The only way to survive is to automate your SOC

Roberto Sponchioni
Senior Manager, Security Engineering, DocuSign

HackInBo® Winter 2019 Edition
13ª EDIZIONE

AGENDA

- Who am I
- DocuSign
- Data Breaches
- SOC automation
- Scenarios (Phishing / Malware)
- Conclusion / Takeaways

WHO AM I

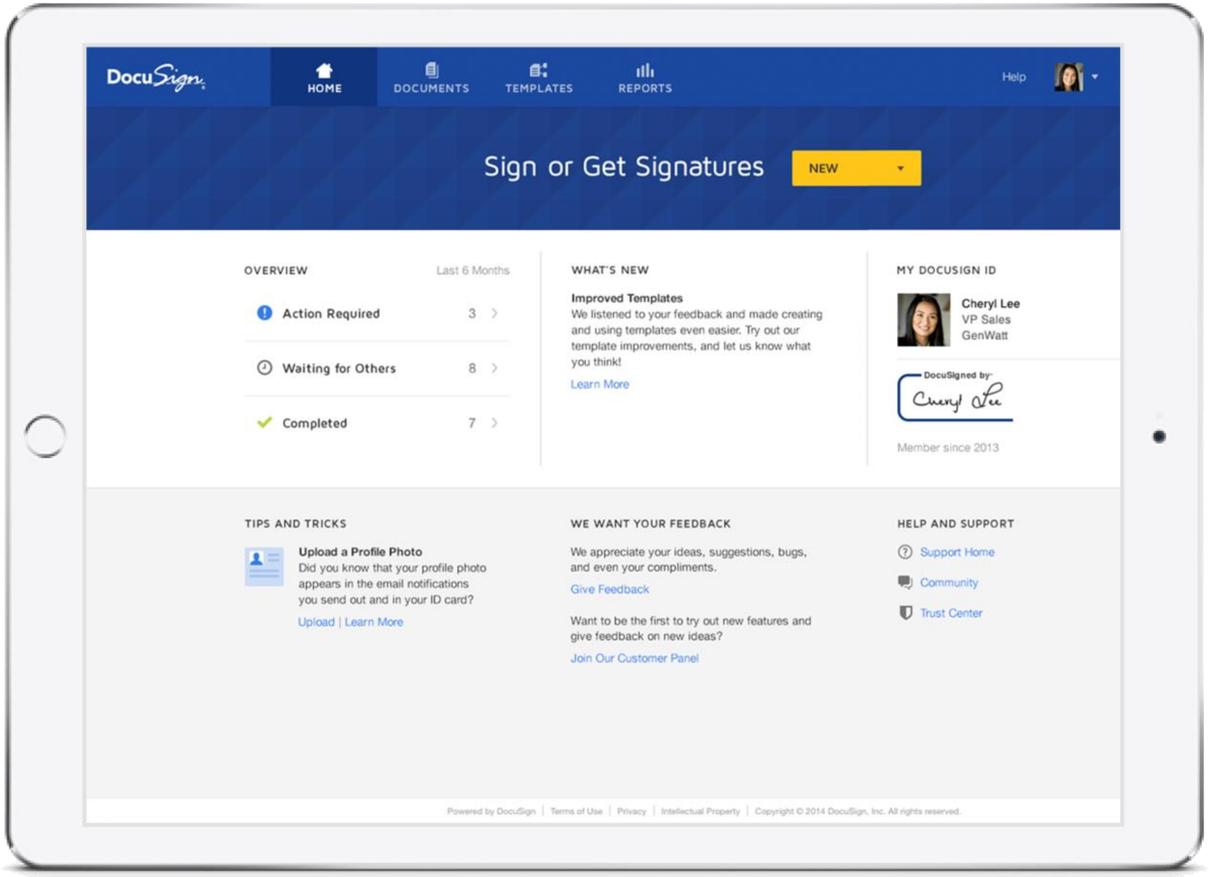
- Italian, based in Dublin, Ireland
- Senior Manager, Security Engineering @DocuSign
- Former Senior Anti-Malware Engineer @Symantec
- Former Security Consultant (PT/VA, Incident Response)

Contacts:

- Twitter @Ptr32Void
- https://www.linkedin.com/in/robertosponchioni/
- Roberto.Sponchioni@docusign.com

DocuSign

- DocuSign digitally transforms how you do business via contracts and other types of agreements.
- API Integration
- Collect Payments
- eSignature
- SaaS



Improved Templates
We listened to your feedback and made creating and using templates even easier. Try out our template improvements, and let us know what you think!
Learn More

Cheryl Lee
VP Sales
GenWatt

Member since 2013

Upload a Profile Photo
Did you know that your profile photo appears in the email notifications you send out and in your ID card?
Upload | Learn More

We appreciate your ideas, suggestions, bugs, and even your compliments.
Give Feedback

Want to be the first to try out new features and give feedback on new ideas?
Join Our Customer Panel

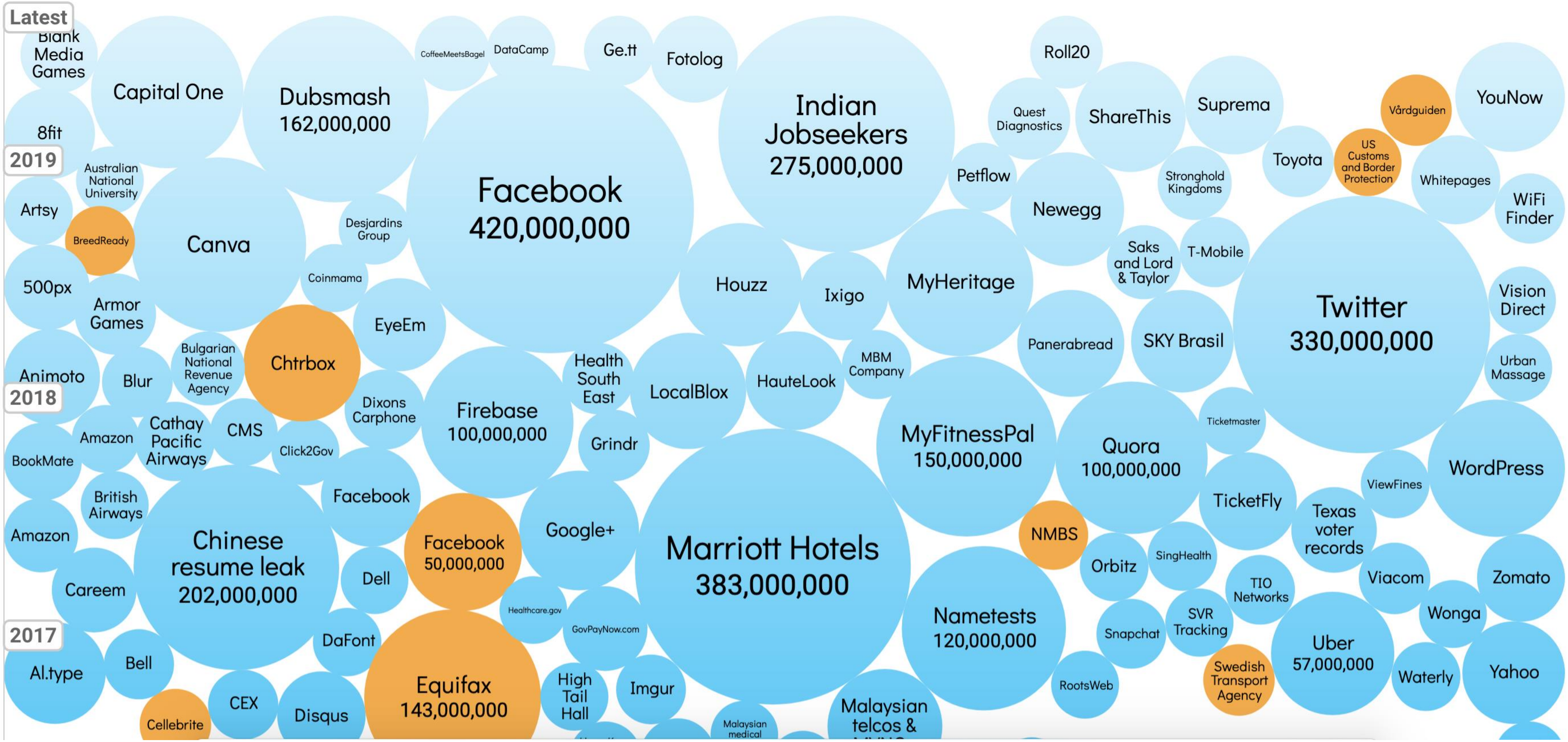
Powered by DocuSign | Terms of Use | Privacy | Intellectual Property | Copyright © 2014 DocuSign, Inc. All rights reserved.

