stoQ’ing your Splunk

Ryan Kovar, Splunk
Marcus LaFerrera, PUNCH

SANS DFIR 2016

splunk>

Ryan Kovar

- Staff Security Strategist @Splunk
- Does Security things and then talks about them
- 17+ years defending networks

PUNCH

Marcus LaFerrera

- Director of Development @PUNCH
- Lead stoQ Developer
- 18+ years supporting the government

Agenda

- Overview of stoQ
- Overview of Splunk
- A DFIR use case walk through
- Questions

TOOL * N == :(

NOTHING COMMUNICATES
AND MOST TOOLS
REQUIRE MANUAL INTERACTION

HOW’S THE WEATHER OUT THERE OLLIE?

IT’S CYBER

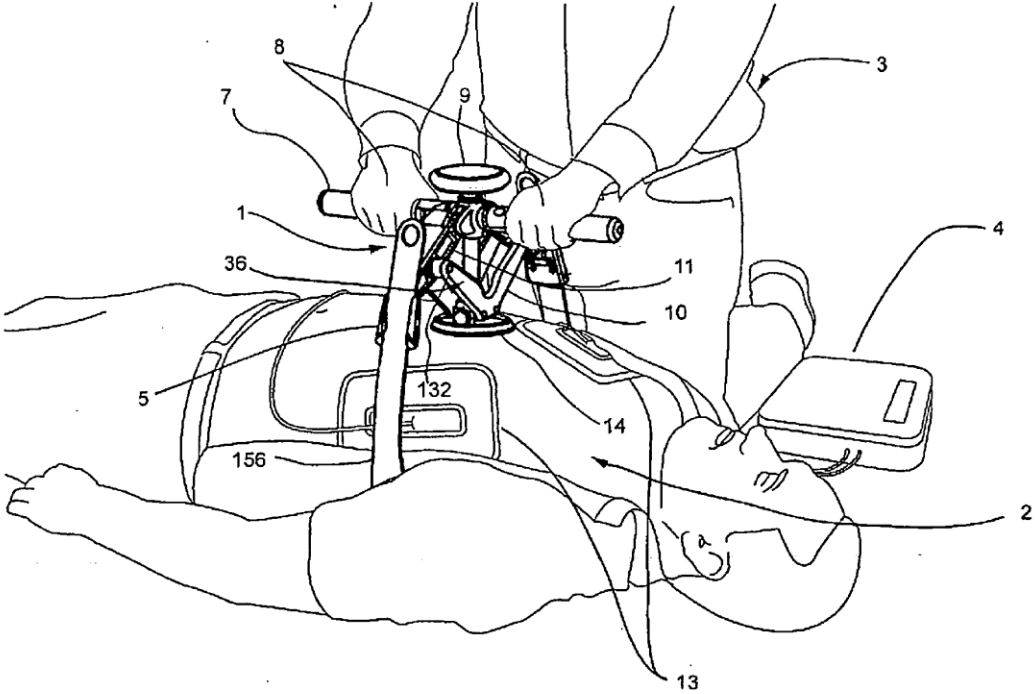
stoQ

STOQ IS A FRAMEWORK THAT ENABLES **EVERYONE** TO AUTOMATE PROCESSES, ANALYTICS, AND JUST ABOUT **ANYTHING** ELSE

AUTOMATE AND REDUCE THE MAJORITY OF YOUR MOST MUNDANE ANALYTIC TASKS

LEVERAGE ALL OF YOUR TOOLS SIMULTANEOUSLY, AND SAVE THOSE RESULTS FOR LATER

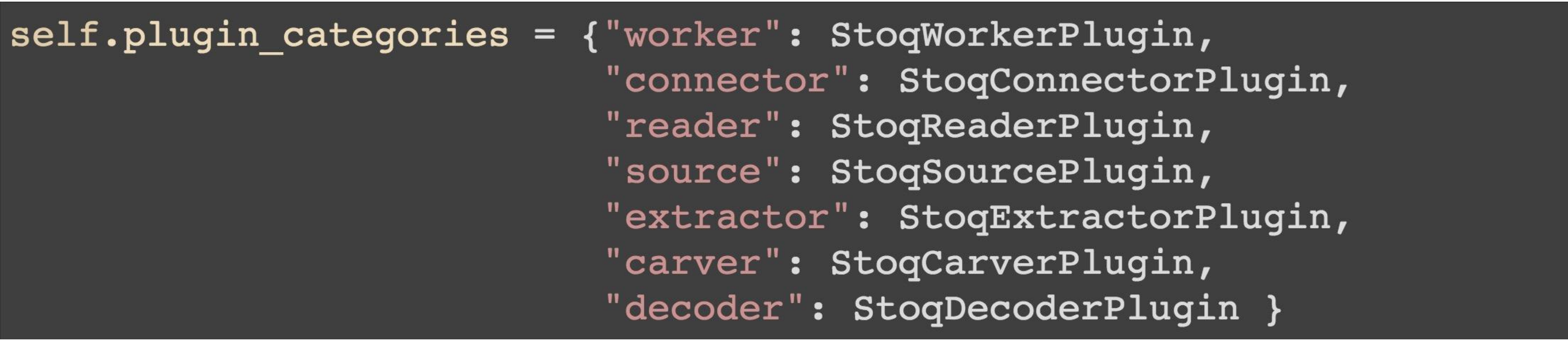
IT’S A FORCE MULTIPLIER



LOOK AT YOUR DATA, RATHER THAN SEEKING WAYS TO CAPTURE OR PRODUCE IT

COMMAND LINE, INTERACTIVE SHELL, OR FULLY AUTOMATED

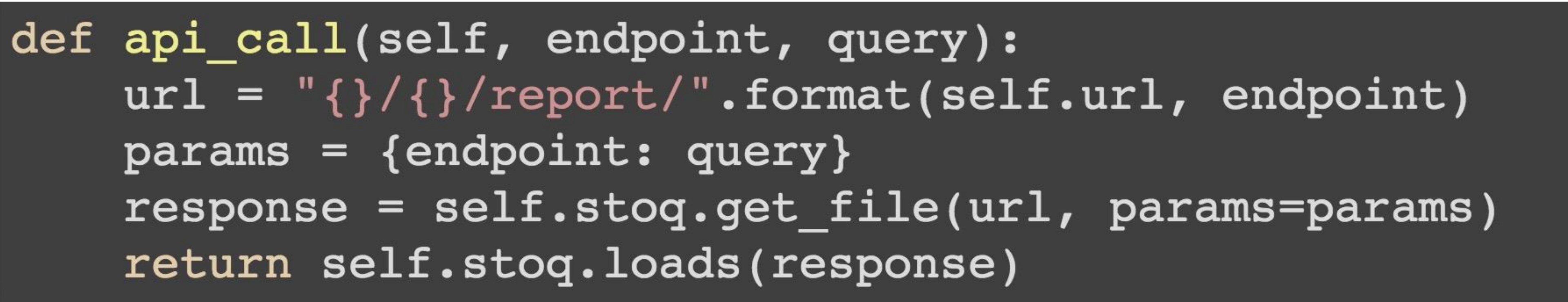
EVERYTHING IS A PLUGIN, FROM INPUT TO OUTPUT AND EVERYTHING IN BETWEEN



```
self.plugin_categories = {"worker": StoqWorkerPlugin,
                          "connector": StoqConnectorPlugin,
                          "reader": StoqReaderPlugin,
                          "source": StoqSourcePlugin,
                          "extractor": StoqExtractorPlugin,
                          "carver": StoqCarverPlugin,
                          "decoder": StoqDecoderPlugin }
```

Tell me more about Plugins...

- Very simple and easy to write
- Lots of documentation and examples
- stoQ does most of the heavy lifting

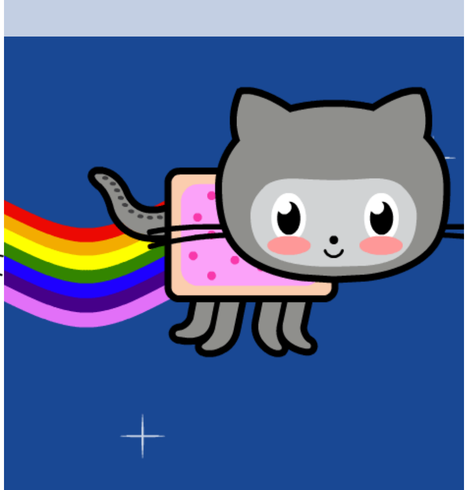


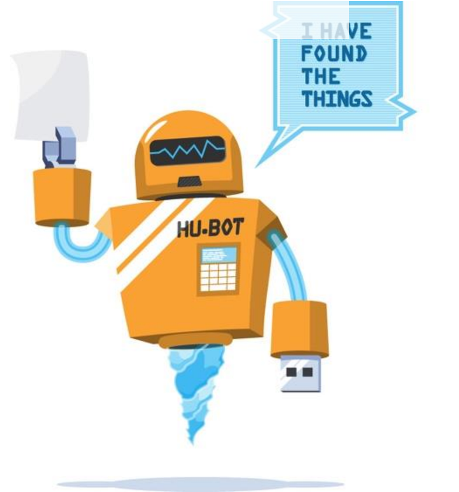
```
def api_call(self, endpoint, query):
    url = "{}/{}/report/".format(self.url, endpoint)
    params = {endpoint: query}
    response = self.stoq.get_file(url, params=params)
    return self.stoq.loads(response)
```

