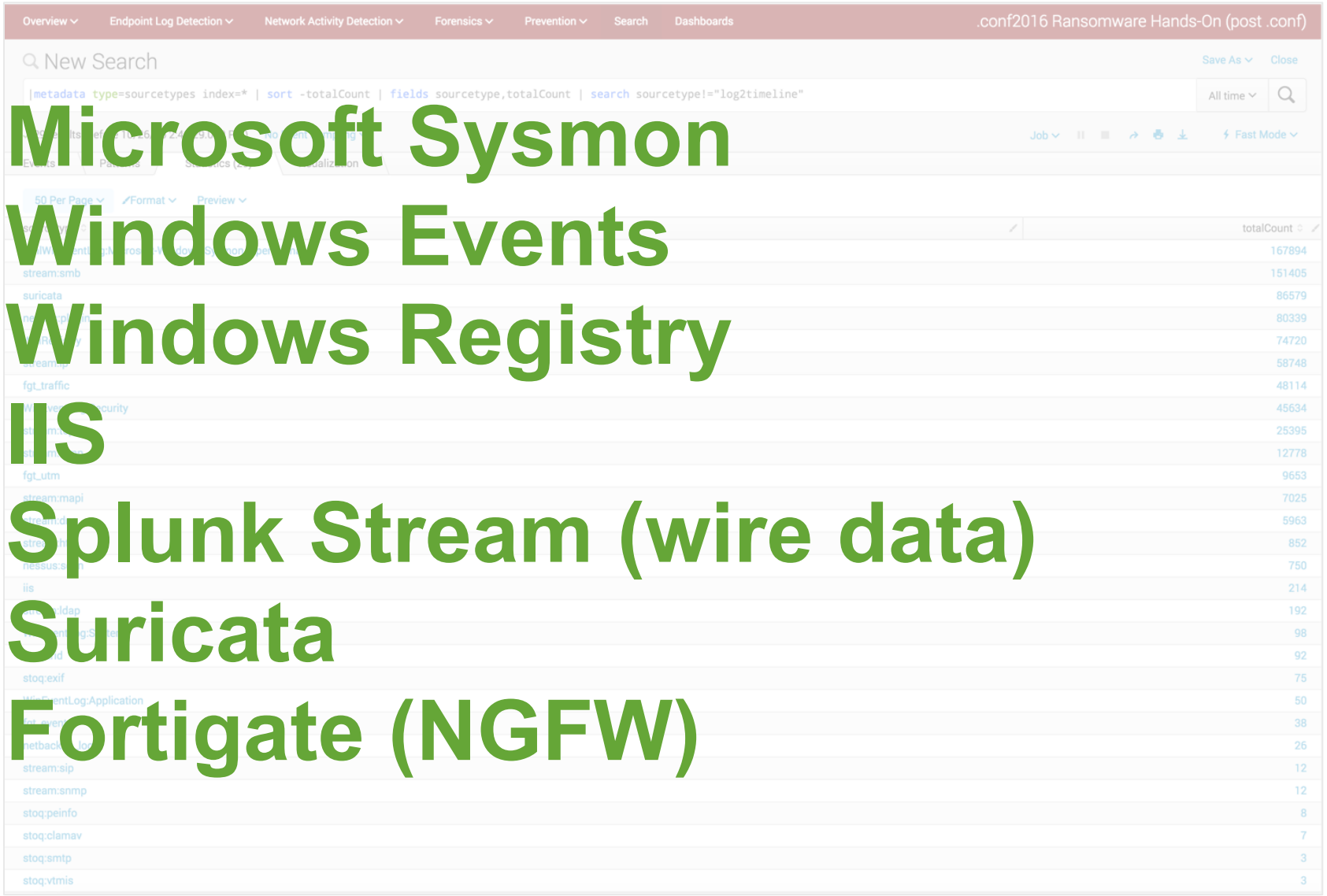
- Ransomware


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://cerberhhyed5frqa.xmfir0.win/30EF-3C4E-A460-005E-93C9
2. http://cerberhhyed5frqa.gkfit9.win/30EF-3C4E-A460-005E-93C9
3. http://cerberhhyed5frqa.305iot.win/30EF-3C4E-A460-005E-93C9
4. http://cerberhhyed5frqa.dkrti5.win/30EF-3C4E-A460-005E-93C9
5. http://cerberhhyed5frqa.cneo59.win/30EF-3C4E-A460-005E-93C9
6. http://cerberhhyed5frqa.onion/30EF-3C4E-A460-005E-93C9 (TOR)
9:49 PM
8/26/2016

