Community Intelligence & Open Source Tools

Building an Actionable Pipeline

Intro

Me:

Scott J Roberts

@sroberts

Han Solo is my Spirit Animal

What do CTI industry analysts say?

"When it comes to eating @sroberts is a thought leader up & to the right on all quadrants!"

~ @rickhholland

DFIRing Since 2006

CTIing Since 2007

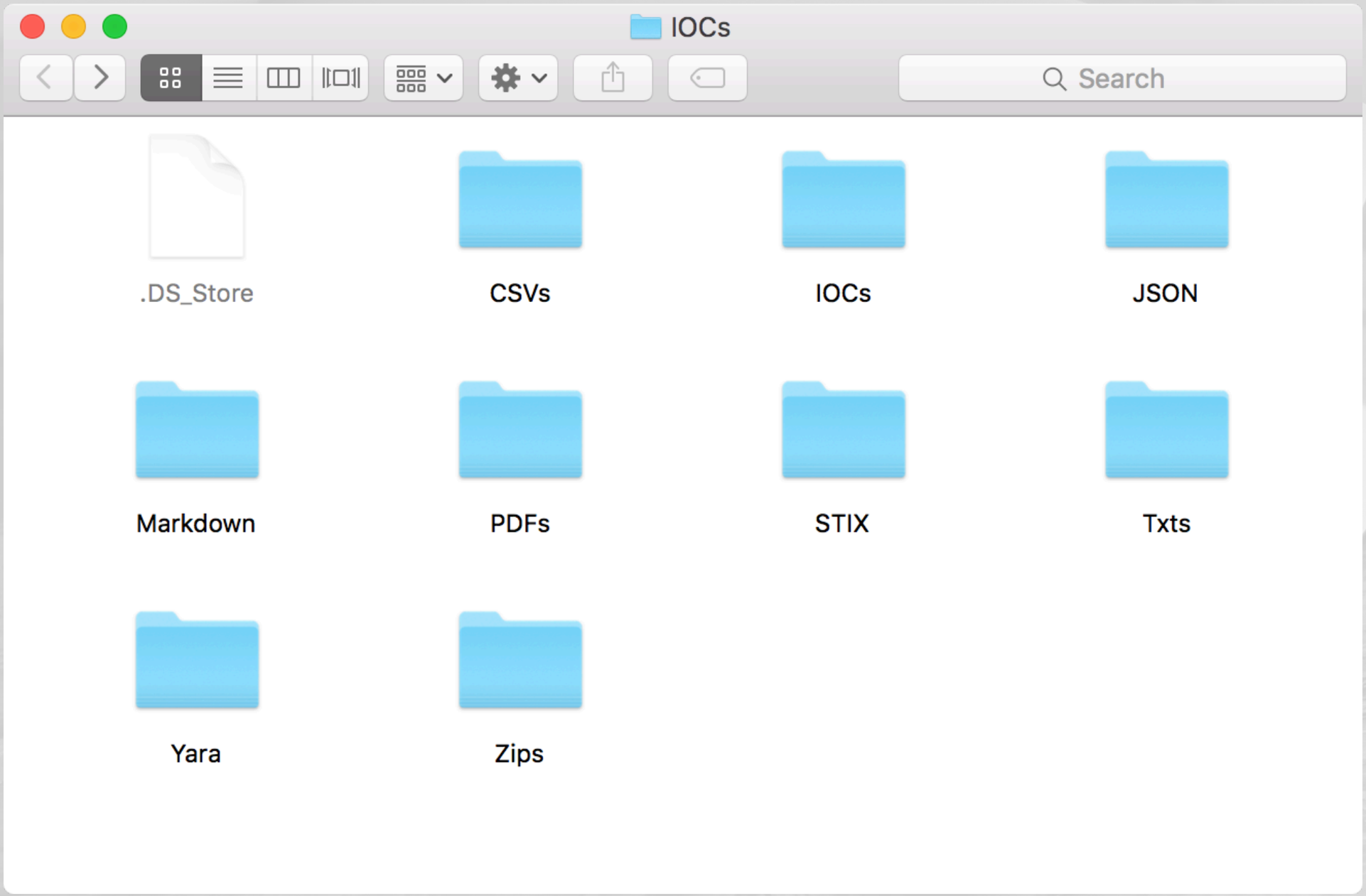
Deving Since 2009


WORK
IN PROGRESS

The Problem

We are spinning up considerable new telemetry using open source tools and we need to feed those tools with actionable intelligence.