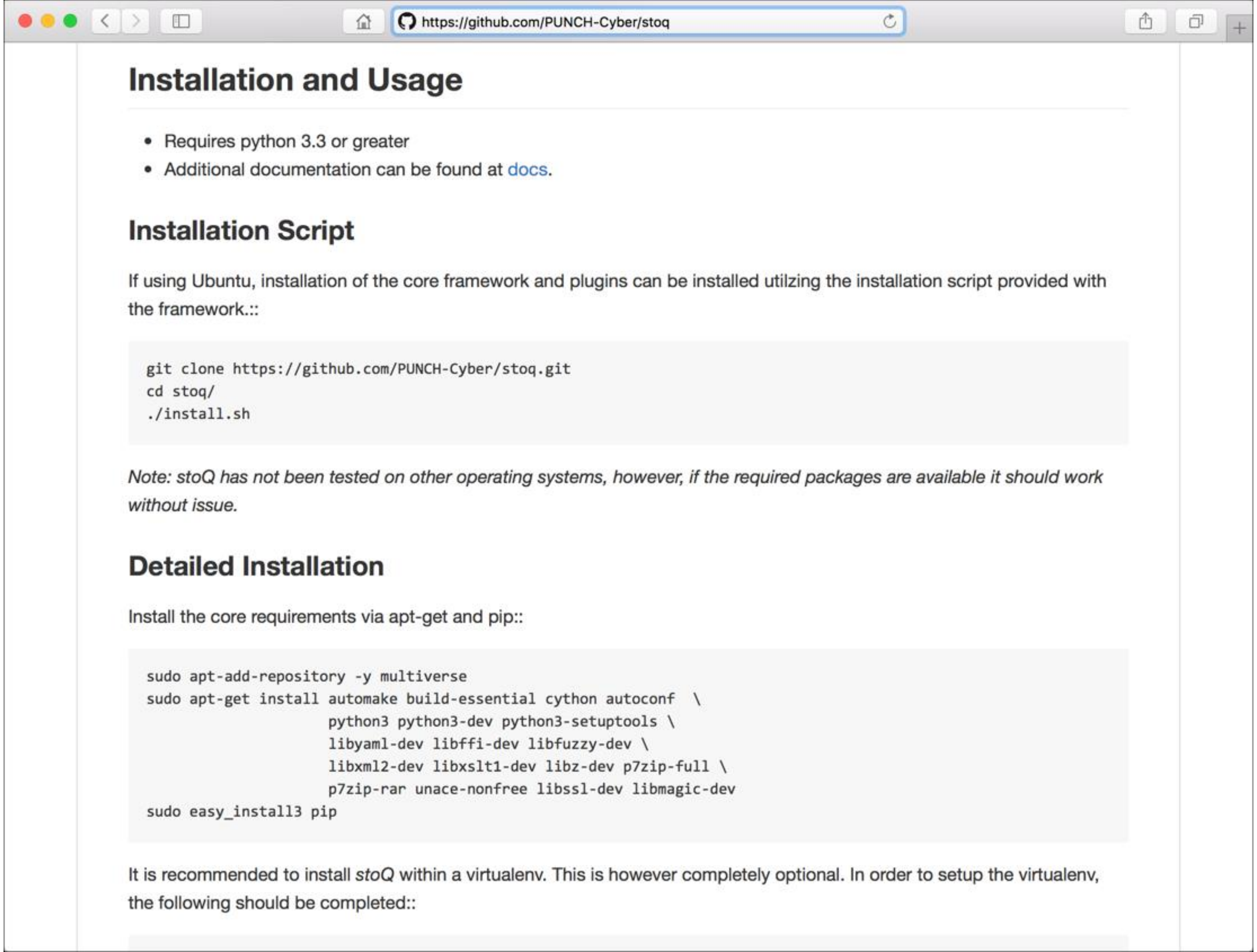
Over 40 stoQ Plugins Available

- E-mail Parser
- **VTMIS**
- TotalHash
- **Yara**
- Censys
- Fireeye
- IOC Extract
- Pastebin
- PassiveTotal
- ClamAV
- Opswat
- **TRiD**
- RabbitMQ
- Suricata
- Tika
- **PEinfo**
- Excel
- XOR
- Base64
- Bit Rotation
- Bro Intel
- Fluentd
- Google Cloud Storage
- Amazon S3
- Slack
- ThreatCrowd
- MongoDB
- ElasticSearch
- **Exif**
- And many more…

IT’S OPENSOURCED







Installation and Usage

- Requires python 3.3 or greater
- Additional documentation can be found at docs.

Installation Script

If using Ubuntu, installation of the core framework and plugins can be installed utilzing the installation script provided with the framework.::

```
git clone https://github.com/PUNCH-Cyber/stoq.git
cd stoq/
./install.sh
```

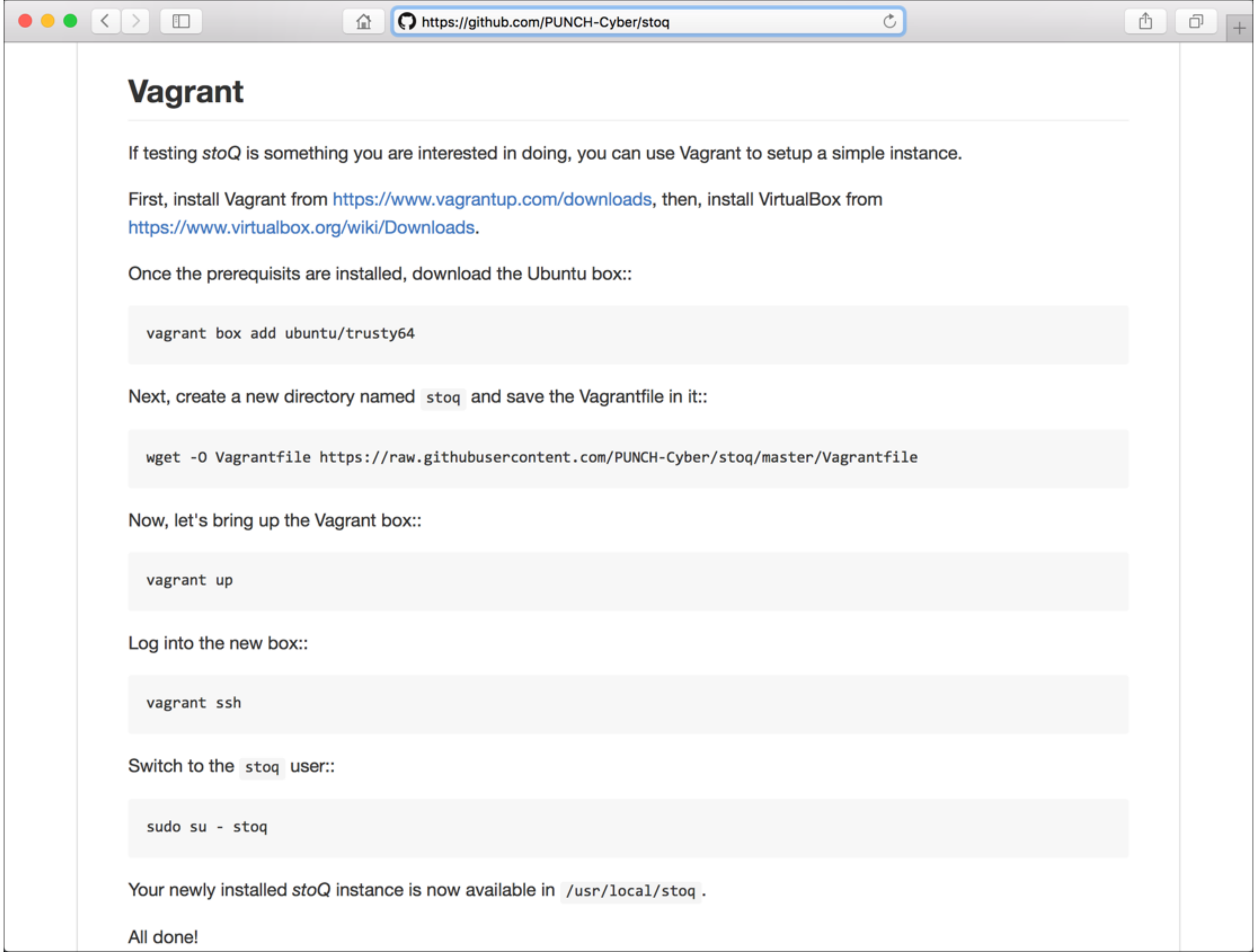
Note: stoQ has not been tested on other operating systems, however, if the required packages are available it should work without issue.

Detailed Installation

Install the core requirements via apt-get and pip::

```
sudo apt-add-repository -y multiverse
sudo apt-get install automake build-essential cython autoconf  \
                     python3 python3-dev python3-setuptools \
                     libyaml-dev libffi-dev libfuzzy-dev \
                     libxml2-dev libxslt1-dev libz-dev p7zip-full \
                     p7zip-rar unace-nonfree libssl-dev libmagic-dev
sudo easy_install3 pip
```

It is recommended to install *stoQ* within a virtualenv. This is however completely optional. In order to setup the virtualenv, the following should be completed::



Vagrant

If testing *stoQ* is something you are interested in doing, you can use Vagrant to setup a simple instance.

First, install Vagrant from https://www.vagrantup.com/downloads, then, install VirtualBox from https://www.virtualbox.org/wiki/Downloads.

Once the prerequisits are installed, download the Ubuntu box::

```
vagrant box add ubuntu/trusty64
```

Next, create a new directory named `stoq` and save the Vagrantfile in it::

```
wget -O Vagrantfile https://raw.githubusercontent.com/PUNCH-Cyber/stoq/master/Vagrantfile
```

Now, let's bring up the Vagrant box::

```
vagrant up
```

Log into the new box::

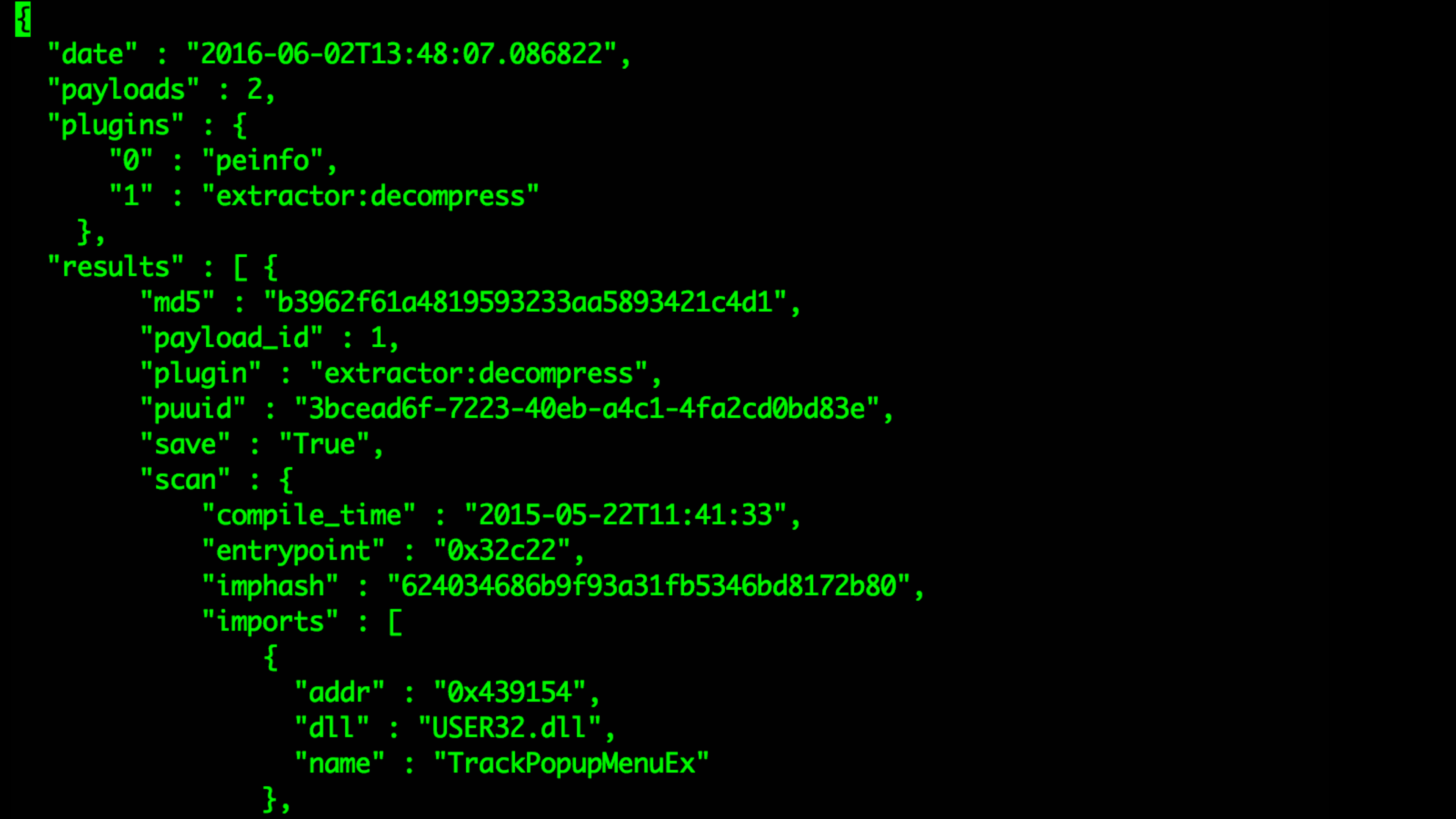
```
vagrant ssh
```

Switch to the `stoq` user::

```
sudo su - stoq
```

Your newly installed *stoQ* instance is now available in `/usr/local/stoq` .

