THREATCONNECT®

Advanced Threat Hunting

botconf
December 8, 2017

Who Am I?

Director of Research Innovation

Research Team

ThreatConnect, Inc.

A Few Definitions

Threat Intelligence

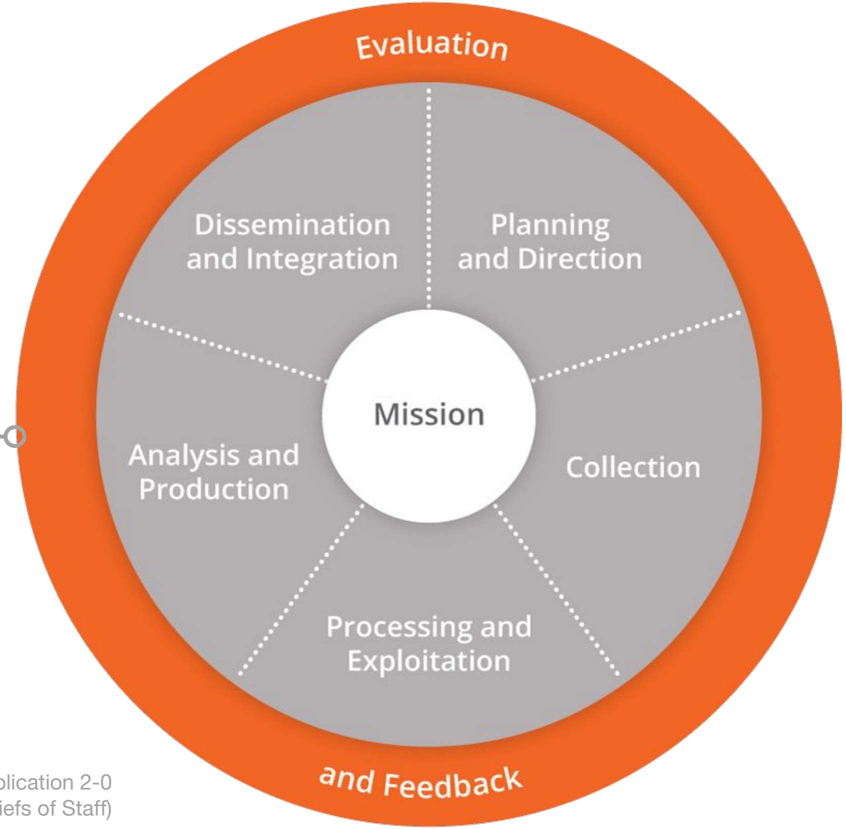
Tactical	Operational
Technical	Strategic

A Few Definitions

Threat Intelligence

Tactical	Operational
Technical	Strategic

The Intelligence Process

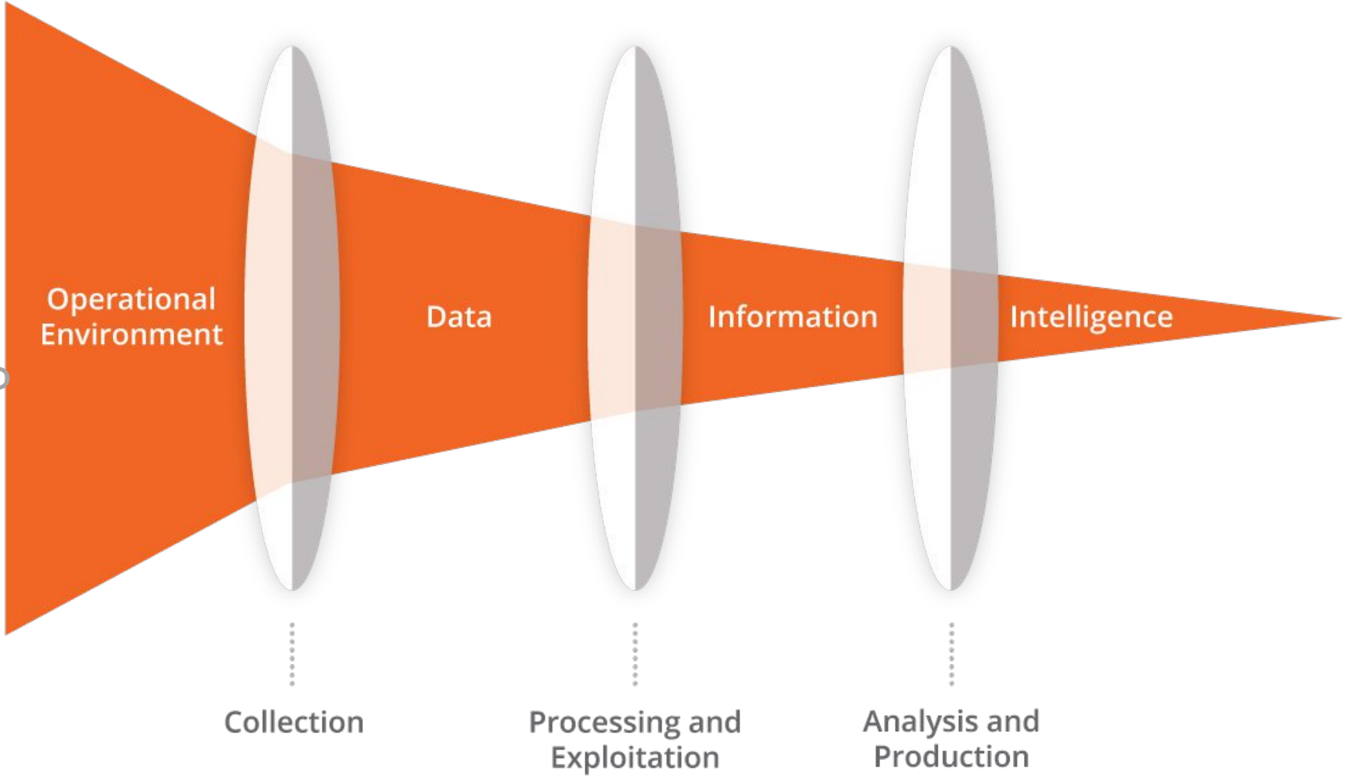


Source: Joint Intelligence / Joint Publication 2-0
(Joint Chiefs of Staff)

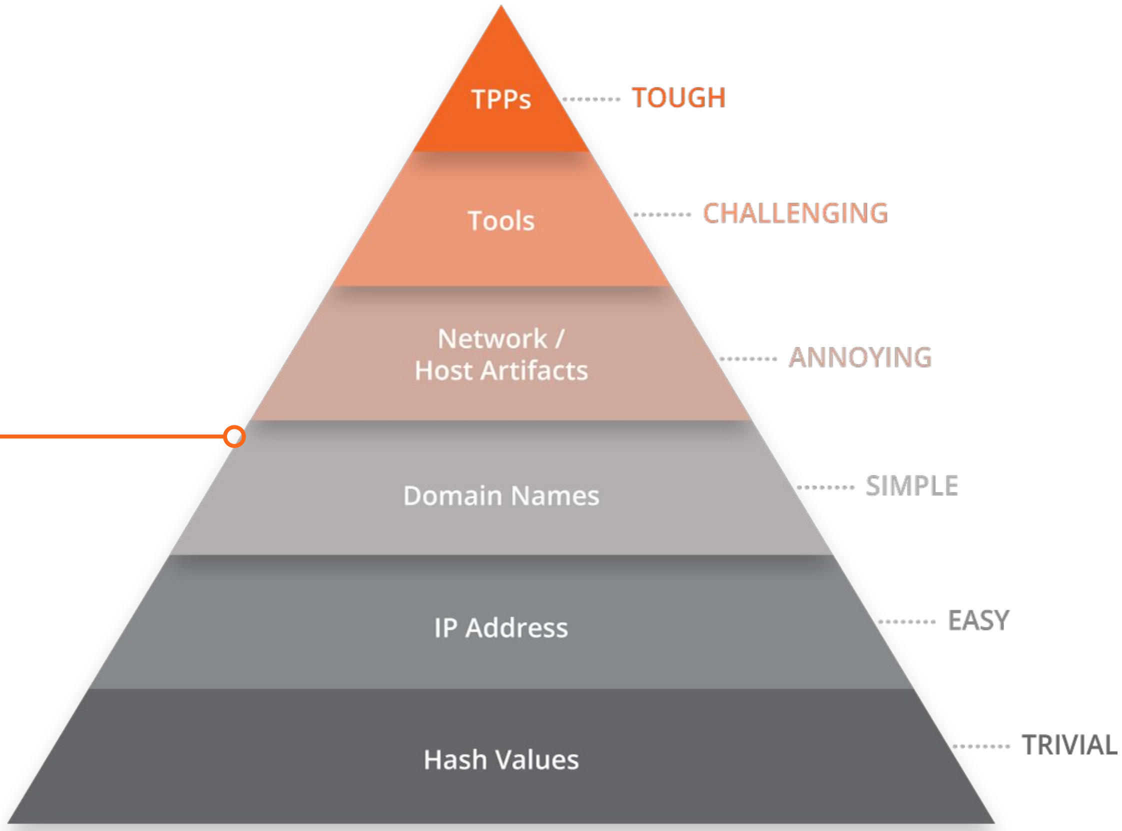
Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

The Intelligence Process

Relationship of Data, Information, and Intelligence

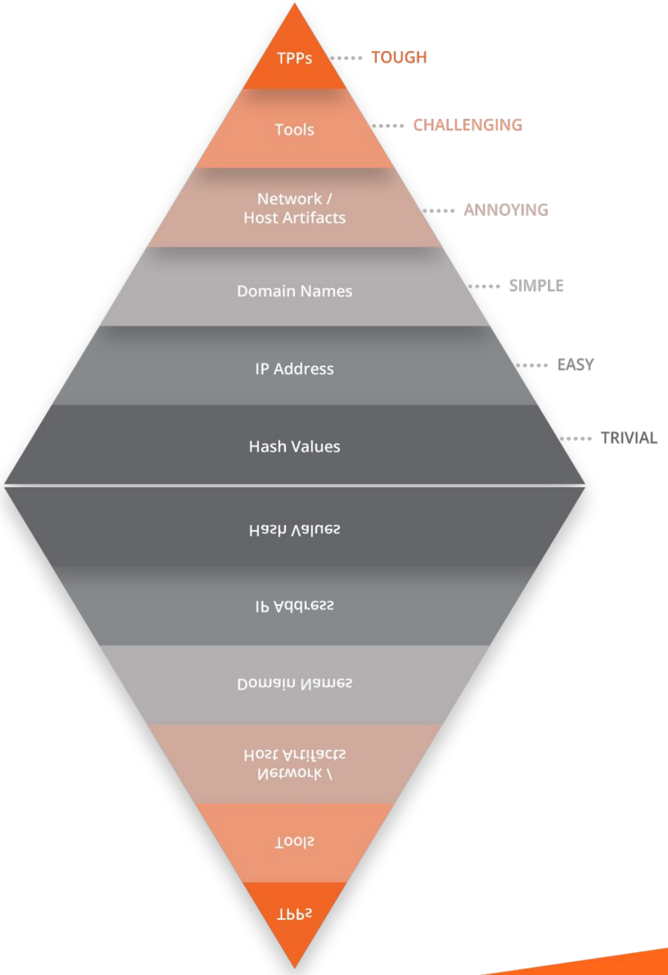


David Bianco's "Pyramid of Pain"



The Pyramid of Pain

Mirrored



Problem Definition, Part 1

Small Teams

We are a team of ten people

© 2018 ThreatConnect, Inc. All Rights Reserved.