Main SaaS Threats / Risks

There are different threats for SaaS platforms, such as:

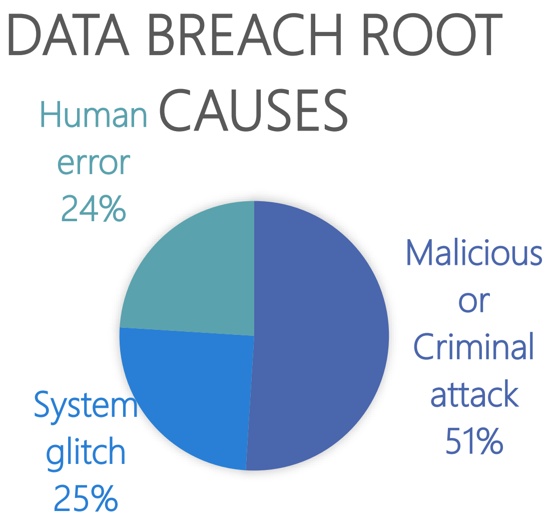
- Phishing – DS is in the top 5 most phished brands
- Fraud / Account Abuse
- Availability / Downtime
- Malware
- Data Security
- CEO Fraud / Social Engineering
- Data Exfiltration
- 3rd Party Risk
- Etc..

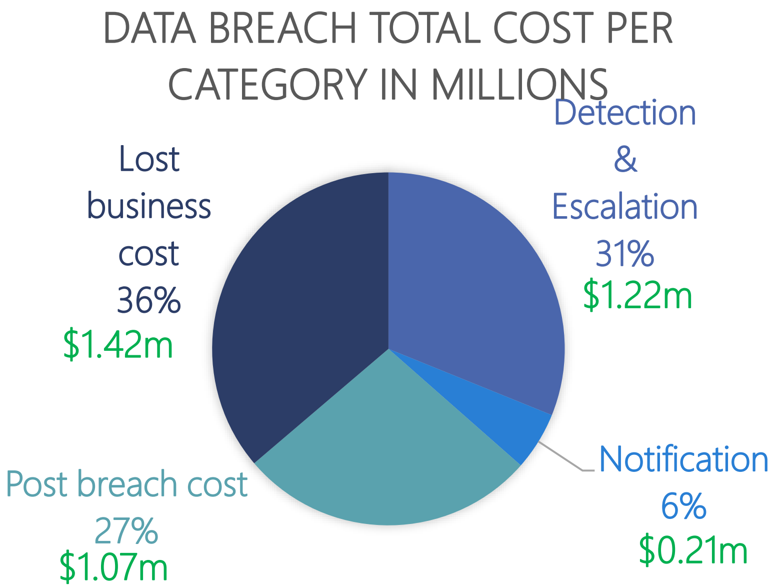
Data breaches over time



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

The importance of keeping your data secure





TIME TO IDENTIFY AND CONTAIN A DATA BREACH

279 DAYS

AVERAGE TOTAL COST OF A DATA BREACH

$3.92 M

Average cost of data breach in orgs without security automation

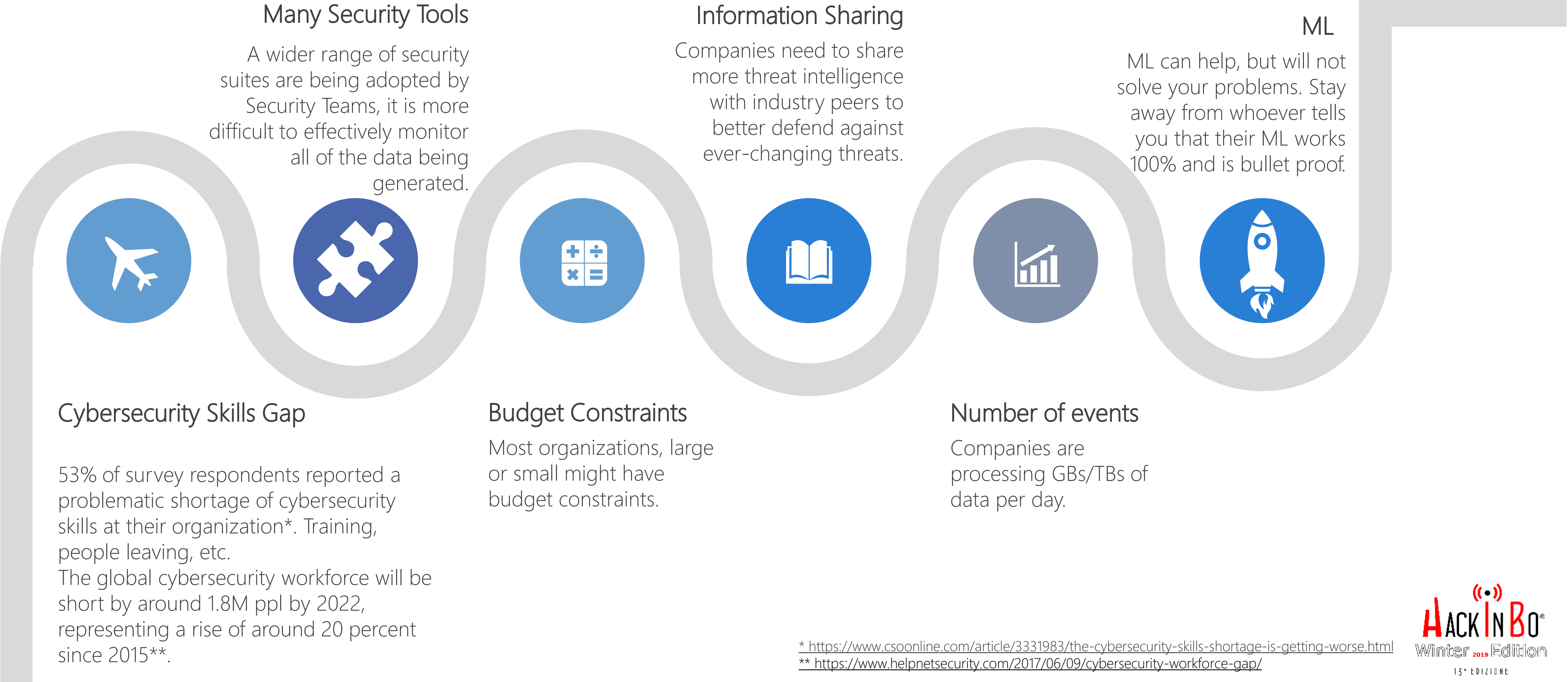
95% higher

AVERAGE SIZE OF A DATA BREACH

25,575 RECORDS

* Cost of a Data Breach Report 2019

Why Automating your SOC environment



Cybersecurity Skills Gap

53% of survey respondents reported a problematic shortage of cybersecurity skills at their organization*. Training, people leaving, etc.
The global cybersecurity workforce will be short by around 1.8M ppl by 2022, representing a rise of around 20 percent since 2015**.

Many Security Tools

A wider range of security suites are being adopted by Security Teams, it is more difficult to effectively monitor all of the data being generated.

Budget Constraints

Most organizations, large or small might have budget constraints.

Information Sharing

Companies need to share more threat intelligence with industry peers to better defend against ever-changing threats.

Number of events

Companies are processing GBs/TBs of data per day.

ML

ML can help, but will not solve your problems. Stay away from whoever tells you that their ML works 100% and is bullet proof.