Luckily Everything Is Captured In Splunk



Yes, Pretty Much Everything

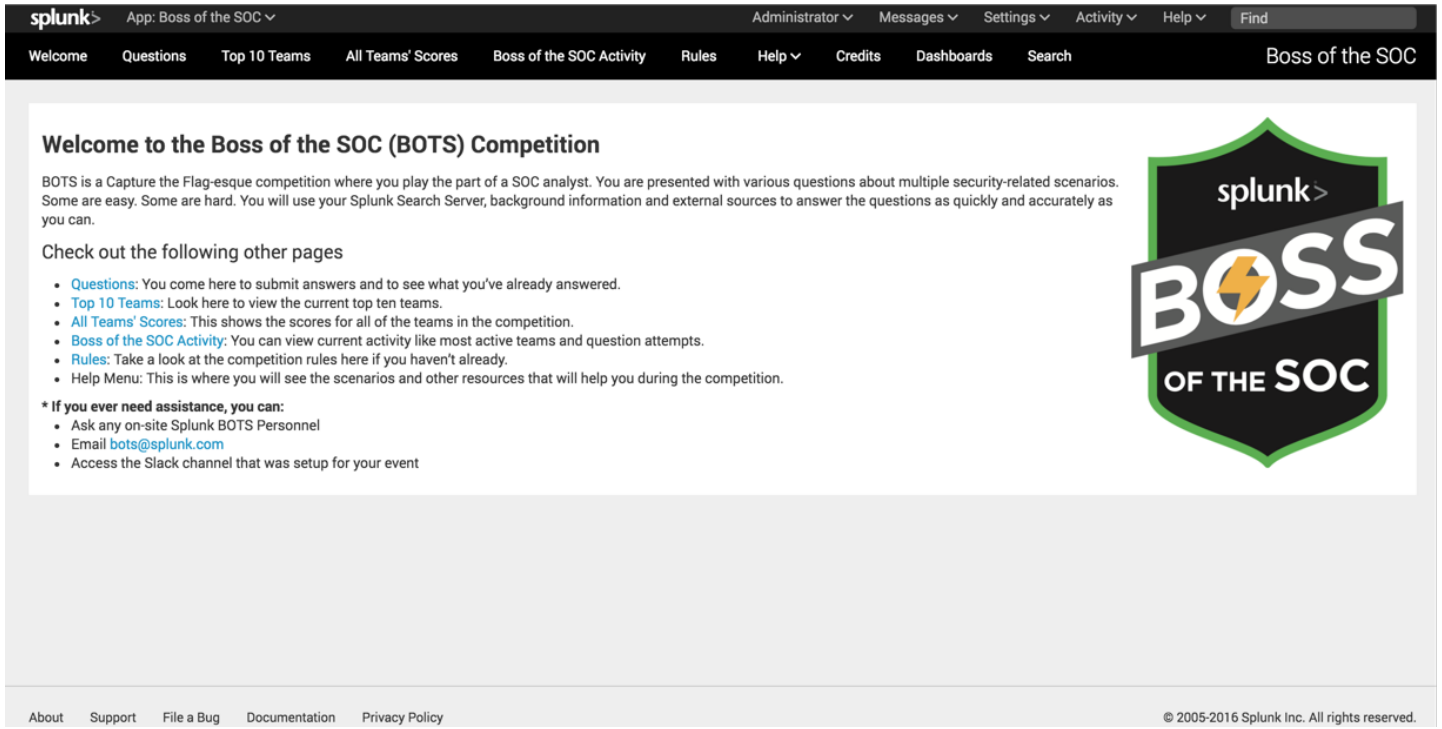


Microsoft Sysmon
Windows Events
Windows Registry
IIS
Splunk Stream (wire data)
Suricata
Fortigate (NGFW)