Problem Definition, Part 2

Limited Resources

Paid data feeds

Large data volume

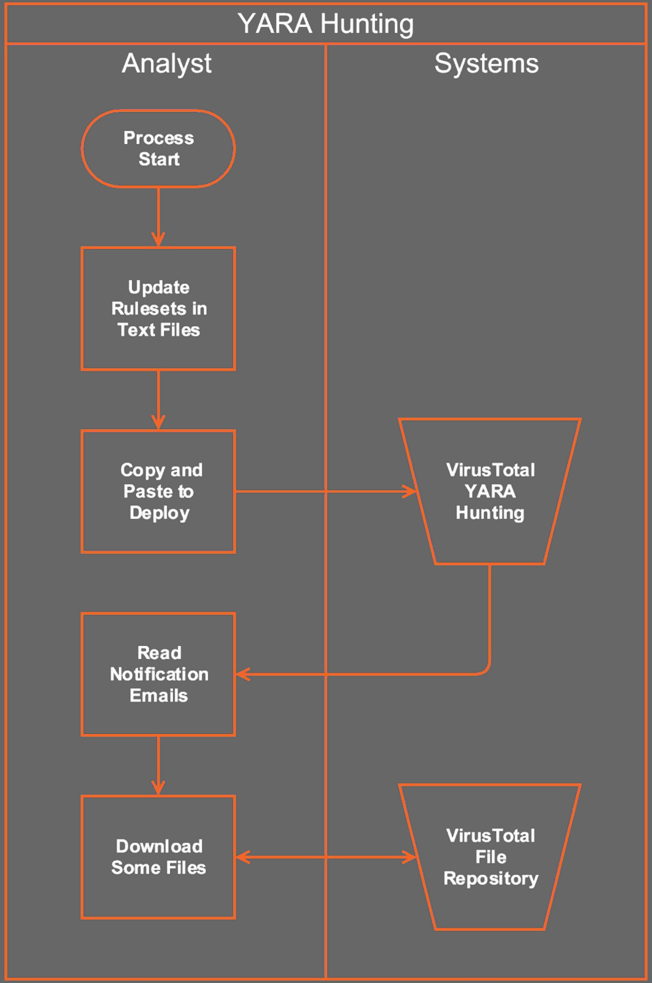
Signal to noise

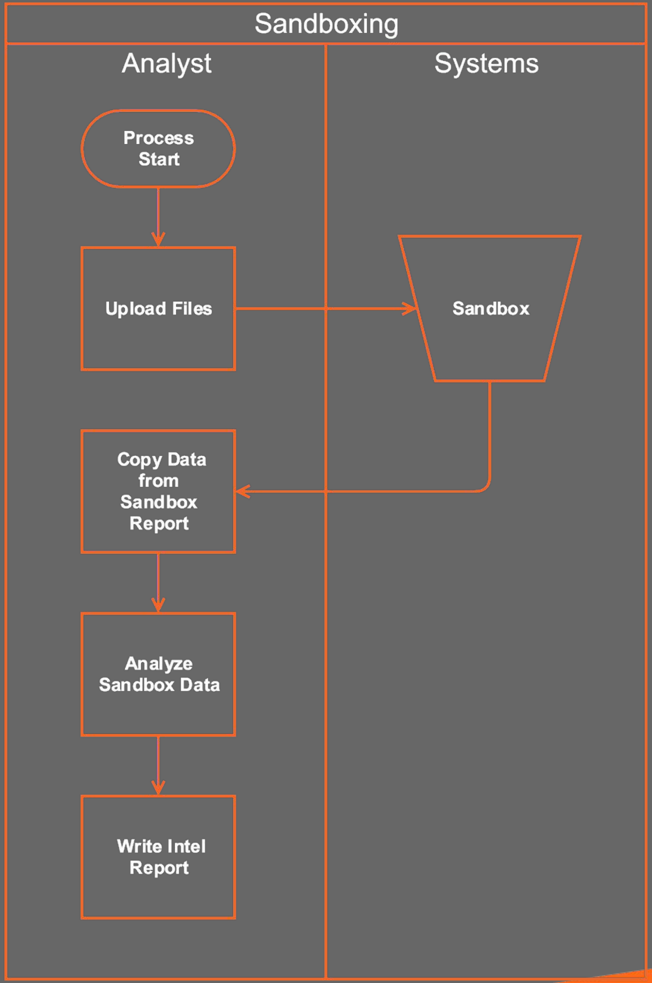
Limited tool capacity

Problem Definition, Part 3

Limited Time

Analysts must spend time analyzing, not moving data around

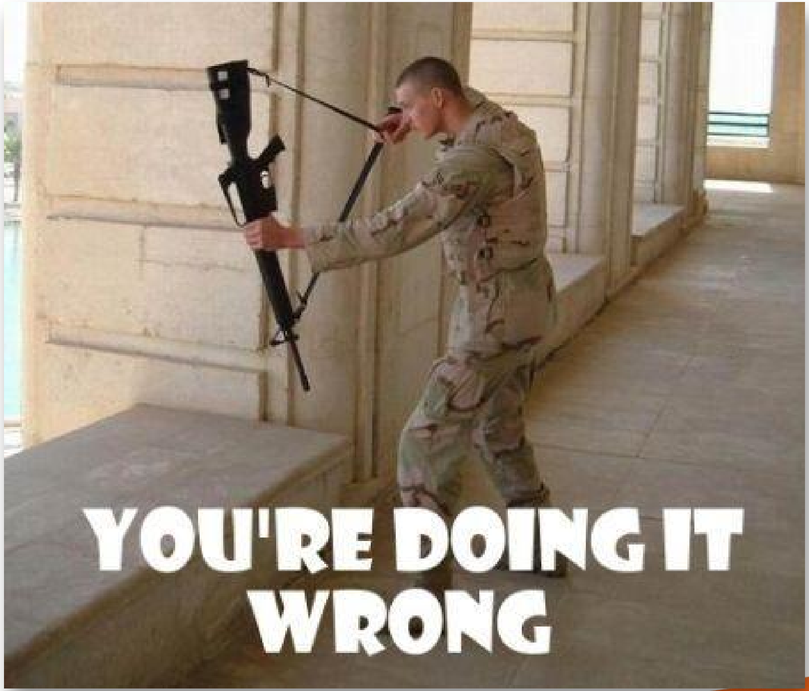

YARA Hunting
Analyst
Systems
Process Start
Update Rulesets in Text Files
Copy and Paste to Deploy
VirusTotal YARA Hunting
Read Notification Emails
Download Some Files
VirusTotal File Repository


Sandboxing
Analyst
Systems
Process Start
Upload Files
Sandbox
Copy Data from Sandbox Report
Analyze Sandbox Data
Write Intel Report

Doing It Wrong

Maintaining team YARA rules:

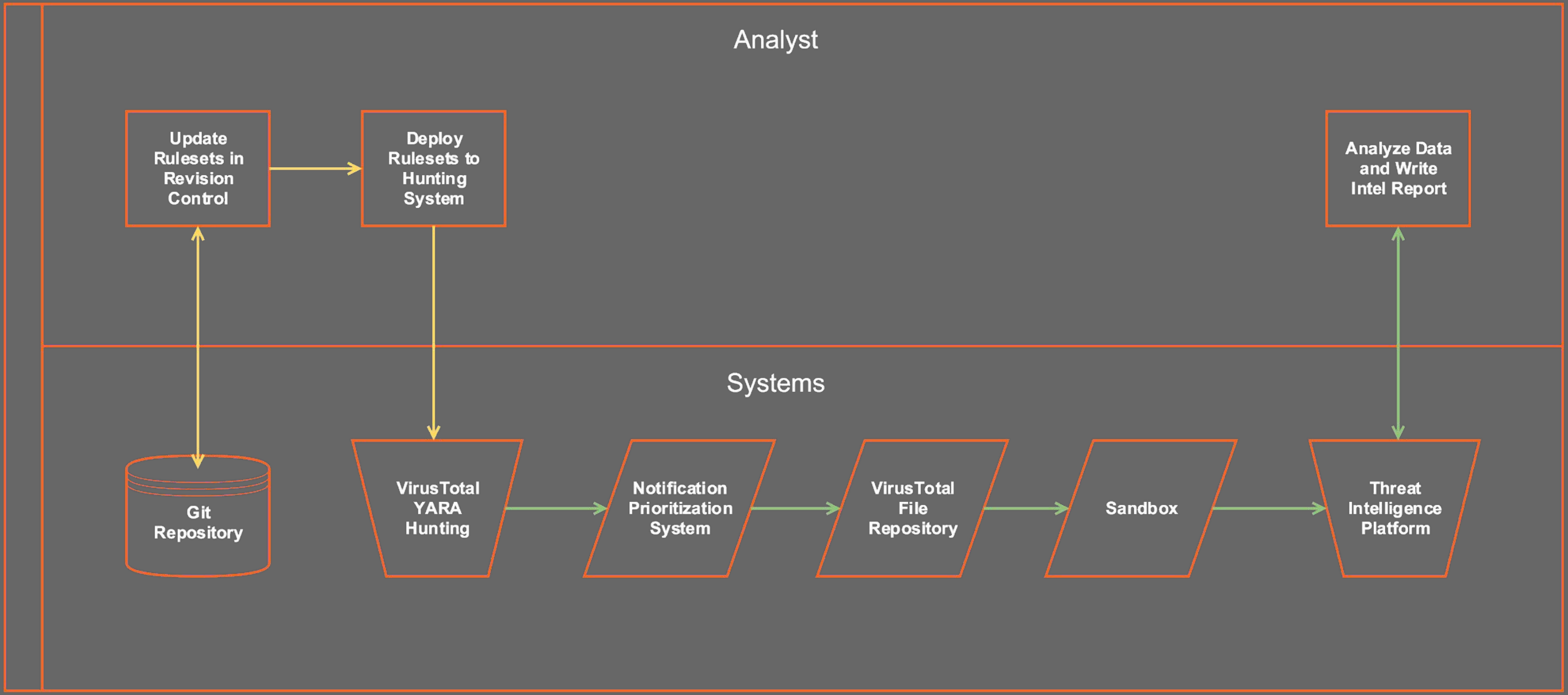
1. On a file server
2. Some person's laptop
3. Lots of people's laptops



