The “Hidden Empires” of Malware

SANS Cyber Threat Intelligence Summit
28-29FEB18

The “Hidden Empires” of Malware

Now with Blockchain!

SANS Cyber Threat Intelligence Summit 28-29FEB18

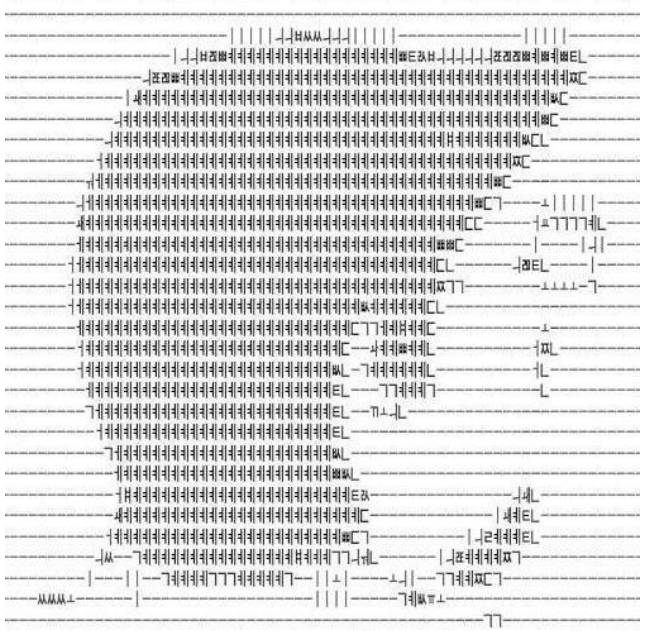
AI!

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a høliday in Sweden this yër? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON Including the majestik møøse A Møøse once bit my Marcus... No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møvies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Mølars of Horst Nordfink"... In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.

whoami > Ryan Kovar

CISSP, MSc(Dist)



Staff Security Strategist

Minster of the OODAloopers

@meansec

- 17 years of cyber security experience
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Also investigating why printers are so insubordinate ʘ_ʘ

whoami > Dave Herrald

CISSP, GIAC G*, GSE #79

Security Architect @splunk

@daveherrald

- 20+ years IT and security
- Information security officer, security architect, pen tester, consultant, SE, system/network engineer
- Former SANS Mentor
- Co-creator of Splunk Boss of the SOC

Agenda

- Answering some **W**'s
  - **W**hy are we doing this talk?
  - **W**hat are we talking about with "Hunting Empires"?
  - **W**hat are SSL certificates and why do I care?
  - **W**hat can I do with them?
- Talk about the "**H**"
  - **H**ow can I get this data myself?
  - **H**ow does ~~Blockchain~~ ~~Automated Intelligence~~ Machine Learning "fit" in?
- And now another **W**
  - **W**here can I get this awesome stuff!

If you don't know what SSL Pivoting and Hunting is…

… Sit Down

If your org can't capture SSL certificates at scale…

… Sit Down

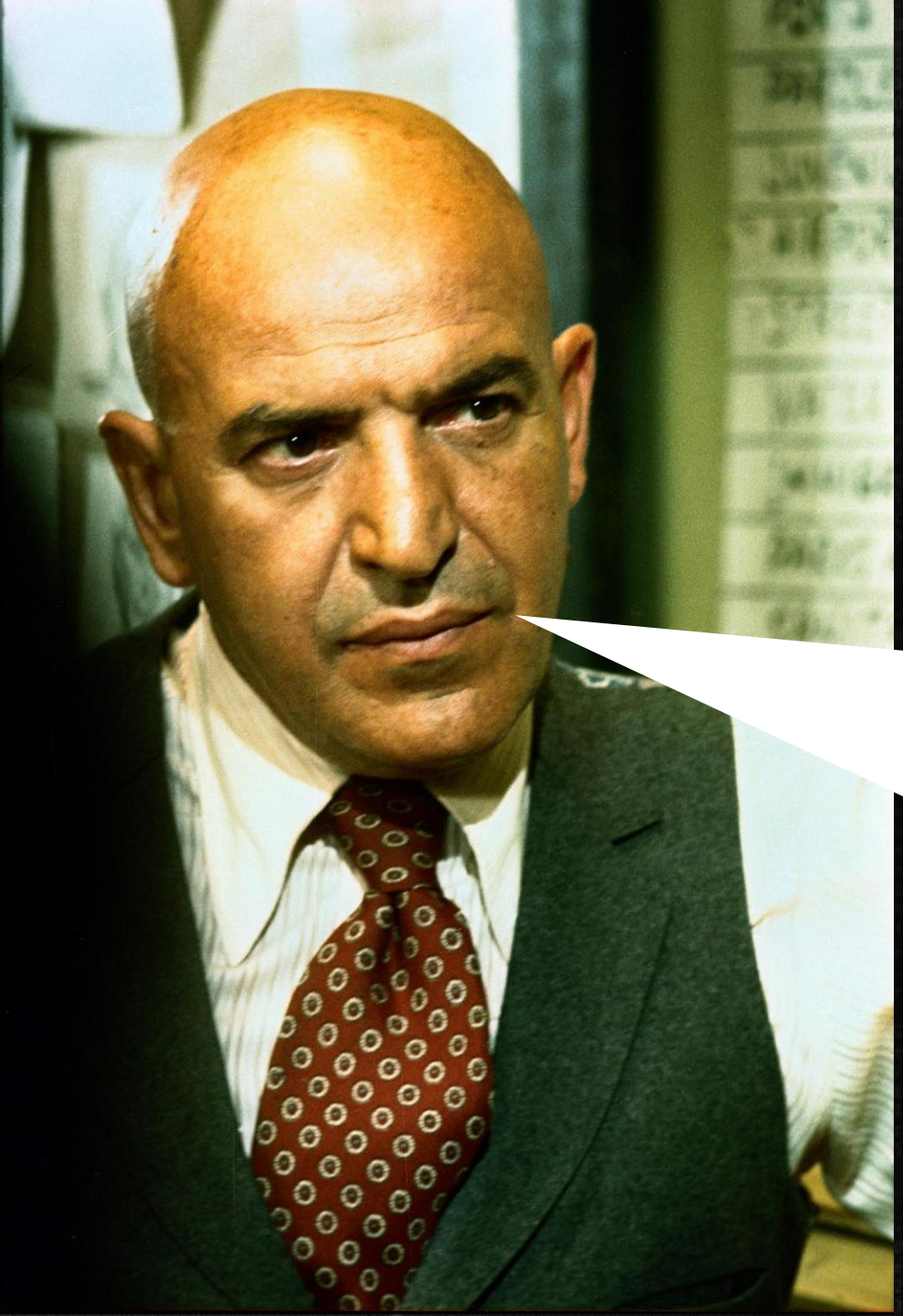
If you've never applied machine learning to SSL certificates

… Sit Down

Look around…

… Sit Down

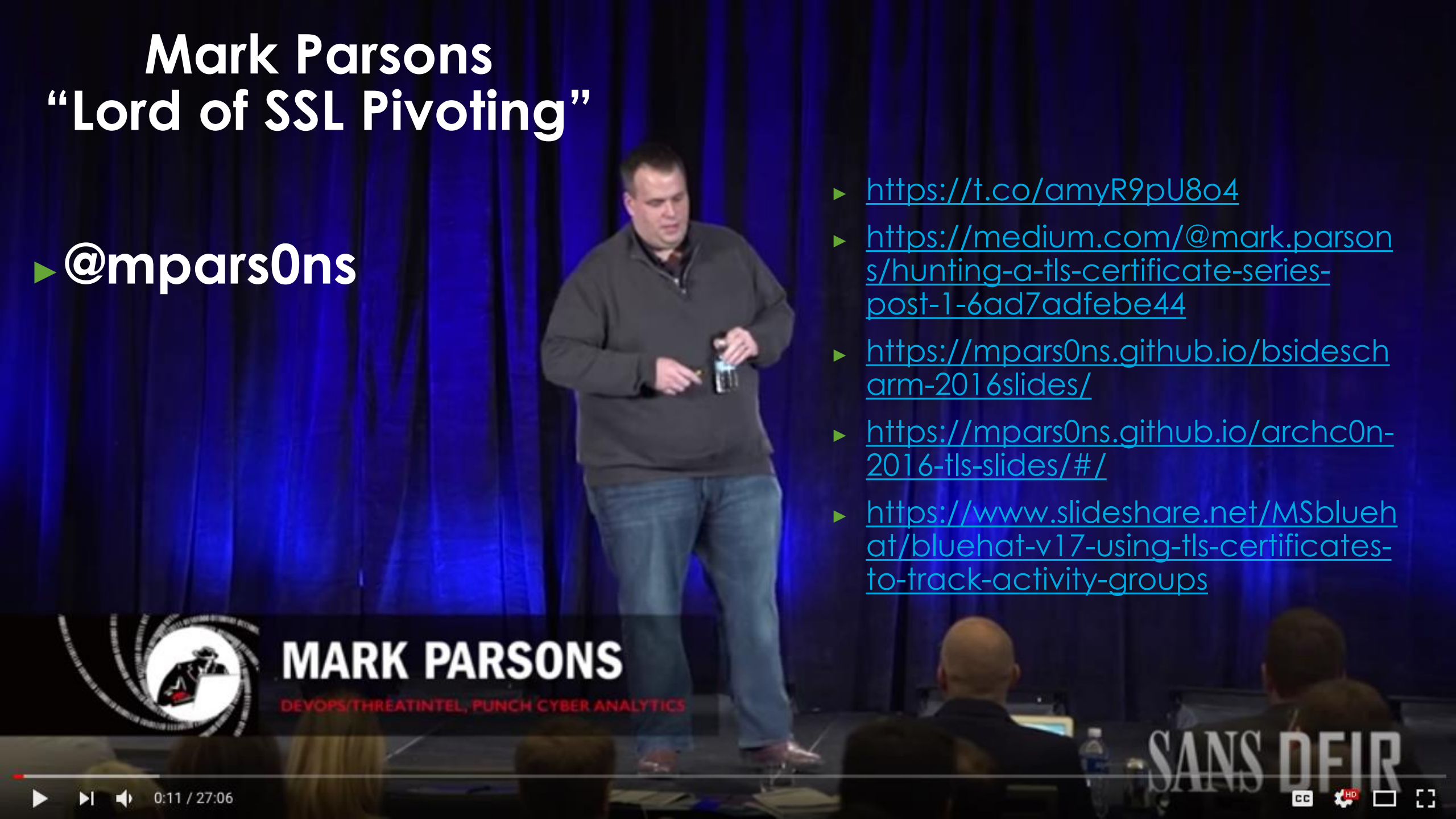

I have approximate knowledge of many things.



What are SSL certificates and why do I care?

Mark Parsons
"Lord of SSL Pivoting"

- @mpars0ns



- https://t.co/amyR9pU8o4
- https://medium.com/@mark.parsons/hunting-a-tls-certificate-series-post-1-6ad7adfebe44
- https://mpars0ns.github.io/bsidescharm-2016slides/
- https://mpars0ns.github.io/archc0n-2016-tls-slides/#/
- https://www.slideshare.net/MSbluehat/bluehat-v17-using-tls-certificates-to-track-activity-groups

FOR578: Cyber Threat Intelligence

- Contents | Additional Info
- **Delivery Methods:** Live | Online
- GCTI Certification
- Affiliate Pricing
- 30 CPEs
- Laptop Required

THERE IS NO TEACHER BUT THE ENEMY!

Every security practitioner should attend the FOR578: Cyber Threat Intelligence course . This course is unlike any other technical training you have experienced. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat

FOR578: Cyber Threat Intelligence course

Get Registered

Free Course Demo

Course List

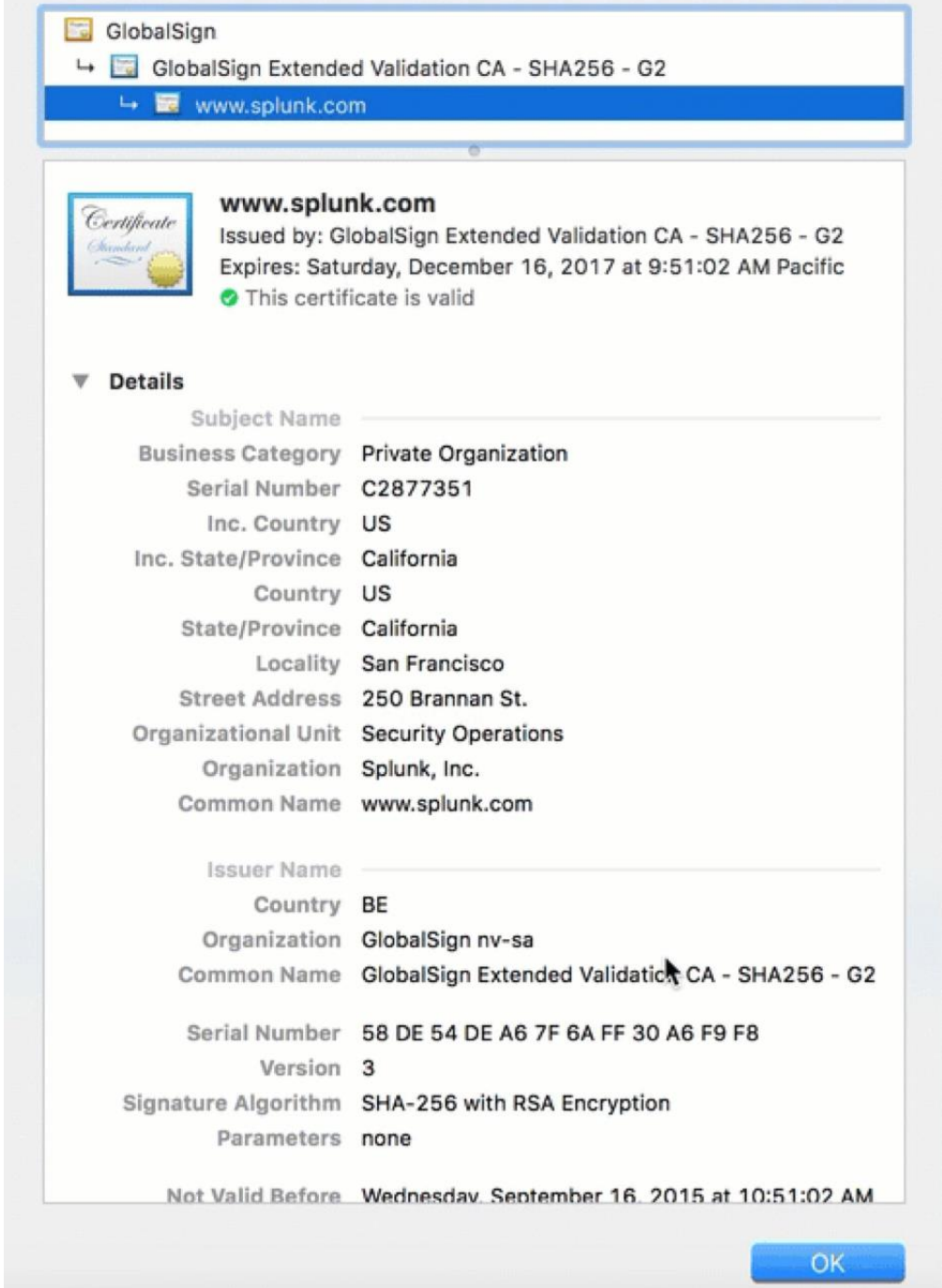
Curricula

Share

Sooo… SSL Certificates?