splunk> listen to your data®

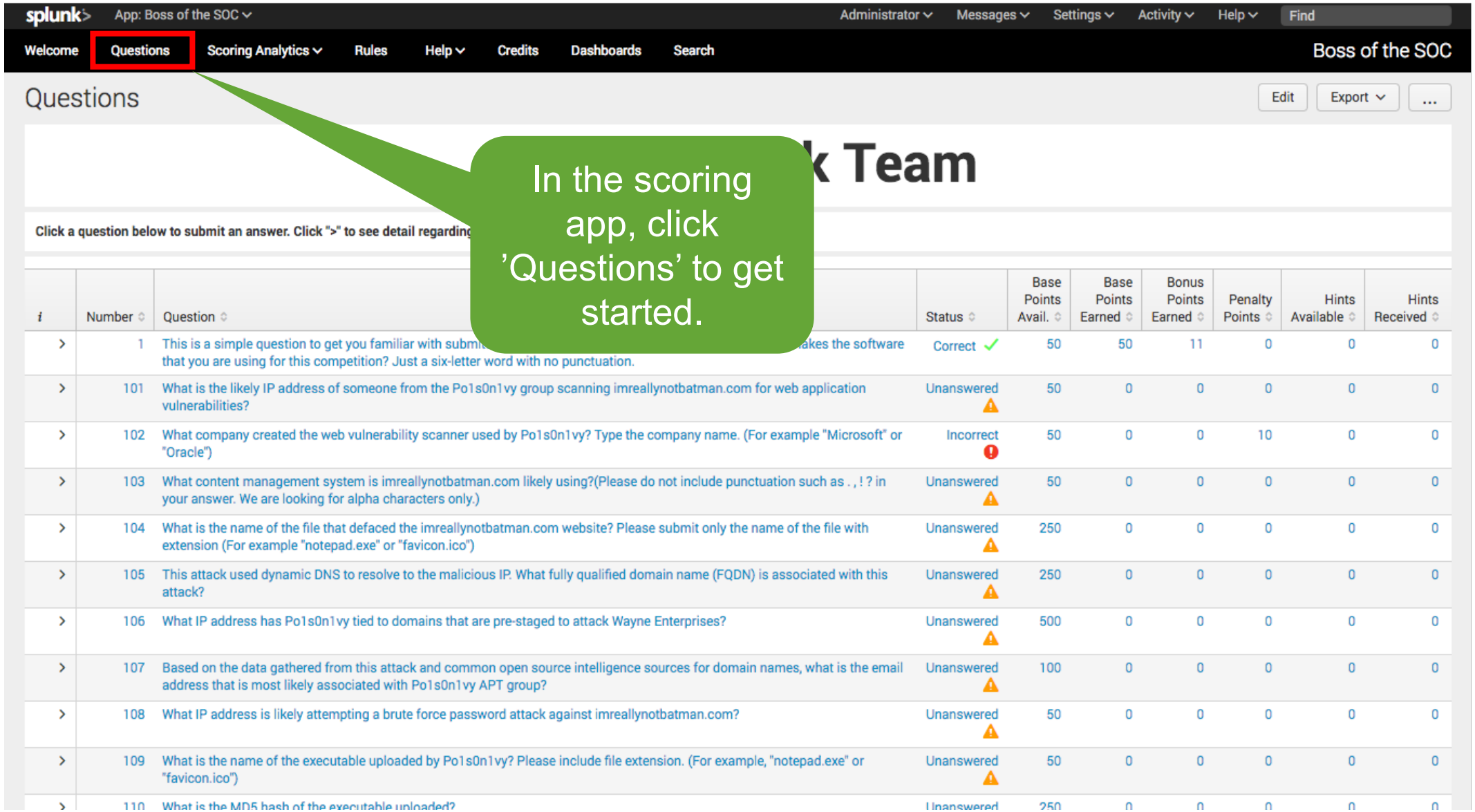
Two Different Splunk Servers

1. BOTS Scoring Server



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