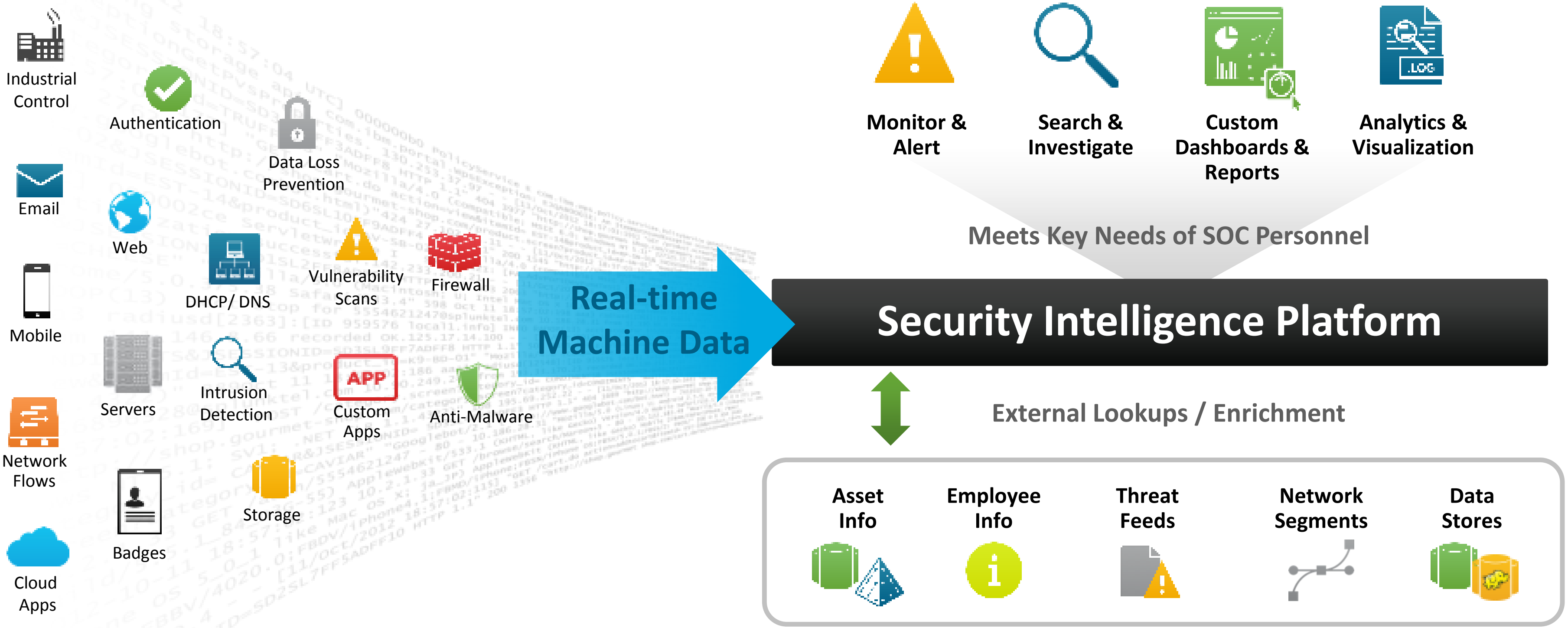
All done!



```
{
  "date" : "2016-06-02T13:48:07.086822",
  "payloads" : 2,
  "plugins" : {
      "0" : "peinfo",
      "1" : "extractor:decompress"
    },
  "results" : [ {
        "md5" : "b3962f61a4819593233aa5893421c4d1",
        "payload_id" : 1,
        "plugin" : "extractor:decompress",
        "puuid" : "3bcead6f-7223-40eb-a4c1-4fa2cd0bd83e",
        "save" : "True",
        "scan" : {
            "compile_time" : "2015-05-22T11:41:33",
            "entrypoint" : "0x32c22",
            "imphash" : "624034686b9f93a31fb5346bd8172b80",
            "imports" : [
                {
                  "addr" : "0x439154",
                  "dll" : "USER32.dll",
                  "name" : "TrackPopupMenuEx"
                },
```