Doing It Wrong

Wasting analyst's time:

1. Downloading files
2. Uploading files
3. Waiting for AMAs to finish


Analyst
Update Rulesets in Revision Control
Deploy Rulesets to Hunting System
Analyze Data and Write Intel Report
Systems
Git Repository
VirusTotal YARA Hunting
Notification Prioritization System
VirusTotal File Repository
Sandbox
Threat Intelligence Platform

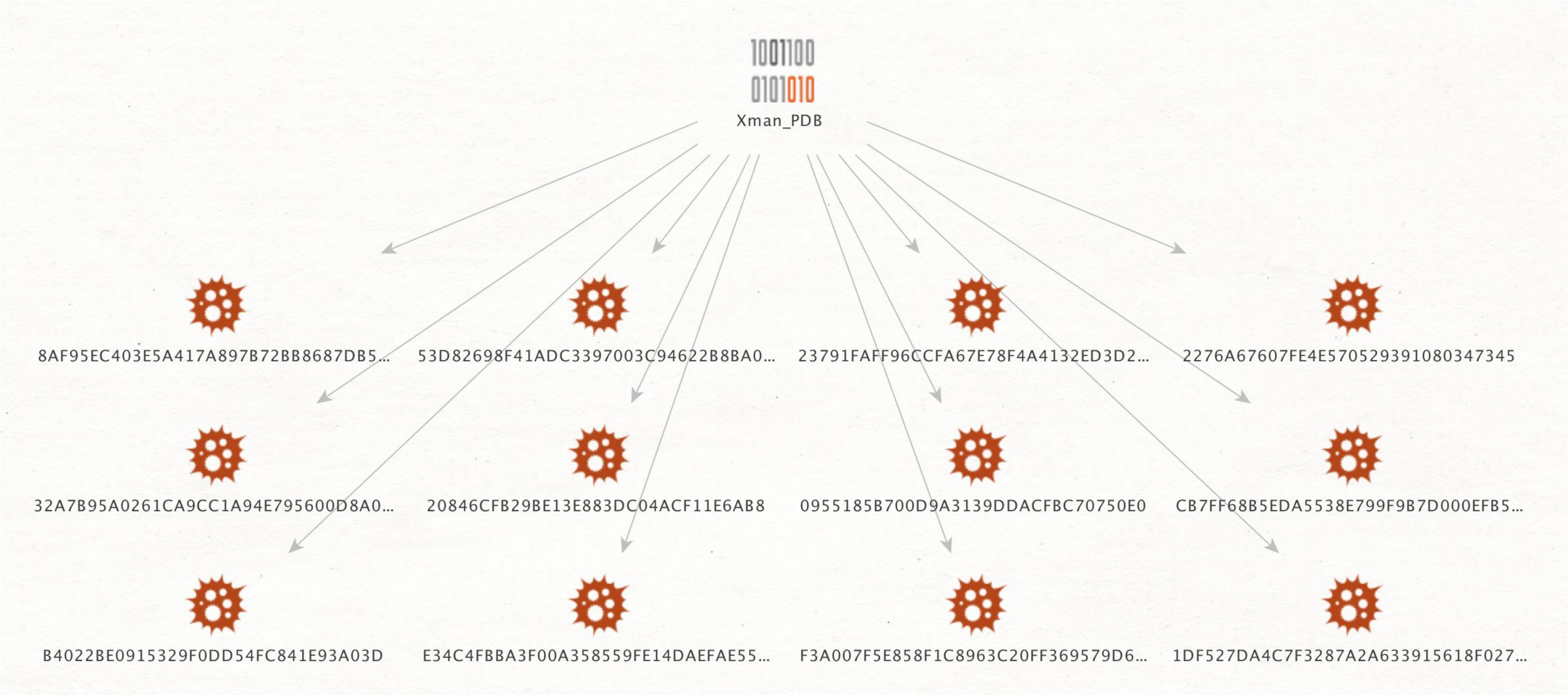
Doing It Right

- Use revision control
- We use git!
- Deployment scripts
- Sync with threat intel platform

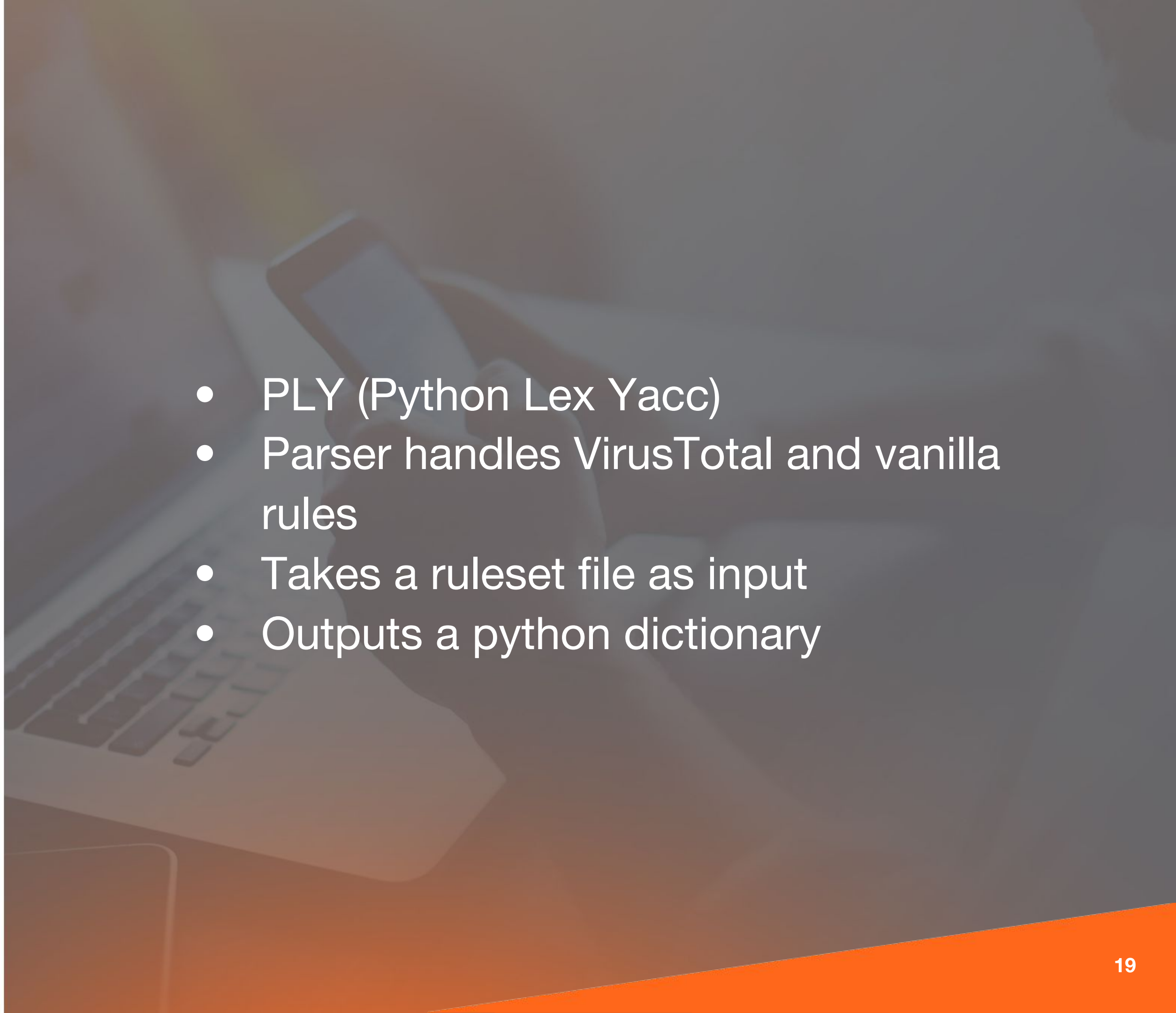
YARA Rule

```
rule Nemucod_JS_Ransom
 {
 meta:
        priority = "Medium"
        confidence = "High"
        sandbox_restricted = true
 strings:
        a$ = "If you do not pay in 3 days YOU LOOSE
                    ALL YOUR FILES" nocase wide ascii
        b$ = " + \"php4ts.dll\";" wide ascii
        c$ = "\"To restore your files you have to
                    pay \"" wide ascii
 condition:
        any of them
        and new_file
 }
```

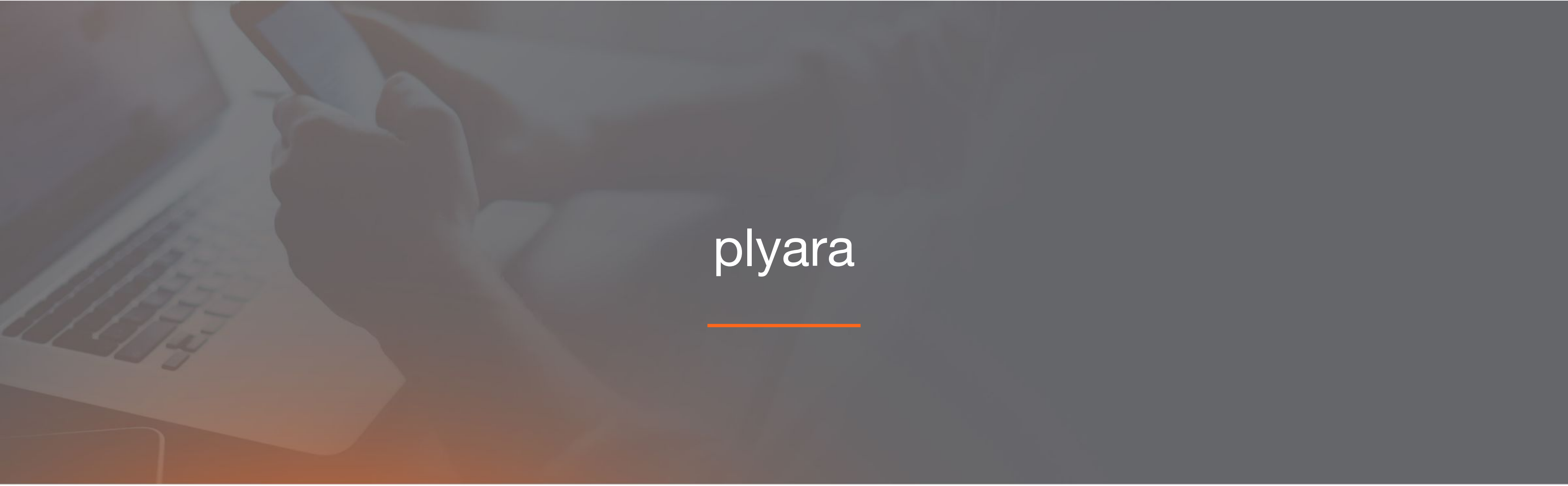
Associations for the Win


1001100
0101010
Xman_PDB
8AF95EC403E5A417A897B72BB8687DB5...
53D82698F41ADC3397003C94622B8BA0...
23791FAFF96CCFA67E78F4A4132ED3D2...
2276A67607FE4E570529391080347345
32A7B95A0261CA9CC1A94E795600D8A0...
20846CFB29BE13E883DC04ACF11E6AB8
0955185B700D9A3139DDACFBC70750E0
CB7FF68B5EDA5538E799F9B7D000EFB5...
B4022BE0915329F0DD54FC841E93A03D
E34C4FBBA3F00A358559FE14DAEFAE55...
F3A007F5E858F1C8963C20FF369579D6...
1DF527DA4C7F3287A2A633915618F027...