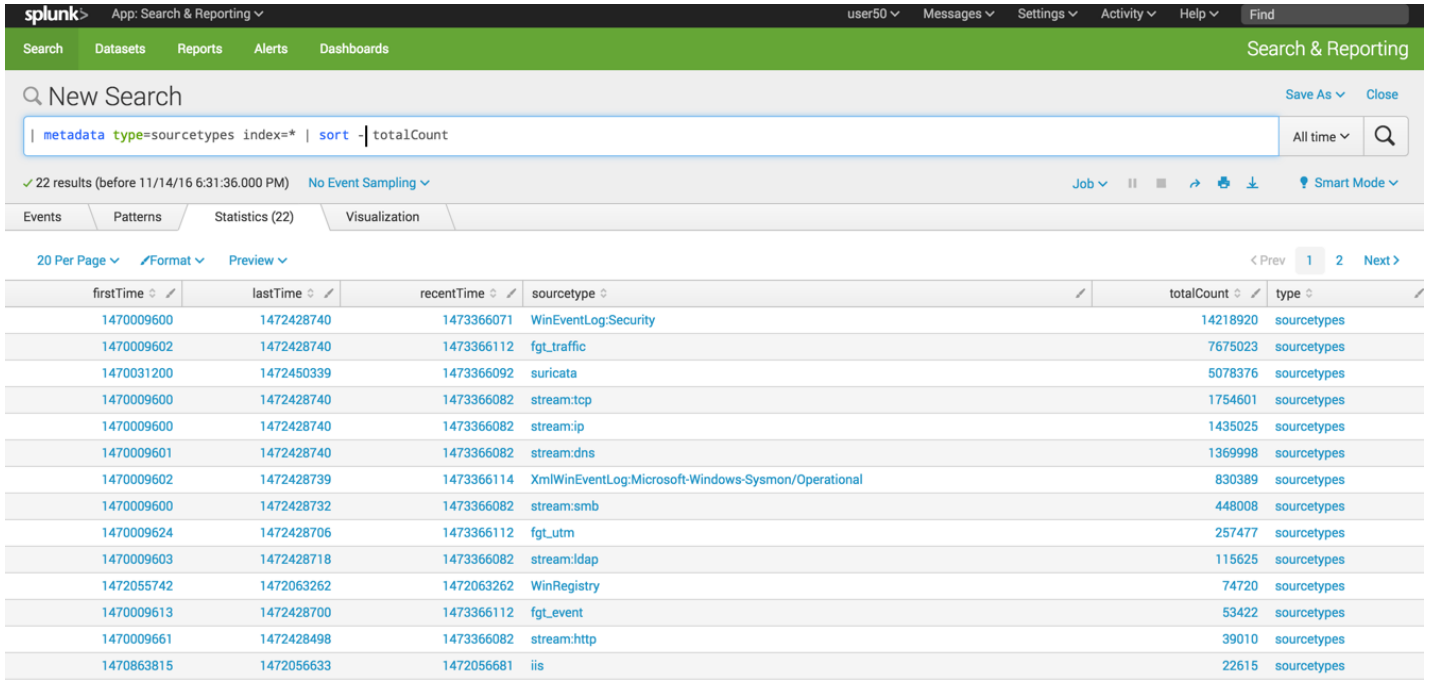
Questions



i	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 submi… akes 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	0	0	0	0	0