splunk®>enterprise

Splunk Can Ingest ALL THE DATA



Industrial Control

Authentication

Data Loss Prevention

Email

Web

Mobile

DHCP/ DNS

Vulnerability Scans

Firewall

Servers

Intrusion Detection

Custom Apps

Anti-Malware

Network Flows

Badges

Storage

Cloud Apps

Real-time Machine Data

Monitor & Alert

Search & Investigate

Custom Dashboards & Reports

Analytics & Visualization

Meets Key Needs of SOC Personnel

Security Intelligence Platform

External Lookups / Enrichment

Asset Info

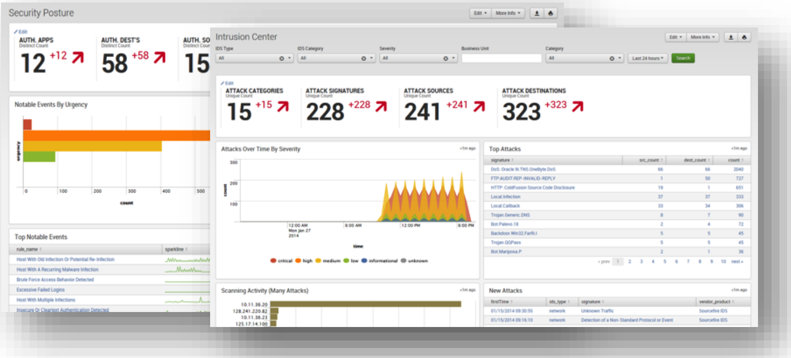
Employee Info

Threat Feeds

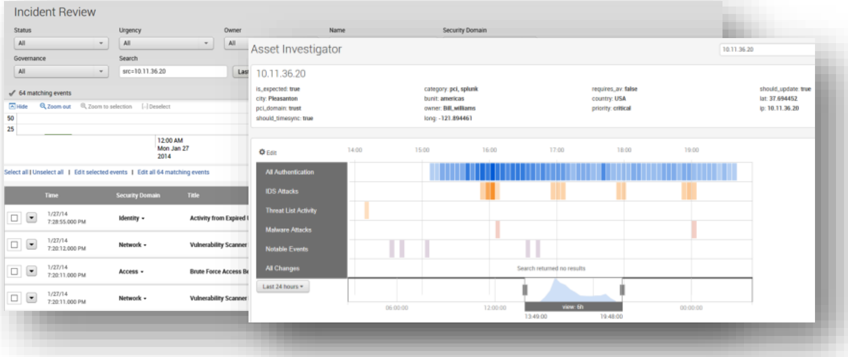
Network Segments

Data Stores

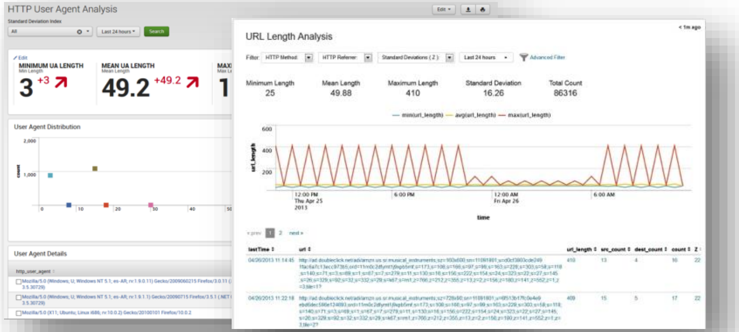
Then Build Security Dashboards



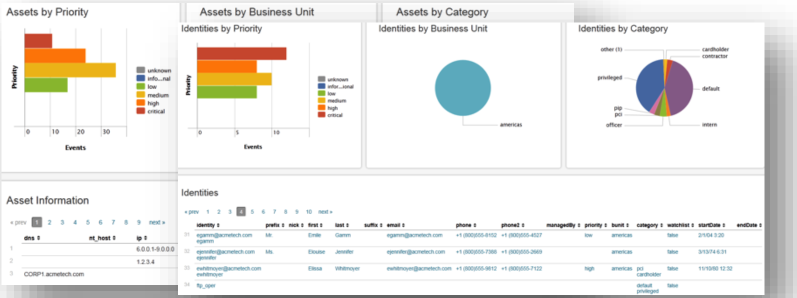
Dashboards and Reports



Incident Investigations & Management



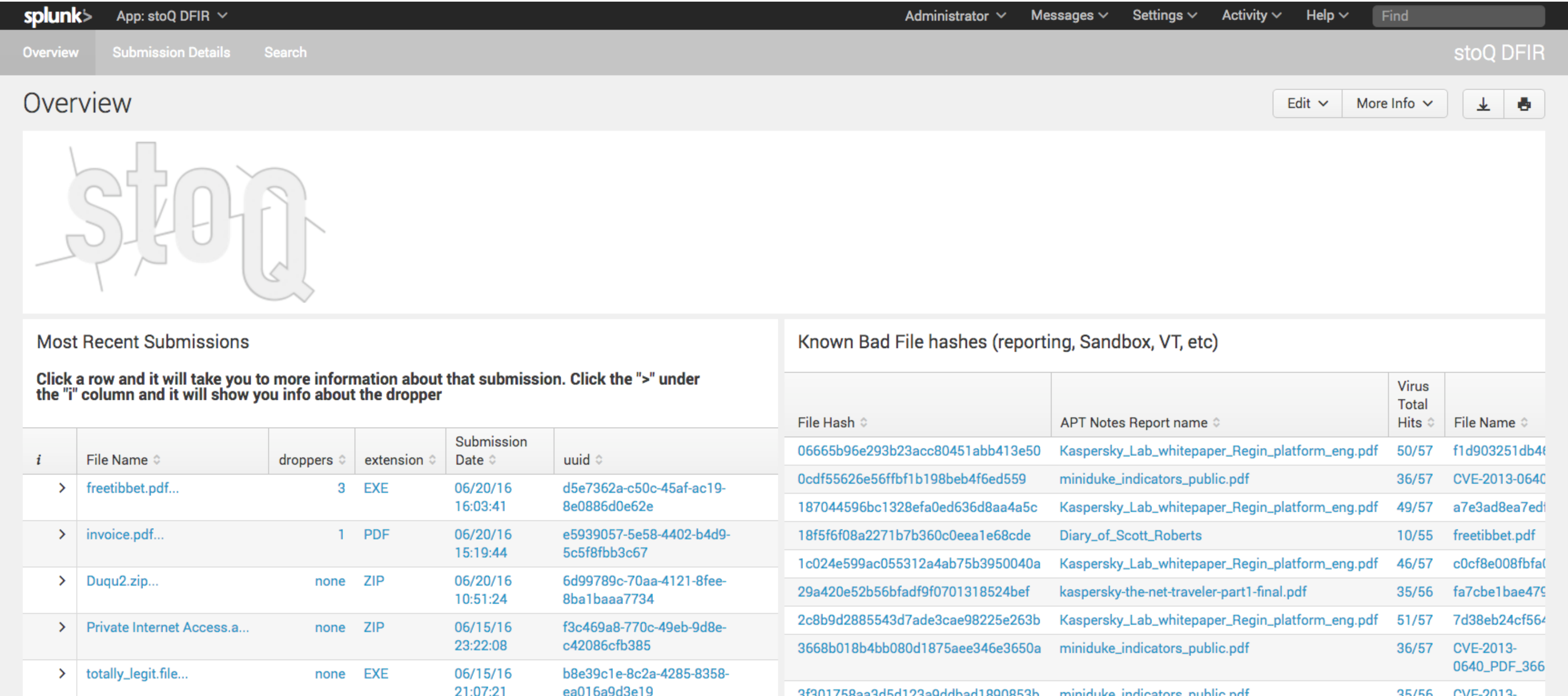
Statistical Outliers



Asset and Identity Aware

By These Tools Combined…

The Splunk App for stoQ



Overview

Most Recent Submissions

Click a row and it will take you to more information about that submission. Click the ">" under the "i" column and it will show you info about the dropper

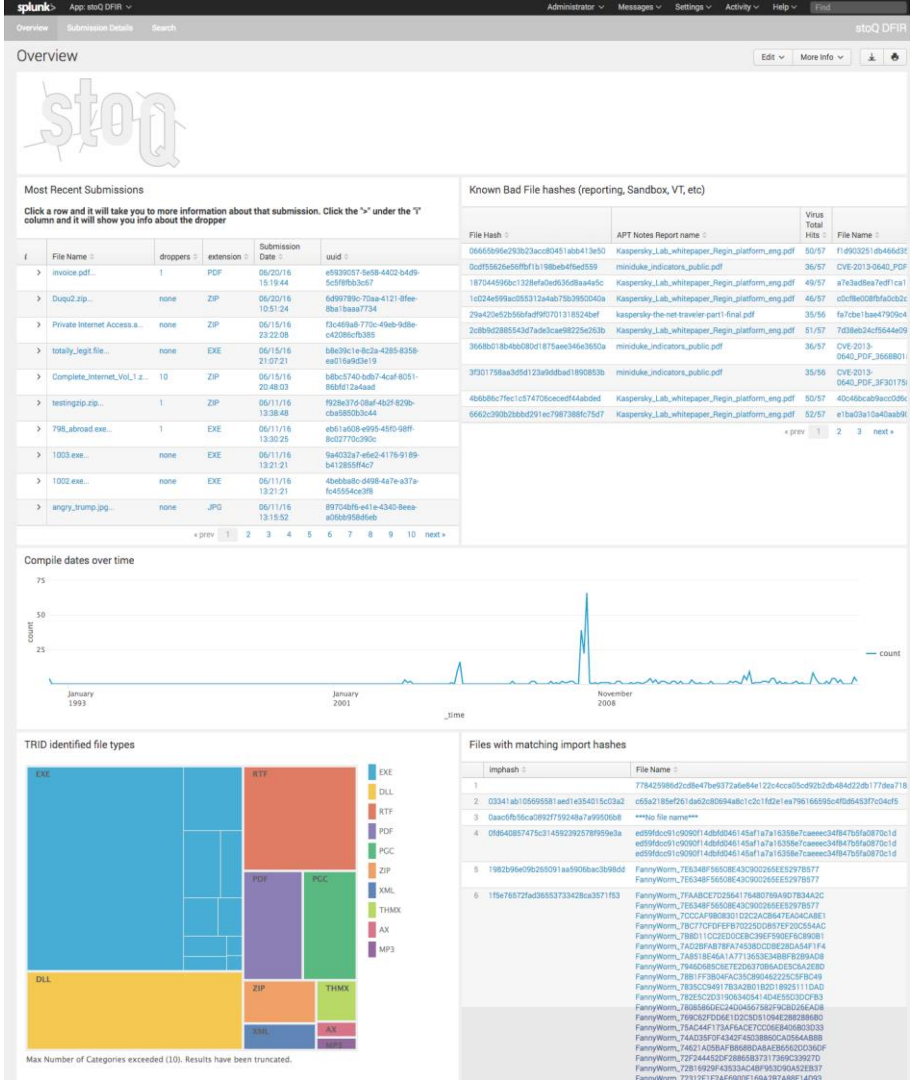
i	File Name	droppers	extension	Submission Date	uuid
>	freetibbet.pdf...	3	EXE	06/20/16 16:03:41	d5e7362a-c50c-45af-ac19-8e0886d0e62e
>	invoice.pdf...	1	PDF	06/20/16 15:19:44	e5939057-5e58-4402-b4d9-5c5f8fbb3c67
>	Duqu2.zip...	none	ZIP	06/20/16 10:51:24	6d99789c-70aa-4121-8fee-8ba1baaa7734
>	Private Internet Access.a...	none	ZIP	06/15/16 23:22:08	f3c469a8-770c-49eb-9d8e-c42086cfb385
>	totally_legit.file...	none	EXE	06/15/16 21:07:21	b8e39c1e-8c2a-4285-8358-ea016a9d3e19

Known Bad File hashes (reporting, Sandbox, VT, etc)

File Hash	APT Notes Report name	Virus Total Hits	File Name
06665b96e293b23acc80451abb413e50	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	50/57	f1d903251db4
0cdf55626e56ffbf1b198beb4f6ed559	miniduke_indicators_public.pdf	36/57	CVE-2013-064
187044596bc1328efa0ed636d8aa4a5c	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	49/57	a7e3ad8ea7ed
18f5f6f08a2271b7b360c0eea1e68cde	Diary_of_Scott_Roberts	10/55	freetibbet.pdf
1c024e599ac055312a4ab75b3950040a	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	46/57	c0cf8e008fbfa
29a420e52b56bfadf9f0701318524bef	kaspersky-the-net-traveler-part1-final.pdf	35/56	fa7cbe1bae47
2c8b9d2885543d7ade3cae98225e263b	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	51/57	7d38eb24cf56
3668b018b4bb080d1875aee346e3650a	miniduke_indicators_public.pdf	36/57	CVE-2013-0640_PDF_366
3f301758aa3d5d123a9ddbad1890853b	miniduke_indicators_public.pdf	35/56	CVE-2013-

THE STOQ DFIR APP FOR SPLUNK!

- ALLOWS YOU TO VISUALIZE STOQ RESULTS
- MAKE CONNECTIONS THAT WERE DIFFICULT TO SEE BEFORE
- QUICKLY PIVOT TO NEW DATA SOURCES
- APPLY THREAT INTELLIGENCE TO STOQ DATA



Most Recent Submissions

Click a row and it will take you to more information about that submission. Click the ">" under the "i" column and it will show you info about the dropper

i	File Name	droppers	extension	Submission Date	uuid
>	invoice.pdf...	1	PDF	06/20/16 15:19:44	e5939057-5e58-4402-b4d9-5c5f8fbb3c67
>	Duqu2.zip...	none	ZIP	06/20/16 10:51:24	6d99789c-70aa-4121-8fee-8ba1baaa7734
>	Private Internet Access.a...	none	ZIP	06/15/16 23:22:08	f3c469a8-770c-49eb-9d8e-c42086cfb385
>	totally_legit.file...	none	EXE	06/15/16 21:07:21	b8e39c1e-8c2a-4285-8358-ea016a9d3e19
>	Complete_Internet_Vol_1.z...	10	ZIP	06/15/16 20:48:03	b8bc5740-bdb7-4caf-8051-86bfd12a4aad
>	testingzip.zip...	1	ZIP	06/11/16 13:38:48	f928e37d-08af-4b2f-829b-cba5850b3c44
>	798_abroad.exe...	1	EXE	06/11/16 13:30:25	eb61a608-e995-45f0-98ff-8c02770c390c
>	1003.exe...	none	EXE	06/11/16 13:21:21	9a4032a7-e6e2-4176-9189-b412855ff4c7
>	1002.exe...	none	EXE	06/11/16 13:21:21	4bebba8c-d498-4a7e-a37a-fc45554ce3f8
>	angry_trump.jpg...	none	JPG	06/11/16 13:15:52	89704bf6-e41e-4340-8eea-a06bb958d6eb

« prev 1 2 3 4 5 6 7 8 9 10 next »

Known Bad File hashes (reporting, Sandbox, VT, etc)

File Hash	APT Notes Report name	Virus Total Hits	File Name
06665b96e293b23acc80451abb413e50	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	50/57	f1d903251db466d35
0cdf55626e56ffbf1b198beb4f6ed559	miniduke_indicators_public.pdf	36/57	CVE-2013-0640_PDF
187044596bc1328efa0ed636d8aa4a5c	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	49/57	a7e3ad8ea7edf1ca1
1c024e599ac055312a4ab75b3950040a	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	46/57	c0cf8e008fbfa0cb2c
29a420e52b56bfadf9f0701318524bef	kaspersky-the-net-traveler-part1-final.pdf	35/56	fa7cbe1bae47909c4
2c8b9d2885543d7ade3cae98225e263b	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	51/57	7d38eb24cf5644e09
3668b018b4bb080d1875aee346e3650a	miniduke_indicators_public.pdf	36/57	CVE-2013-0640_PDF_3668B01
3f301758aa3d5d123a9ddbad1890853b	miniduke_indicators_public.pdf	35/56	CVE-2013-0640_PDF_3F30175
4b6b86c7fec1c574706cecedf44abded	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	50/57	40c46bcab9acc0d6c
6662c390b2bbbd291ec7987388fc75d7	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	52/57	e1ba03a10a40aab90

« prev 1 2 3 next »

Compile dates over time

TRID identified file types

Max Number of Categories exceeded (10). Results have been truncated.