plyara



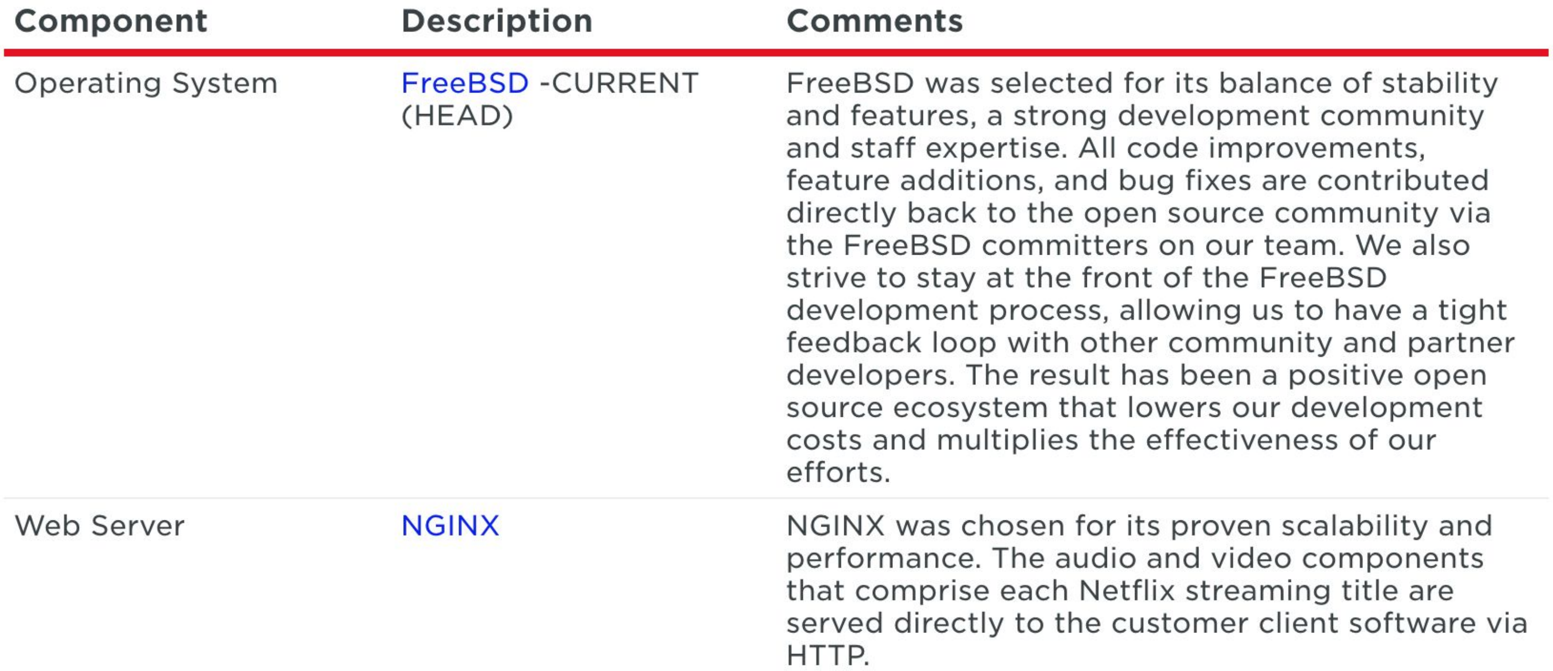
- PLY (Python Lex Yacc)
- Parser handles VirusTotal and vanilla rules
- Takes a ruleset file as input
- Outputs a python dictionary



plyara

https://github.com/8u1a/plyara

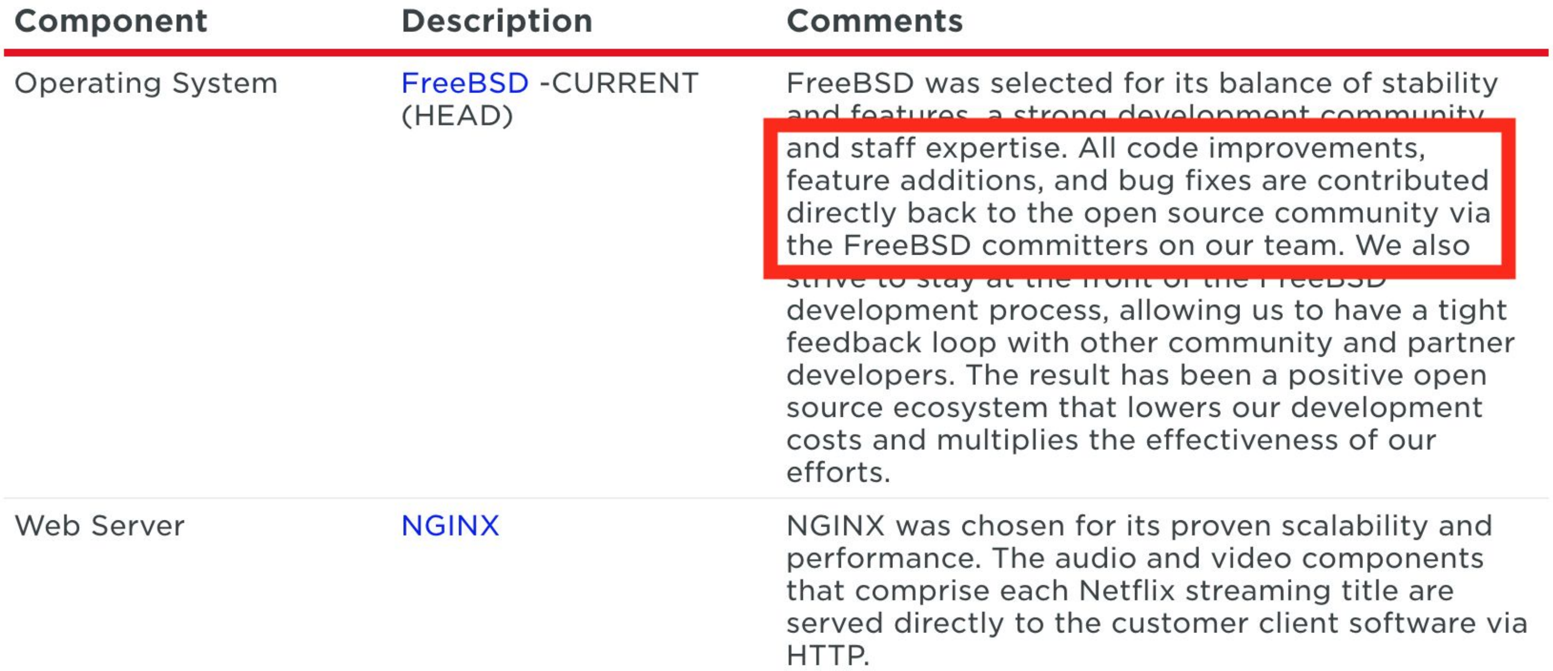
Send Improvements Upstream!



Component	Description	Comments
Operating System	FreeBSD -CURRENT (HEAD)	FreeBSD was selected for its balance of stability and features, a strong development community and staff expertise. All code improvements, feature additions, and bug fixes are contributed directly back to the open source community via the FreeBSD committers on our team. We also strive to stay at the front of the FreeBSD development process, allowing us to have a tight feedback loop with other community and partner developers. The result has been a positive open source ecosystem that lowers our development costs and multiplies the effectiveness of our efforts.
Web Server	NGINX	NGINX was chosen for its proven scalability and performance. The audio and video components that comprise each Netflix streaming title are served directly to the customer client software via HTTP.

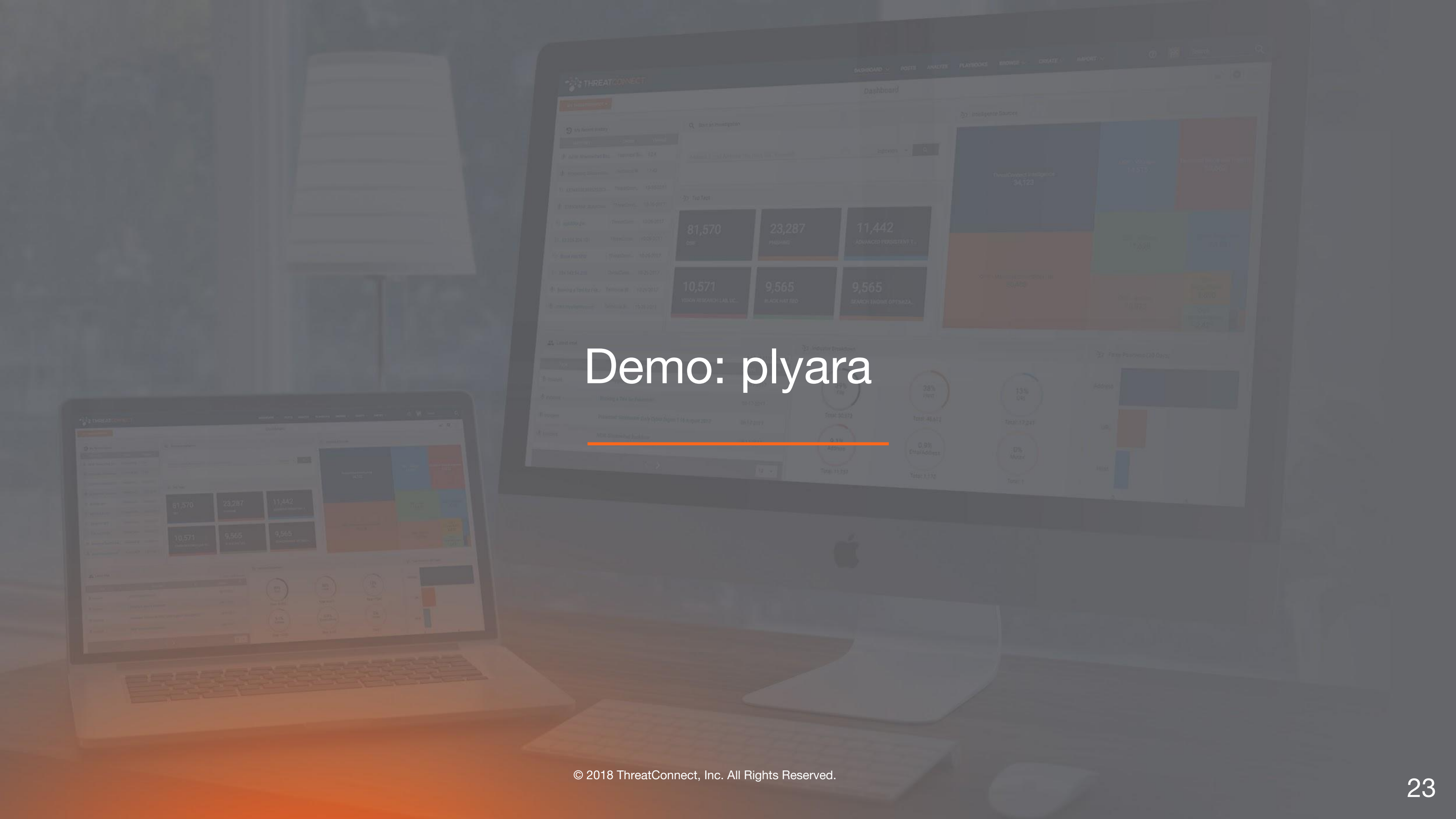
Netflix Open Connect Appliance: https://openconnect.netflix.com/en/software/