* https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html
** https://www.helpnetsecurity.com/2017/06/09/cybersecurity-workforce-gap/

Security Orchestration, Automation & Response Tool

Commercial & Free

Commercials:

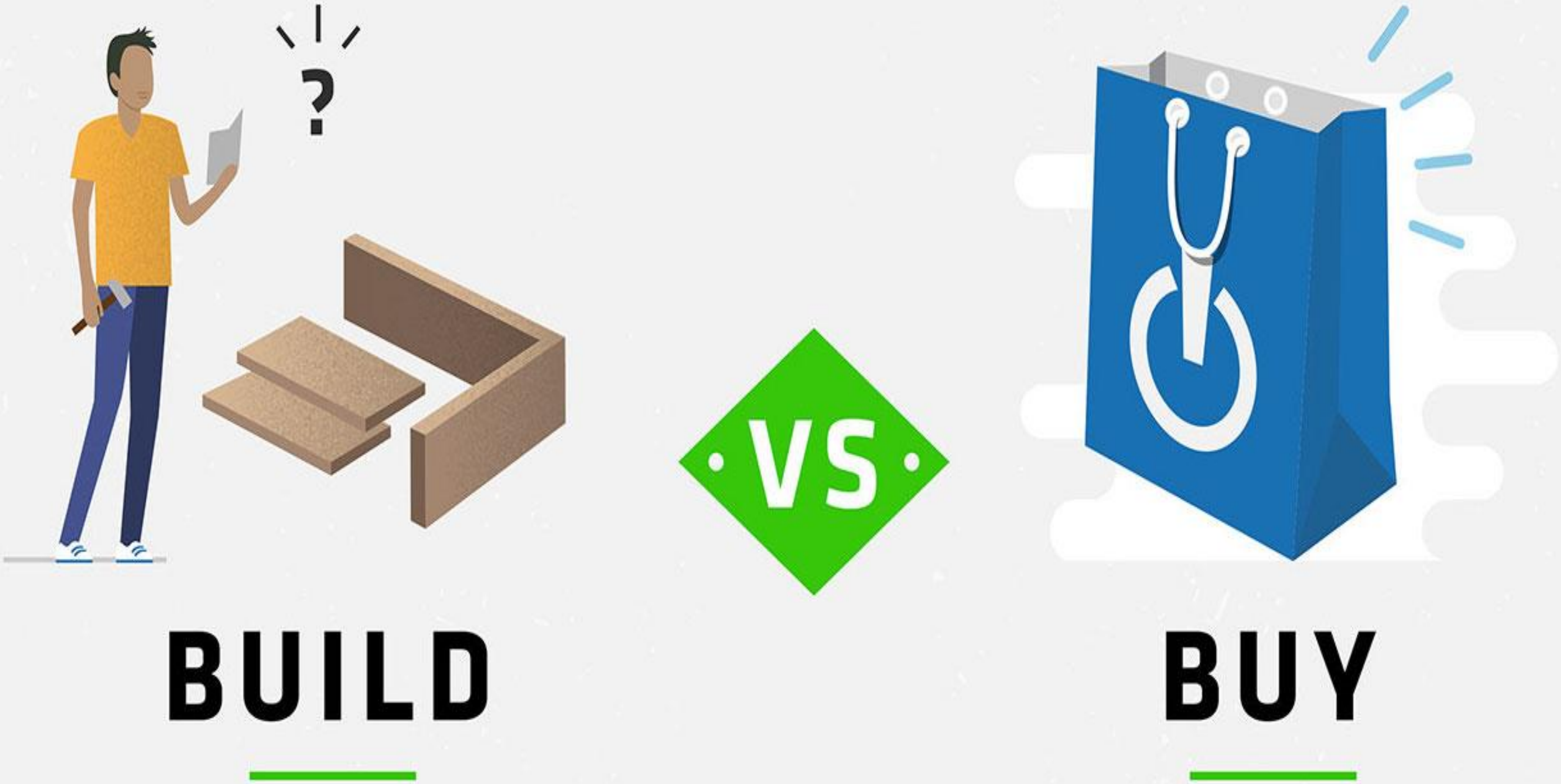
- Splunk Phantom Security Orchestration
- PaloAlto Demisto
- Gartner: “Market Guide for Security Orchestration, Automation and Response Solutions"

Free (a couple of examples):

- Luigi - https://github.com/spotify/luigi
- Huginn - https://github.com/huginn/huginn

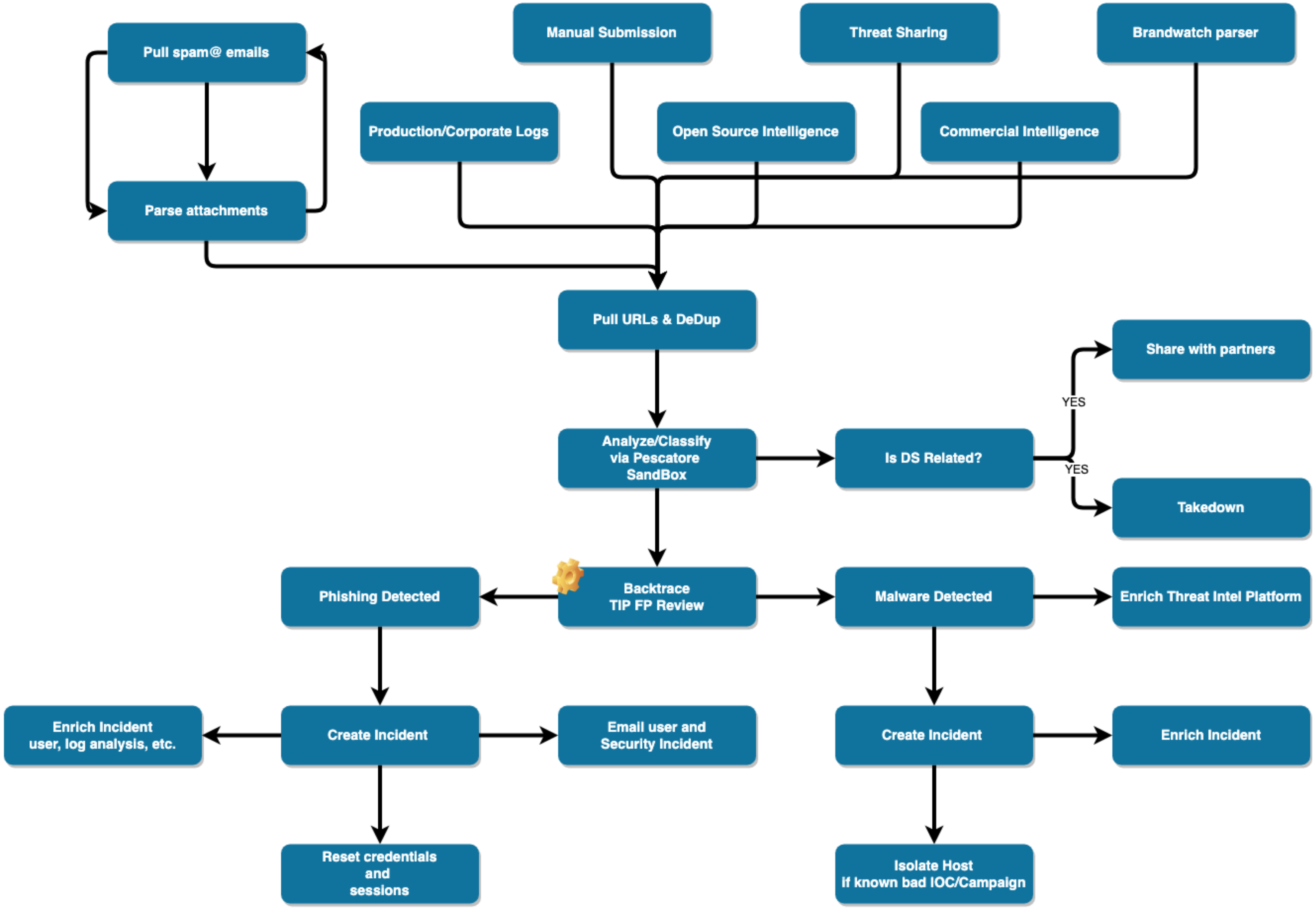
Build Vs Buy

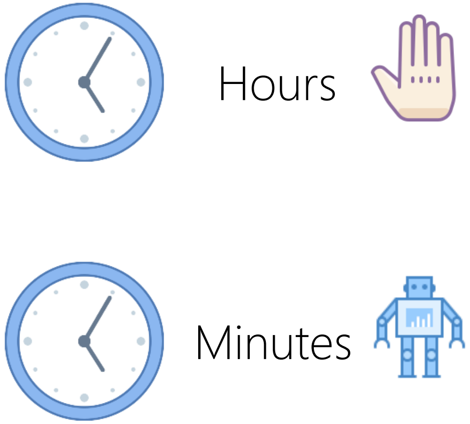
Why we made the decision to build vs buy for some of the tools we use?