The Other Problem



Pocket

Chat

Note Books

And all the other sources...

So I did what anyone with a little Python experience does

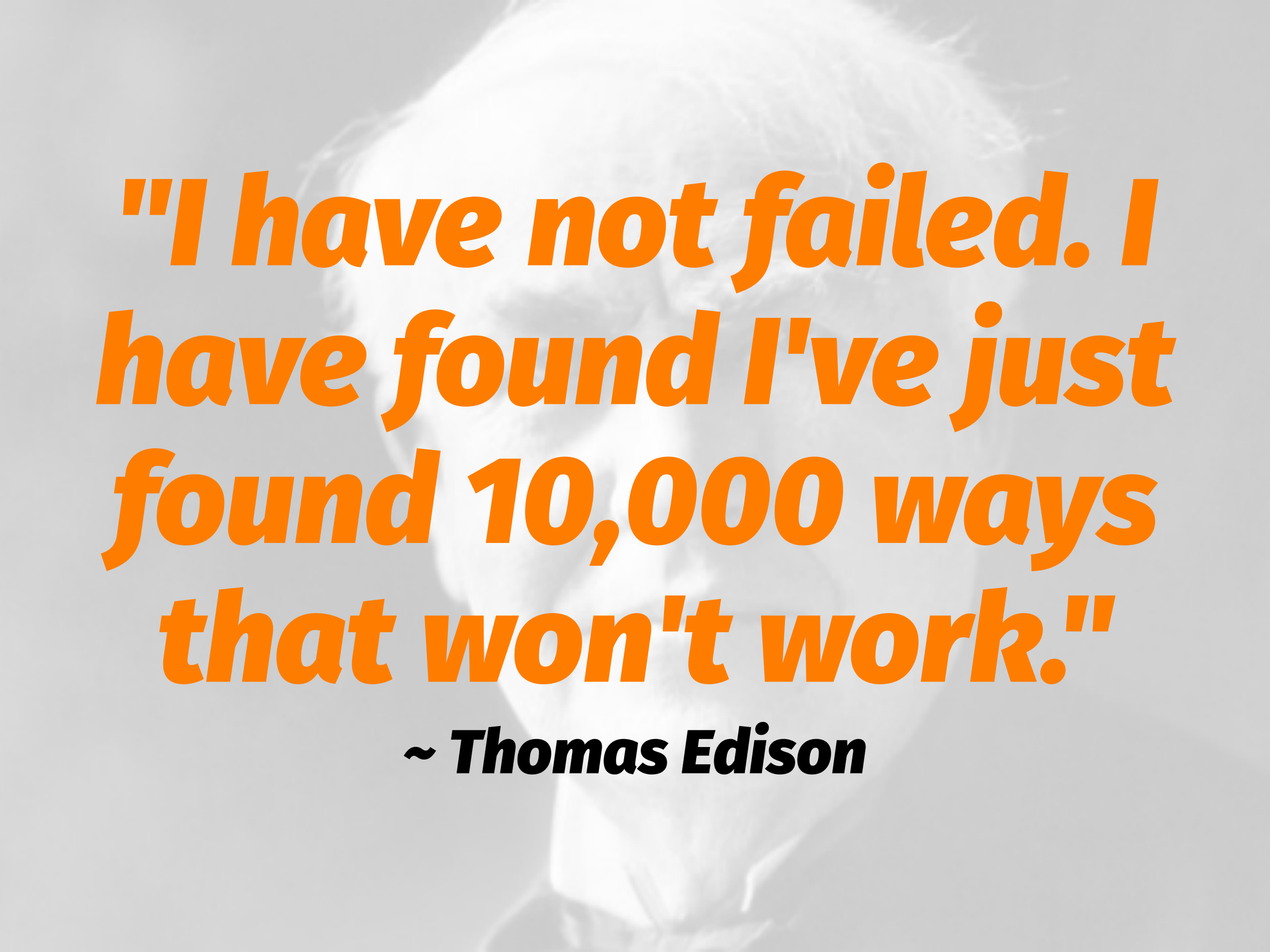
I built my own...