Send Improvements Upstream!



Component	Description	Comments
Operating System	FreeBSD -CURRENT (HEAD)	FreeBSD was selected for its balance of stability and features, a strong development community and staff expertise. All code improvements, feature additions, and bug fixes are contributed directly back to the open source community via the FreeBSD committers on our team. We also strive to stay at the front of the FreeBSD development process, allowing us to have a tight feedback loop with other community and partner developers. The result has been a positive open source ecosystem that lowers our development costs and multiplies the effectiveness of our efforts.
Web Server	NGINX	NGINX was chosen for its proven scalability and performance. The audio and video components that comprise each Netflix streaming title are served directly to the customer client software via HTTP.

Netflix Open Connect Appliance: https://openconnect.netflix.com/en/software/



Demo: plyara

Jupyter

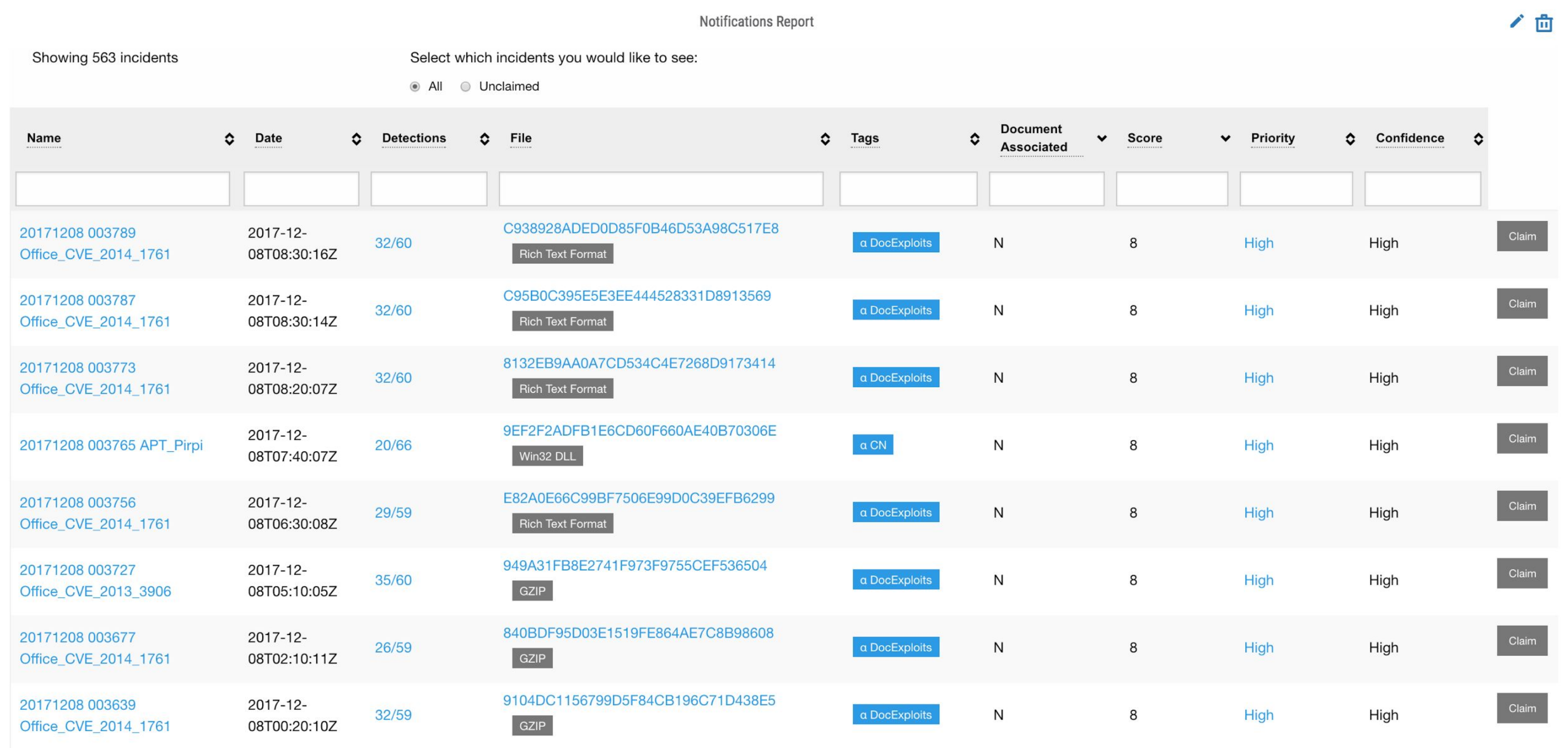
Notebook Programming

Cells

Somewhere between REPL and monolithic script

https://jupyter.org/

Prioritization



Notifications Report

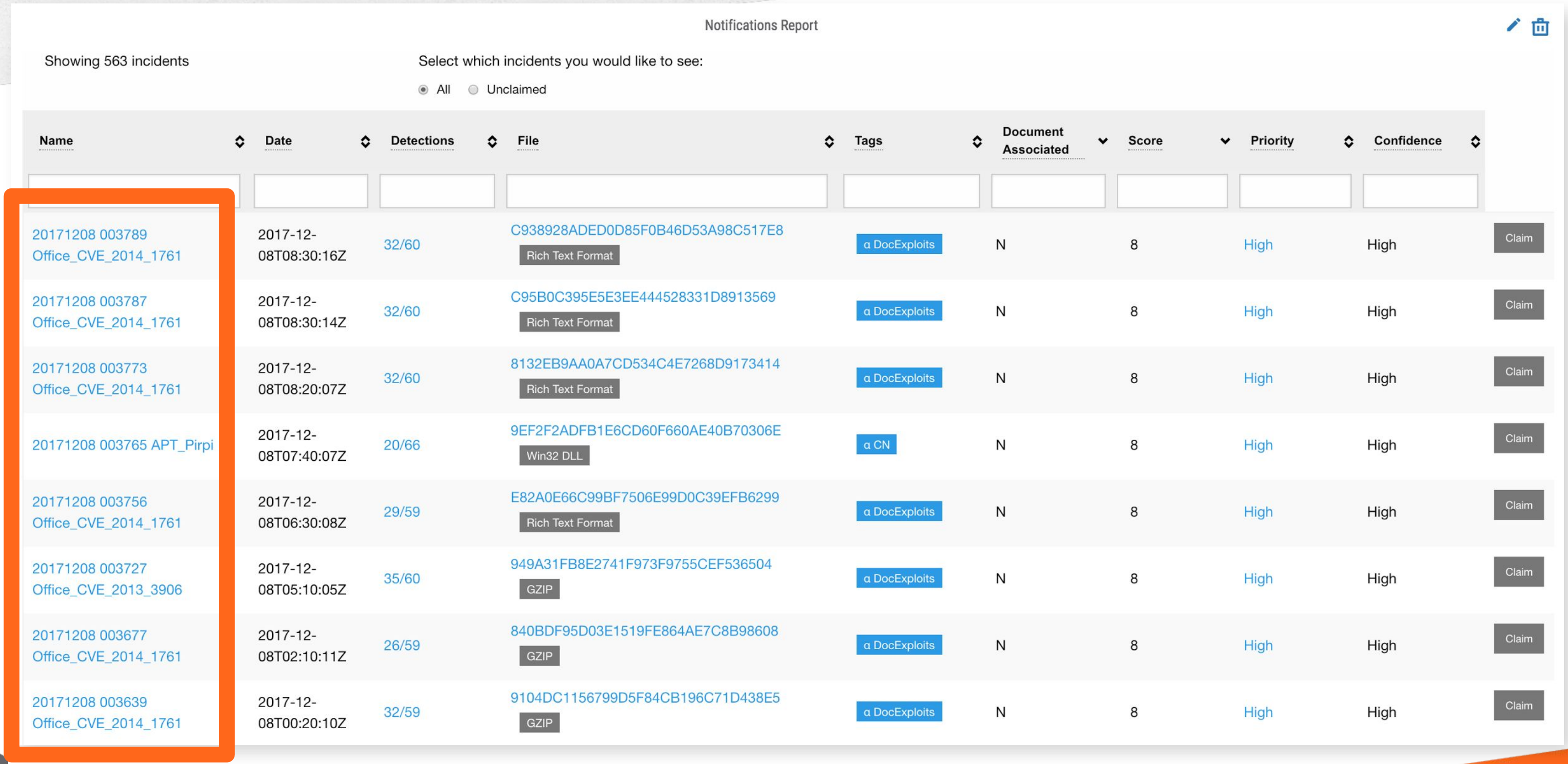
Showing 563 incidents

Select which incidents you would like to see:

● All ○ Unclaimed

Name	Date	Detections	File	Tags	Document Associated	Score	Priority	Confidence	
20171208 003789 Office_CVE_2014_1761	2017-12-08T08:30:16Z	32/60	C938928ADED0D85F0B46D53A98C517E8 Rich Text Format	ɑ DocExploits	N	8	High	High	Claim
20171208 003787 Office_CVE_2014_1761	2017-12-08T08:30:14Z	32/60	C95B0C395E5E3EE444528331D8913569 Rich Text Format	ɑ DocExploits	N	8	High	High	Claim
20171208 003773 Office_CVE_2014_1761	2017-12-08T08:20:07Z	32/60	8132EB9AA0A7CD534C4E7268D9173414 Rich Text Format	ɑ DocExploits	N	8	High	High	Claim
20171208 003765 APT_Pirpi	2017-12-08T07:40:07Z	20/66	9EF2F2ADFB1E6CD60F660AE40B70306E Win32 DLL	ɑ CN	N	8	High	High	Claim
20171208 003756 Office_CVE_2014_1761	2017-12-08T06:30:08Z	29/59	E82A0E66C99BF7506E99D0C39EFB6299 Rich Text Format	ɑ DocExploits	N	8	High	High	Claim
20171208 003727 Office_CVE_2013_3906	2017-12-08T05:10:05Z	35/60	949A31FB8E2741F973F9755CEF536504 GZIP	ɑ DocExploits	N	8	High	High	Claim
20171208 003677 Office_CVE_2014_1761	2017-12-08T02:10:11Z	26/59	840BDF95D03E1519FE864AE7C8B98608 GZIP	ɑ DocExploits	N	8	High	High	Claim
20171208 003639 Office_CVE_2014_1761	2017-12-08T00:20:10Z	32/59	9104DC1156799D5F84CB196C71D438E5 GZIP	ɑ DocExploits	N	8	High	High	Claim

Lottery Queue



Notifications Report

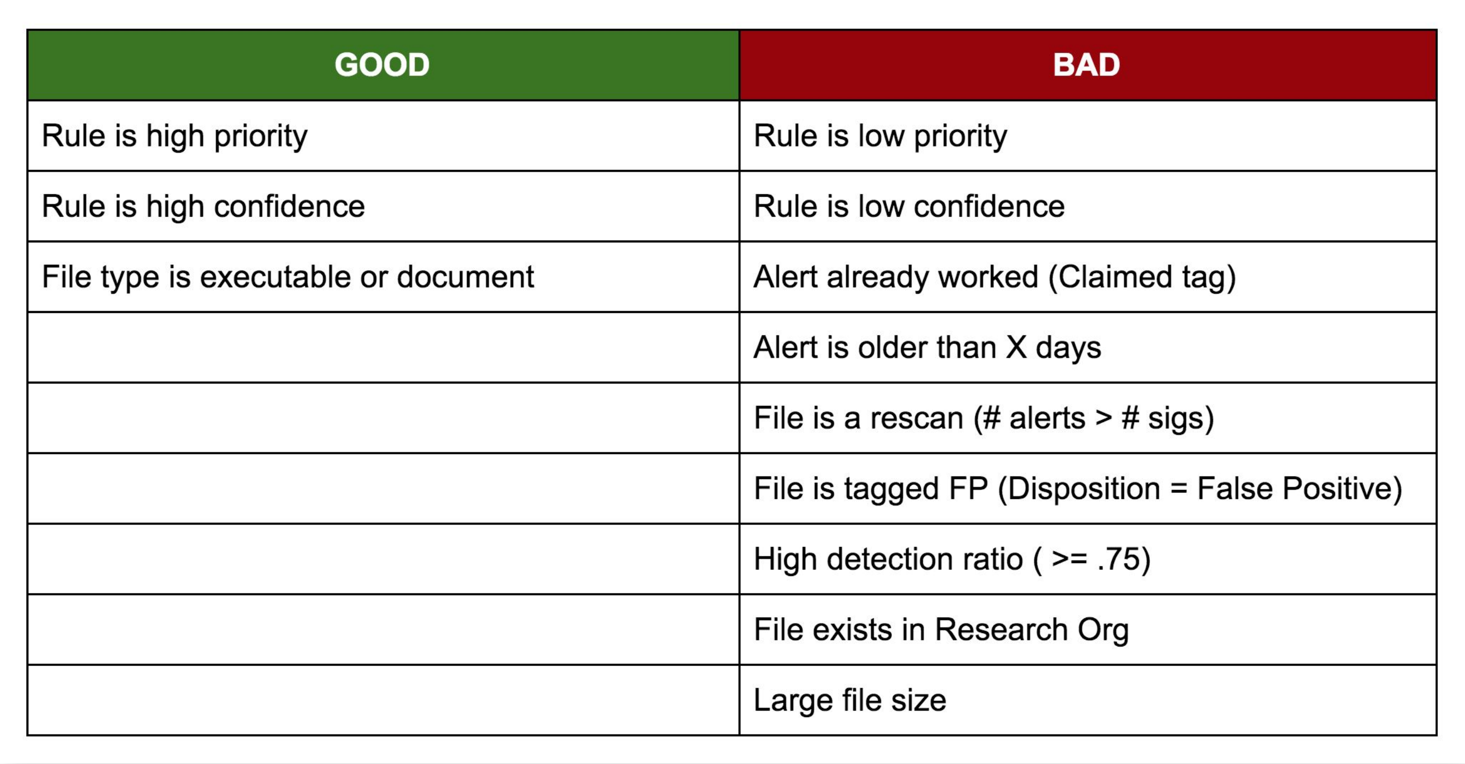
Showing 563 incidents

Select which incidents you would like to see:

● All ○ Unclaimed

Name	Date	Detections	File	Tags	Document Associated	Score	Priority	Confidence	
20171208 003789 Office_CVE_2014_1761	2017-12-08T08:30:16Z	32/60	C938928ADED0D85F0B46D53A98C517E8 Rich Text Format	α DocExploits	N	8	High	High	Claim
20171208 003787 Office_CVE_2014_1761	2017-12-08T08:30:14Z	32/60	C95B0C395E5E3EE444528331D8913569 Rich Text Format	α DocExploits	N	8	High	High	Claim
20171208 003773 Office_CVE_2014_1761	2017-12-08T08:20:07Z	32/60	8132EB9AA0A7CD534C4E7268D9173414 Rich Text Format	α DocExploits	N	8	High	High	Claim
20171208 003765 APT_Pirpi	2017-12-08T07:40:07Z	20/66	9EF2F2ADFB1E6CD60F660AE40B70306E Win32 DLL	α CN	N	8	High	High	Claim
20171208 003756 Office_CVE_2014_1761	2017-12-08T06:30:08Z	29/59	E82A0E66C99BF7506E99D0C39EFB6299 Rich Text Format	α DocExploits	N	8	High	High	Claim
20171208 003727 Office_CVE_2013_3906	2017-12-08T05:10:05Z	35/60	949A31FB8E2741F973F9755CEF536504 GZIP	α DocExploits	N	8	High	High	Claim
20171208 003677 Office_CVE_2014_1761	2017-12-08T02:10:11Z	26/59	840BDF95D03E1519FE864AE7C8B98608 GZIP	α DocExploits	N	8	High	High	Claim
20171208 003639 Office_CVE_2014_1761	2017-12-08T00:20:10Z	32/59	9104DC1156799D5F84CB196C71D438E5 GZIP	α DocExploits	N	8	High	High	Claim

Scoring



GOOD	BAD
Rule is high priority	Rule is low priority
Rule is high confidence	Rule is low confidence
File type is executable or document	Alert already worked (Claimed tag)
	Alert is older than X days
	File is a rescan (# alerts > # sigs)
	File is tagged FP (Disposition = False Positive)
	High detection ratio (>= .75)
	File exists in Research Org
	Large file size