[SSL certificates are] Small [unencrypted] data files that digitally bind a cryptographic key to an organization's details." [1]

[1] https://www.godaddy.com/help/what-is-an-ssl-certificate-542




So that shows SSL certificates?

censys

About Search Reports API Raw Data

77437e1ca6d924e2bf090aed1f121b652bbbba53656b9da88099e02682fe17aa

Search

C=US, ST=California, L=San Francisco, O=Splunk, Inc., CN=splunk.com

Certificate | Trust Paths | CT | ZLint 1 | Raw Data | Explore

Basic Data

Subject C=US, ST=California, L=San Francisco, O=Splunk, Inc., CN=splunk.com

Issuer C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

Serial 71757581524838284869335420926754302 67

Validity 2017-12-12 00:00:00 **to** 2019-12-17 12:00:00 (735 days, 12:00:00)

Names alias.splunk.com, banner.splunk.com, base.splunk.com, blogs.splunk.com, carabiner.splunk.com, communities.splunk.com, community.splunk.com, company.splunk.com, conf.splunk.com, de-de.splunk.com, de.splunk.com, demo.splunk.com, dev.splunk.com, developers.splunk.com, docs.splunk.com, documentation.splunk.com, download.splunk.com, education.splunk.com, embargo.splunk.com, en-us.splunk.com, en.splunk.com, es-es.splunk.com, es.splunk.com, fr-fr.splunk.com, fr.splunk.com, it-it.splunk.com, it.splunk.com, ja-jp.splunk.com, ja.splunk.com, ko-kr.splunk.com, ko.splunk.com, legacyapi.splunk.com, login.splunk.com, partners.splunk.com, piton.splunk.com, preview.splunk.com, product.splunk.com, pt-pt.splunk.com, pt.splunk.com, quickdraw.splunk.com, ru-ru.splunk.com, ru.splunk.com, services.splunk.com, solutions.splunk.com, splunk.com, splunklive.com, store.splunk.com, support.splunk.com, usergroups.splunk.com, web.splunk.com, webmservices.splunk.com, wiki.splunk.com, www.splunk.com, www.splunklive.com, zh-cn.splunk.com, zh-hans.splunk.com, zh-hant.splunk.com, zh-hk.splunk.com, zh-mo.splunk.com, zh-my.splunk.com, zh-sg.splunk.com, zh-tw.splunk.com

Fingerprint

SHA-256 `77437e1ca6d924e2bf090aed1f121b652bbbba53656b9da88099e02682fe17aa`

Browser Trust

Apple	Browser Trusted
Microsoft	Browser Trusted
Mozilla NSS	Browser Trusted

Key Usage and Constraints

Is CA?	False
Key Usage	Digital Signature, Key Encipherment

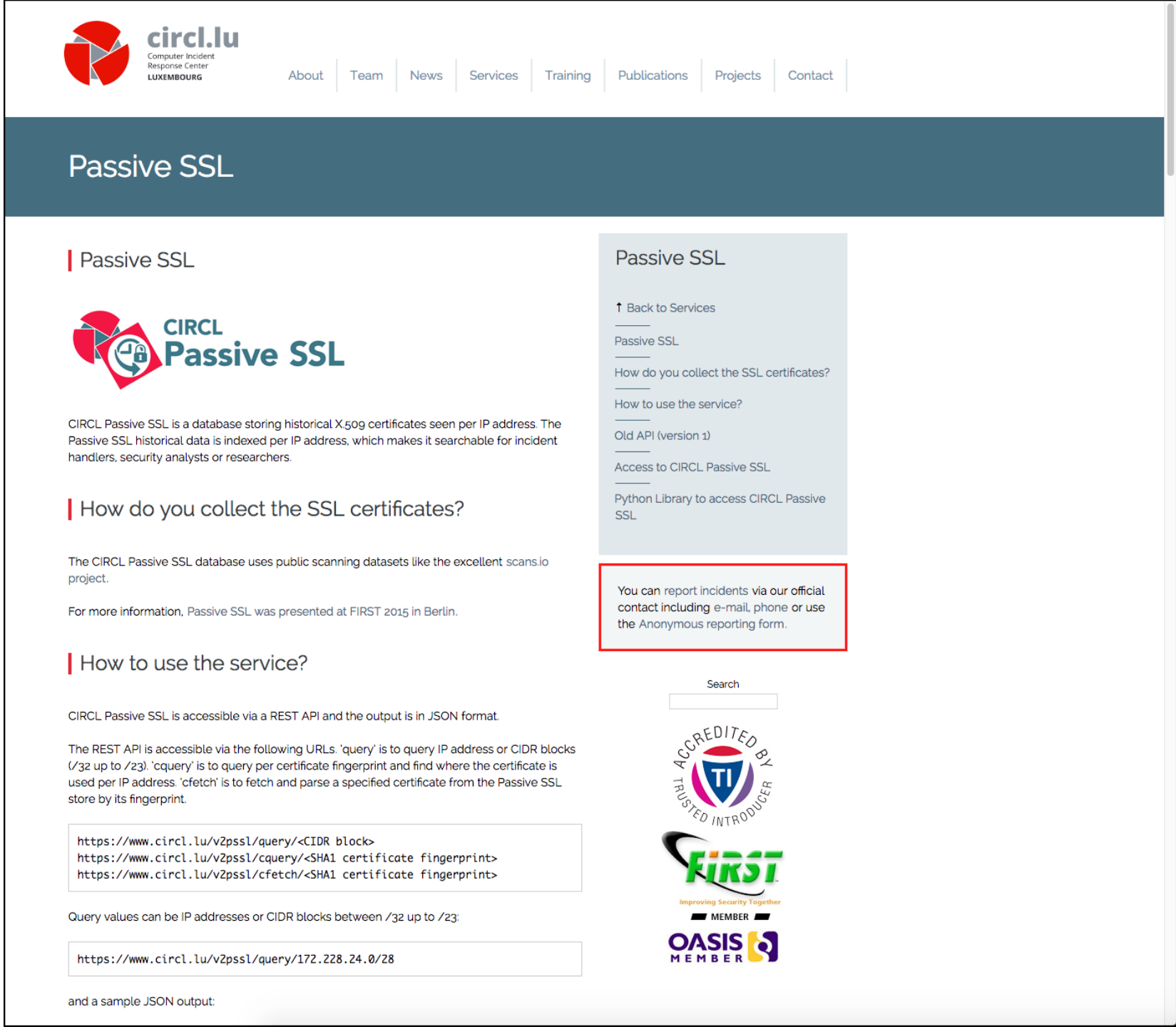
Certificate Transparency

Argon 2019	2017-12-18 06:38 664,374
G Pilot	2017-12-17 03:22 188,429,216
G Rocketeer	2017-12-16 22:17 182,486,898
G Submariner	2017-12-16 20:08 690,119

Censys Metadata

Censys.io

Circl.lu



circl.lu
Computer Incident Response Center LUXEMBOURG

About | Team | News | Services | Training | Publications | Projects | Contact

Passive SSL

Passive SSL

CIRCL Passive SSL

CIRCL Passive SSL is a database storing historical X.509 certificates seen per IP address. The Passive SSL historical data is indexed per IP address, which makes it searchable for incident handlers, security analysts or researchers.

How do you collect the SSL certificates?

The CIRCL Passive SSL database uses public scanning datasets like the excellent scans.io project.

For more information, Passive SSL was presented at FIRST 2015 in Berlin.

How to use the service?

CIRCL Passive SSL is accessible via a REST API and the output is in JSON format.

The REST API is accessible via the following URLs. 'query' is to query IP address or CIDR blocks (/32 up to /23). 'cquery' is to query per certificate fingerprint and find where the certificate is used per IP address. 'cfetch' is to fetch and parse a specified certificate from the Passive SSL store by its fingerprint.

```
https://www.circl.lu/v2pssl/query/<CIDR block>
https://www.circl.lu/v2pssl/cquery/<SHA1 certificate fingerprint>
https://www.circl.lu/v2pssl/cfetch/<SHA1 certificate fingerprint>
```

Query values can be IP addresses or CIDR blocks between /32 up to /23:

```
https://www.circl.lu/v2pssl/query/172.228.24.0/28
```

and a sample JSON output:

Passive SSL

↑ Back to Services

Passive SSL

How do you collect the SSL certificates?

How to use the service?

Old API (version 1)

Access to CIRCL Passive SSL

Python Library to access CIRCL Passive SSL

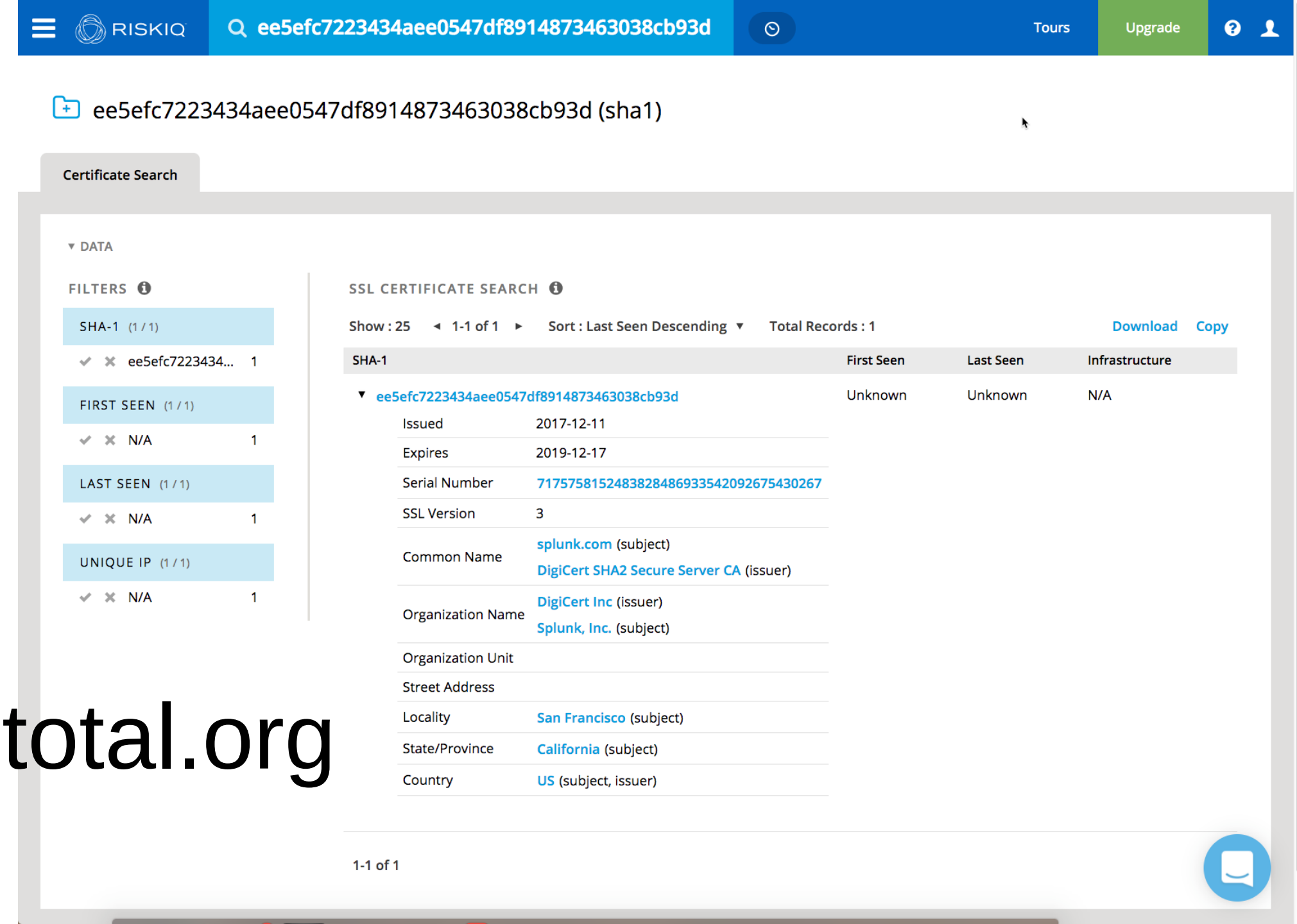
You can report incidents via our official contact including e-mail, phone or use the Anonymous reporting form.

Search

ACCREDITED BY TRUSTED INTRODUCER

FIRST Improving Security Together MEMBER

OASIS MEMBER



Passivetotal.org

Certificate Observations

Edit Export ...

Hash

57d0156c6f8221a197b918cdea1930c All time Submit Hide Filters

First Seen

2017-12-04

Last Seen

2017-12-04

Certificate Details

i	Time	Event
>	12/28/17 5:46:47.000 PM	{ [-] SignatureAlgorithm: ecdsa-with-SHA256 bits: 256 extensions: { [+] } hash_id: 57d0156c6f8221a197b918cdea1930c7da85ec0d issuer: { [+] } md5: a7fa4a19f5896c42df600fac053ac861 notAfter: 2018-11-21T23:59:59 notBefore: 2017-11-21T00:00:00 sha1: 57d0156c6f8221a197b918cdea1930c7da85ec0d sha256: b902786dea9db7047d4d6c4bd22f057b4fb51d260f1a04e95ad837eb1ac484c8 sn: 3ed5d5d0204af3787cbbcba45c757040 subject: { [-] C: US CN: www.splunk.com L: San Francisco O: Splunk Inc. ST: California } subject_name_hash: 3497664767 version: 2 } Show as raw text host = ip-172-31-32-157 source = /sonar/sonar.ssl/2017-12-05-1512435601-https_get_443_certs.gz sourcetype = sonarsslcert

Splunk!