Scenario 1 – Phishing Attack

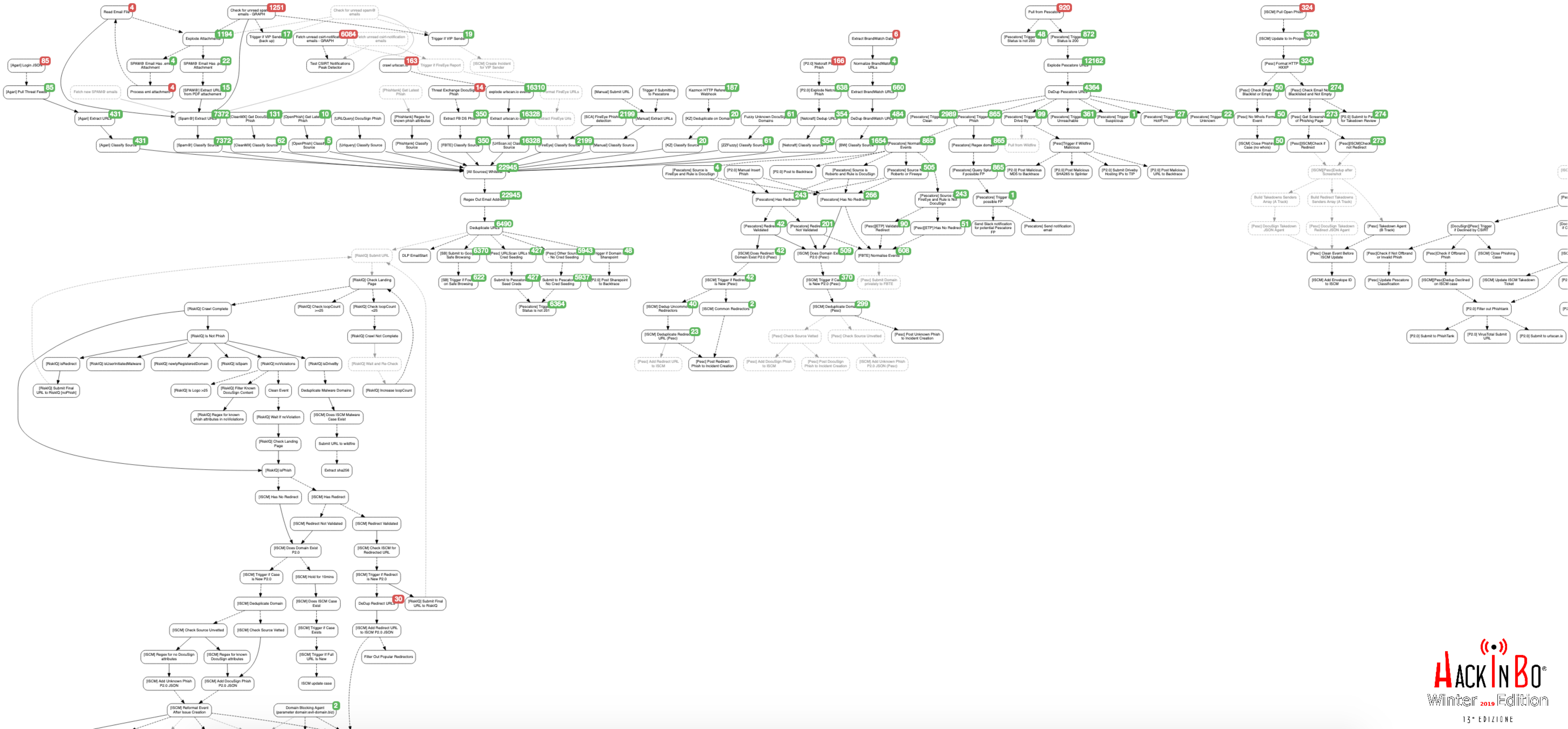
Automated Response



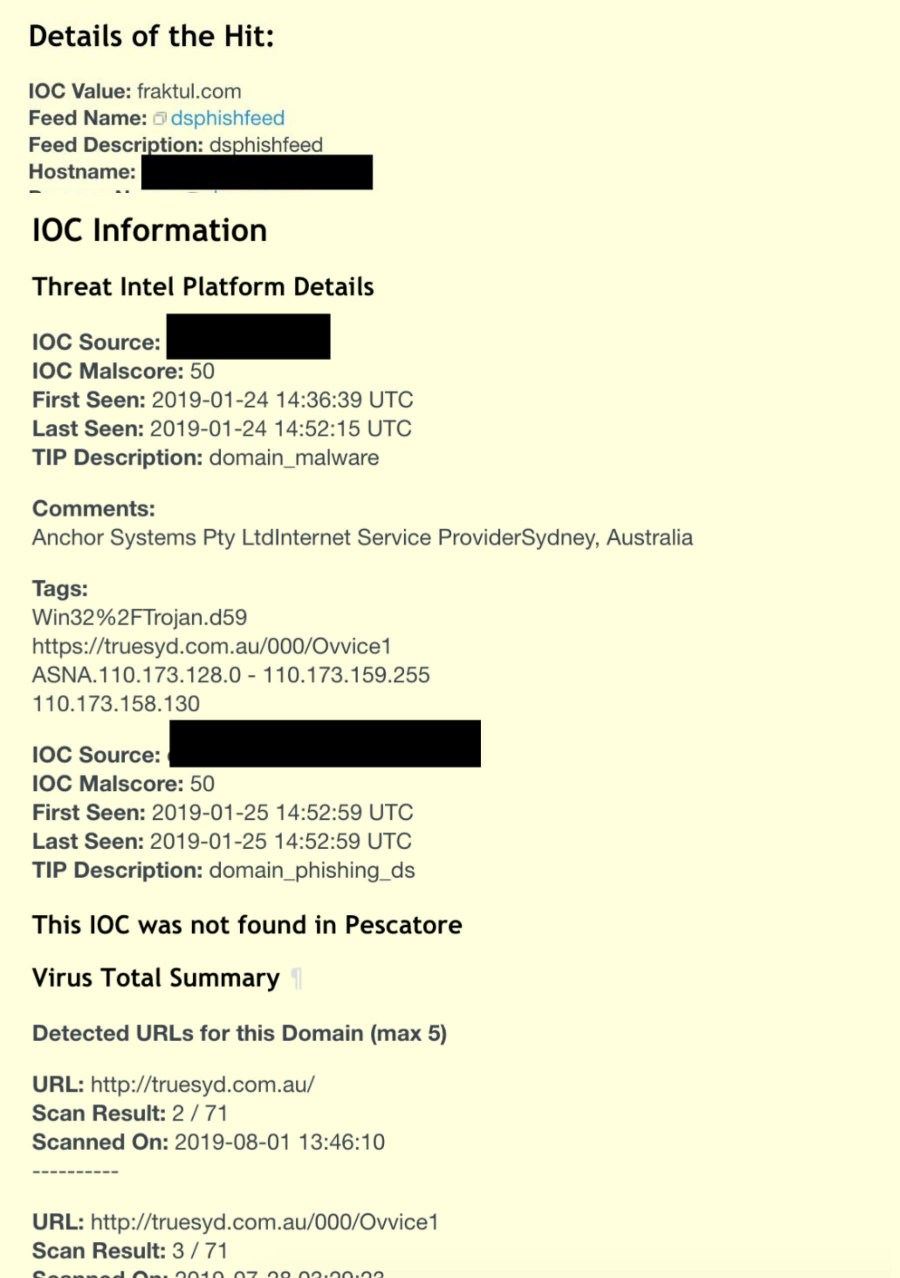


Scenario 1 – Phishing Attack

Automated Response (partial)