And I built my own again...

And another time...

In the end I built about 5 or 6...

They all sorta sucked... 😢



"I have not failed. I have found I've just found 10,000 ways that won't work."

~ Thomas Edison

Direction

Breath vs. Depth

OSX, Linux, & GitHub centric threats

Collection

Twitter

Email Lists

Feeds

Ongoing Incidents

Manual

Exploitation

To Use a Technical Term

Indicator Extraction

sucks...

But we did it anyway...[1]

[1] YOLO!!!

Jager & Caçador [2]

[2] *Look it means hunter in Portuguese.*

OnionDuke: APT Attacks Via the Tor Network

www.f-secure.com
November 14th, 2014

View Original
rfi

Recently, research was published identifying a Tor exit node, located in Russia, that was consistently and maliciously modifying any uncompressed Windows executables downloaded through it. Naturally this piqued our interest, so we decided to peer down the rabbit hole. Suffice to say, the hole was a lot deeper than we expected! In fact, it went all the way back to the notorious Russian APT family MiniDuke, known to have been used in targeted attacks against NATO and European government agencies. The malware used in this case is, however, not a version of MiniDuke. It is instead a separate, distinct family of malware that we have since taken to calling OnionDuke. But lets start from the beginning.

When a user attempts to download an executable via the malicious Tor exit node, what they actually receive is an executable "wrapper" that embeds both the original executable and a second, malicious executable.

Command

```
$ pbpaste | cacador | jq '.[]'
```

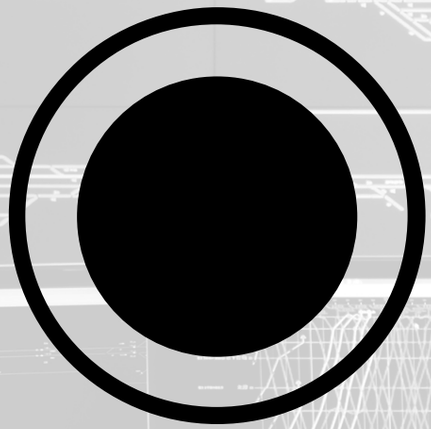
Output

2. sroberts@Echo: ~ (zsh)

```
➜  ~  pbpaste | cacador | jq '.'
{
  "Md5s": [
    "a75995f94854dea8799650a2f4a97980",
    "b491c14d8cfb48636f6095b7b16555e9",
    "d433f281cf56015941a1c2cb87066ca6"
  ],
  "Sha1s": [
    "a75995f94854dea8799650a2f4a97980b71199d2",
    "b491c14d8cfb48636f6095b7b16555e9a575d57f",
    "d433f281cf56015941a1c2cb87066ca62ea1db37"
  ],
  "Sha256s": null,
  "Sha512s": null,
  "Ssdeeps": null,
  "Domains": [
    "overpict.com",
    "airtravelabroad.com",
    "beijingnewsblog.net",
    "grouptumbler.com",
    "leveldelta.com",
    "nasdaqblog.net",
    "natureinhome.com",
    "nestedmail.com",
```