Certificate Observation History

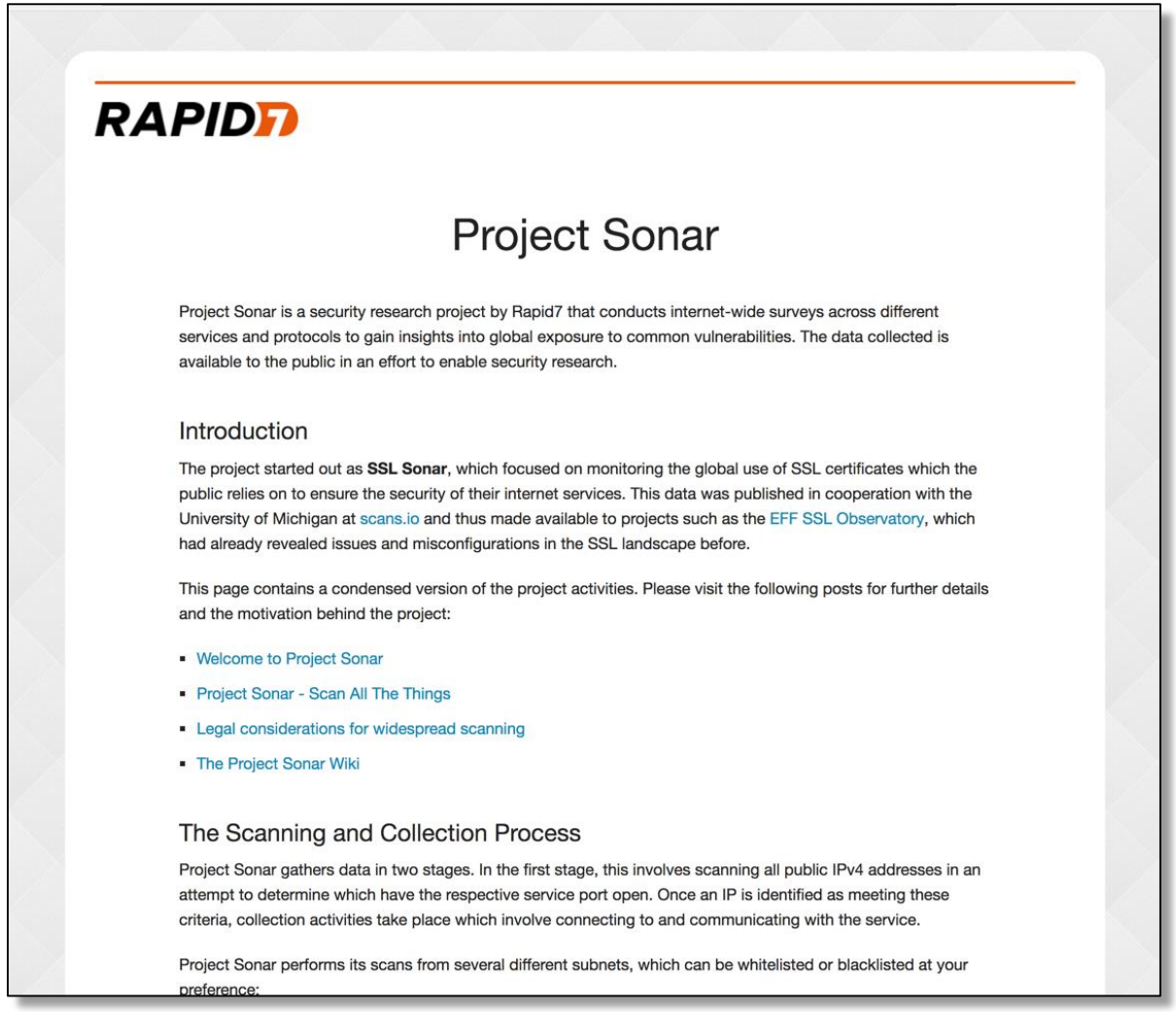
i	Time	Event
>	12/24/17 5:44:47.000 AM	{ [-] asn: AS39015 Mena Broadband Services WLL country_code: US country_name: United States hash: 57d0156c6f8221a197b918cdea1930c7da85ec0d host: 23.0.66.226 seen: 20171205 seen_epoch: 1512432000

Certificate Observation Timeline

Internet-Wide Scan Data Repository

- Public archive of research data
- Hosted by the Censys team at the University of Michigan
- Perform scans, and host results from other teams
- The data on the site is restricted to non-commercial use
- https://scans.io (https://scans.io/json)

Project Sonar by Rapid7



RAPID7

Project Sonar

Project Sonar is a security research project by Rapid7 that conducts internet-wide surveys across different services and protocols to gain insights into global exposure to common vulnerabilities. The data collected is available to the public in an effort to enable security research.

Introduction

The project started out as **SSL Sonar**, which focused on monitoring the global use of SSL certificates which the public relies on to ensure the security of their internet services. This data was published in cooperation with the University of Michigan at scans.io and thus made available to projects such as the EFF SSL Observatory, which had already revealed issues and misconfigurations in the SSL landscape before.

This page contains a condensed version of the project activities. Please visit the following posts for further details and the motivation behind the project:

- Welcome to Project Sonar
- Project Sonar - Scan All The Things
- Legal considerations for widespread scanning
- The Project Sonar Wiki

The Scanning and Collection Process

Project Sonar gathers data in two stages. In the first stage, this involves scanning all public IPv4 addresses in an attempt to determine which have the respective service port open. Once an IP is identified as meeting these criteria, collection activities take place which involve connecting to and communicating with the service.

Project Sonar performs its scans from several different subnets, which can be whitelisted or blacklisted at your preference:

- Many studies
  - SSL Certificates
  - HTTP Content
  - HTTPS Content
  - DNS
  - Various TCP/UDP services (SSH, SMB, Telnet, etc.)
- Hosted at scans.io
- Please review Project Sonar TOS
- Thanks to Rapid7 Labs!

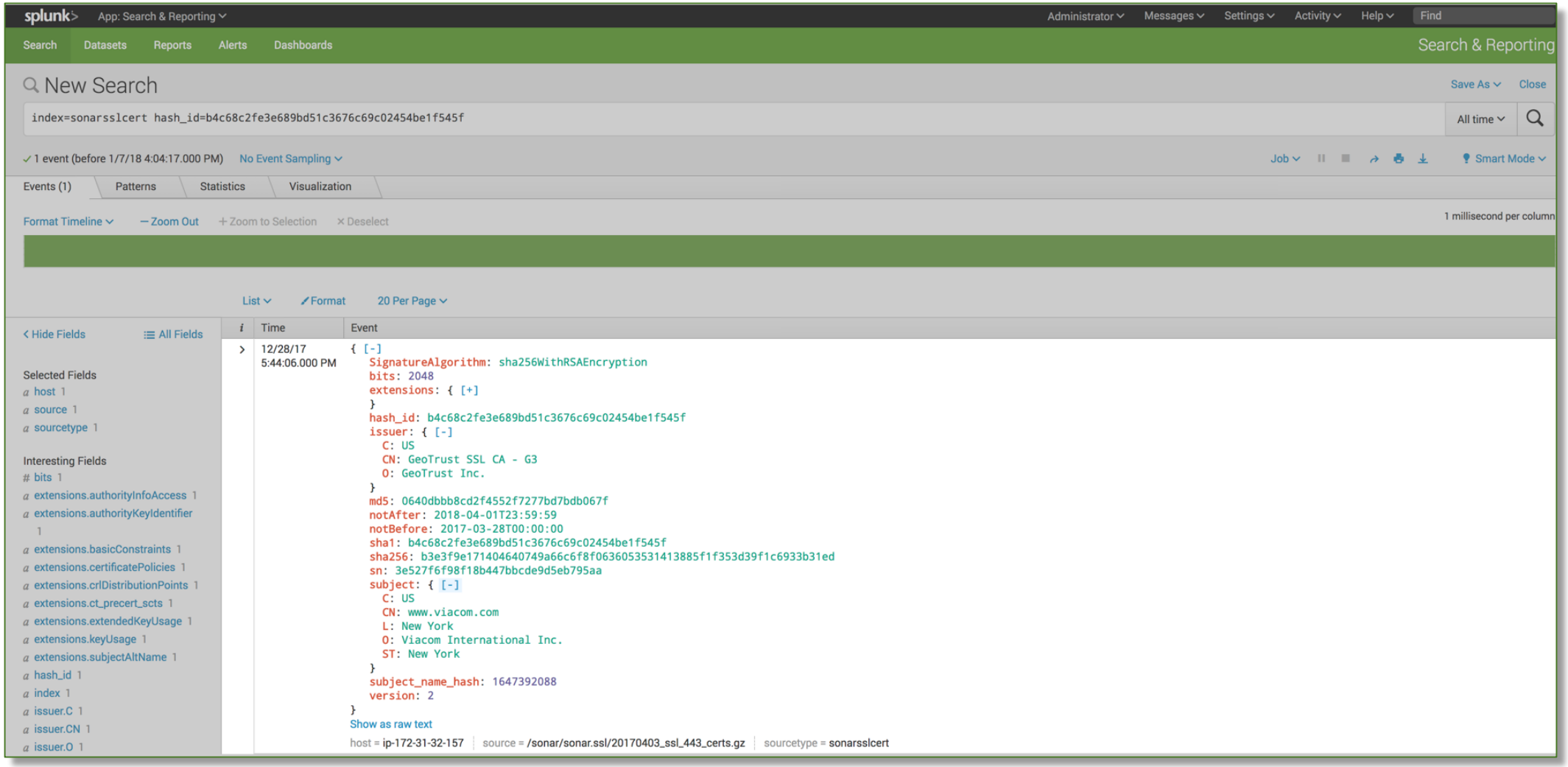
https://sonar.labs.rapid7.com/

SSL Certificates Study (sonar.ssl)

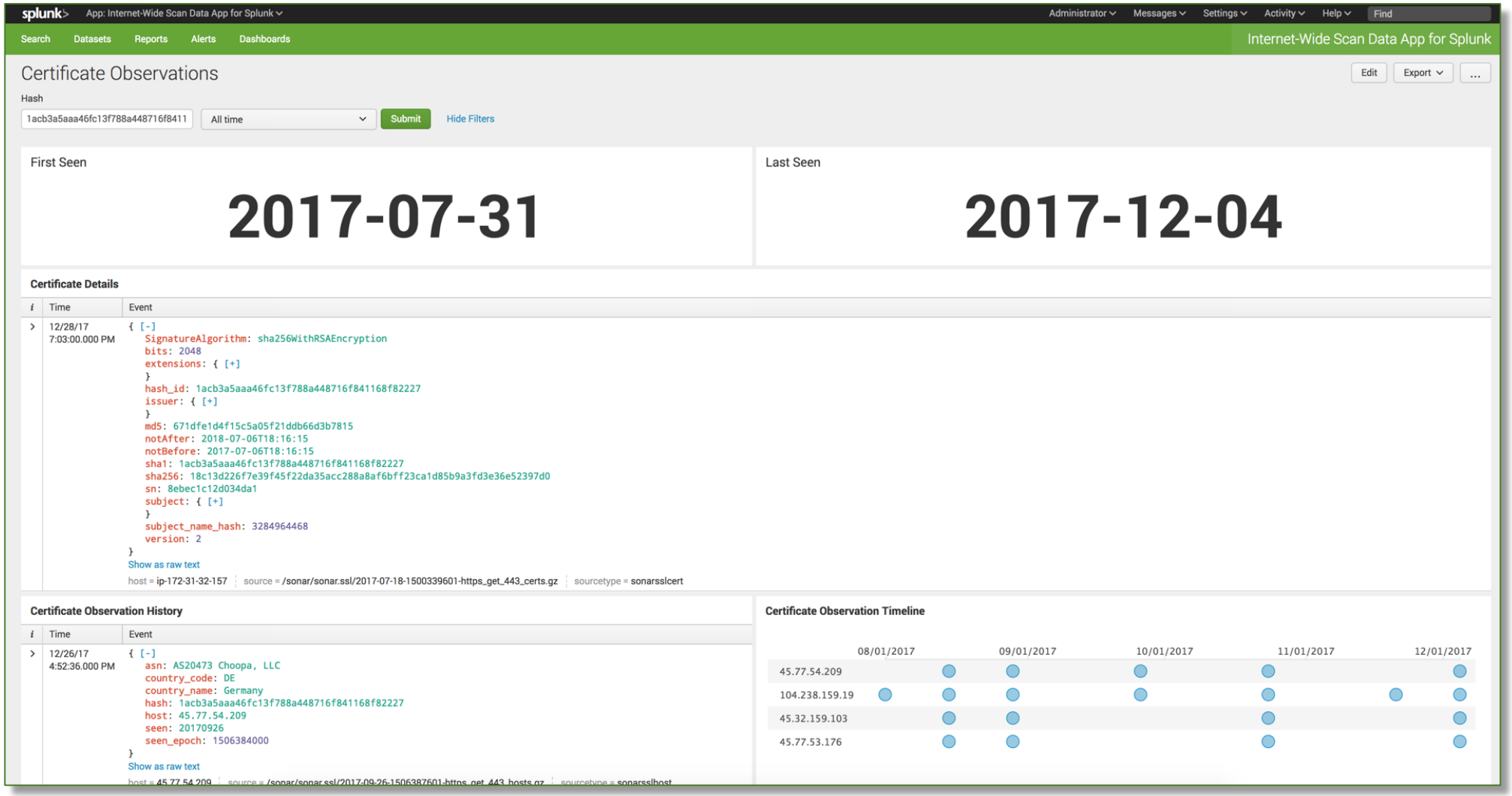
- October 30, 2013 – Present
- Raw size
  - Entire data set: 315 GB compressed (as of 02JAN2017)
  - Weekly: ~1.5 - 2.0 GB compressed
- Entire data set indexed in Splunk: ~1.2TB
- Scan the entire Internet (TCP/443 only)
- Comprised of:
  - Observed certificates *
  - Observed IP address / certificate *
  - Names (FQDNS)
  - Endpoints

sonar.ssl Certificate in Splunk

`index=sonarsslcert earliest=0 hash_id=b4c68c2fe3e689bd51c3676c69c02454be1f545f`



sonar.ssl First/Last seen



Search for a hash, or pivot here from search


But what do we do with it?

You can do at least two things with SSL Certificate information

THE SSL CERTIFICATES IN YOUR

INCIDENTS ARE REAL.