Files with matching import hashes

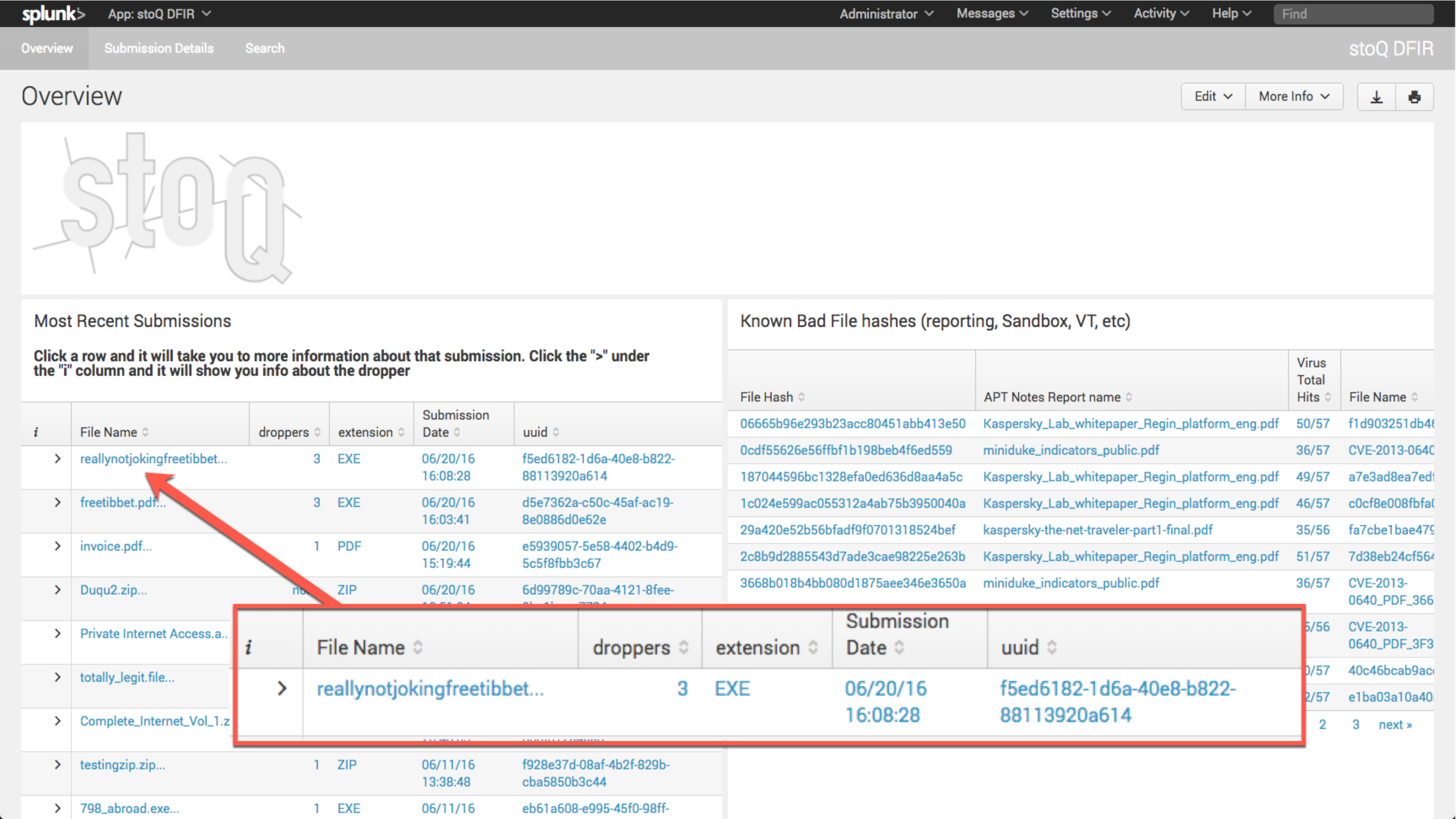
	imphash	File Name
1		778425986d2cd8e47be9372a6e84e122c4cca05cd92b2db484d22db177dea718
2	03341ab105695581aed1e354015c03a2	c65a2185ef261da62c80694a8c1c2c1fd2e1ea796166595c4f0d6453f7c04cf5
3	0aac6fb56ca0892f759248a7a99506b8	***No file name***
4	0fd640857475c314592392578f959e3a	ed59fdcc91c9090f14dbfd046145af1a7a16358e7caeeec34f847b5fa0870c1d ed59fdcc91c9090f14dbfd046145af1a7a16358e7caeeec34f847b5fa0870c1d ed59fdcc91c9090f14dbfd046145af1a7a16358e7caeeec34f847b5fa0870c1d
5	1982b96e09b265091aa5906bac3b98dd	FannyWorm_7E6348F56508E43C900265EE5297B577 FannyWorm_7E6348F56508E43C900265EE5297B577
6	1f5e76572fad36553733428ca3571f53	FannyWorm_7FAABCE7D2564176480769A9D7B34A2C FannyWorm_7E6348F56508E43C900265EE5297B577 FannyWorm_7CCCAF9B08301D2C2ACB647EA04CA8E1 FannyWorm_7BC77CFDFEFB70225DDB57EF20C554AC FannyWorm_7B8D11CC2ED0CEBC39EF590EF6C890B1 FannyWorm_7AD2BFAB78FA74538DCDBE28DA54F1F4 FannyWorm_7A8518E46A1A7713653E34B8FB289AD8 FannyWorm_7946D685C6E7E2D6370B6ADE5C6A2EBD FannyWorm_78B1FF3B04FAC35C890462225C5FBC49 FannyWorm_7835CC94917B3A2B01B2D18925111DAD FannyWorm_782E5C2D319063405414D4E55D3DCFB3 FannyWorm_7808586DEC24D04567582F9CBD26EAD8 FannyWorm_769C62FDD6E1D2C5D51094E2882886B0 FannyWorm_75AC44F173AF6ACE7CC06E8406B03D33 FannyWorm_74AD35F0F4342F45038860CA0564AB8B FannyWorm_74621A05BAFB8688DA8AEB6562DD36DF FannyWorm_72F244452DF28865B37317369C33927D FannyWorm_72B16929F43533AC48F953D90A52EB37 FannyWorm_72312E1F2AE6900E169A287A88E14D93

A DFIR Scenario

You are an analyst at a Fortune 100 company

A user reports an email with a suspicious attachment

We need to quickly identify if the file is good or bad



Overview

Most Recent Submissions

Click a row and it will take you to more information about that submission. Click the ">" under the "i" column and it will show you info about the dropper

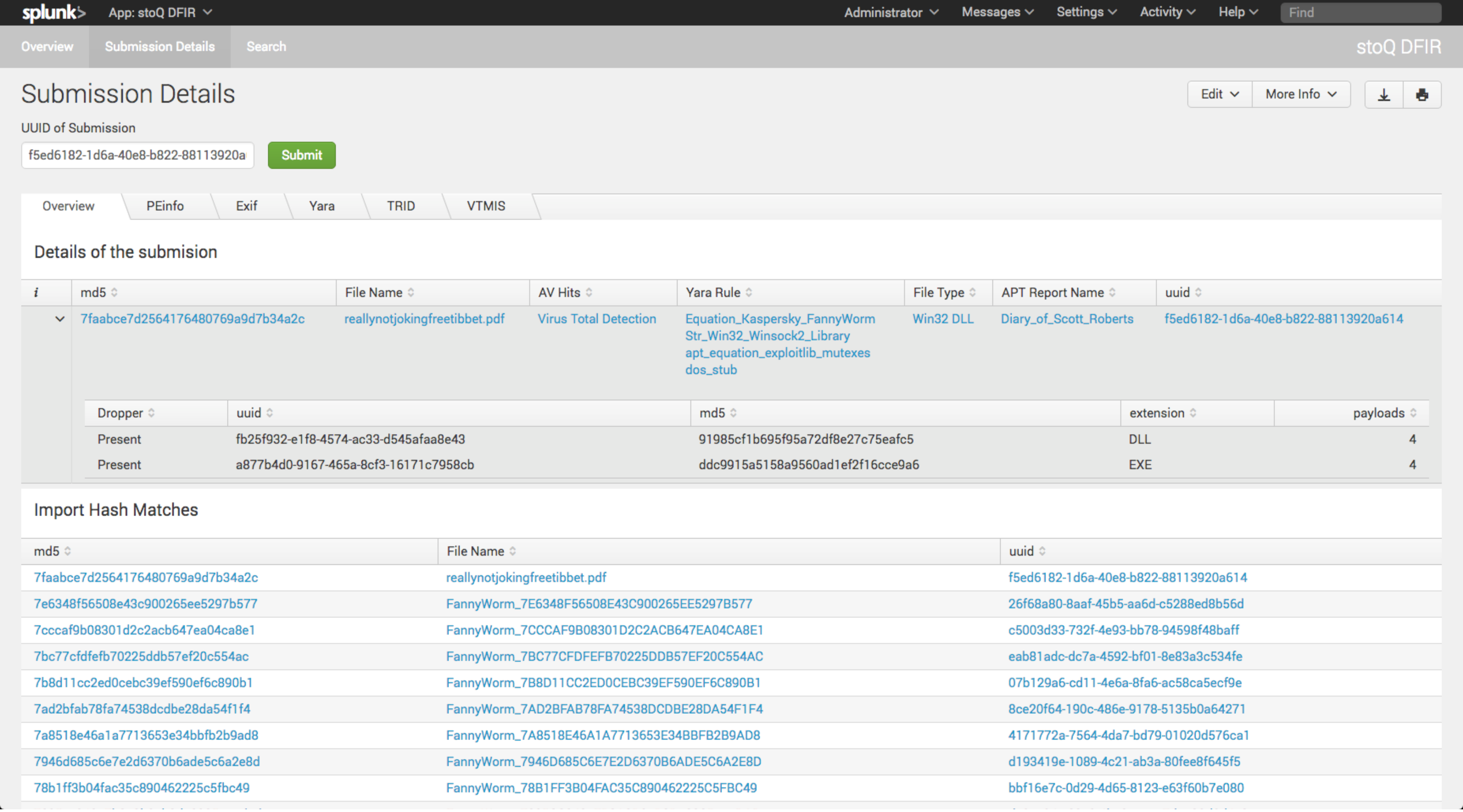
i	File Name	droppers	extension	Submission Date	uuid
>	reallynotjokingfreetibbet...	3	EXE	06/20/16 16:08:28	f5ed6182-1d6a-40e8-b822-88113920a614
>	freetibbet.pdf...	3	EXE	06/20/16 16:03:41	d5e7362a-c50c-45af-ac19-8e0886d0e62e
>	invoice.pdf...	1	PDF	06/20/16 15:19:44	e5939057-5e58-4402-b4d9-5c5f8fbb3c67
>	Duqu2.zip...	no	ZIP	06/20/16	6d99789c-70aa-4121-8fee-
>	Private Internet Access.a...				
>	totally_legit.file...				
>	Complete_Internet_Vol_1.z				
>	testingzip.zip...	1	ZIP	06/11/16 13:38:48	f928e37d-08af-4b2f-829b-cba5850b3c44
>	798_abroad.exe...	1	EXE	06/11/16	eb61a608-e995-45f0-98ff-

i	File Name	droppers	extension	Submission Date	uuid
>	reallynotjokingfreetibbet...	3	EXE	06/20/16 16:08:28	f5ed6182-1d6a-40e8-b822-88113920a614