Two Different Splunk Servers

2. BOTS Search Server



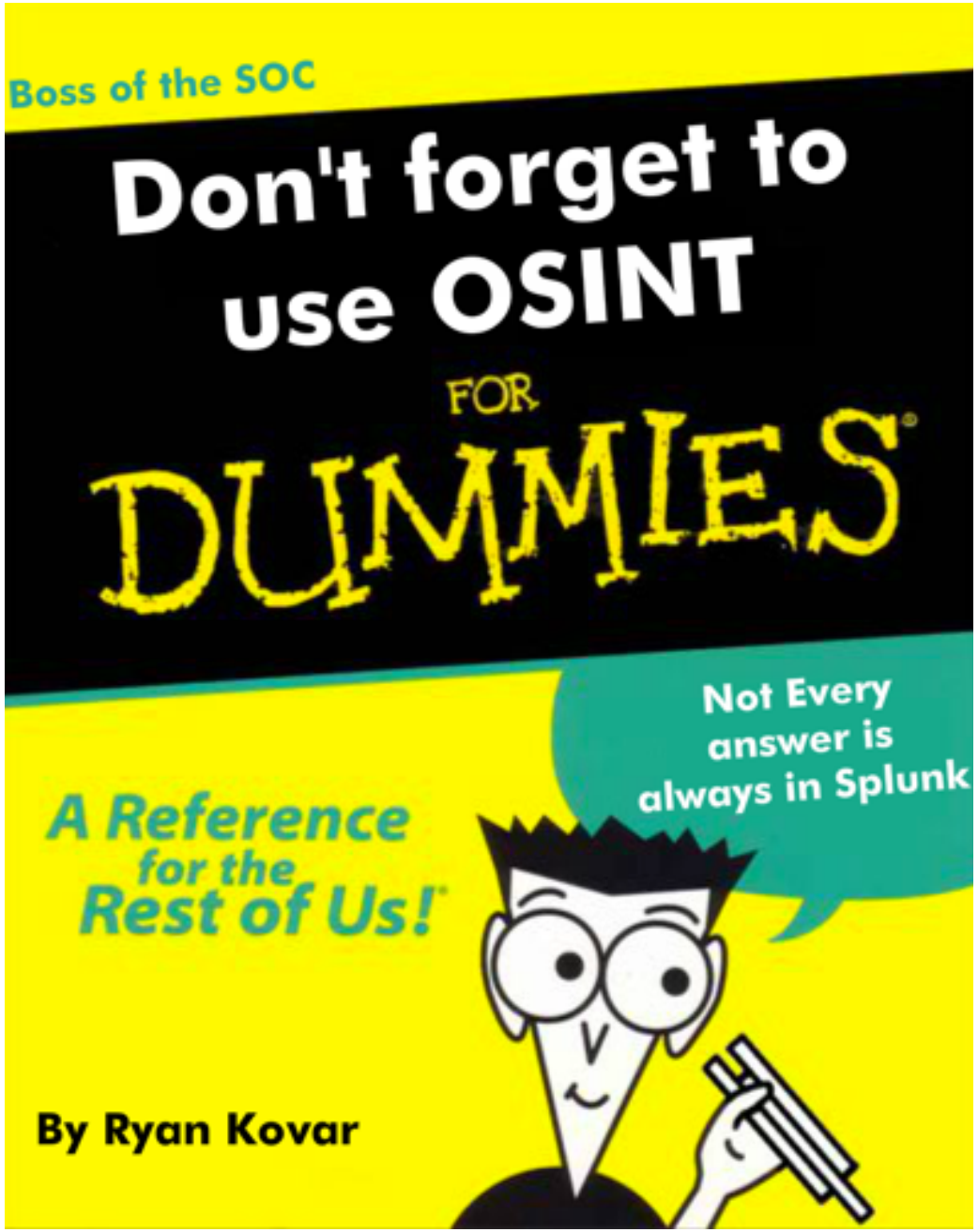
firstTime	lastTime	recentTime	sourcetype	totalCount	type
1470009600	1472428740	1473366071	WinEventLog:Security	14218920	sourcetypes
1470009602	1472428740	1473366112	fgt_traffic	7675023	sourcetypes
1470031200	1472450339	1473366092	suricata	5078376	sourcetypes
1470009600	1472428740	1473366082	stream:tcp	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:ldap	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