Start with some known naughty SSL SHA1 fingerprints

Secure | https://sslbl.abuse.ch

Analysis | Sysadmin stuff | Programming/scripti... | Splunk SEAL | capture.jpg | 11 new message. Me... | Splunk Search Job | ಠ_ಠ ಠ_ಠ Disapproval Look | SSL | Other Bookma

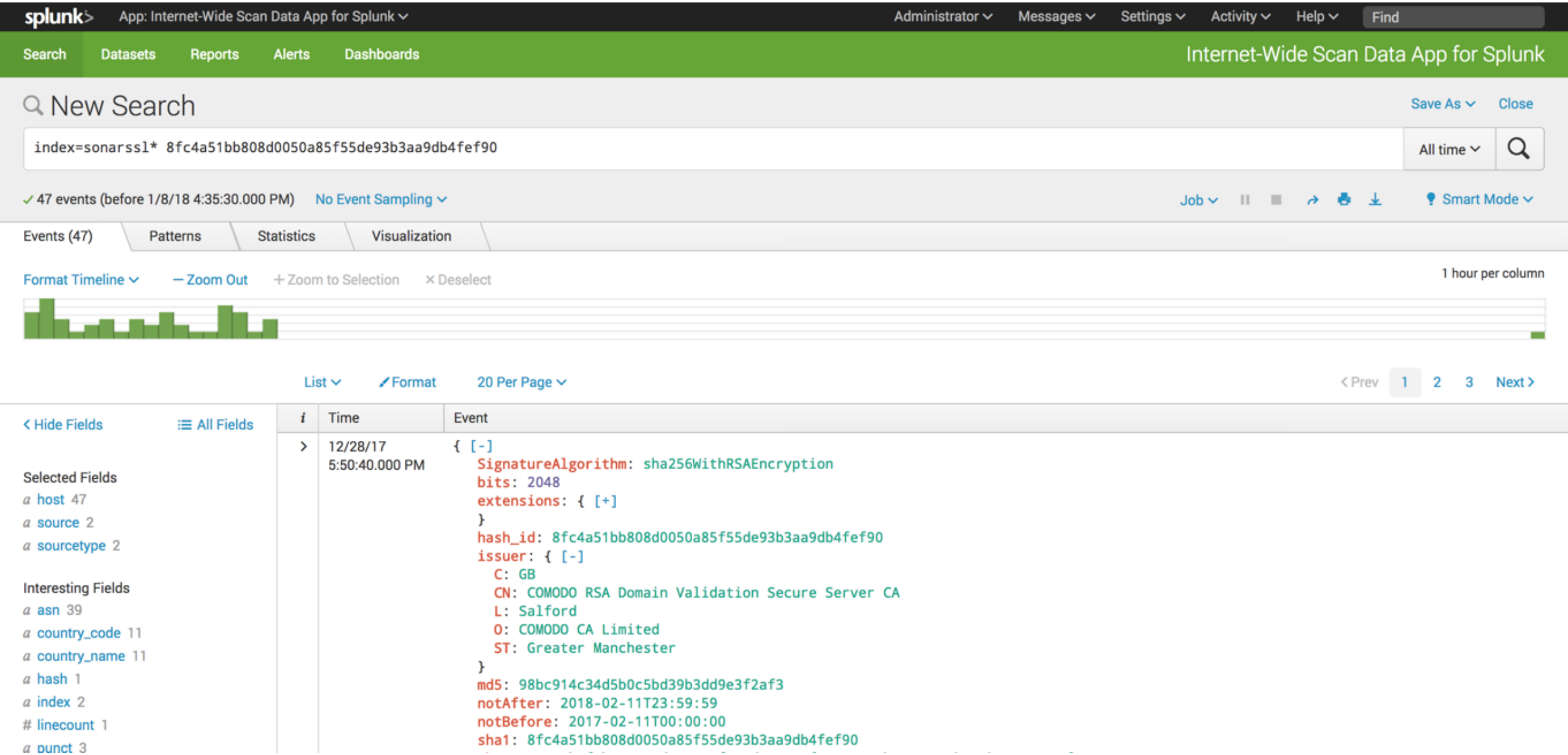
8fc4a51bb808d0050a85f55d 1/1

2017-02-18 09:02:25	c0d63a9d2d306d3d862057df53682c978b04d874	www.example.com	
2017-02-18 09:02:16	3c12f2496d67941938718f8283d638b9329eb981	www.example.com	Android Marcher C&C
2017-02-18 09:02:07	e602afd1f7e1250c03df84e27ad242afc1099f6a	www.example.com	Android Marcher C&C
2017-02-18 09:01:53	e8d1b7885f5133a601468cf2c02dcc2b5c59c23e	www.example.com	Android Marcher C&C
2017-02-17 06:47:40	53ba46ad70662e1d3eebce454cd4062512f717c8	labdon.com/emailAddress=web@labdon.com	Gootkit C&C
2017-02-16 15:46:00	512263416240f664f5b6c8e765498c0ffd45729e	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C
2017-02-16 10:05:26	8fc4a51bb808d0050a85f55de93b3aa9db4fef90	treesaboutword.com	Gozi MITM
2017-02-15 08:40:18	41a180cfb9e2ec1b709d2fe8c62dcf5a7e8c911e	deutch.com/emailAddress=web@deutch.com	Gootkit C&C
2017-02-14 15:55:16	888730fb84c11dd0aeff4999104b4779a8f6deb0	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C
2017-02-14 14:38:08	f3bea1f2ef233f48b83d60fd6b6ae8d1f0b95573	CN=asdallls.com	Gozi MITM
2017-02-14 14:36:25	63158d8297be13aeb41e57d3f3e09b90086f6d0d	nopassworddomaine.com	Gozi MITM
2017-02-13 08:17:33	e3a06ba97d6e74c1a2f8e4bb79a08ad49e232611	CN=dremongo.com	Gozi MITM
2017-02-10	abf5ce4f1c12525760015968182515 2a8ae87e1b	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C

Gozi Trojan

2017-02-18 09:02:25	c0d63a9d2d306d3d862057df53682c978b04d874	www.example.com	
2017-02-18 09:02:16	3c12f2496d67941938718f8283d638b9329eb981	www.example.com	Android Marcher C&C
2017-02-18 09:02:07	e602afd1f7e1250c03df84e27ad242afc1099f6a	www.example.com	Android Marcher C&C
2017-02-18 09:01:53	e8d1b7885f5133a601468cf2c02dcc2b5c59c23e	www.example.com	Android Marcher C&C
2017-02-16 15:46:00	512263416240f664f5b6c8e765498c0ffd45729e	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C
2017-02-16 10:05:26	8fc4a51bb808d0050a85f55de93b3aa9db4fef90	treesaboutword.com	Gozi MITM
2017-02-15 08:40:18	41a180cfb9e2ec1b709d2fe8c62dcf5a7e8c911e	deutch.com/emailAddress=web@deutch.com	Gootkit C&C
2017-02-14 15:55:16	888730fb84c11dd0aeff4999104b4779a8f6deb0	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C
2017-02-14 14:38:08	f3bea1f2ef233f48b83d60fd6b6ae8d1f0b95573	CN=asdallls.com	Gozi MITM
2017-02-14 14:36:25	63158d8297be13aeb41e57d3f3e09b90086f6d0d	nopassworddomaine.com	Gozi MITM
2017-02-13 08:17:33	e3a06ba97d6e74c1a2f8e4bb79a08ad49e232611	CN=dremongo.com	Gozi MITM
2017-02-10	abf5ce4f1c12525760015968182515 2a8ae87e1b	C=US, ST=Denial, L=Springfield, O=Dis	TorrentLocker C&C

8fc4a51bb808d0050a85f55de93b3aa9db4fef90


splunk> App: Internet-Wide Scan Data App for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Search
Datasets
Reports
Alerts
Dashboards
Internet-Wide Scan Data App for Splunk
New Search
Save As
Close
index=sonarssl* 8fc4a51bb808d0050a85f55de93b3aa9db4fef90
All time
✓ 47 events (before 1/8/18 4:35:30.000 PM)
No Event Sampling
Job
Smart Mode
Events (47)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
List
Format
20 Per Page
< Prev
1
2
3
Next >
< Hide Fields
All Fields
Selected Fields
a host 47
a source 2
a sourcetype 2
Interesting Fields
a asn 39
a country_code 11
a country_name 11
a hash 1
a index 2
linecount 1
a punct 3
i
Time
Event
12/28/17
5:50:40.000 PM
{ [-]
SignatureAlgorithm: sha256WithRSAEncryption
bits: 2048
extensions: { [+]
}
hash_id: 8fc4a51bb808d0050a85f55de93b3aa9db4fef90
issuer: { [-]
C: GB
CN: COMODO RSA Domain Validation Secure Server CA
L: Salford
O: COMODO CA Limited
ST: Greater Manchester
}
md5: 98bc914c34d5b0c5bd39b3dd9e3f2af3
notAfter: 2018-02-11T23:59:59
notBefore: 2017-02-11T00:00:00
sha1: 8fc4a51bb808d0050a85f55de93b3aa9db4fef90

Certificate Observations

Edit | Export | ...

Hash

8fc4a51bb808d0050a85f55de93b3aa9 | All time | Submit | Hide Filters

First Seen

2017-03-05

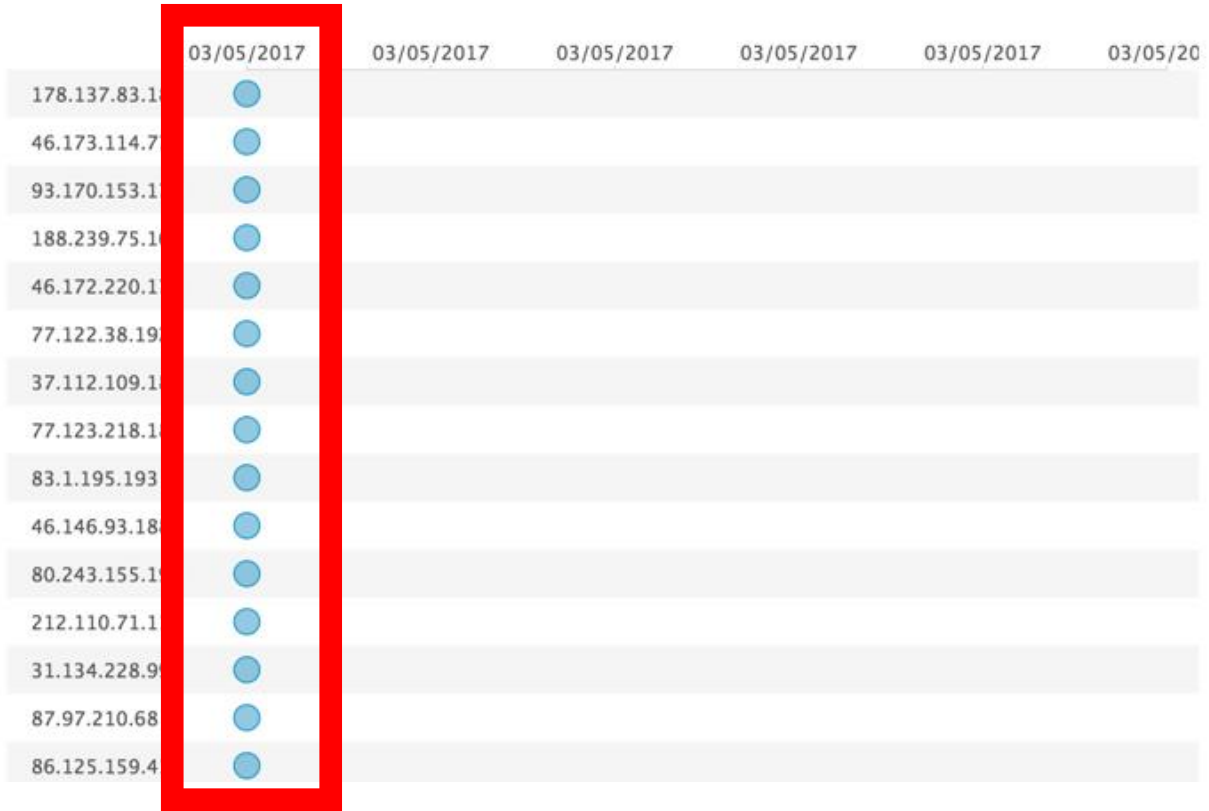
Last Seen

2017-03-05

Certificate Details

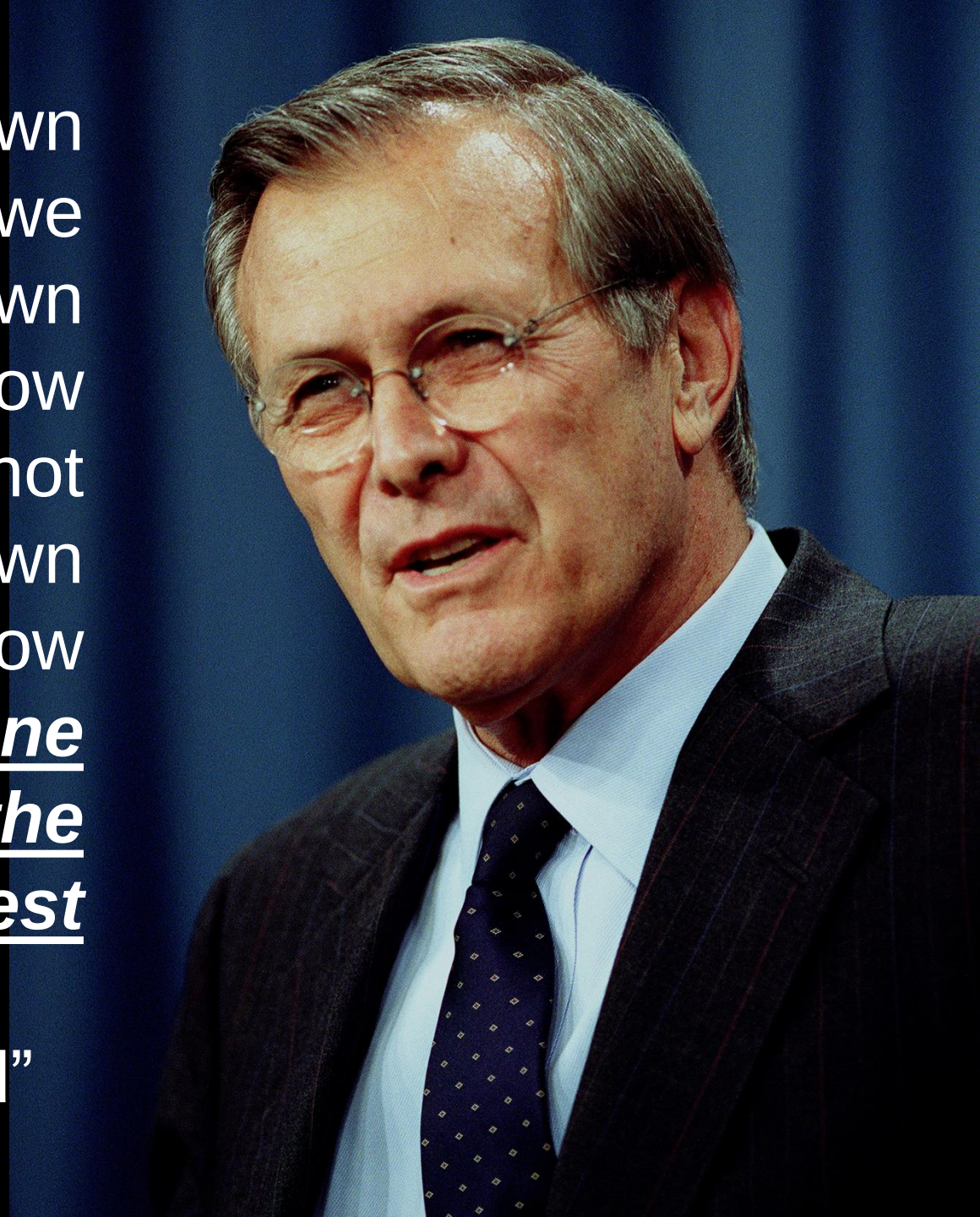
i	Time	Event
>	12/28/17 5:50:40.000 PM	{ [-] SignatureAlgorithm: sha256WithRSAEncryption bits: 2048 extensions: { [+] } hash_id: 8fc4a51bb808d0050a85f55de93b3aa9db4fef90 issuer: { [+] } md5: 98bc914c34d5b0c5bd39b3dd9e3f2af3 notAfter: 2018-02-11T23:59:59 notBefore: 2017-02-11T00:00:00 sha1: 8fc4a51bb808d0050a85f55de93b3aa9db4fef90 sha256: ec8b9f6b27c183d075379f373dae93eefc242279abce8c45ed592d99355902ef sn: a64a10eeb4fa73b0bfa7241f1791744e subject: { [+] } subject_name_hash: 1861167684 version: 2 } Show as raw text host = ip-172-31-32-157 | source = /sonar/sonar.ssl/20170220_ssl_443_certs.gz | sourcetype = sonarsslcert