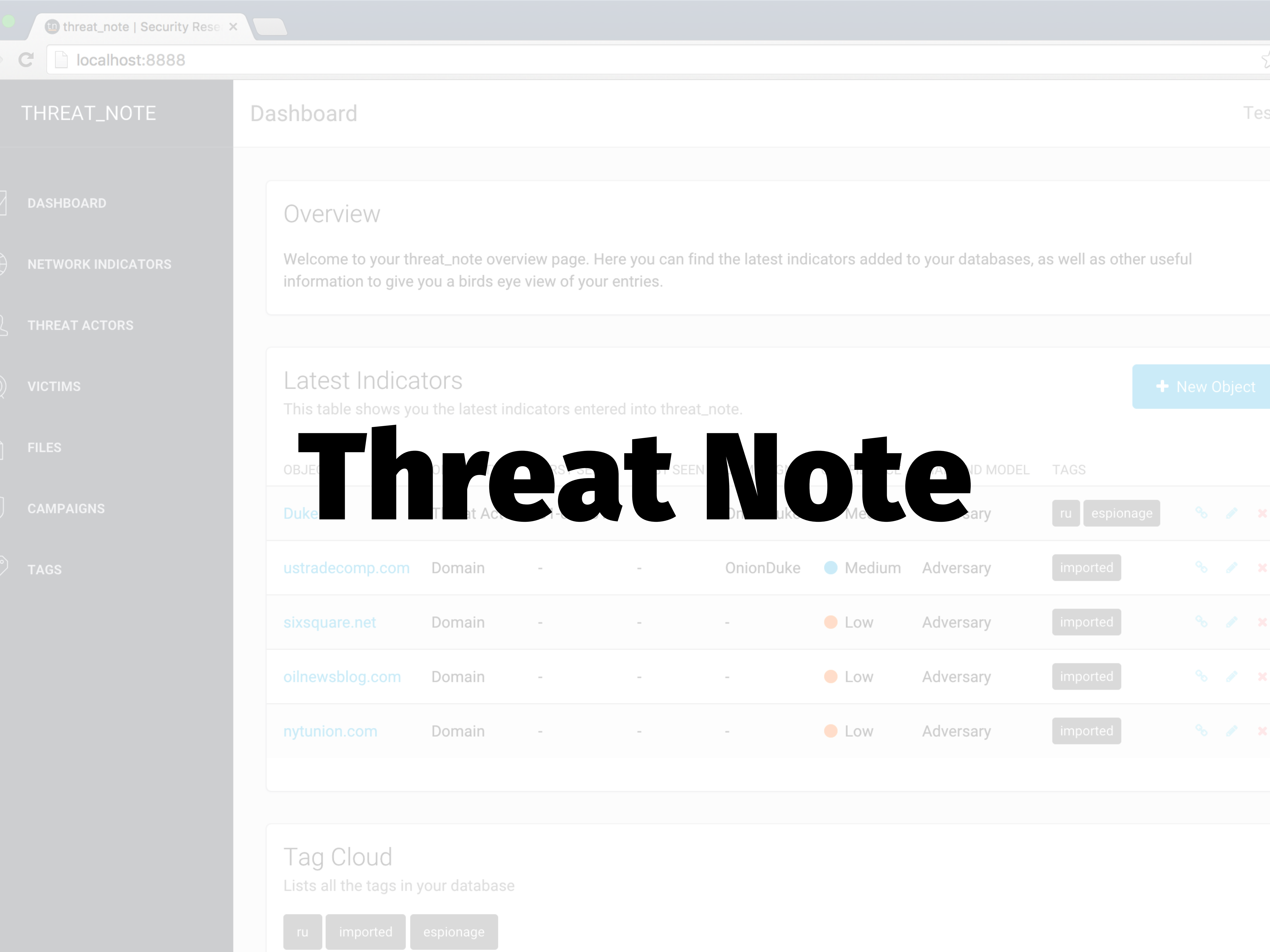
Tada!!!