Known Bad File hashes (reporting, Sandbox, VT, etc)

File Hash	APT Notes Report name	Virus Total Hits	File Name
06665b96e293b23acc80451abb413e50	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	50/57	f1d903251db4
0cdf55626e56ffbf1b198beb4f6ed559	miniduke_indicators_public.pdf	36/57	CVE-2013-0640
187044596bc1328efa0ed636d8aa4a5c	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	49/57	a7e3ad8ea7ed
1c024e599ac055312a4ab75b3950040a	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	46/57	c0cf8e008fbfa
29a420e52b56bfadf9f0701318524bef	kaspersky-the-net-traveler-part1-final.pdf	35/56	fa7cbe1bae47
2c8b9d2885543d7ade3cae98225e263b	Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf	51/57	7d38eb24cf56
3668b018b4bb080d1875aee346e3650a	miniduke_indicators_public.pdf	36/57	CVE-2013-0640_PDF_366
		5/56	CVE-2013-0640_PDF_3F3
		0/57	40c46bcab9ac
		2/57	e1ba03a10a40

2 3 next »



Submission Details

UUID of Submission: f5ed6182-1d6a-40e8-b822-88113920a

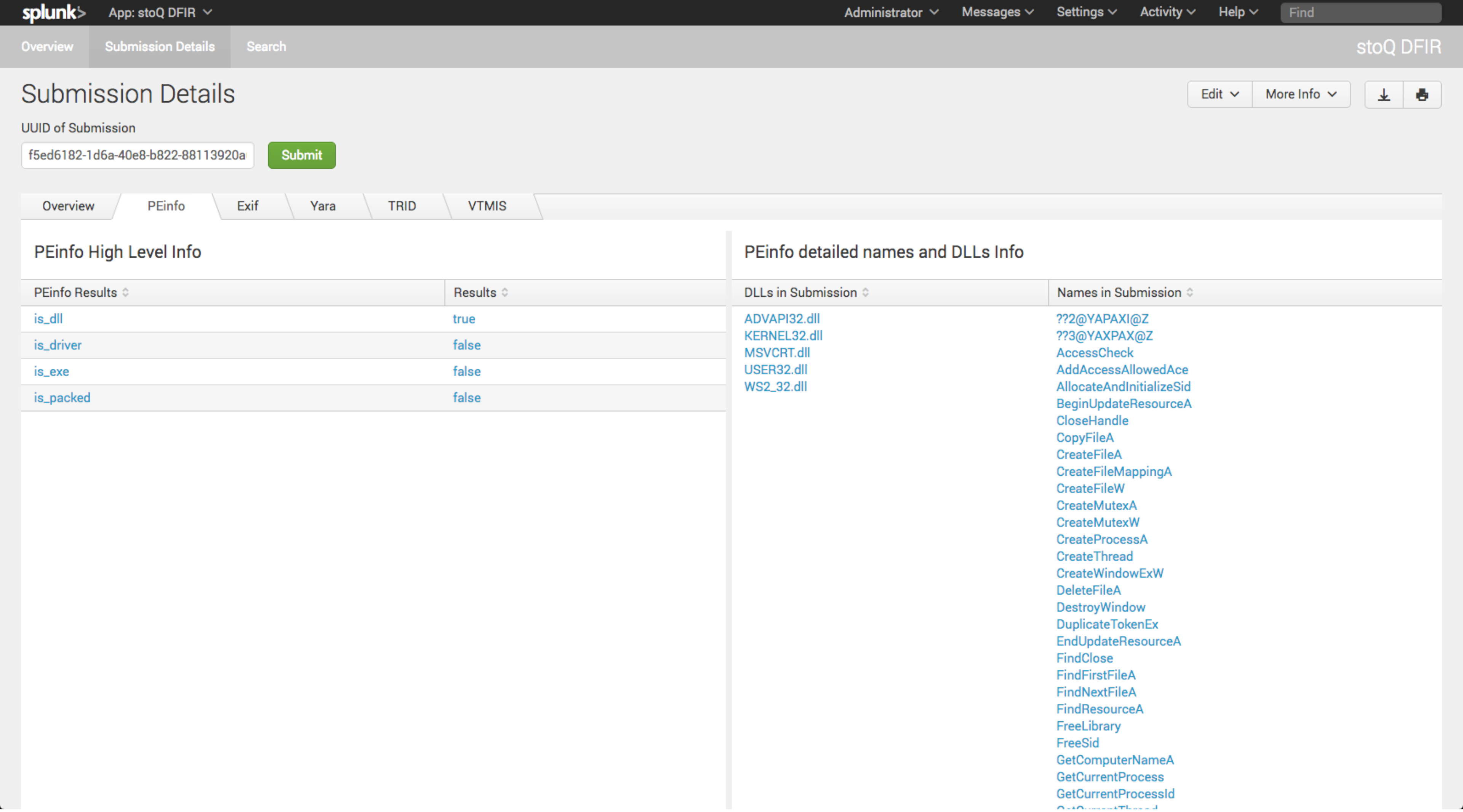
Details of the submision

i	md5	File Name	AV Hits	Yara Rule	File Type	APT Report Name	uuid
˅	7faabce7d2564176480769a9d7b34a2c	reallynotjokingfreetibbet.pdf	Virus Total Detection	Equation_Kaspersky_FannyWorm Str_Win32_Winsock2_Library apt_equation_exploitlib_mutexes dos_stub	Win32 DLL	Diary_of_Scott_Roberts	f5ed6182-1d6a-40e8-b822-88113920a614

Dropper	uuid	md5	extension	payloads
Present	fb25f932-e1f8-4574-ac33-d545afaa8e43	91985cf1b695f95a72df8e27c75eafc5	DLL	4
Present	a877b4d0-9167-465a-8cf3-16171c7958cb	ddc9915a5158a9560ad1ef2f16cce9a6	EXE	4

Import Hash Matches

md5	File Name	uuid
7faabce7d2564176480769a9d7b34a2c	reallynotjokingfreetibbet.pdf	f5ed6182-1d6a-40e8-b822-88113920a614
7e6348f56508e43c900265ee5297b577	FannyWorm_7E6348F56508E43C900265EE5297B577	26f68a80-8aaf-45b5-aa6d-c5288ed8b56d
7cccaf9b08301d2c2acb647ea04ca8e1	FannyWorm_7CCCAF9B08301D2C2ACB647EA04CA8E1	c5003d33-732f-4e93-bb78-94598f48baff
7bc77cfdfefb70225ddb57ef20c554ac	FannyWorm_7BC77CFDFEFB70225DDB57EF20C554AC	eab81adc-dc7a-4592-bf01-8e83a3c534fe
7b8d11cc2ed0cebc39ef590ef6c890b1	FannyWorm_7B8D11CC2ED0CEBC39EF590EF6C890B1	07b129a6-cd11-4e6a-8fa6-ac58ca5ecf9e
7ad2bfab78fa74538dcdbe28da54f1f4	FannyWorm_7AD2BFAB78FA74538DCDBE28DA54F1F4	8ce20f64-190c-486e-9178-5135b0a64271
7a8518e46a1a7713653e34bbfb2b9ad8	FannyWorm_7A8518E46A1A7713653E34BBFB2B9AD8	4171772a-7564-4da7-bd79-01020d576ca1
7946d685c6e7e2d6370b6ade5c6a2e8d	FannyWorm_7946D685C6E7E2D6370B6ADE5C6A2E8D	d193419e-1089-4c21-ab3a-80fee8f645f5
78b1ff3b04fac35c890462225c5fbc49	FannyWorm_78B1FF3B04FAC35C890462225C5FBC49	bbf16e7c-0d29-4d65-8123-e63f60b7e080



Submission Details

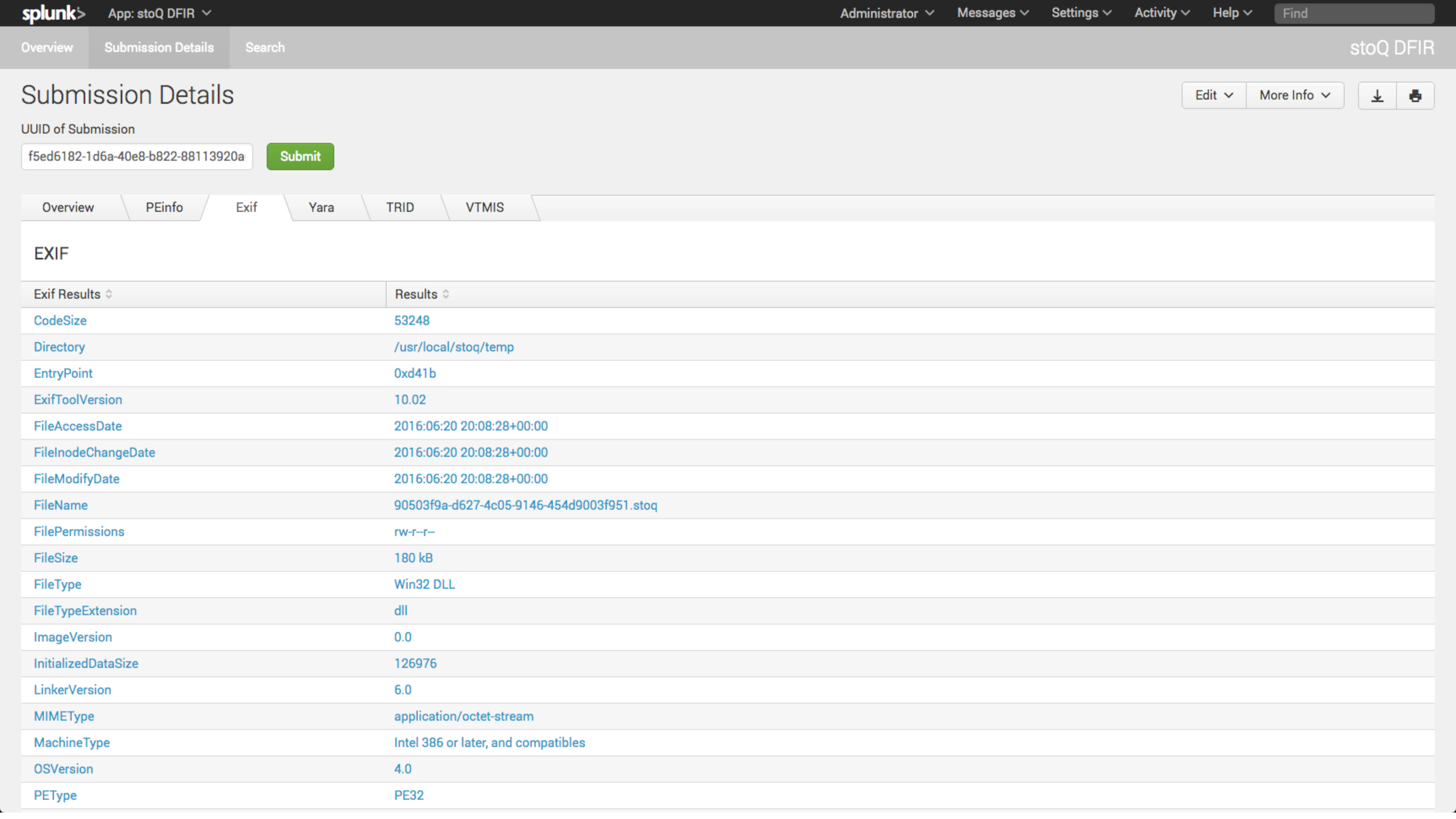
UUID of Submission: f5ed6182-1d6a-40e8-b822-88113920a