Certificate Observation Timeline



“As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. ***And when someone tries to hunt in CyberSpace the known unknowns are the hardest to find*** ”

- Donald “Cybersfeld”



Hunting PowerShell Empire

Branch: master ▾ Empire / setup / cert.sh

Find file | Copy

dchrastil Updated comments to match the new openssl call 399528e on Jun 9,

3 contributors

Executable File | 14 lines (10 sloc) | 694 Bytes

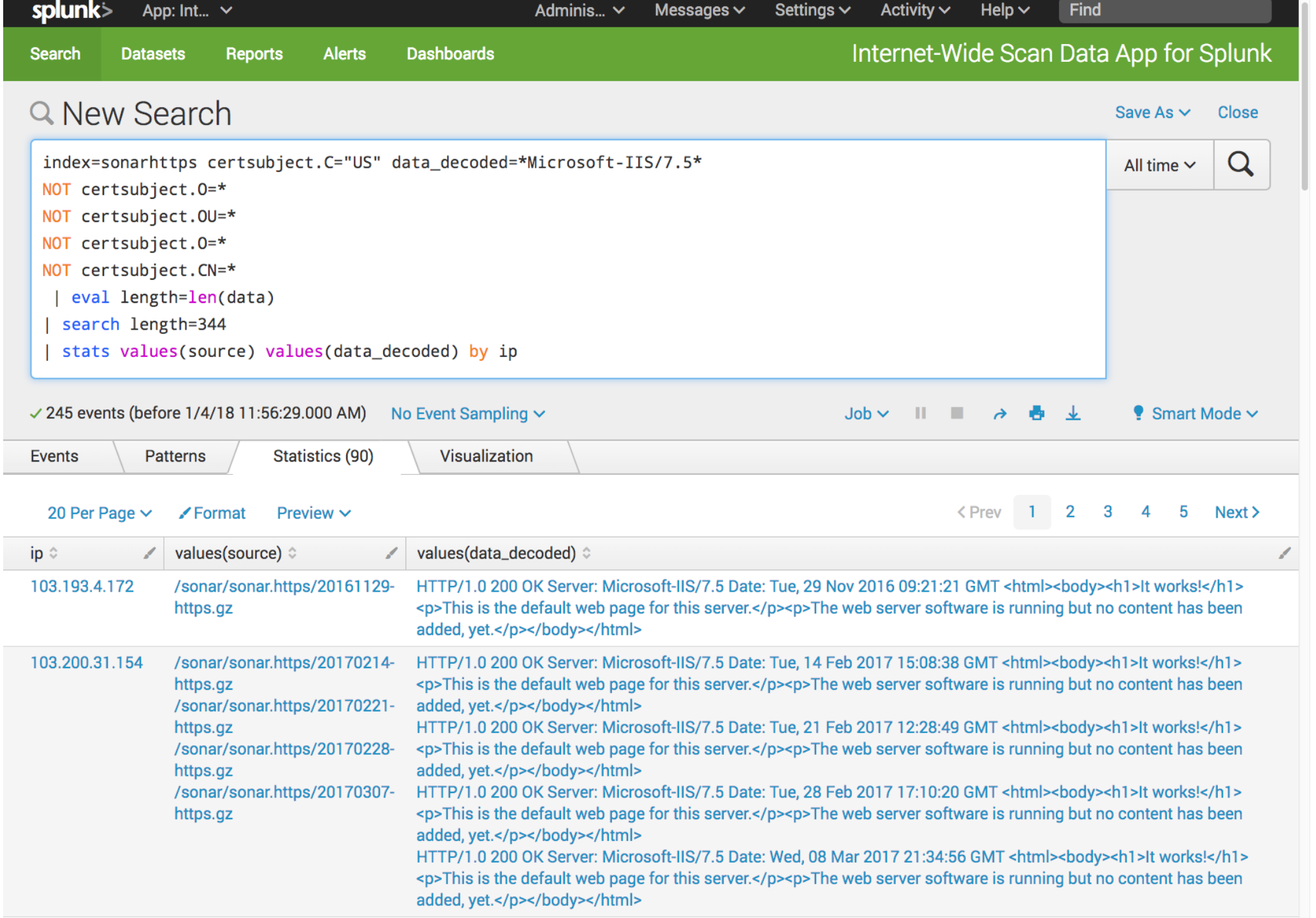
Raw | Blame | History

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

```
openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1
```

C=US is weird…

SSL Cert Subject and Issuer fields	www.google.com	PowerShell Empire	Splunk
subject.C	US	US	US
subject.CN	*.google.com		splunk.com
subject.L	Mountain View		San Francisco
subject.O	Google Inc		Splunk, Inc.
subject.ST	California		California
issuer.C	US	US	US
issuer.CN	Google Internet Authority G2		DigiCert SHA2 Secure Server CA
issuer.O	Google Inc		DigiCert Inc


splunk> App: Int... Adminis... Messages Settings Activity Help Find
Search Datasets Reports Alerts Dashboards
Internet-Wide Scan Data App for Splunk
New Search
Save As Close
index=sonarhttps certsubject.C="US" data_decoded=*Microsoft-IIS/7.5*
NOT certsubject.O=*
NOT certsubject.OU=*
NOT certsubject.O=*
NOT certsubject.CN=*
| eval length=len(data)
| search length=344
| stats values(source) values(data_decoded) by ip
All time
✓ 245 events (before 1/4/18 11:56:29.000 AM)
No Event Sampling
Job
Smart Mode
Events Patterns Statistics (90) Visualization
20 Per Page
Format
Preview
Prev 1 2 3 4 5 Next
ip
values(source)
values(data_decoded)
103.193.4.172
/sonar/sonar.https/20161129-https.gz
HTTP/1.0 200 OK Server: Microsoft-IIS/7.5 Date: Tue, 29 Nov 2016 09:21:21 GMT <html><body><h1>It works!</h1> This is the default web page for this server. The web server software is running but no content has been added, yet. </body></html>
103.200.31.154
/sonar/sonar.https/20170214-https.gz
/sonar/sonar.https/20170221-https.gz
/sonar/sonar.https/20170228-https.gz
/sonar/sonar.https/20170307-https.gz
HTTP/1.0 200 OK Server: Microsoft-IIS/7.5 Date: Tue, 14 Feb 2017 15:08:38 GMT <html><body><h1>It works!</h1> This is the default web page for this server. The web server software is running but no content has been added, yet. </body></html>
HTTP/1.0 200 OK Server: Microsoft-IIS/7.5 Date: Tue, 21 Feb 2017 12:28:49 GMT <html><body><h1>It works!</h1> This is the default web page for this server. The web server software is running but no content has been added, yet. </body></html>
HTTP/1.0 200 OK Server: Microsoft-IIS/7.5 Date: Tue, 28 Feb 2017 17:10:20 GMT <html><body><h1>It works!</h1> This is the default web page for this server. The web server software is running but no content has been added, yet. </body></html>
HTTP/1.0 200 OK Server: Microsoft-IIS/7.5 Date: Wed, 08 Mar 2017 21:34:56 GMT <html><body><h1>It works!</h1> This is the default web page for this server. The web server software is running but no content has been added, yet. </body></html>

```
notyobox:pylanos rkovar$ sudo python pylanos.py  -f PSE_list


Scanning 103.193.4.172 with nmap ...
|___ it's up ... Unknow system.Unable to determine                    the OS type.
Scanning 103.200.31.154 with nmap ...
|___ it's up ... Unknow system.Unable to determine                    the OS type.
Scanning 103.208.86.222 with nmap ...
|___ it's up ... Linux system.
Scanning 103.236.201.112 with nmap ...
|___ it's up ... Unknow system.Unable to determine                    the OS type.
Scanning 103.253.41.38 with nmap ...
|___ it\s down.
Scanning 104.130.231.211 with nmap ...
|___ it's up ... Unknow system.Unable to determine                    the OS type.
Scanning 104.130.51.215 with nmap ...
|___ it\s down.
Scanning 104.131.157.244 with nmap ...
|___ it's up ... Linux system.
Scanning 104.145.225.69 with nmap ...
|___ it's up ... Unknow system.Unable to determine                    the OS type.
```

```
notyobox:iccs_research rkovar$ python mp_pse.py
Requesting IP: 103.193.4.172 now
IP: 103.193.4.172 had an exception ('Connection aborted.', error(61, 'Connection refused'))

Requesting IP: 104.238.147.87 now
IP: 104.238.147.87 had an exception ('Connection aborted.', error(61, 'Connection refused'))

Requesting IP: 103.200.31.154 now
IP: 103.200.31.154 had an exception ('Connection aborted.', error(61, 'Connection refused'))

Requesting IP: 103.208.86.222 now
/Users/rkovar/Library/Python/2.7/lib/python/site-packages/requests/packages/urllib3/connectionpool.py:768: Ins
ecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advis
ed. See: https://urllib3.readthedocs.org/en/latest/security.html
  InsecureRequestWarning)
Requesting IP: 103.236.201.112 now
IP: 103.236.201.112 had an exception ('Connection aborted.', error(61, 'Connection refused'))

Requesting IP: 103.253.41.38 now
IP: 103.253.41.38 had an exception ('Connection aborted.', error(51, 'Network is unreachable'))

Requesting IP: 104.130.231.211 now
```