2. sroberts@Echo: ~/Documents/src/threat_note_utilities (zsh)
(venv) ➜ threat_note_utilities git:(master) ✗ pbpaste | cacador | python ioc_importer.py
{"upload status": "success"}
(venv) ➜ threat_note_utilities git:(master) ✗



Analysis

Threat Note



threat_note | Security Rese
localhost:8888
THREAT_NOTE
Dashboard
DASHBOARD
NETWORK INDICATORS
THREAT ACTORS
VICTIMS
FILES
CAMPAIGNS
TAGS
Overview
Welcome to your threat_note overview page. Here you can find the latest indicators added to your databases, as well as other useful information to give you a birds eye view of your entries.
Latest Indicators
This table shows you the latest indicators entered into threat_note.
New Object
TAGS
ru
espionage
ustradecomp.com Domain - - OnionDuke Medium Adversary imported
sixsquare.net Domain - - - Low Adversary imported
oilnewsblog.com Domain - - - Low Adversary imported
nytunion.com Domain - - - Low Adversary imported
Tag Cloud
Lists all the tags in your database
ru
imported
espionage

Dashboard

Tes

Overview

Welcome to your threat_note overview page. Here you can find the latest indicators added to your databases, as well as other useful information to give you a birds eye view of your entries.

Latest Indicators

This table shows you the latest indicators entered into threat_note.

+ New Object

OBJECT	OBJECT TYPE	FIRST SEEN	LAST SEEN	CAMPAIGN	CONFIDENCE	DIAMOND MODEL	TAGS
Duke	Threat Actor	01-02-2013	-	OnionDuke	Medium	Adversary	ru espionage
ustradecomp.com	Domain	-	2015-11-22	OnionDuke	Medium	Adversary	imported
sixsquare.net	Domain	-	-	OnionDuke	Low	Adversary	imported
oilnewsblog.com	Domain	-	-	OnionDuke	Low	Adversary	imported
nytunion.com	Domain	-	-	OnionDuke	Low	Adversary	imported

Tag Cloud

Lists all the tags in your database

ru imported espionage

Network Indicators

This page contains all the network indicators in the threat_note database, which includes IP Addresses, Domains and Network Blocks. Along with your indicators, you'll also find key attributes and their values that have been entered.

Network Indicators

This table shows you all of your network indicators.

+ New Object

OBJECT	OBJECT TYPE	FIRST SEEN	LAST SEEN	CAMPAIGN	CONFIDENCE	DIAMOND MODEL	TAGS
overpict.com	Domain	-	-	OnionDuke	Medium	Adversary	imported
airtravelabroad.com	Domain	-	-	OnionDuke	Medium	Adversary	imported
beijingnewsblog.net	Domain	-	-	OnionDuke	Medium	Adversary	imported
grouptumbler.com	Domain	-	-	OnionDuke	Low	Adversary	imported
leveldelta.com	Domain	-	-	-	Low	Adversary	imported
nasdaqblog.net	Domain	-	-	OnionDuke	Medium	Adversary	imported
natureinhome.com	Domain	-	-	-	Low	Adversary	imported
nestedmail.com	Domain	-	-	-	Low	Adversary	imported
nostressjob.com	Domain	-	-	-	Low	Adversary	imported
nytunion.com	Domain	-	-	OnionDuke	Low	Adversary	imported
oilnewsblog.com	Domain	-	-	OnionDuke	Low	Adversary	imported
sixsquare.net	Domain	-	-	OnionDuke	Low	Adversary	imported
ustradecomp.com	Domain	-	2015-11-22	OnionDuke	Medium	Adversary	imported

Files

This page contains all the files/hashes in the threat_note database. Along with the files and hashes, you'll also find key attributes and their values that have been entered.

Files and Hashes

This table shows you all of the files and hashes

+ New Object

OBJECT	OBJECT TYPE	FIRST SEEN	LAST SEEN	CAMPAIGN	CONFIDENCE	DIAMOND MODEL	TAGS
a75995f94854dea8799650a2f4a97980	Hash	-	-	OnionDuke	High	Adversary	imported
b491c14d8cfb48636f6095b7b16555e9	Hash	-	-	-	Low	Adversary	imported
d433f281cf56015941a1c2cb87066ca6	Hash	-	-	-	Low	Adversary	imported
a75995f94854dea8799650a2f4a97980b71199d2	Hash	-	-	-	Low	Adversary	imported
b491c14d8cfb48636f6095b7b16555e9a575d57f	Hash	-	-	-	Low	Adversary	imported
d433f281cf56015941a1c2cb87066ca62ea1db37	Hash	-	-	-	Low	Adversary	imported

This page contains information on a75995f94854dea8799650a2f4a97980 that was manually entered, as well as 3rd party supplemental information that can aide an analyst in research. 3rd party sources can include VirusTotal, PassiveTotal, Whois, geolocational data, and more. You can enable these 3rd party integrations in the settings menu.