PEinfo High Level Info

PEinfo Results	Results
is_dll	true
is_driver	false
is_exe	false
is_packed	false

PEinfo detailed names and DLLs Info

DLLs in Submission	Names in Submission
ADVAPI32.dll	??2@YAPAXI@Z
KERNEL32.dll	??3@YAXPAX@Z
MSVCRT.dll	AccessCheck
USER32.dll	AddAccessAllowedAce
WS2_32.dll	AllocateAndInitializeSid
	BeginUpdateResourceA
	CloseHandle
	CopyFileA
	CreateFileA
	CreateFileMappingA
	CreateFileW
	CreateMutexA
	CreateMutexW
	CreateProcessA
	CreateThread
	CreateWindowExW
	DeleteFileA
	DestroyWindow
	DuplicateTokenEx
	EndUpdateResourceA
	FindClose
	FindFirstFileA
	FindNextFileA
	FindResourceA
	FreeLibrary
	FreeSid
	GetComputerNameA
	GetCurrentProcess
	GetCurrentProcessId



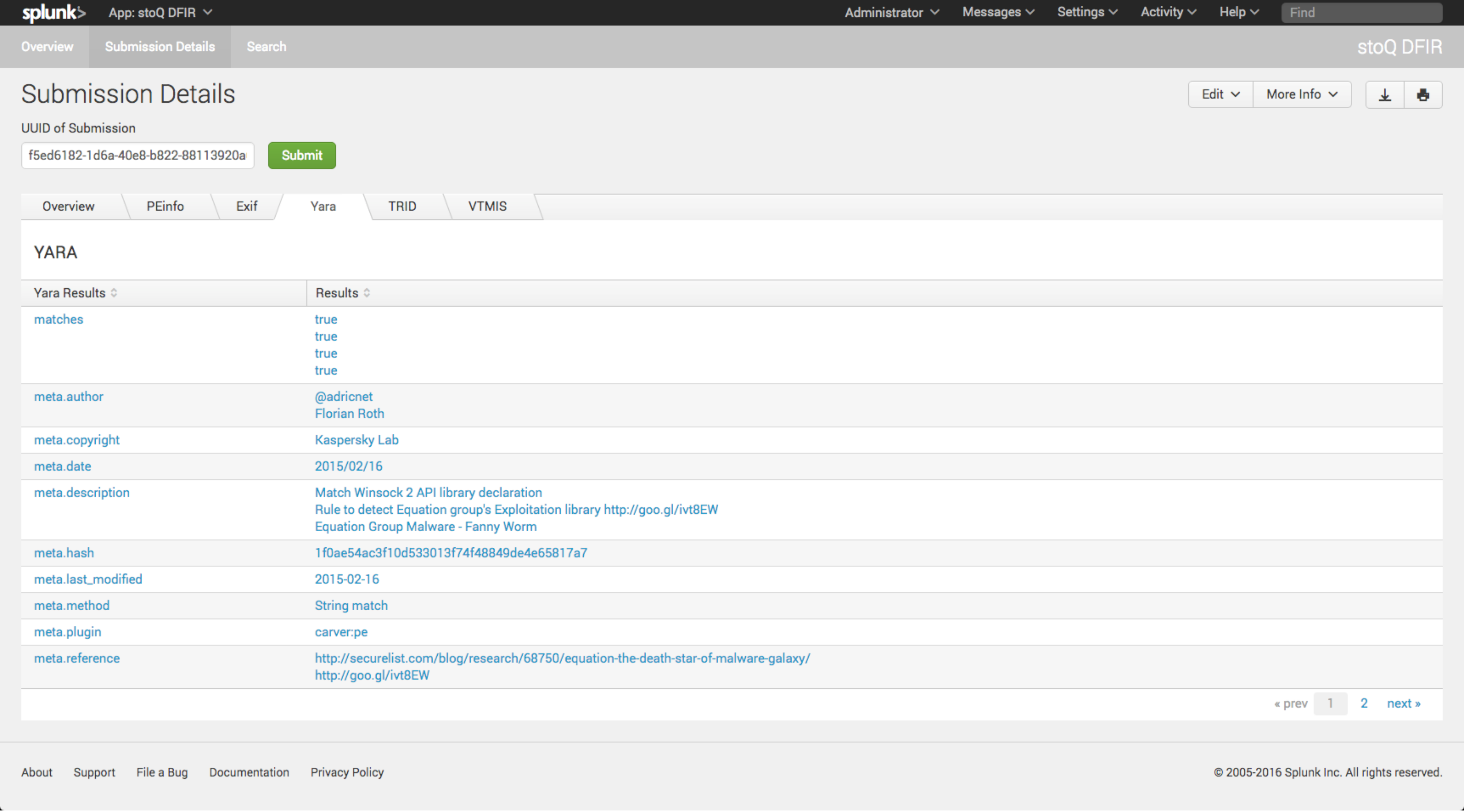
Submission Details

UUID of Submission

f5ed6182-1d6a-40e8-b822-88113920a

EXIF

Exif Results	Results
CodeSize	53248
Directory	/usr/local/stoq/temp
EntryPoint	0xd41b
ExifToolVersion	10.02
FileAccessDate	2016:06:20 20:08:28+00:00
FileInodeChangeDate	2016:06:20 20:08:28+00:00
FileModifyDate	2016:06:20 20:08:28+00:00
FileName	90503f9a-d627-4c05-9146-454d9003f951.stoq
FilePermissions	rw-r--r–
FileSize	180 kB
FileType	Win32 DLL
FileTypeExtension	dll
ImageVersion	0.0
InitializedDataSize	126976
LinkerVersion	6.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0
PEType	PE32

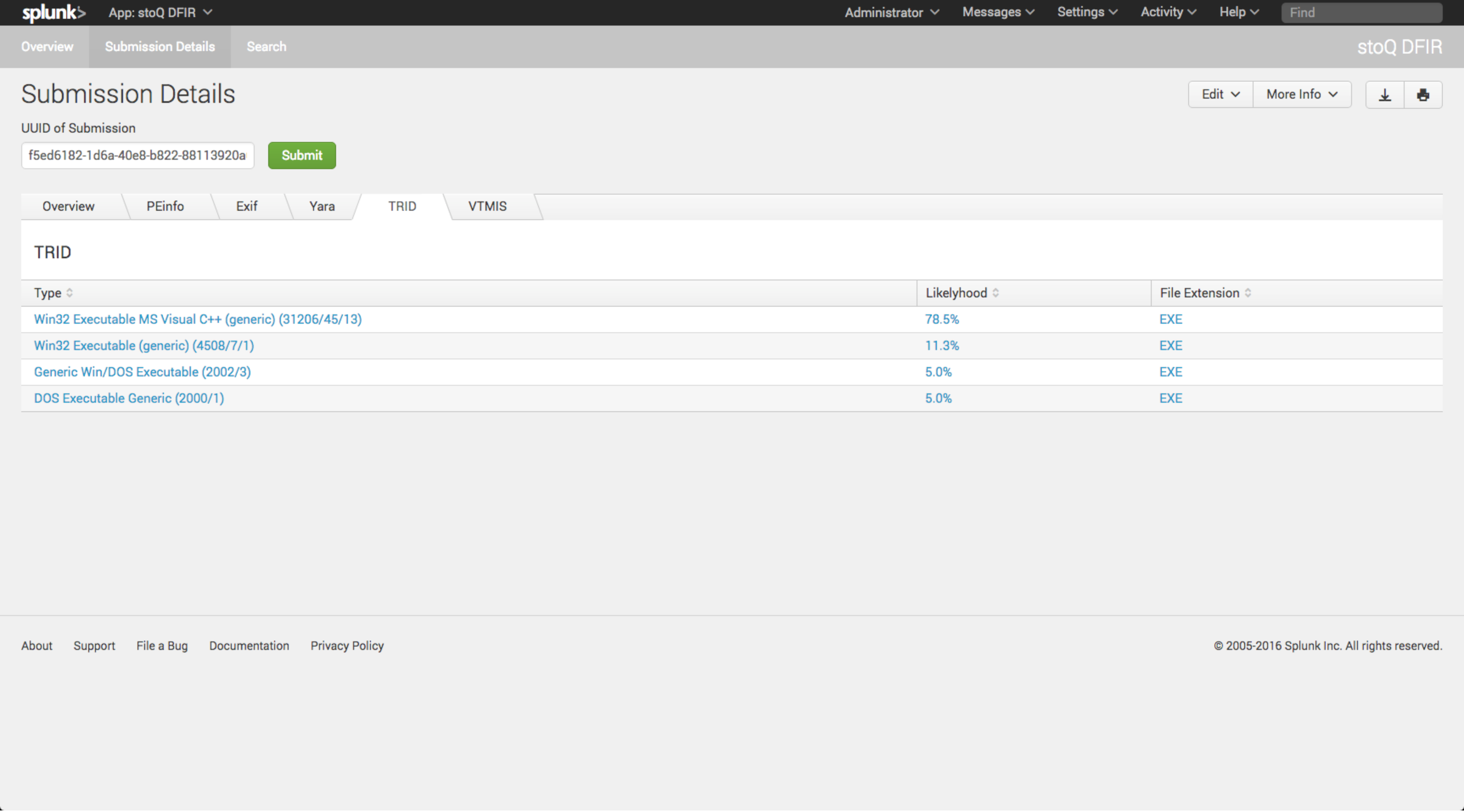


Submission Details

UUID of Submission: f5ed6182-1d6a-40e8-b822-88113920a

YARA

Yara Results	Results
matches	true true true true
meta.author	@adricnet Florian Roth
meta.copyright	Kaspersky Lab
meta.date	2015/02/16
meta.description	Match Winsock 2 API library declaration Rule to detect Equation group's Exploitation library http://goo.gl/ivt8EW Equation Group Malware - Fanny Worm
meta.hash	1f0ae54ac3f10d533013f74f48849de4e65817a7
meta.last_modified	2015-02-16
meta.method	String match
meta.plugin	carver:pe
meta.reference	http://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/ http://goo.gl/ivt8EW