good_results.txt

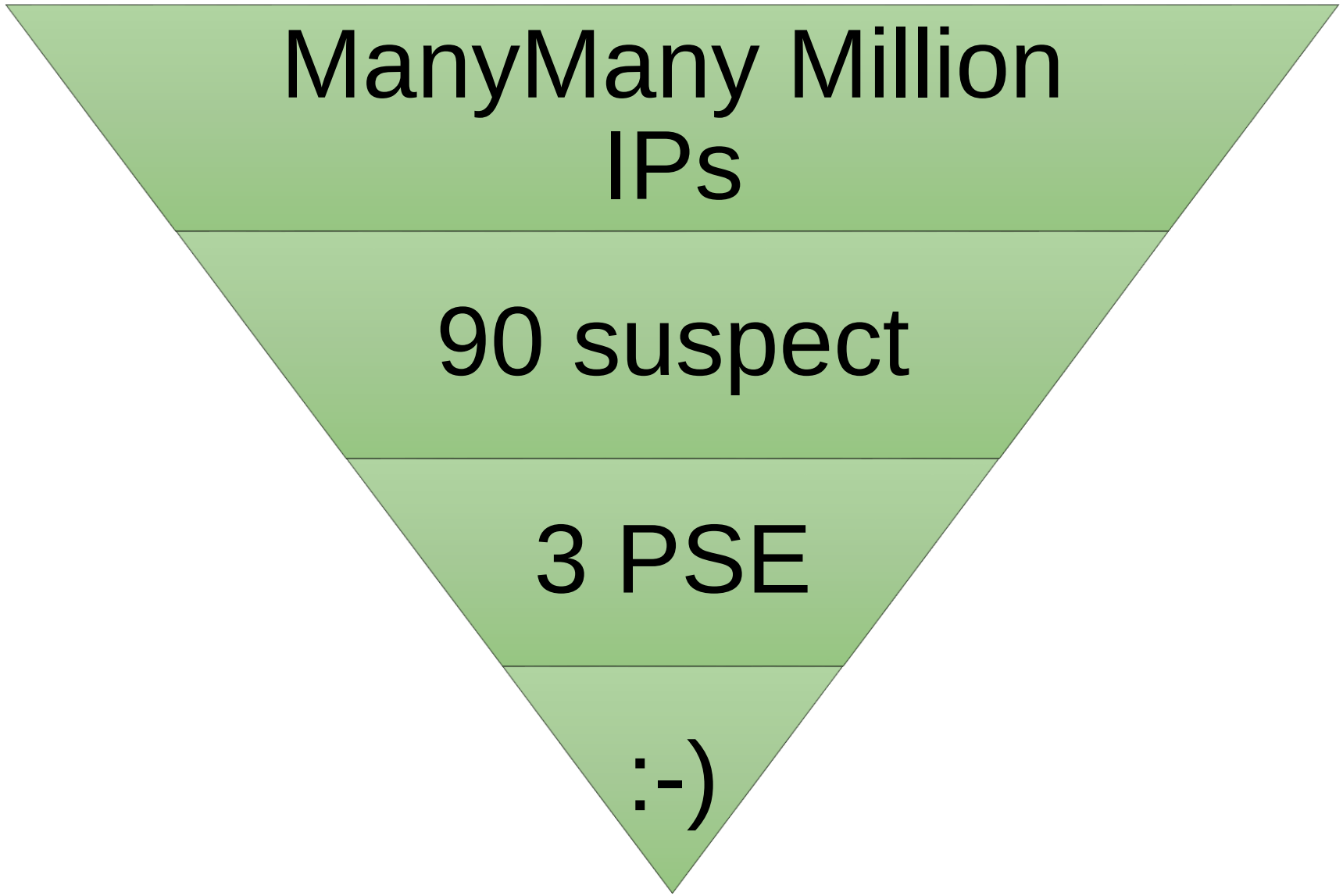
UNREGISTERED

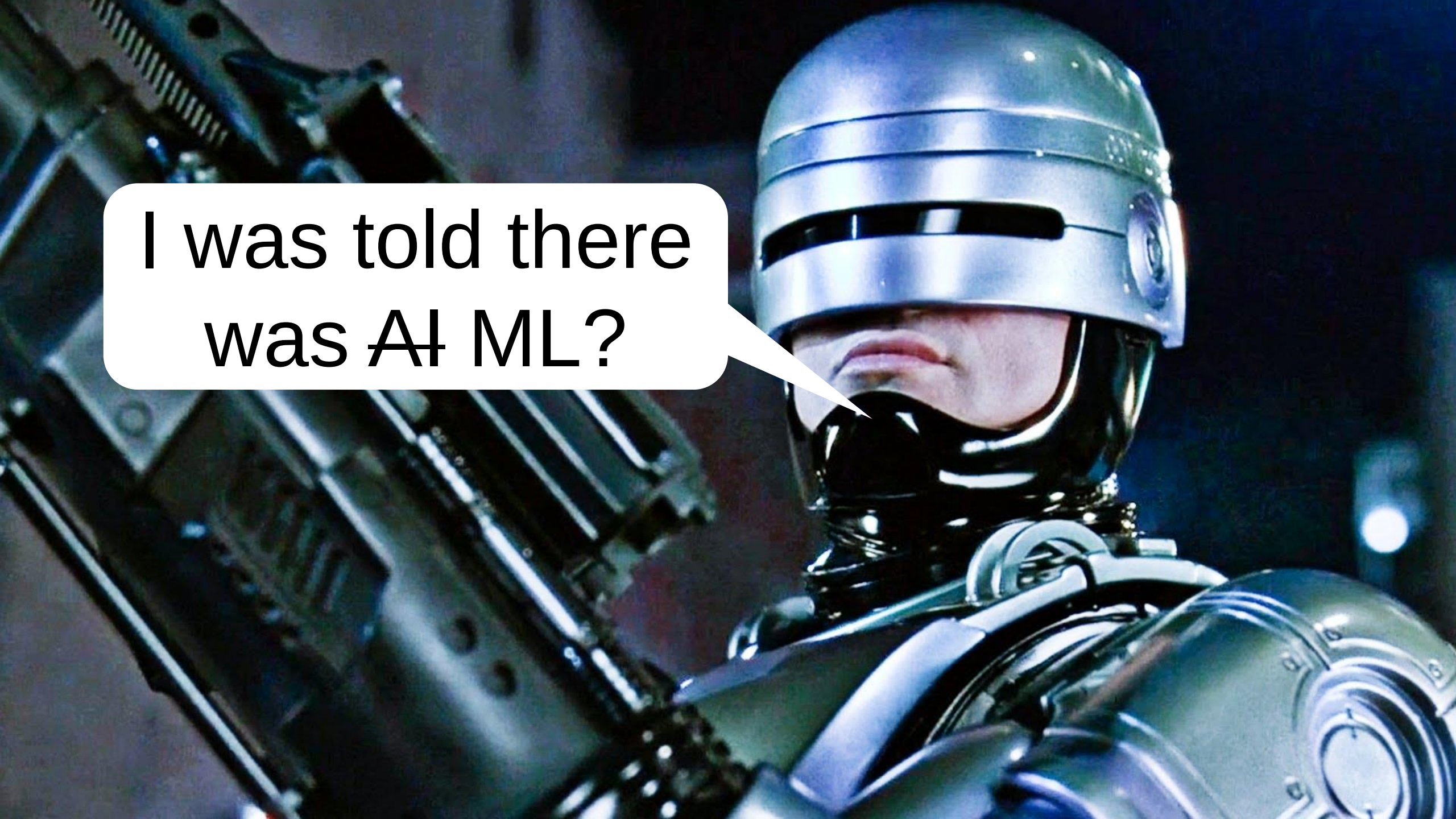
good_results.txt

```
104.238.147.87 has a valid status code and headers of  {'content-length': '173', 'expires': '0', 'server': 'Microsoft-IIS/7.5', 'pragma': 'no-cache', 'cache-control': 'no-cache, no-store, must-revalidate', 'date': 'Fri, 05 Jan 2018 18:59:27 GMT', 'content-type': 'text/html; charset=utf-8'} and defaullt it works payload

218.255.22.254 has a valid status code and headers of  {'date': 'Fri, 05 Jan 2018 19:01:41 GMT', 'server': 'Microsoft-IIS/7.5'} and defaullt it works payload

38.126.169.109 has a valid status code and headers of  {'date': 'Fri, 05 Jan 2018 19:00:16 GMT', 'content-length': '173', 'content-type': 'text/html; charset=utf-8', 'server': 'Microsoft-IIS/7.5'} and defaullt it works payload
```


ManyMany Million
IPs
90 suspect
3 PSE
:-)


I was told there was ~~AI~~ ML?

The Pinto Test


We use Splunk
But you don’t have to!

Home | SSL Blacklist | Contact

SSL Blacklist :: Home

SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on **SHA1 fingerprints** of malicious SSL certificates and offers various blacklists that can found in the SSL Blacklist section.

If you are interested in SSL in general or you are looking for a way to implement SSL securely, you might want to have a look at the following links:

- Qualys - SSL Server Tester
- Qualys - SSL Client Tester
- Qualys - SSL/TLS Deployment Best Practices
- BetterCrypto.org - Applied Crypto Hardening
- mbed TLS - An alternative open source and commercial SSL library (formerly known as PolarSSL)
- Hiawatha Webserver - An advanced and secure webserver for Unix that implements mbed TLS

Below is an overview over all blacklisted SSL certificates. You can sort the list by clicking on any column title (please note that JavaScript must be enabled in your web browser in order to use this function). In addition, you can click on a SSL Fingerprint (SHA1) to receive more information about a specific entry in the SSL Blacklist.

If you are looking for a parsable format of the list below, you should take a look at SSLBL Extended (or for Dyre: Dyre SSLBL Extended).

SSBL RSS feed
SSBL RSS feed (Dyre only)

Overview of blacklisted SSL certificates (malicious Dyre C&C SSL certificates excluded):

Listing date (UTC)	SHA1 fingerprint	Common Name	Listing reason
2018-01-24 14:45:58	d0351b59fdd6e82b260780f2b60c156e25303fa4	C=XX, L=Default City, O=Default Company Ltd	PandaZeuS C&C
2018-01-23 12:46:18	eecb6b2d3e8d46a21c6ff98d3ad75b5dace4af7a	XX	PandaZeuS C&C
2018-01-23 12:46:08	d5071bc4e4efb4b3af448ad1bcfe334f057d2bbf	XX	PandaZeuS C&C
2018-01-20 12:58:17	cb06cd0cdd50db37647e444a9a092ffc3a298e95	domain.com/O=My Company Name LTD./C=US	PandaZeuS C&C
2018-01-19 14:49:07	58aeab46c6cdfec4667f683ed15b84d541513857	example.com	TrickBot C&C
2018-01-19 14:48:23	22c5ece6639c9ced35d6a2d45d7dc18f9d4f5256	example.com	TrickBot C&C
2018-01-19 14:48:22	7e2feb5c7eaf880e8587b349d3dee94a77650dd4	example.com	TrickBot C&C
2018-01-19 14:47:59	ebd99519da72873ae03f9210996f49af6b169fa0	example.com	TrickBot C&C
2018-01-19 14:47:40	d197587bbc145b81eb2eac5b067f027f3d17d0c3	example.com	TrickBot C&C
2018-01-19 14:47:38	ace94d19d9d78c915d9ee080bf60cd41ac8db91a	example.com	TrickBot C&C
2018-01-19 14:45:15	9b585b4014ef6cc5eabc235f63b81a01b6a7d091	example.com	TrickBot C&C
2018-01-19 14:41:00	d0f17091244f892ea27aacd3d64adcb9822832b4	example.com	TrickBot C&C
2018-01-19 14:40:59	ec18e0406f3eafa3eed3caff61f59e2e5ce26fff	example.com	TrickBot C&C
2018-01-19 14:40:57	a48fcb663de8dbbadcd17b8f836e2c5d4ed3b330	example.com	TrickBot C&C
2018-01-18 12:28:17	702d015c520fd5b76ee7ed49b38f8892372ac54f	example.com	TrickBot C&C
2018-01-18 12:28:15	c88092cf532a46b3c9fabdff6361f8a338b7d292	example.com	TrickBot C&C
2018-01-18 12:27:41	0cd05bb43a7baf3f5c07760bf6d17ccc9de0bb19	example.com	TrickBot C&C
2018-01-18 12:27:31	602c5dbad07fd4c9825a2dfc160446497c396bbd	example.com	TrickBot C&C
2018-01-18 12:27:29	fcf57e831a5fe834b0cd2540d1c19af71baf21a1	example.com	TrickBot C&C
2018-01-16 12:49:07	c8a237c907b33ee1e3431c45d3abdd76f96f8e43	domain.com/O=My Company Name LTD./C=US	PandaZeuS C&C
2018-01-06 16:49:38	afc8d119cad2f1177e1c51248153cb26a367cdbf	bqeu.us	Quakbot C&C
2018-01-06 11:38:38	519af40067c719749b8626479fac81c14e248b48	kfhnjyba.com	Quakbot C&C
2018-01-04 09:03:31	9d00d62b06a97c1e439750ed2c5d44c303683202	C=XX, L=Default City, O=Default Company Ltd	PandaZeuS C&C
2018-01-03 15:17:41	31d2d913ea305ddfa3c275184f3d138627a0c86e	domain.com/O=My Company Name LTD./C=US	PandaZeuS C&C
2018-01-03 15:14:17	802018d0950eda31a304f42c25e7743aa39a2ab5	example.com	TrickBot C&C
2018-01-03 15:14:15	207a31fb22bde2b236d36bd4647622064efcdd6a	example.com	TrickBot C&C
2018-01-03 13:44:40	daadd88d8ee8a1e2719bdf5d386c744f93ebc025	domain.com/O=My Company Name LTD./C=US	PandaZeuS C&C

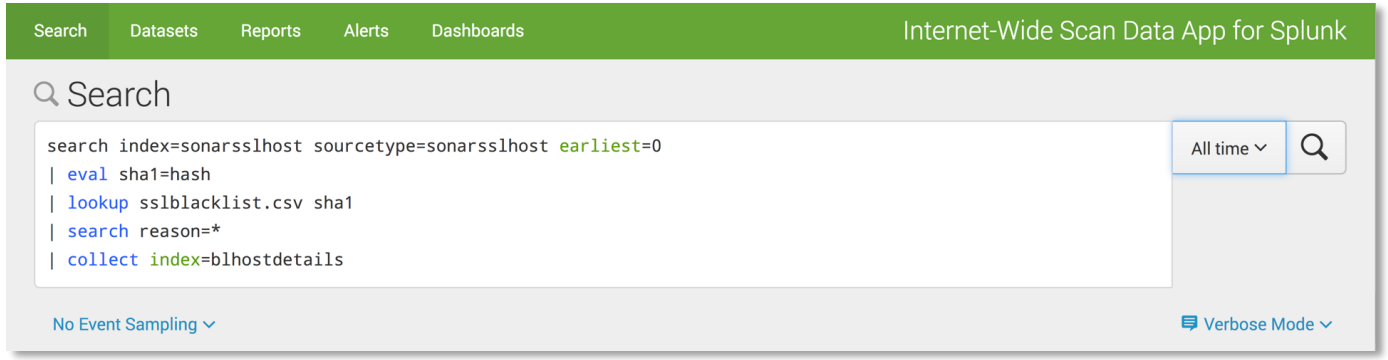
SSL Blacklist

https://sslbl.abuse.ch/

Can we build a model to predict inclusion on the SSL blacklist?

More importantly, can such a model alert us to badness that we otherwise would not detect?

We have labeled data…



"Bad" (blacklisted) certs

```
search index=sonarsslcert sourcetype=sonarsslcert
| lookup sslblacklist.csv sha1
| search reason=*
| collect index=blcertdetails
```

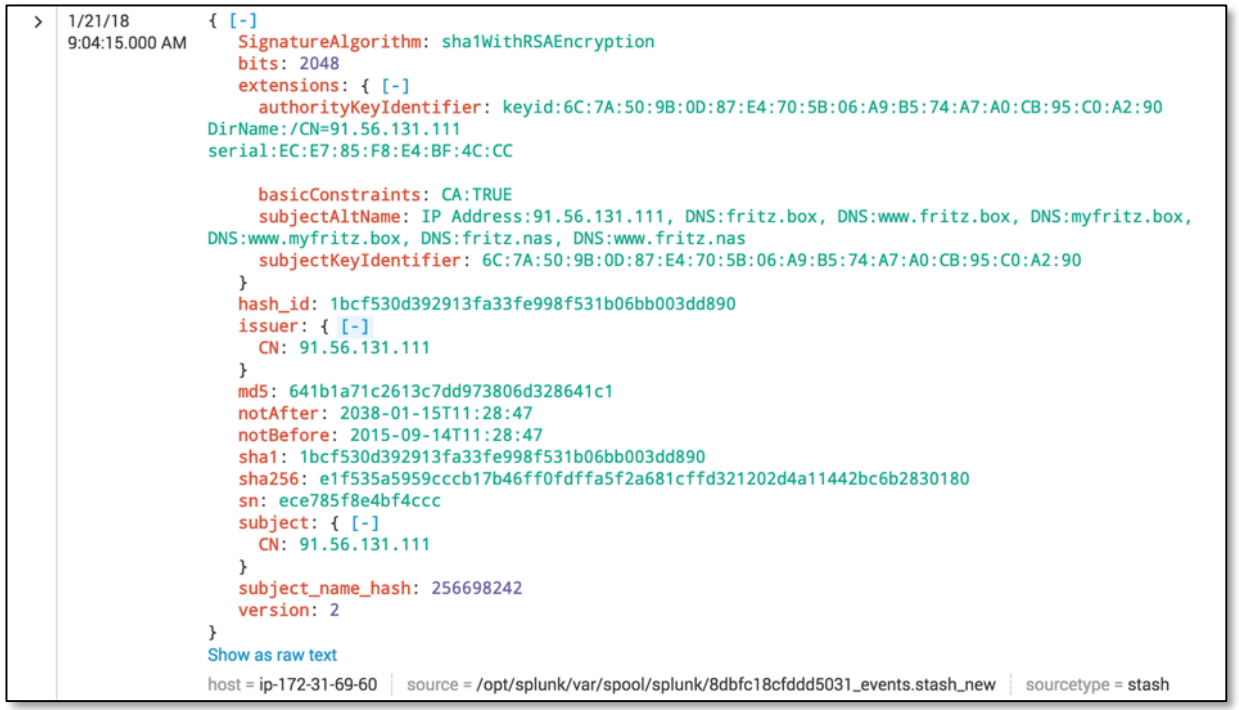
(About 1500)

"Good" (non-blacklisted) certs (note sampling ratio)

```
search index=sonarsslcert sourcetype=sonarsslcert
| lookup sslblacklist.csvsha1
| search NOT reason=*
| collect index=nonblcertdetails
```

(About 1700)