On this page, you can also edit the entry to add new fields or change any attributes previously entered. You can also delete the entry if it's no longer needed.

a75995f94854dea8799650a2f4a97980

a75995f94854dea8799650a2f4a97980

ATTRIBUTE	VALUE
Object Type	Hash
Campaign	OnionDuke
Confidence	High
Diamond Model	Adversary
First Seen	-
Last Seen	-
Comments	Automatically imported.
Tags	imported

OnionDuke

Campaign Description

+ Download Indicators

INDICATOR
nasdaqblog.net
grouptumbler.com
Duke
airtravelabroad.com
beijingnewsblog.net
ustradecomp.com
overpict.com
nytunion.com
sixsquare.net
a75995f94854dea8799650a2f4a97980
oilnewsblog.com

54dea8799650a2f4a97980b71199d2/info

Actors

ge contains all the threat actors in the threa ote da ba A g wi h hreat a ors o
een entered.

reat Actors

table shows you all of the threat actors.

CT	OBJECT TYPE	FIRST SEEN	LAST SEEN	CAMPAIGN	CONFIDENCE	DIAMOND
	Threat Actor	01-02-2013	-	OnionDuke	Medium	Adversar

Credits

Enrichments

Whois

PassiveTotal

Shodan

VirusTotal

VirusTotal Information

More information can be found at VirusTotal

ATTRIBUTE	VALUE
Scan Date	2016-01-30 06:55:21
Positives/Total	42/55

SCANNER	RESULT
MicroWorld-eScan	Backdoor.OnionDuke.A
nProtect	Backdoor.OnionDuke.A
Heal	TrojanAPT.OnionDuke.DR5
ALYac	Trojan.Dropper.OnionDuke
VIPRE	Trojan.Win32.Generic!BT
AegisLab	Backdoor.W32.MiniDuke.x!c
K7GW	Trojan (0001140e1)
K ntiVirus	Trojan (0001140e1)
NANO-Antivirus	Trojan.Win32.OnionDuke.dwkodj
ESET-NOD32	a variant of Win32/TrojanDropper.OnionDuk
TrendMicro-HouseCall	TROJ_ONIONDUKE.A

VirusTotal Information

More information can be found at VirusTotal

ATTRIBUTE	VALUE
Scan Date	2016-01-30 06:55:21
Positives/Total	42/55

SCANNER	RESULT	UPDATE
MicroWorld-eScan	Backdoor.OnionDuke.A	20160130
nProtect	Backdoor.OnionDuke.A	20160129
CAT-QuickHeal	TrojanAPT.OnionDuke.DR5	20160129
ALYac	Trojan.Dropper.OnionDuke	20160130
VIPRE	Trojan.Win32.Generic!BT	20160130
AegisLab	Backdoor.W32.MiniDuke.x!c	20160130
K7GW	Trojan (0001140e1)	20160129
K7AntiVirus	Trojan (0001140e1)	20160129
NANO-Antivirus	Trojan.Win32.OnionDuke.dwkodj	20160130
ESET-NOD32	a variant of Win32/TrojanDropper.OnionDuke.A	20160130
TrendMicro-HouseCall	TROJ_ONIONDUKE.A	20160130