Read Email File 4
Check for unread spam emails - GRAPH 1251
Check for unread spam@ emails
Explode Attachments 1194
Trigger if VIP Sender (back up) 17
Fetch unread csirt-notification emails - GRAPH 6084
Fetch unread csirt-notification emails
Trigger if VIP Sender 19
[Agari] Login JSON 85
SPAM@ Email Has .eml Attachment 4
SPAM@ Email Has .pdf Attachment 22
Test CSIRT Notifications Peak Detector
crawl urlscan.io 163
Trigger if FireEye Report
[ISCM] Create Incident for VIP Sender
[Agari] Pull Threat Feeds 85
Fetch new SPAM@ emails
Process eml attachment 4
[SPAM@] Extract URLs from PDF attachement 15
[Phishtank] Get Latest Phish
Threat Exchange DocuSign Phish 14
explode urlscan.io events 16310
Format FireEye URLs
[Manual] Submit URL
Trigger if Submitting to Pescatore
Kazmon HTTP Referer Webhook 187
[P2.0] Netcraft Phish 166
Extract BrandWatch Data 6
Normalize BrandWatch URLs 4
Pull from Pescatore 920
[Pescatore] Trigger Status is not 200 48
[Pescatore] Trigger Status is 200 872
Explode Pescatore URLs 12162
DeDup Pescatore URLs 4364
[ISCM] Pull Open Phish 324
[ISCM] Update to In-Progress 324
[Pesc] Format HTTP HXXP 324
[Pesc] Check Email in Blacklist or Empty 50
[Pesc] Check Email Not Blacklisted and Not Empty 274
[Agari] Extract URLs 431
[Spam@] Extract URLs 7372
[CleanMX] Get DocuSign Phish 131
[OpenPhish] Get Latest Phish 10
[URLQuery] DocuSign Phish
[Phishtank] Regex for known phish attributes
Extract FB DS Phish 350
Extract urlscan.io urls 16328
Extract FireEye Urls
[SCA] FireEye Phishing detection 2199
[Manual] Extract URLs
[KZ] Deduplicate on Domain 20
Fuzzy Unknown DocuSign Domains 61
[P2.0] Explode Netcraft Phish 638
[Netcraft] Dedup URLs 354
Extract BrandWatch URLs 660
DeDup BrandWatch URLs 484
[Pescatore] Trigger Clean 2989
[Pescatore] Trigger Phish 865
[Pescatore] Trigger Drive-By 99
[Pescatore] Trigger Unreachable 361
[Pescatore] Trigger Suspicious 1
[Pescatore] Trigger HotPorn 27
[Pescatore] Trigger Unknown 22
[Pesc] No Whois Format Event 50
[Pesc] Get Screenshot of Phishing Page 273
[P2.0] Submit to Pescatore for Takedown Review 274
[Agari] Classify Source 431
[Spam@] Classify Source 7372
[CleanMX] Classify Source 62
[OpenPhish] Classify Source 5
[Urlquery] Classify Source
[Phishtank] Classify Source
[FBTE] Classify Source 350
[UrlScan.io] Classify Source 16328
[FireEye] Classify Source 2199
[Manual] Classify Source
[KZ] Classify Source 20
[ZZFuzzy] Classify Source 61
[Netcraft] Classify source 354
[BW] Classify Source 1654
[Pescatore] Normalize Events 865
[Pescatore] Regex domain 865
Pull from Wildfire
[Pesc]Trigger if Wildfire Malicious
[ISCM] Close Phishing Case (no whois) 50
[Pesc][ISCM]Check if Redirect
[Pesc][ISCM]Check not Redirect 273
[All Sources] Whitelist 22945
[Pescatore] Source is FireEye and Rule is DocuSign 4
[P2.0] Manual Insert Phish
[P2.0] Post to Backtrace
[Pescatore] Source is Roberto and Rule is DocuSign
[Pescatore] Source Not Roberto or Fireeye 505
[Pescatore] Query Splunk if possible FP 865
[P2.0] Post Malicious MD5 to Backtrace
[P2.0] Post Malicious SHA265 to Splinter
[P2.0] Submit Driveby Hosting IPs to TIP
[P2.0] Post Malicious URL to Backtrace
[ISCM][Pesc]Dedup after Screenshot
Regex Out Email Address 22945
[Pescatore] Has Redirect 243
[Pescatore] Has No Redirect 266
[Pescatore] Source is FireEye and Rule is Not DocuSign 243
[Pescatore] Trigger possible FP 1
Build Takedowns Senders Array (A Track)
Build Redirect Takedowns Senders Array (A Track)
Deduplicate URLs 6490
[Pescatore] Redirect Validated 42
[Pescatore] Redirect Not Validated 201
[Pesc][ETP] Validated Redirect 90
[Pesc][ETP] Has No Redirect 51
Send Slack notification for potential Pescatore FP
[Pescatore] Send notification email
[Pesc] DocuSign Takedown JSON Agent
[Pesc] DocuSign Takedown Redirect JSON Agent
[Pesc] Takedown Agent (B Track)
[DocuSign][Pesc] Trigger if Declined by CSIRT
[RiskIQ] Submit URL
DLP EmailStart
[SB] Submit to Google Safe Browsing 6370
[Pesc] URLScan URLs for Cred Seeding 427
[Pesc] Other Sources - No Cred Seeding 5943
Trigger if Domain is Sharepoint 48
[ISCM] Does Redirect Domain Exist P2.0 (Pesc) 42
[ISCM] Does Domain Exist P2.0 (Pesc) 509
[FBTE] Normalise Events 608
[Pesc] Clean Event Before ISCM Update
[Pesc]Check if Not Offbrand or Invalid Phish
[Pesc]Check if Offbrand Phish
[ISCM] Close Phishing Case
[RiskIQ] Check Landing Page
[SB] Trigger if Found on Safe Browsing 622
Submit to Pescatore Seed Creds 427
Submit to Pescatore No Cred Seeding 5937
[P2.0] Post Sharepoint to Backtrace
[ISCM] Trigger if Redirect is New (Pesc) 42
[ISCM] Trigger if Case is New P2.0 (Pesc) 370
[Pesc] Submit Domain privately to FBTE
[ISCM] Add Envelope ID to ISCM
[Pesc] Update Pescatore Classification
[ISCM][Pesc]Dedup Declined on ISCM case
[ISCM] Update ISCM Takedown Ticket
[RiskIQ] Crawl Complete
[RiskIQ] Check loopCount >=25
[RiskIQ] Check loopCount <25
[Pescatore] Trigger Status is not 201 6364
[ISCM] Dedup Uncommon Redirectors 40
[ISCM] Common Redirectors 2
[ISCM] Deduplicate Domain (Pesc) 299
[P2.0] Filter out Phishtank
[RiskIQ] Is Not Phish
[RiskIQ] Crawl Not Complete
[ISCM] Deduplicate Redirect URL (Pesc) 23
[Pesc] Check Source Vetted
[Pesc] Check Source Unvetted
[Pesc] Post Unknown Phish to Incident Creation
[P2.0] Submit to PhishTank
[P2.0] VirusTotal Submit URL
[P2.0] Submit to urlscan.io
[RiskIQ] isRedirect
[RiskIQ] isUserInitiatedMalware
[RiskIQ] newlyRegisteredDomain
[RiskIQ] isSpam
[RiskIQ] noViolations
[RiskIQ] isDriveBy
[RiskIQ] Wait and Re-Check
[Pesc] Add Redirect URL to ISCM
[Pesc] Post Redirect Phish to Incident Creation
[Pesc] Add DocuSign Phish to ISCM
[Pesc] Post DocuSign Phish to Incident Creation
[ISCM] Add Unknown Phish P2.0 JSON (Pesc)
[RiskIQ] Submit Final URL to RiskIQ [noPhish]
[RiskIQ] Is Logo >25
[RiskIQ] Filter Known DocuSign Content
Clean Event
Deduplicate Malware Domains
[RiskIQ] Increase loopCount
[RiskIQ] Regex for known phish attributes in noViolations
[RiskIQ] Wait If noViolation
[ISCM] Does ISCM Malware Case Exist
[RiskIQ] Check Landing Page
Submit URL to wildfire
[RiskIQ] isPhish
Extract sha256
[ISCM] Has No Redirect
[ISCM] Has Redirect
[ISCM] Redirect Not Validated
[ISCM] Redirect Validated
[ISCM] Does Domain Exist P2.0
[ISCM] Check ISCM for Redirected URL
[ISCM] Trigger if Case is New P2.0
[ISCM] Hold for 10mins
[ISCM] Trigger if Redirect is New P2.0
[ISCM] Deduplicate Domain
[ISCM] Does ISCM Case Exist
DeDup Redirect URLs 30
[RiskIQ] Submit Final URL to RiskIQ
[ISCM] Check Source Unvetted
[ISCM] Check Source Vetted
[ISCM] Trigger if Case Exists
[ISCM] Add Redirect URL to ISCM P2.0 JSON
[ISCM] Regex for no DocuSign attributes
[ISCM] Regex for known DocuSign attributes
[ISCM] Trigger If Full URL Is New
Filter Out Popular Redirectors
[ISCM] Add Unknown Phish P2.0 JSON
[ISCM] Add DocuSign Phish P2.0 JSON
ISCM update case
[ISCM] Reformat Event After Issue Creation
Domain Blocking Agent (parameter domain:evil-domain.biz) 2