Feature Selection and Prep



1/21/18
9:04:15.000 AM

{ [-]
  SignatureAlgorithm: sha1WithRSAEncryption
  bits: 2048
  extensions: { [-]
    authorityKeyIdentifier: keyid:6C:7A:50:9B:0D:87:E4:70:5B:06:A9:B5:74:A7:A0:CB:95:C0:A2:90
DirName:/CN=91.56.131.111
serial:EC:E7:85:F8:E4:BF:4C:CC

    basicConstraints: CA:TRUE
    subjectAltName: IP Address:91.56.131.111, DNS:fritz.box, DNS:www.fritz.box, DNS:myfritz.box,
DNS:www.myfritz.box, DNS:fritz.nas, DNS:www.fritz.nas
    subjectKeyIdentifier: 6C:7A:50:9B:0D:87:E4:70:5B:06:A9:B5:74:A7:A0:CB:95:C0:A2:90
  }
  hash_id: 1bcf530d392913fa33fe998f531b06bb003dd890
  issuer: { [-]
    CN: 91.56.131.111
  }
  md5: 641b1a71c2613c7dd973806d328641c1
  notAfter: 2038-01-15T11:28:47
  notBefore: 2015-09-14T11:28:47
  sha1: 1bcf530d392913fa33fe998f531b06bb003dd890
  sha256: e1f535a5959cccb17b46ff0fdffa5f2a681cffd321202d4a11442bc6b2830180
  sn: ece785f8e4bf4ccc
  subject: { [-]
    CN: 91.56.131.111
  }
  subject_name_hash: 256698242
  version: 2
}

Show as raw text

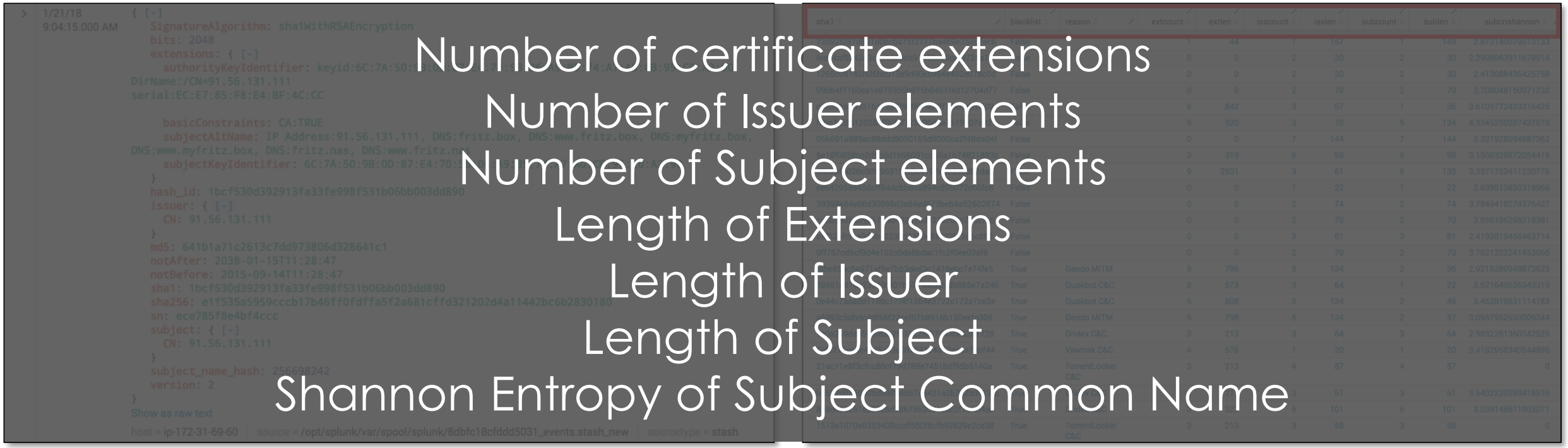
host = ip-172-31-69-60 | source = /opt/splunk/var/spool/splunk/8dbfc18cfddd5031_events.stash_new | sourcetype = stash

For analysts

sha1	blacklist	reason	extcount	extlen	isscount	isslen	subcount	sublen	subcnshannon
73d92f287d891d0bc6a75f3717ba469e258c2ecb	False		1	44	7	157	7	149	2.873140679513133
fee84af824243c4e1030cb91093e39ccf9725a10	False		0	0	2	30	2	30	2.2998963911678914
1265c08145f6f6bc913e9d90eb984e492e078c0d	False		0	0	2	30	2	30	2.413088436425758
09bb4f7160ea1e875956b975b8461f4d12704d77	False		0	0	2	70	2	70	3.708048150071232
c3853ba25351b1128f298997407ff7f969d2b502	False		8	842	3	67	1	36	3.6105772433316425
f5bc7d3fd120284ffb79f723000d5e7b19107a02	False		9	920	3	70	5	134	4.3345250287437675
05b691a989ac88ddd8050155d0000ca2f48da04f	False		0	0	7	144	7	144	3.321928094887362
5e18f0838cc2d5bdd1b96091cd65a1b74821893c	False		3	319	6	98	6	98	3.1808329872054415
0f63d49026c30ff9631f4b0a4197e50336d82dab	False		9	2501	3	61	6	135	3.3371753411230776
ee64295e845dcff84dcbbdca894c895072e60fc8	False		0	0	1	22	1	22	2.699513850319966
39398e84e66d30566d3e64ed573beb4a52602874	False		0	0	2	74	2	74	3.7849418274376427
cc3b940fedf9217130102310de212702c7062f06	False		0	0	2	70	2	70	3.856196298219381
b8f525fcfea3d4b4023bd3308e85132f23dbc863	False		0	0	3	81	3	81	2.4193819456463714
0ff767cd6cf9d4e102c0de6bdac1fc2f0ee03af8	False		0	0	2	70	2	70	3.7821222241453065
fdbe85ac5a971af5e7bb3ded3c1416ebc7e74fe5	True	Geodo MITM	9	796	5	134	2	36	2.9219280948873623
39651dd1be23369f801b4779ac2d7db865e7a246	True	Quakbot C&C	8	573	3	64	1	22	3.521640636343319
0e44c7aaadd1186c17f4f1364e3722c172a7ce2e	True	Quakbot C&C	9	808	5	134	2	45	3.452819531114783
a6993c5dbdcddf56f22cef07b8916b150eefa309	True	Geodo MITM	9	798	5	134	2	37	3.0957952550009344
1e0a269dac505f8ac2fc13c2fb57d43be52b1728	True	Dridex C&C	3	213	3	64	3	64	2.985228136034252 5
7cfe275ceae4245c73e08763124d17ccaa19bf44	True	Vawtrak C&C	4	576	1	20	1	20	3.4182958340544896
21ac11e8f3cfcc86cf79d789e7451bdf95b5140a	True	TorrentLocker C&C	3	213	4	57	4	57	0
bc532d0559006d8989d667d5421a3b7a2bd913fb	True	Dridex C&C	3	213	3	61	3	61	3.6402239289418516
859d05bc51e253d6d28675630d1eac2f1e1ff4ae	True	Dridex C&C	3	322	6	101	6	101	3.039148671903071
1513e1070a6353408ccdf550f8cfb92829e2ce38	True	TorrentLocker C&C	3	213	3	58	3	58	0

Some quantitative features for supervised machine learning Models

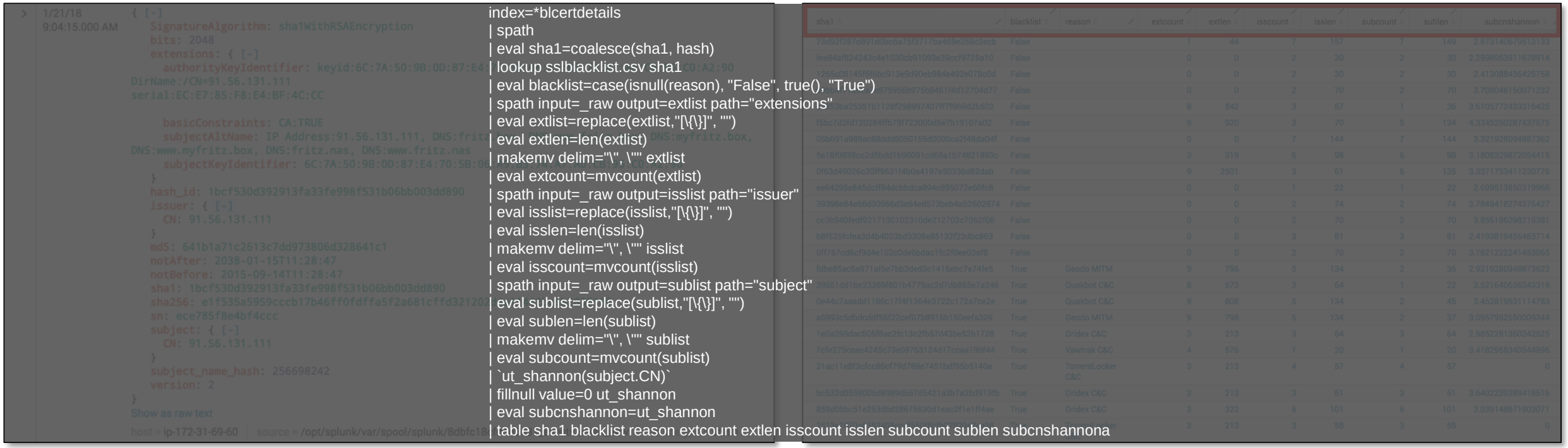
Features



Number of certificate extensions
Number of Issuer elements
Number of Subject elements
Length of Extensions
Length of Issuer
Length of Subject
Shannon Entropy of Subject Common Name

Surprisingly simple list of quantitative features

Features



Splunk search. Long but simple.

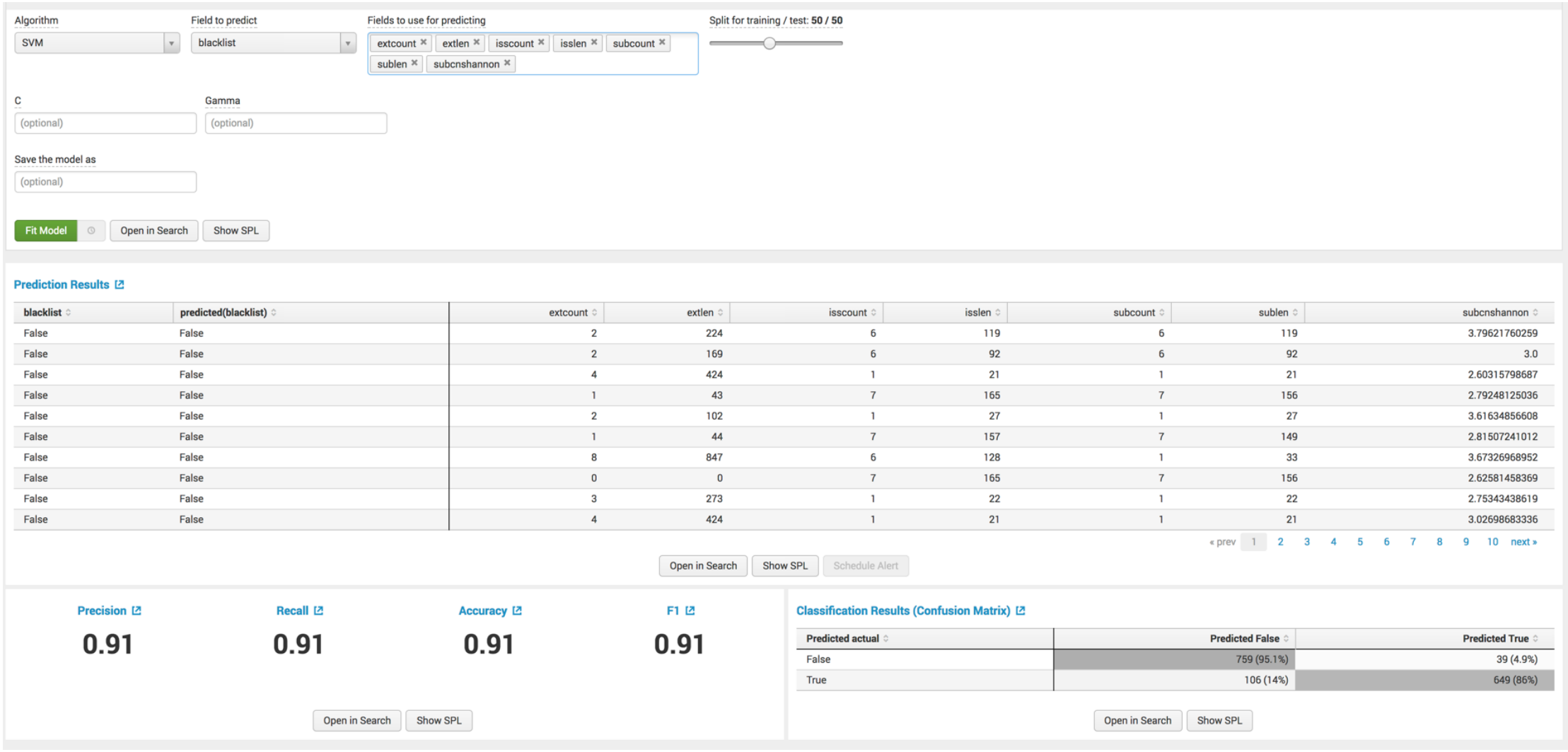
Select a model

Categorical Prediction Algorithm	Accuracy	FP Rate
Logistic Regression	0.75	24.90%
Support Vector Machine (SVM)	0.91	4.90%
Random Forest Classifier	0.91	8.10%
Gaussian Naive Bayes (GaussianNB)	0.71	18.40%
Decision Tree Classifier	0.91	9.80%

Select a model

Categorical Prediction Algorithm	Accuracy	FP Rate
Logistic Regression	0.75	24.90%
Support Vector Machine (SVM)	0.91	4.90%
Random Forest Classifier	0.91	8.10%
Gaussian Naive Bayes (GaussianNB)	0.71	18.40%
Decision Tree Classifier	0.91	9.80%

Build the Model



Apply the Model

Search | Showcase | Models | Assistants | Scheduled Jobs | Docs | Video Tutorials

New Search

```
earliest=0 index=sonarsslcert
| lookup sslblacklist.csv sha1
| search NOT reason=*
| eval sha1=coalesce(sha1, hash)
| lookup sslblacklist.csv sha1
| eval blacklist=case(isnull(reason), "False", true(), "True")
| search blacklist=False
| spath input=_raw output=extlist path="extensions"
| eval extlist=replace(extlist,"[\{\}]", "")
| eval extlen=len(extlist)
| makemv delim="\", \"" extlist
| eval extcount=mvcount(extlist)
| spath input=_raw output=isslist path="issuer"
| eval isslist=replace(isslist,"[\{\}]", "")
| eval isslen=len(isslist)
| makemv delim="\", \"" isslist
| eval isscount=mvcount(isslist)
| spath input=_raw output=sublist path="subject"
| eval sublist=replace(sublist,"[\{\}]", "")
| eval sublen=len(sublist)
| makemv delim="\", \"" sublist
| eval subcount=mvcount(sublist)
| `ut_shannon(subject.CN)`
| fillnull value=0 ut_shannon
| eval subcnshannon=ut_shannon
| table sha1 blacklist reason extcount extlen isscount isslen subcount sublen subcnshannon
| apply "BL_2018012301"
| search "predicted(blacklist)"=True
| table sha1 blacklist predicted(blacklist)
```