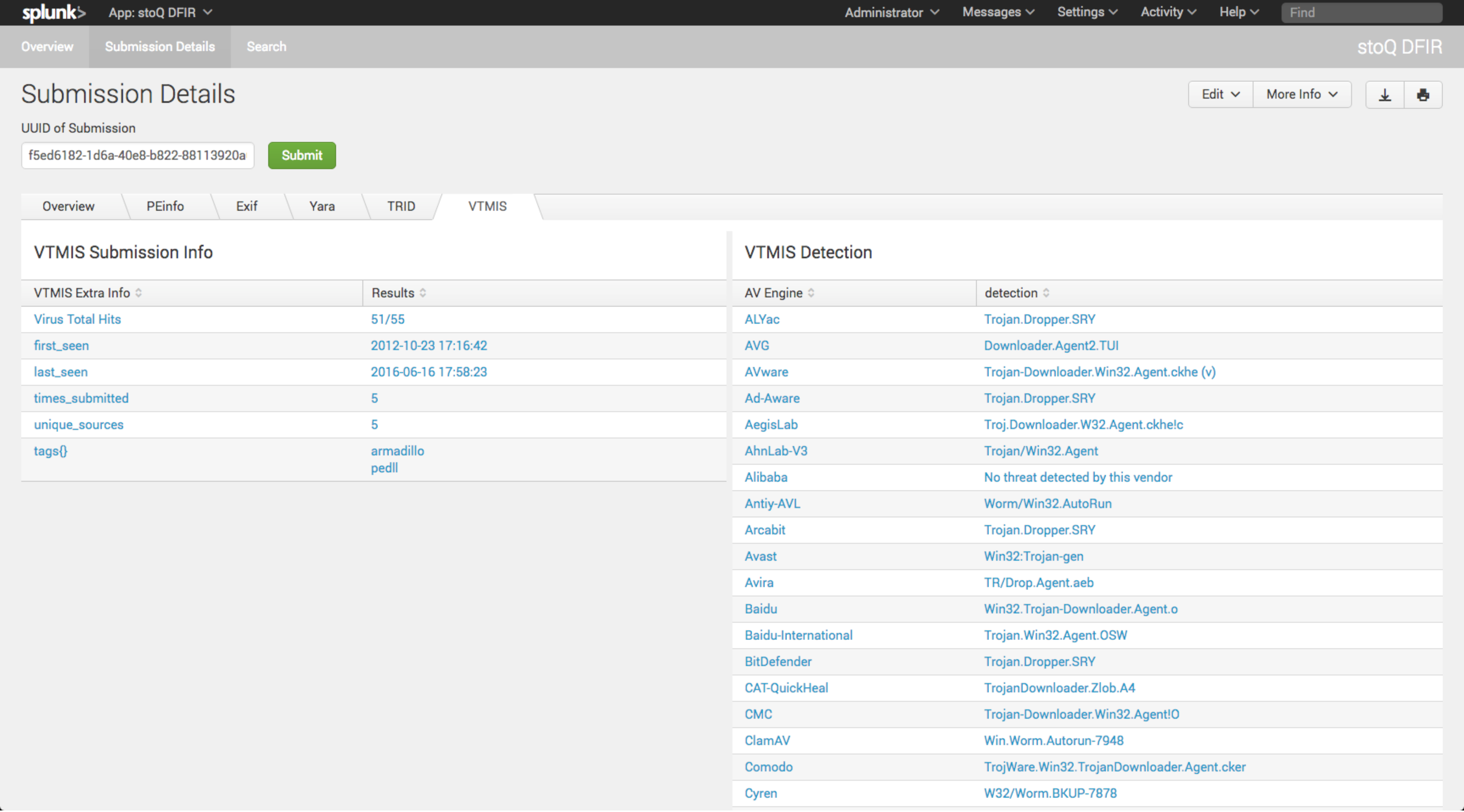


Submission Details

UUID of Submission: f5ed6182-1d6a-40e8-b822-88113920a

TRID

Type	Likelyhood	File Extension
Win32 Executable MS Visual C++ (generic) (31206/45/13)	78.5%	EXE
Win32 Executable (generic) (4508/7/1)	11.3%	EXE
Generic Win/DOS Executable (2002/3)	5.0%	EXE
DOS Executable Generic (2000/1)	5.0%	EXE



Submission Details

UUID of Submission: f5ed6182-1d6a-40e8-b822-88113920a

VTMIS Submission Info

VTMIS Extra Info	Results
Virus Total Hits	51/55
first_seen	2012-10-23 17:16:42
last_seen	2016-06-16 17:58:23
times_submitted	5
unique_sources	5
tags{}	armadillo pedll

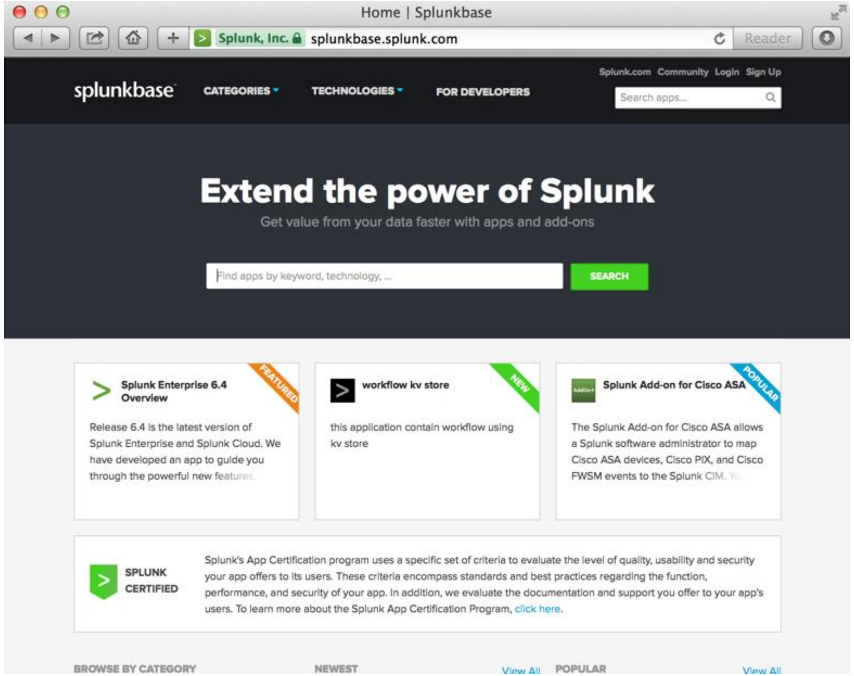
VTMIS Detection

AV Engine	detection
ALYac	Trojan.Dropper.SRY
AVG	Downloader.Agent2.TUI
AVware	Trojan-Downloader.Win32.Agent.ckhe (v)
Ad-Aware	Trojan.Dropper.SRY
AegisLab	Troj.Downloader.W32.Agent.ckhe!c
AhnLab-V3	Trojan/Win32.Agent
Alibaba	No threat detected by this vendor
Antiy-AVL	Worm/Win32.AutoRun
Arcabit	Trojan.Dropper.SRY
Avast	Win32:Trojan-gen
Avira	TR/Drop.Agent.aeb
Baidu	Win32.Trojan-Downloader.Agent.o
Baidu-International	Trojan.Win32.Agent.OSW
BitDefender	Trojan.Dropper.SRY
CAT-QuickHeal	TrojanDownloader.Zlob.A4
CMC	Trojan-Downloader.Win32.Agent!O
ClamAV	Win.Worm.Autorun-7948
Comodo	TrojWare.Win32.TrojanDownloader.Agent.cker
Cyren	W32/Worm.BKUP-7878

WHERE DO I GET ALL OF THIS INCREDIBLENESS???

https://splunkbase.splunk.com/app/3196/

http://stoq.punchcyber.com



Home | Splunkbase

Extend the power of Splunk

Get value from your data faster with apps and add-ons

Splunk Enterprise 6.4 Overview

Release 6.4 is the latest version of Splunk Enterprise and Splunk Cloud. We have developed an app to guide you through the powerful new features.

workflow kv store

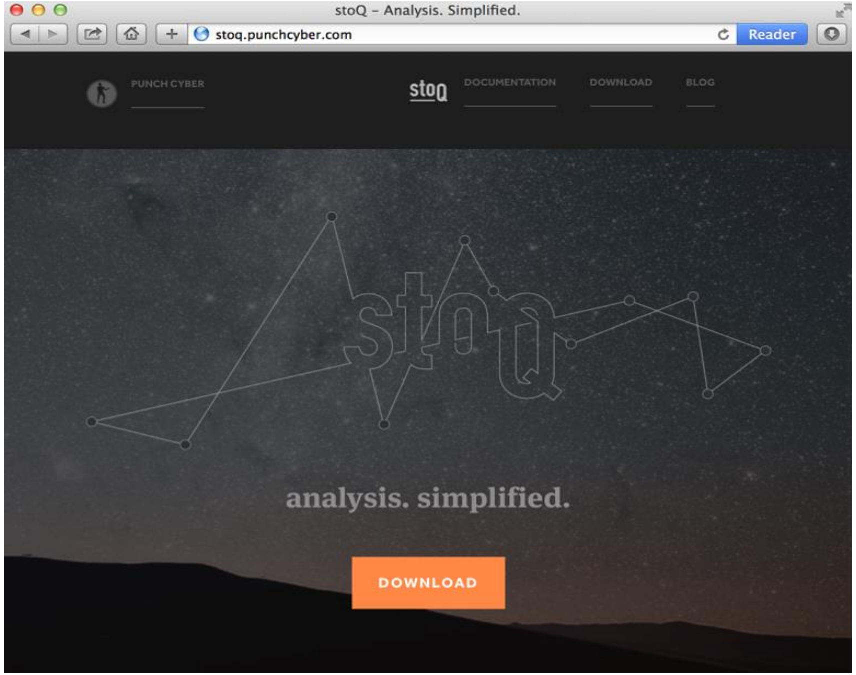
this application contain workflow using kv store

Splunk Add-on for Cisco ASA

The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA devices, Cisco PIX, and Cisco FWSM events to the Splunk CIM. Yo

SPLUNK CERTIFIED

Splunk's App Certification program uses a specific set of criteria to evaluate the level of quality, usability and security your app offers to its users. These criteria encompass standards and best practices regarding the function, performance, and security of your app. In addition, we evaluate the documentation and support you offer to your app's users. To learn more about the Splunk App Certification Program, click here.



stoQ – Analysis. Simplified.

analysis. simplified.

Questions? Try it out instead ☺

https://demo.stoq.io
Username: dfir2016
Password: stoqingyoursplunk

Ryan Kovar
rkovar@splunk.com
@meansec

Marcus LaFerrera
marcus@punchcyber.com
@mlaferrera