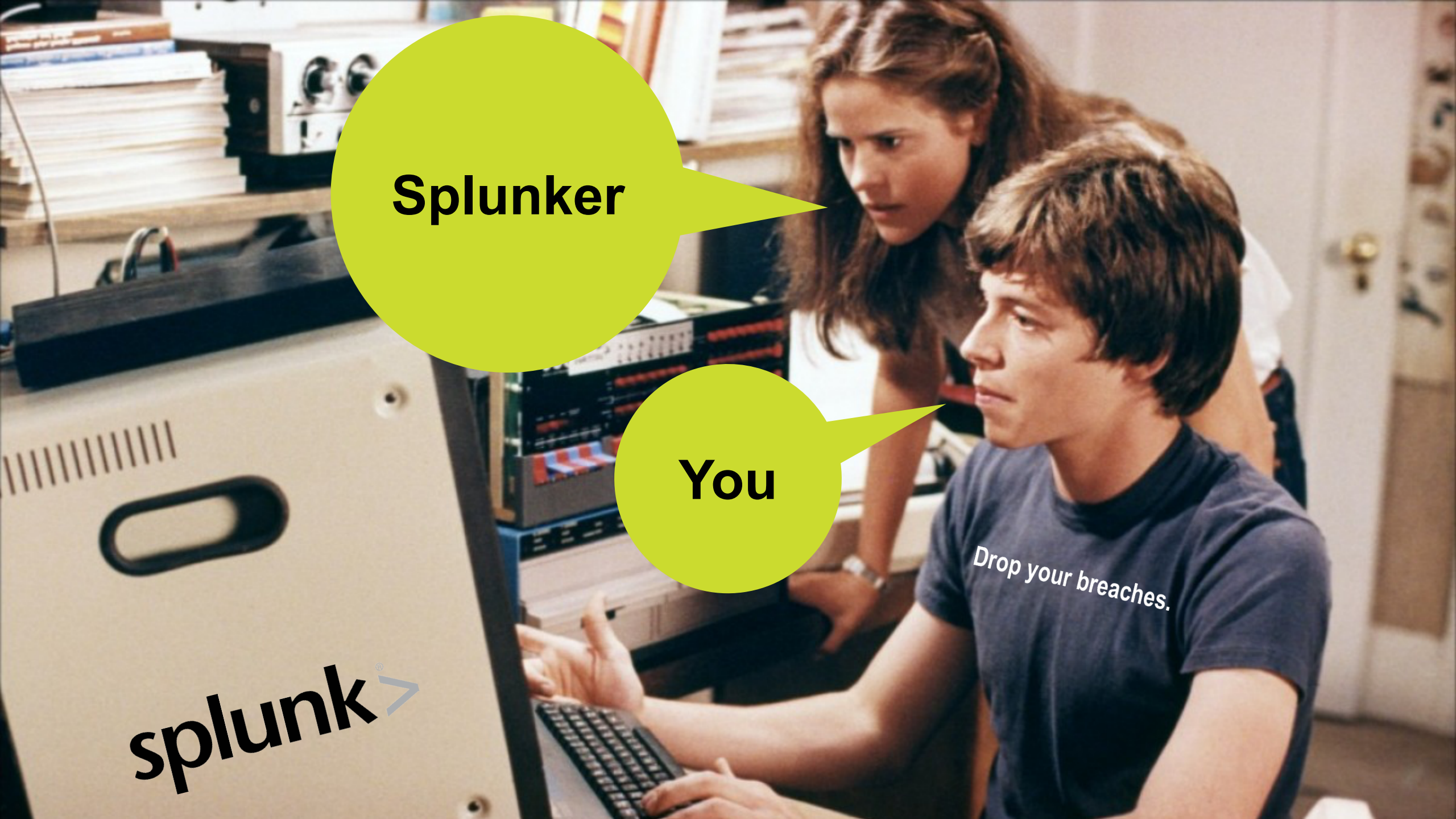
- Just search!
- Core Splunk only
  - ☺ url toolbox
- index=main
- Shouldn't need wildcards


KISS
splunk>

Just one more thing...

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




Splunker
You
Drop your breaches.
splunk>