PassiveTotal Passive DNS

More information can be found at PassiveTotal

RESOLVED	FIRST SEEN	LAST SEEN
69.195.129.72	2014-04-21 03:37:56	2016-02-03 14:30:12
69.195.129.70	2015-04-18 12:48:35	2015-07-06 05:42:57
178.62.193.125	2015-04-09 12:44:27	2015-04-18 09:44:38
69.195.129.72	2014-04-20 08:50:57	2015-04-09 05:50:35
208.91.197.194	2014-01-30 16:19:00	2014-03-12 23:07:26
173.194.70.101	2013-02-28 08:00:13	2014-01-30 16:19:00
200.63.46.22	2013-04-01 00:00:00	2013-04-01 00:00:00
173.194.70.101	2013-03-01 20:11:59	2013-03-01 20:11:59
200.63.46.22	2012-05-27 02:07:10	2013-02-28 08:00:13
204.13.160.28	2011-02-03 04:22:01	2011-02-05 03:22:47

Shodan Information

More information can be found at Shodan.io

ATTRIBUTE	VALUE

Maltego
Maltego Chlorine 3.6.1
Manage
View
Organize
Machines
Collaboration
Number of Results
12 50 255 10k
Transforms
Quick Find
Find
Entity Selection
Select All
Invert Selection
Select None
Add Similar Siblings
Add Path
Select Parents
Select Children
Select Neighbors
Add Parents
Add Children
Add Neighbors
Select Bookmarked
Select by Type
Select Links
Reverse Links
Selection
Zoom to
Zoom to Fit
Zoom 100%
Zoom In
Zoom Out
Zoom Selection
Zoom
Come enjoy Maltego Training by the Paterva team
SAS 2016 - Tenerife, Spain - February 7-11, 2016!
CE: We've dropped support for Java 6. Maltego Chlorine runs only on Java 7 or Java 8.
MALTEGO CHLORINE
PATERVA CTAS
Paterva
Standard Paterva Transforms
FREE
INSTALLED
From Transform Hub
SocialLinks
SocialLinks
PAID
RecordedFuture
Recorded Future Inc.
Query Recorded Future for threat intelligence information
ThreatConnect
ThreatConnect
ThreatConnect Platform Transform Set
Intel 471
Intel 471
Query Intel 471 for actor-centric intelligence information.
PAID
CrowdStrike Intelligence API Transforms
Hyas
HYAS Inc.
Reverse Whois, Phishing, Malware, and Reputation Data.
PAID
NewsLink
Paul@Paterva
Monitoring News
FREE
Digital Shadows
Digital Shadows
Query the Digital Shadows cyber threat intelligence database.
PAID
PassiveTotal
PassiveTotal
Query PassiveTotal source and account data.
FREE
SocialNet
ShadowDragon MalNet