Non-Intuitive Ordering

High Priority / High Confidence

High Priority / Medium Confidence

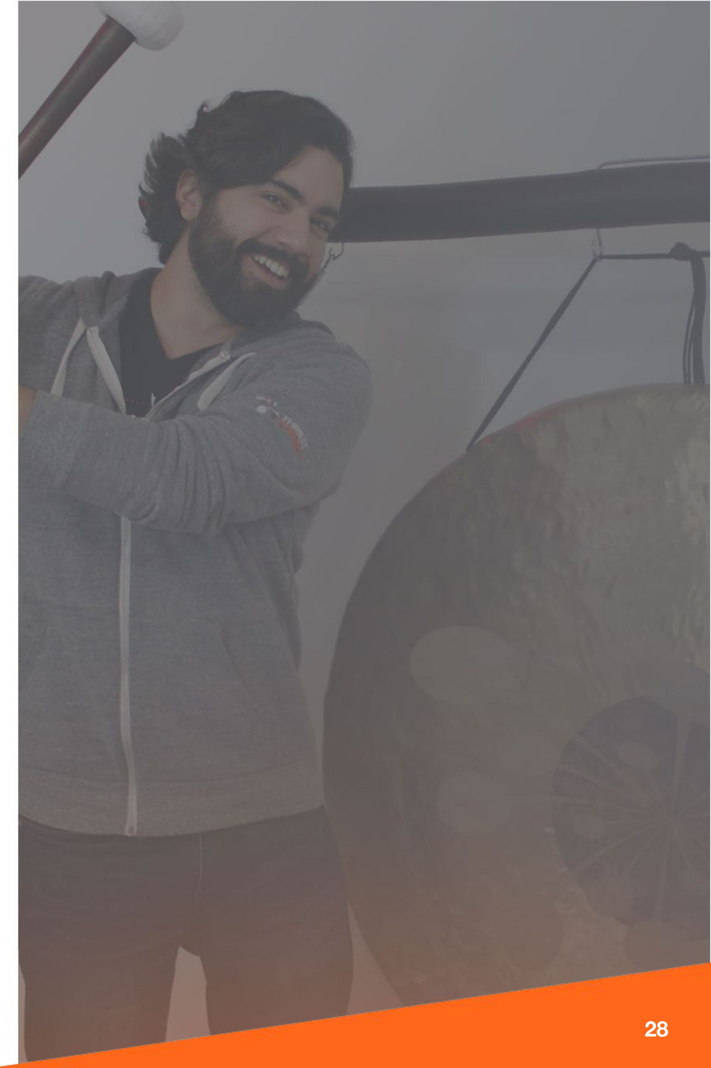
Medium Priority / High Confidence

Medium Priority / Medium Confidence

High Priority / Low Confidence

Medium Priority / Low Confidence

Low Priority / Low Confidence



Non-Intuitive Ordering

High Priority / High Confidence

High Priority / Medium Confidence

Medium Priority / High Confidence

Medium Priority / Medium Confidence

High Priority / Low Confidence

Medium Priority / Low Confidence

Low Priority / Low Confidence

Prioritization Meetings

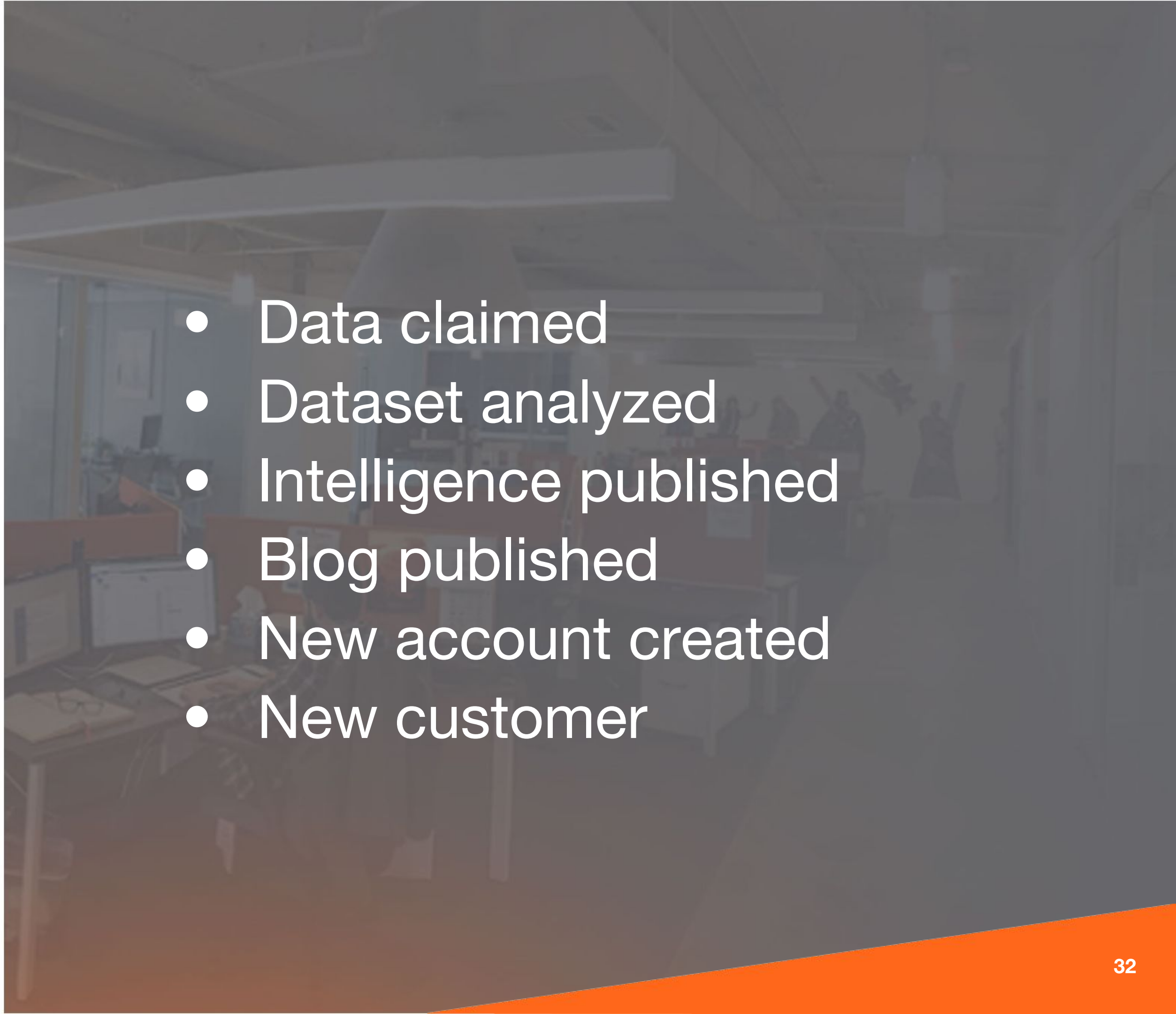
I DON'T ALWAYS SHOW UP TO MEETINGS
BUT WHEN I DO, I DERAIL THEM WITH STUPID QUESTIONS

Automate AMAs

- Cuckoo Sandbox
- Joe Sandbox Cloud
- VxStream
- VMRay
- Lastline
- ThreatGrid
- ReversingLabs
- Your AMA Here!

Future Work

Business Value (BV)



- Data claimed
- Dataset analyzed
- Intelligence published
- Blog published
- New account created
- New customer

Budgets

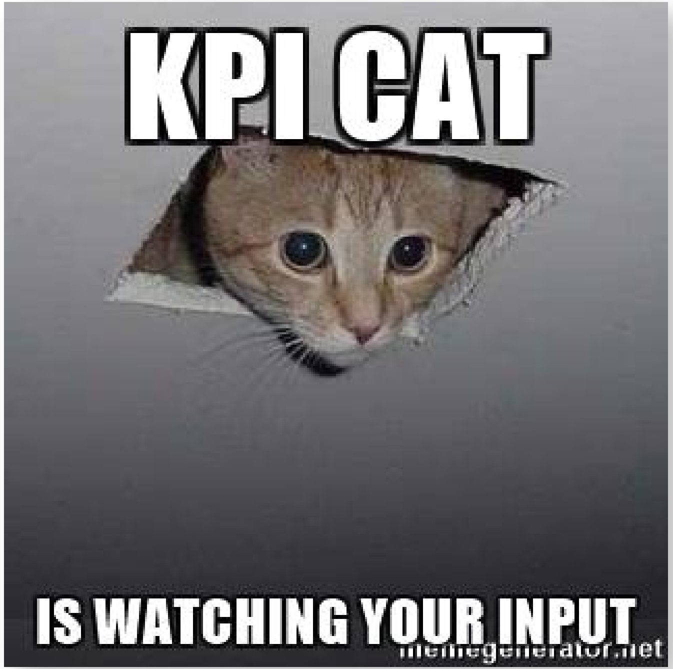
Happy Bean Counters

- Maximize collection -> exploitation
- Collect metrics on utilization
- Establish KPIs
- AMAs at maximum capacity

Speaking to Management

Key Performance Indicators

A **Key Performance Indicator** is a measurable value that demonstrates how effectively a company is achieving key business objectives.



Sources of Samples

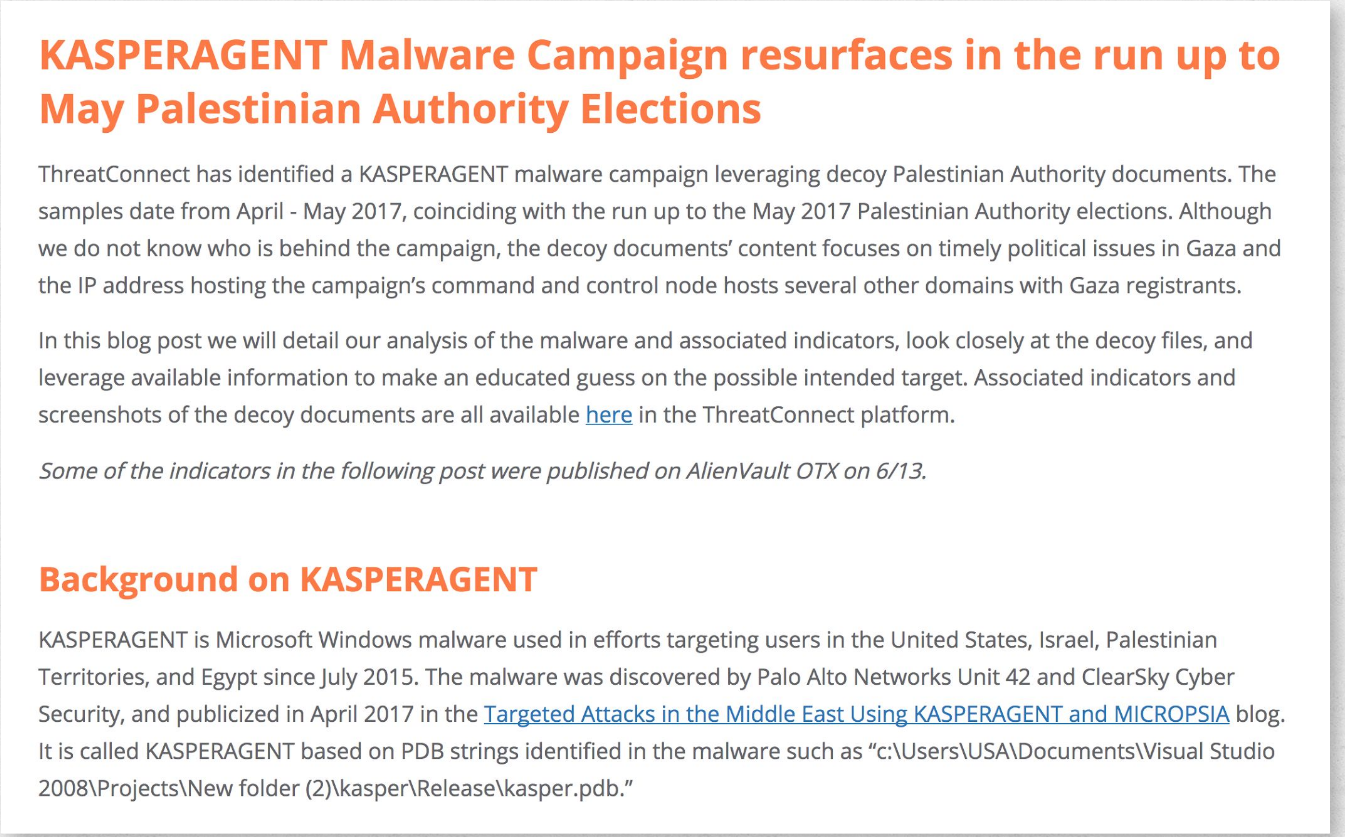
- Carved from Network Capture (Use Bro!!)
- Incoming email attachments
- Endpoint collections (AV and otherwise)

Sources of Samples

- Carved from Network Capture (Use Bro!!)
- Incoming email attachments
- Endpoint collections (AV and otherwise)
- Supply chain (CCleaner!!!!!!!!!!)