Apply to Sonar SSL Certificates

Events | Patterns | Statistics (6,866) | Visualization

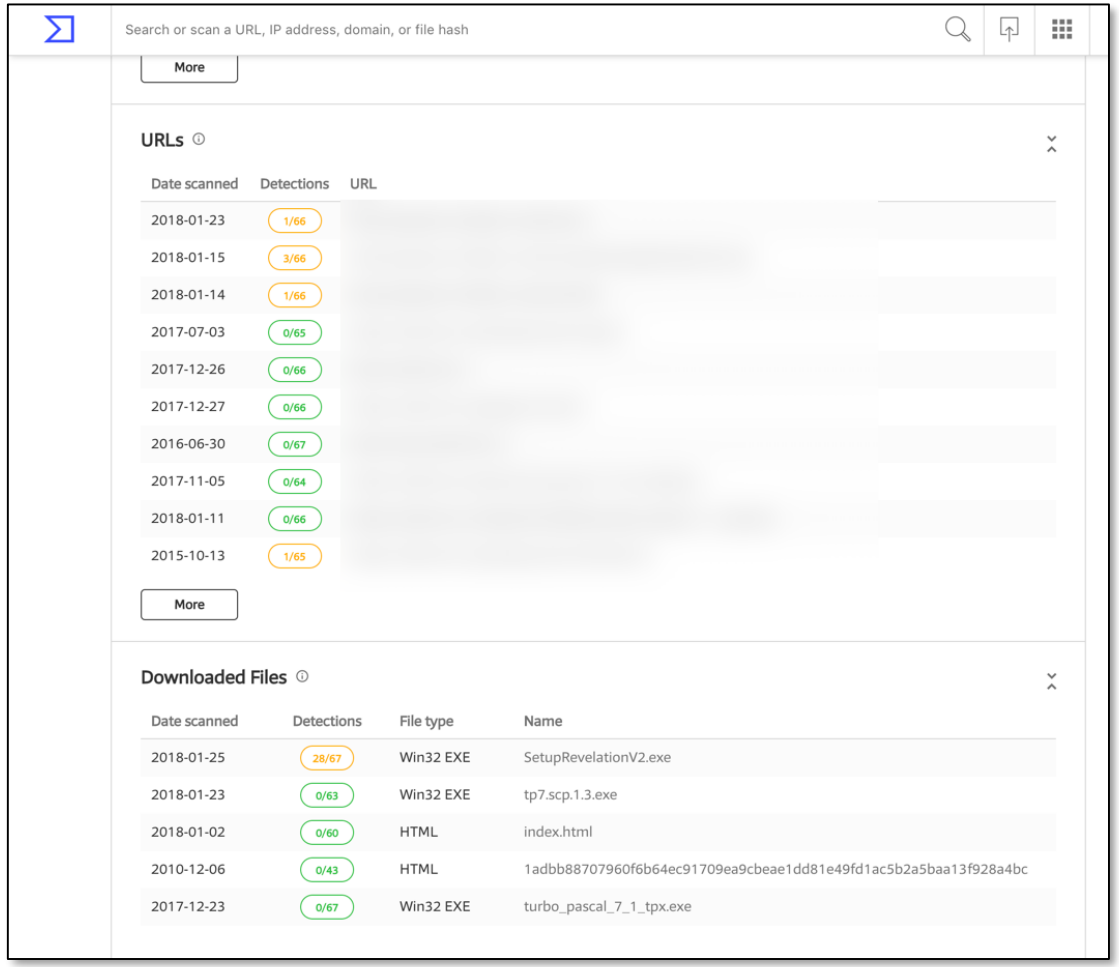
20 Per Page | Format | Preview

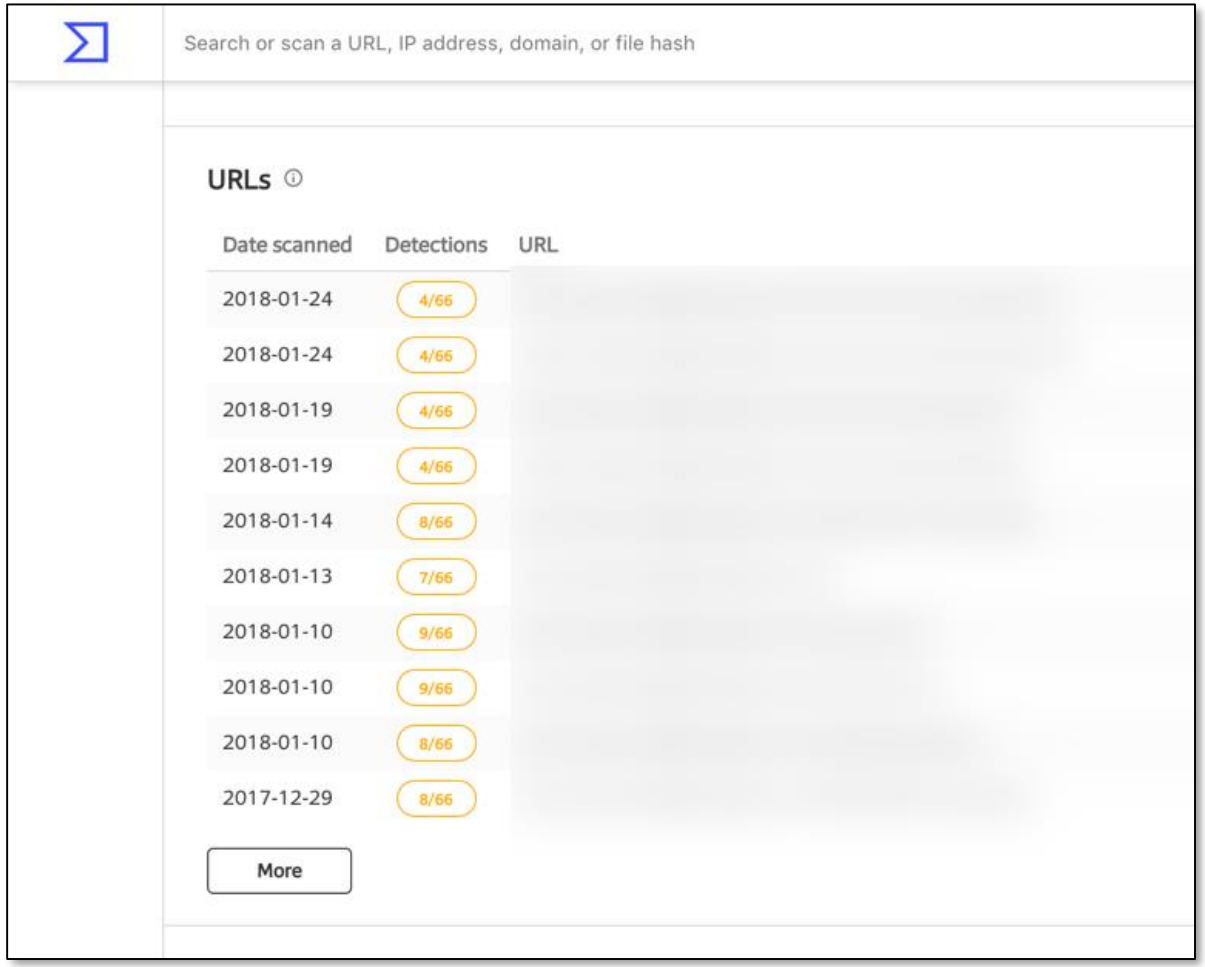
< Prev 1 2 3 4 5

sha1	blacklist	predicted
cd87440476139edb108b43b94ce955b6f1b90778	False	True
fbd2db181dd346e402e45b525c8f47d6bd179f76	False	True
e807e9a1feab8306a2e299795894b7b15bc7d78a	False	True
231fc07bee4707354ab5410376cbf55c8466abf4	False	True
fcfc61ecf230247de4656f5f899a2d09836780e0	False	True
fc2db1edf40ecd736de4f5e4579683b92fa220f8	False	True
67499304f3b00112e0f0b4d313c7d315e2f0e964	False	True
344e83f669766865457b006427be10dd1e3f6ee1	False	True
29abd09b20fa8dda3a863ab00a99f51a17234e2d	False	True
7867105a35ccd91c20b091df12ddca282730c247	False	True
3748e47e846781e3b93d27aaf47f9c62669e108a	False	True
96025b5f2208c3dc7c238db56579a3cf4b4ceaf7	False	True
072294d04e11183d9e51d49acca4e90dac7fc69b	False	True
4a98a3c9c0fa11cf0712ccb75402085f5c5e87f4	False	True
63cb21e72d21c16fe14c0d3f46791c3df9e995c7	False	True
23b447641d9d233c3dd4ba1acc85e36ad5e026af	False	True
80f6472643ca2aac43ff04611500b0bc4dd8b09d	False	True
af64a08b59669d9d38211ef668970aba9e969211	False	True
5696f345ffd9b272557f38801cf973085b6221d6	False	True
407c5e2eef8a7babe332e3c67f4405e445608264	False	True

Suspicious maybe…

Yes some are definitely bad…






And I care why?

Stop Hackers
In their tracks

SNAKE ML

Now with 100% more AI, Blockchain,
Algos, fairy dust, and Rob Lee Beard.

Based on child's ability.

E = Excellent
S = Satisfactory
I = Is Improving
N = Needs to Improve

Grade	Level
K	R
1	1,2, 3, 4, 5
2	6, 7
3	8, 9
4	10
5	11
6	12

Grade	Level
1	A
2	B
3	C
4	D
5	E
6	F

ACHIEVEMENT

√++ = 95-100 Excellent
√+ = 90-94 Very Good
√ = 80-89 Good
— = 70-79 Needs Improvement
F = 69 and below Failure

NAME Ryan Kovar GRADE 1

SCHOOL YEAR 1987-88 TEACHER'S NAME

SOCIAL GROWTH AND RESPONSIBILITIES

	1	2	3	4
1. Observes school and classroom rules	S	S	S	S
2. Works and plays well with others	S	S	S	S
3. Respects rights and property of others	S	S	S	S
4. Makes good use of time	N	I	I	S
5. Is courteous	S	S	S	S
6. Is self-controlled	S	S	S	S
7. Accepts suggestions in good spirits	S	S	S	S

	1	2	3	4
Listens to and follows directions	S	S	S	S
Completes work promptly	S	S	S	S
Works accurately	N	I	I	I
Shows initiative	N	S	S-	S
Listens to and follows directions	S	S	S	S
Shows initiative	S	S	S	S
Listens to and follows directions	S	S	S	S
Shows initiative	S	S	S	S
Listens to and follows directions	S	S	S	S
Shows initiative	N	S	S	S
		S	S	S
	S	E	E	S
	S	E	S	S
	S	S	S	S

	1	2	3	4
Reading Mark	√	√	√	√
Teacher Level	1	2	3	4
Math Mark	√	—	F	—
Science Mark				
Social Studies Mark	√	√	√	√
Spelling Mark	—	√	√+	√
Level				
Art Sakeim Teacher		√	√	√
Vocal Music Wilson Teacher	√	√+	√+	√
Physical Education Amador Teacher	√+	√+	√+	√+
Library	S	S	S	S

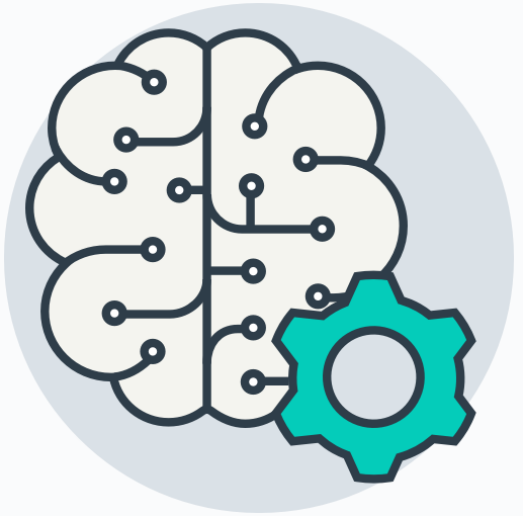
Math Mark √ — F —

3		4-22- Requested of Mrs Sch that I be better inform of Ry's progress-or lack o in MATH. She has
4	I hope Ryan will improve his work habits. After he is mentally alert to the readiness skills that are not knowing I hope he will continue to practice his number facts over the summer.	agreed to do this. I will be tutoring h at home and expe to see a di Feren

Machine learning can help add context to events

+

+



=

Machine learning can help reduce your dataset...

…So you can find your bears

Machine learning doesn't solve cyber... But it can help ;-)


Oh… Just one more thing…

Certificate Research Platform Resources

https://www.slideshare.net/RyanKovar/hidden-empires-of-malware

- How to build an SSL hunting platform with Splunk

https://github.com/daveherrald/scansio-sonar-splunk

- Download any scans.io study, load sonar.ssl & sonar.https into Splunk for analysis

https://github.com/mpars0ns/scansio-sonar-es

- Download sonar.ssl load into Elasticsearch


Can we wrap this up?

Conclusion

- SSL certificates can be a great way to track adversary behavior
- Consider tracking from known and unknown
- Machine Learning can help add context and reduce datasets

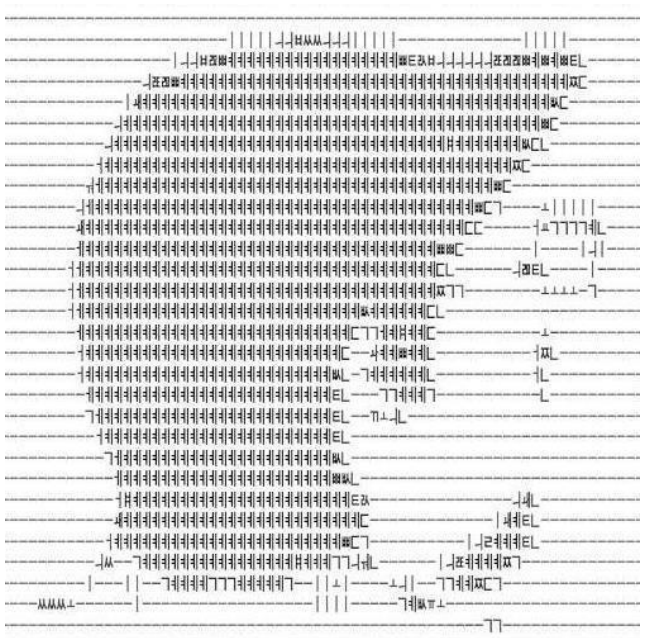
Special Thanks

- Mark Parsons
- IKBD
- Rapid 7
- Censys team at University of Michigan
- John Lankau and Lauren Deason @ PunchCyber

Contact info

Dave Herrald

@daveherrald



Ryan Kovar

@meansec