Fast Incident Response

Dissemination

Now

Manual

Soon™

osquery & Bro Intelligence

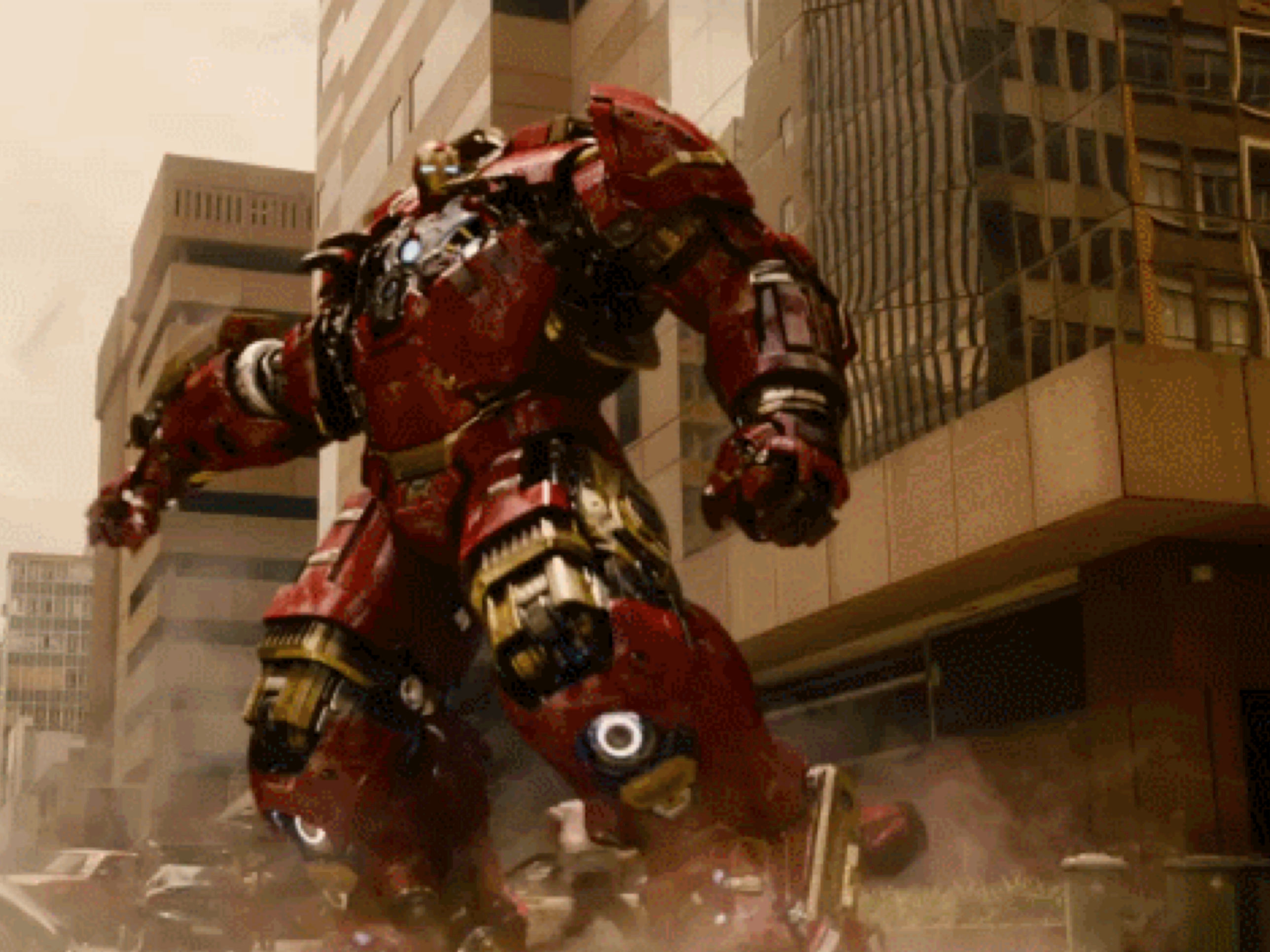
Chat with Hubot

Intelligence Reports

Application Integration

Feedback

The Result



The (REAL) Result

A (somewhat) automated system providing centralized *threat data* & *intelligence management* made up of a single source of truth supported by purpose built collection, processing, and analysis integrations.

Lessons

This isn't easy

But parts are.

Threat Intel Tools Work When They're Integrated

~

collection | analysis | dissemination

High Value Investments

Tool: **Paterva Maltego ~ $760**

Service: **PassiveTotal ~ $??**

Learning: **Introducing Python ~ $33**

Learn to Code

Unix Philosophy

Small is beautiful

Make each program do one thing well

Portability over efficiency

Store data in flat files

Make every program a filter

Data formats matter less than format openness

CSV & JSON

Perfect

Is the Enemy Of

Good

The Future:

Scaling Up Collection & Storage

Expanded Threat_Notes APIs & Integrations

Reputation & Fuzzy Indicators

Links

github.com/defpoint/threat*note*
github.com/certsocietegenerale/FIR
github.com/sroberts/jager
github.com/sroberts/cacador
github.com/kbandla/APTnotes
*github.com/armbues/ioc*parser
github.com/ivanlei/threatbutt

Thanks

Threat Note: **@brianwarehime**

FIR: **@thomchop_**

APTNotes: **@kbandla**

Jager: **@kylemaxwell, @kbandla, & @deadbits**

Questions???

~

@sroberts

http://sroberts.github.io