Success Stories

https://threatconnect.com/blog/kasperagent-malware-campaign/



KASPERAGENT Malware Campaign resurfaces in the run up to May Palestinian Authority Elections

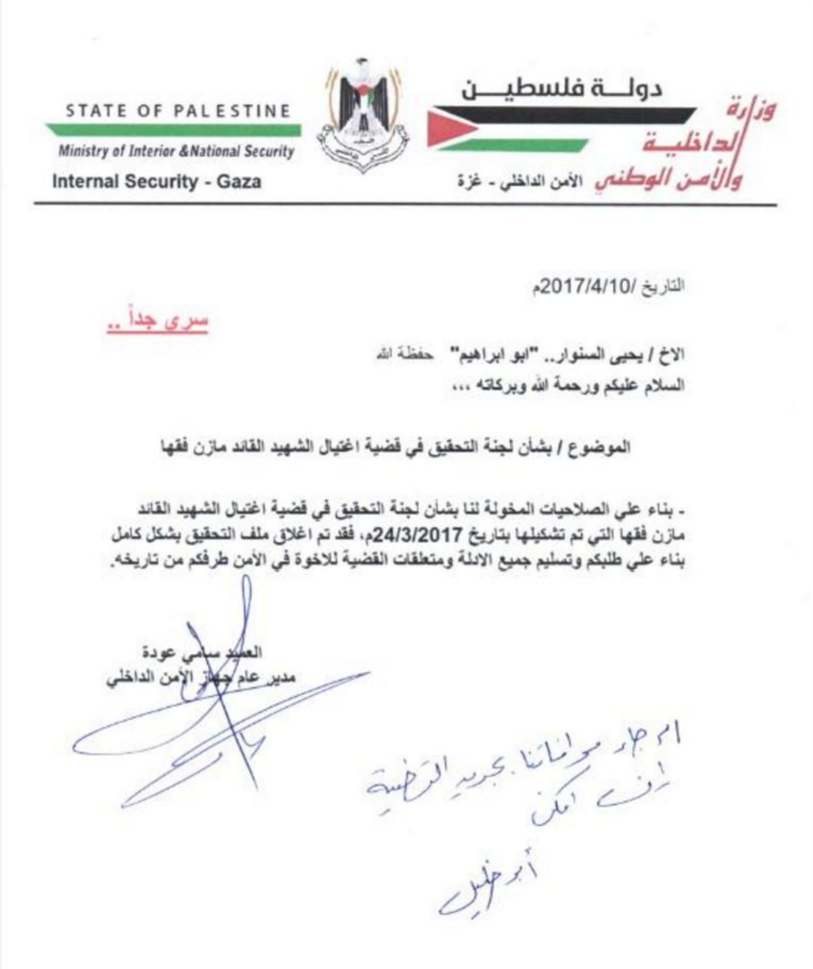
ThreatConnect has identified a KASPERAGENT malware campaign leveraging decoy Palestinian Authority documents. The samples date from April - May 2017, coinciding with the run up to the May 2017 Palestinian Authority elections. Although we do not know who is behind the campaign, the decoy documents' content focuses on timely political issues in Gaza and the IP address hosting the campaign's command and control node hosts several other domains with Gaza registrants.

In this blog post we will detail our analysis of the malware and associated indicators, look closely at the decoy files, and leverage available information to make an educated guess on the possible intended target. Associated indicators and screenshots of the decoy documents are all available here in the ThreatConnect platform.

Some of the indicators in the following post were published on AlienVault OTX on 6/13.

Background on KASPERAGENT

KASPERAGENT is Microsoft Windows malware used in efforts targeting users in the United States, Israel, Palestinian Territories, and Egypt since July 2015. The malware was discovered by Palo Alto Networks Unit 42 and ClearSky Cyber Security, and publicized in April 2017 in the Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA blog. It is called KASPERAGENT based on PDB strings identified in the malware such as "c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper\Release\kasper.pdb."



STATE OF PALESTINE
Ministry of Interior &National Security
Internal Security - Gaza

دولـــة فلسطيـــن
وزارة الداخليـة والأمـن الوطنـي
الأمن الداخلي - غزة

التاريخ /2017/4/10م

سري جداً ..

الاخ / يحيى السنوار.. "ابو ابراهيم" حفظه الله
السلام عليكم ورحمة الله وبركاته ،،،

الموضوع / بشأن لجنة التحقيق في قضية اغتيال الشهيد القائد مازن فقها

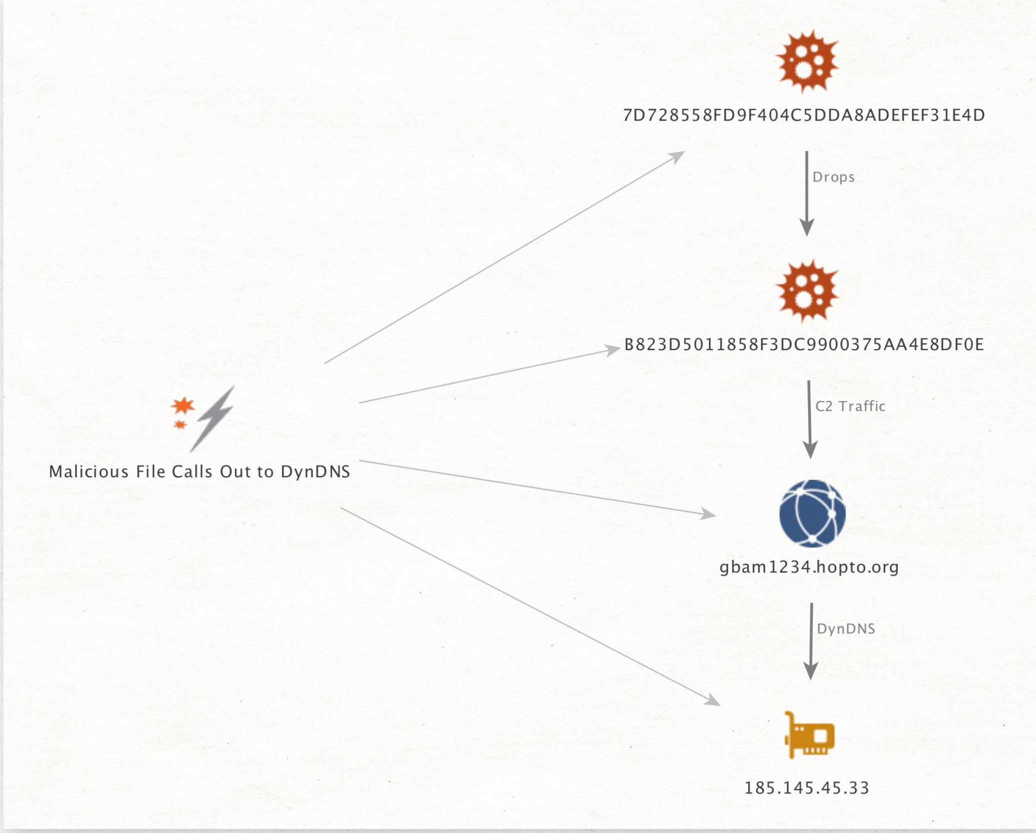
- بناء علي الصلاحيات المخولة لنا بشأن لجنة التحقيق في قضية اغتيال الشهيد القائد مازن فقها التي تم تشكيلها بتاريخ **24/3/2017**م، فقد تم اغلاق ملف التحقيق بشكل كامل بناء علي طلبكم وتسليم جميع الادلة ومتعلقات القضية للاخوة في الأمن طرفكم من تاريخه.

العميد سامي عودة
مدير عام جهاز الأمن الداخلي

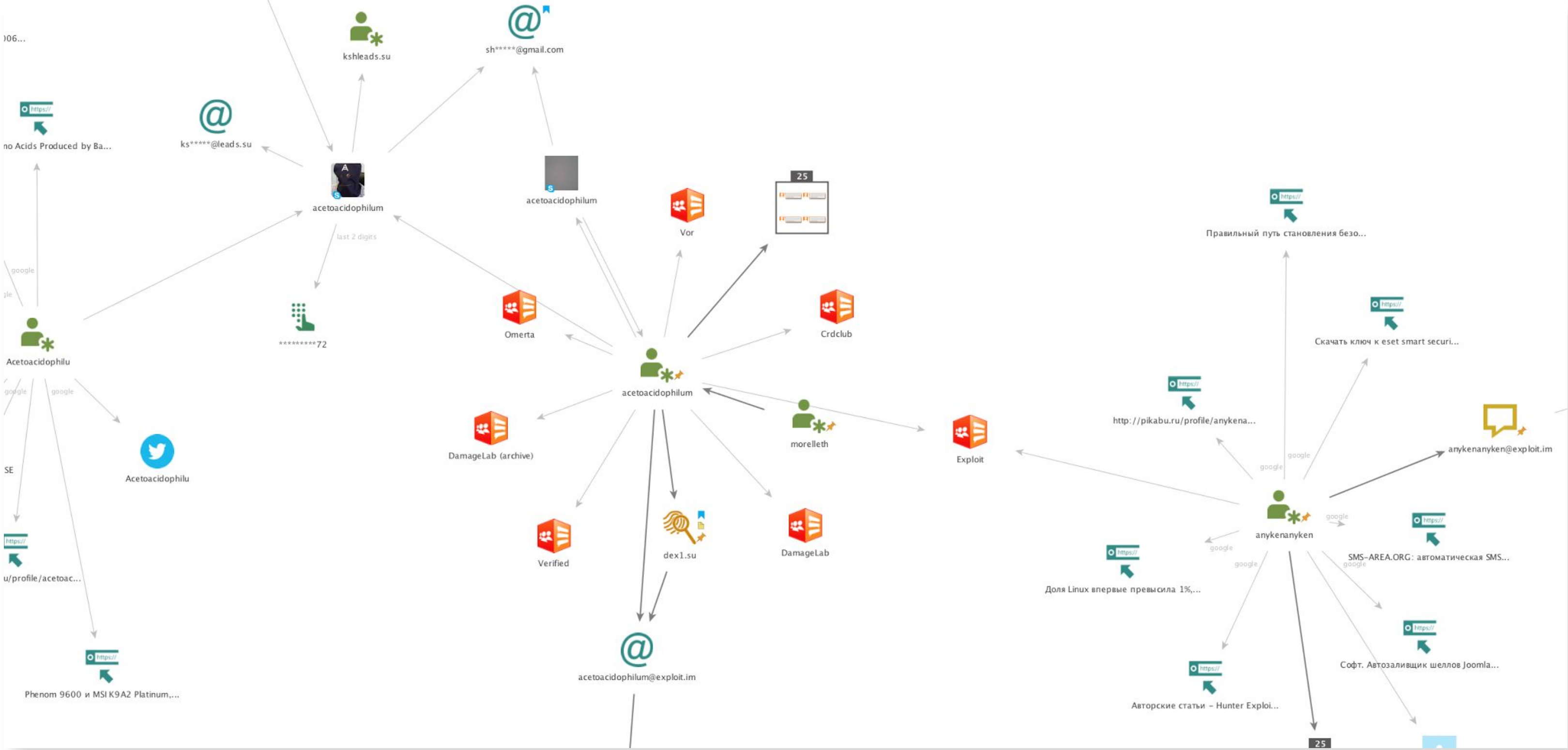
ارجو موافاتنا بجريدة الرسمية
ان امكن

أبو خليل

Success Stories


7D728558FD9F404C5DDA8ADEFEF31E4D
Drops
B823D5011858F3DC9900375AA4E8DF0E
C2 Traffic
Malicious File Calls Out to DynDNS
gbam1234.hopto.org
DynDNS
185.145.45.33

Success Stories



Key Takeaways and Lessons Learned

- Organize signatures in revision control
- Automate between systems in tool chain
- Separate queues by signature type
  - Attack Pattern
  - Malware family / Adversary
- Periodic prioritization meetings
- SEND YOUR OPEN SOURCE CHANGES UPSTREAM!!!!!

PEPE

Thank You

threatconnect.com/blog

@ThreatConnect

@MalwareUtkonos