Scenario 1 – Phishing



Details of the Hit:

IOC Value: fraktul.com
Feed Name: dsphishfeed
Feed Description: dsphishfeed
Hostname: [redacted]

IOC Information

Threat Intel Platform Details

IOC Source: [redacted]
IOC Malscore: 50
First Seen: 2019-01-24 14:36:39 UTC
Last Seen: 2019-01-24 14:52:15 UTC
TIP Description: domain_malware

Comments:
Anchor Systems Pty LtdInternet Service ProviderSydney, Australia

Tags:
Win32%2FTrojan.d59
https://truesyd.com.au/000/Ovvice1
ASNA.110.173.128.0 - 110.173.159.255
110.173.158.130

IOC Source: [redacted]
IOC Malscore: 50
First Seen: 2019-01-25 14:52:59 UTC
Last Seen: 2019-01-25 14:52:59 UTC
TIP Description: domain_phishing_ds

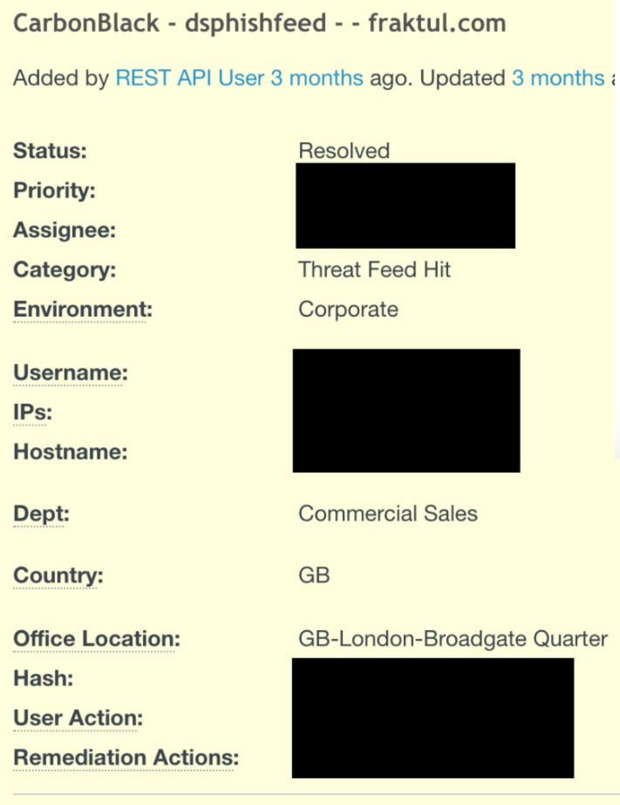
This IOC was not found in Pescatore

Virus Total Summary

Detected URLs for this Domain (max 5)

URL: http://truesyd.com.au/
Scan Result: 2 / 71
Scanned On: 2019-08-01 13:46:10

URL: http://truesyd.com.au/000/Ovvice1
Scan Result: 3 / 71



CarbonBlack - dsphishfeed - - fraktul.com

Added by REST API User 3 months ago. Updated 3 months a

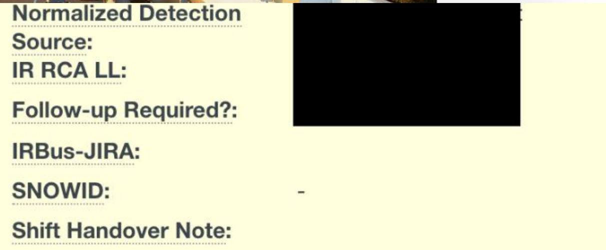
Status: Resolved
Priority: [redacted]
Assignee:
Category: Threat Feed Hit
Environment: Corporate

Username: [redacted]
IPs:
Hostname:

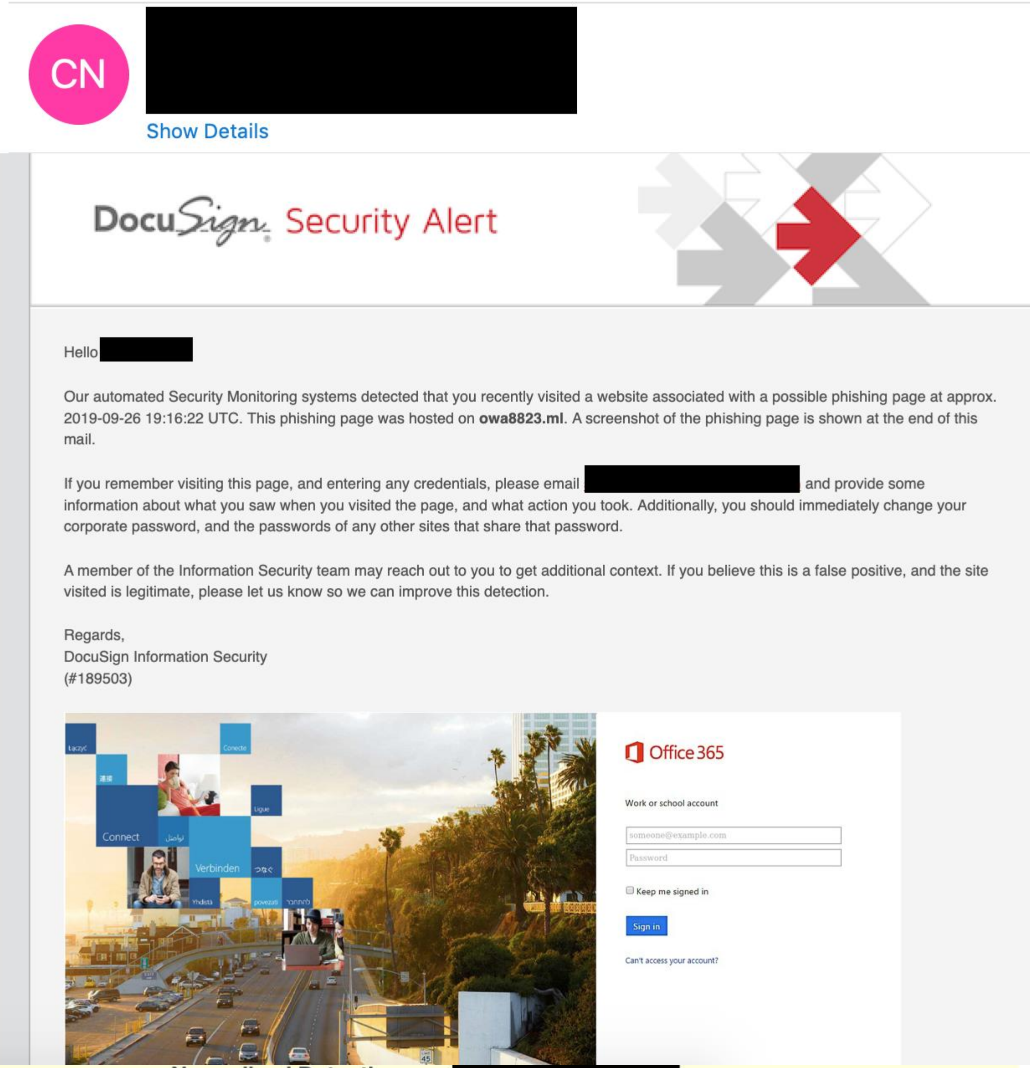
Dept: Commercial Sales

Country: GB

Office Location: GB-London-Broadgate Quarter
Hash: [redacted]
User Action:
Remediation Actions:



Normalized Detection Source: [redacted]
IR RCA LL:
Follow-up Required?:
IRBus-JIRA:
SNOWID: -
Shift Handover Note:



[redacted]

Show Details

DocuSign Security Alert

Hello [redacted]

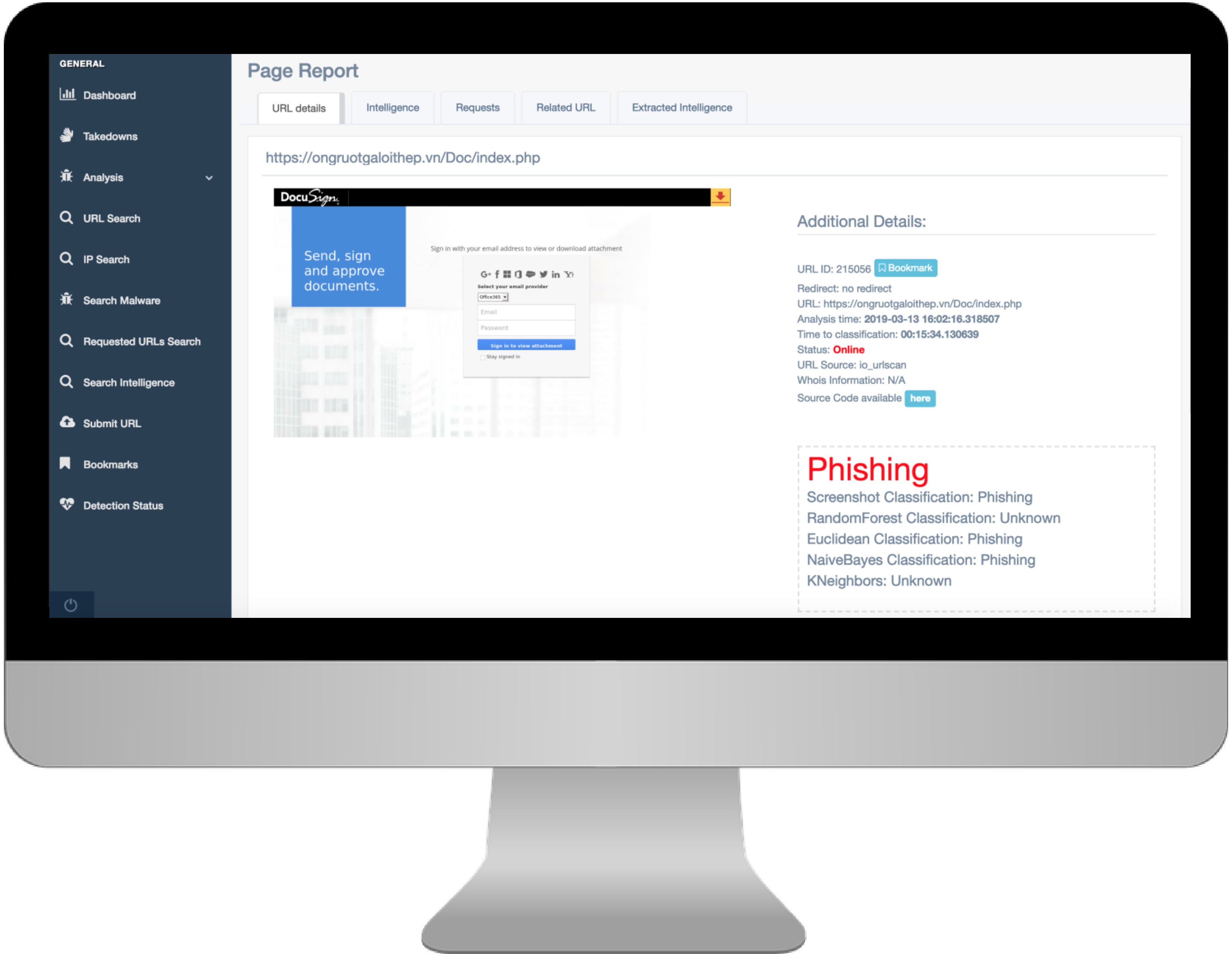
Our automated Security Monitoring systems detected that you recently visited a website associated with a possible phishing page at approx. 2019-09-26 19:16:22 UTC. This phishing page was hosted on **owa8823.ml**. A screenshot of the phishing page is shown at the end of this mail.

If you remember visiting this page, and entering any credentials, please email [redacted] and provide some information about what you saw when you visited the page, and what action you took. Additionally, you should immediately change your corporate password, and the passwords of any other sites that share that password.

A member of the Information Security team may reach out to you to get additional context. If you believe this is a false positive, and the site visited is legitimate, please let us know so we can improve this detection.

Regards,
DocuSign Information Security
(#189503)

Pescatore



Page Report

https://ongruotgaloithep.vn/Doc/index.php

Sign in with your email address to view or download attachment

Select your email provider: Office365

Email

Password

□ Stay signed in

Additional Details:

URL ID: 215056

Redirect: no redirect

URL: https://ongruotgaloithep.vn/Doc/index.php

Analysis time: **2019-03-13 16:02:16.318507**

Time to classification: **00:15:34.130639**

Status: **Online**

URL Source: io_urlscan

Whois Information: N/A

Source Code available here

Phishing

Screenshot Classification: Phishing

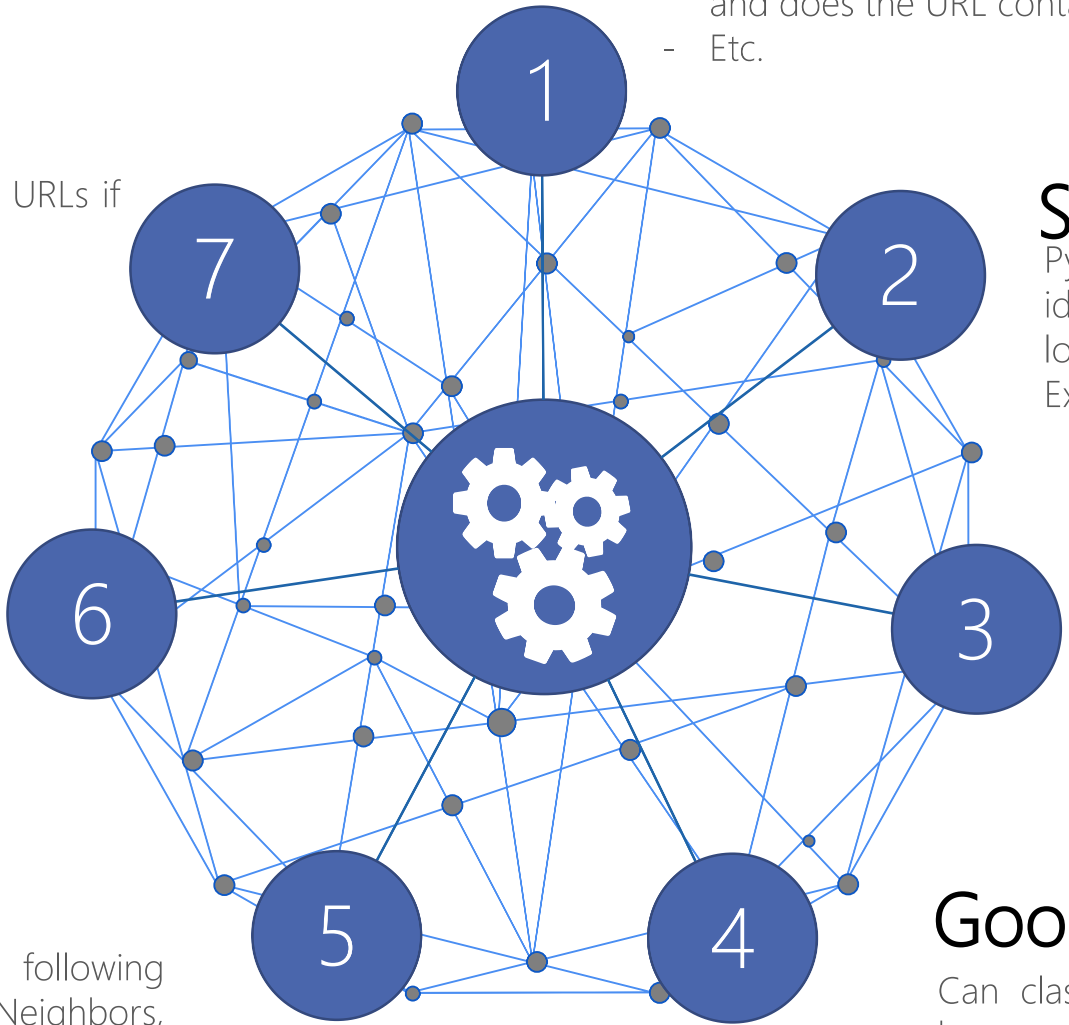
RandomForest Classification: Unknown

Euclidean Classification: Phishing

NaiveBayes Classification: Phishing

KNeighbors: Unknown

Pescatore in a nutshell..



DB Heuristic

DB Heuristic classifications can classify URLs based on extracted features; for example:

- Is the URL reachable?
- Does the requested page contain login forms, a password box and does the URL contains "/wp-content" or "/images"?
- Etc.

Static Classification

Python code can be written in order to identify specific URLs that cannot be loaded using the headless browser (eg.: Exploit kits).

Bad Reputation

Can classify URLs based on Bad Reputation

Good Reputation

Can classify URLs based on known good domains

RF, KNN, Euclidean, ScreenShot

ML classification is performed using the following algorithms RandomForest, K-Nearest Neighbors, Euclidean & Screenshot

Naive Bayes

Naive Bayes classifier uses specific features extracted from the requests and responses that the headless browser makes

Yara Rules

Yara rules can be used to classify URLs if Yara risk >= 100

Phishing Analysis System: Pescatore - some numbers…

NUMBER OF SUSPICIOUS PROCESSED URLs PER MONTH

~ 17,000

NUMBER OF DocuSign TAKE DOWNS PER MONTH

~ 500*

* And counting…

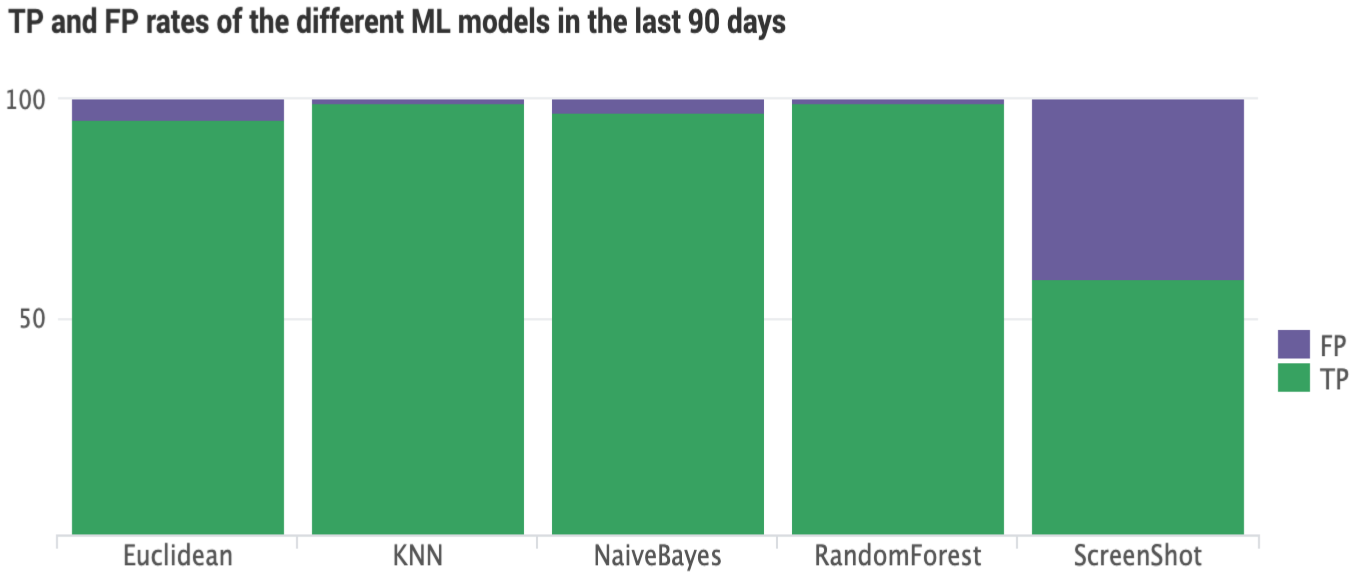
YEARLY CLOUD PROVIDER COST

$4,000

COST CUT

$150k +

MACHINE LEARNING TRUE POSITIVE VS FALSE POSITIVE RATE



AVERAGE TIME TO AUTOMATICALLY CLASSIFY A URL

5/10 MINS

AVERAGE TIME TO ALERT WHEN A PHISHING SITE IS HIT

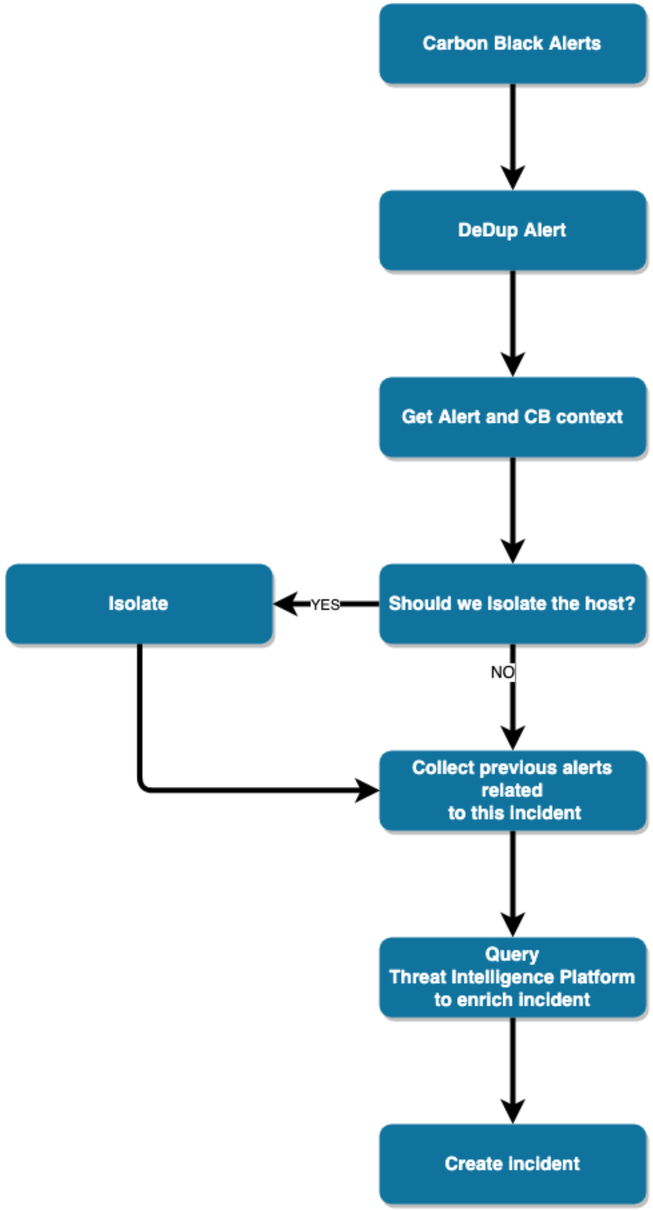
3 MINS

AVERAGE TIME TO GET A SITE TAKEN DOWN

2 DAYS

Scenario 2 – HIDS & Data Enrichment

Malicious Code or Suspicious Behavior



Carbon Black Alerts

DeDup Alert

Get Alert and CB context

Should we Isolate the host?

YES

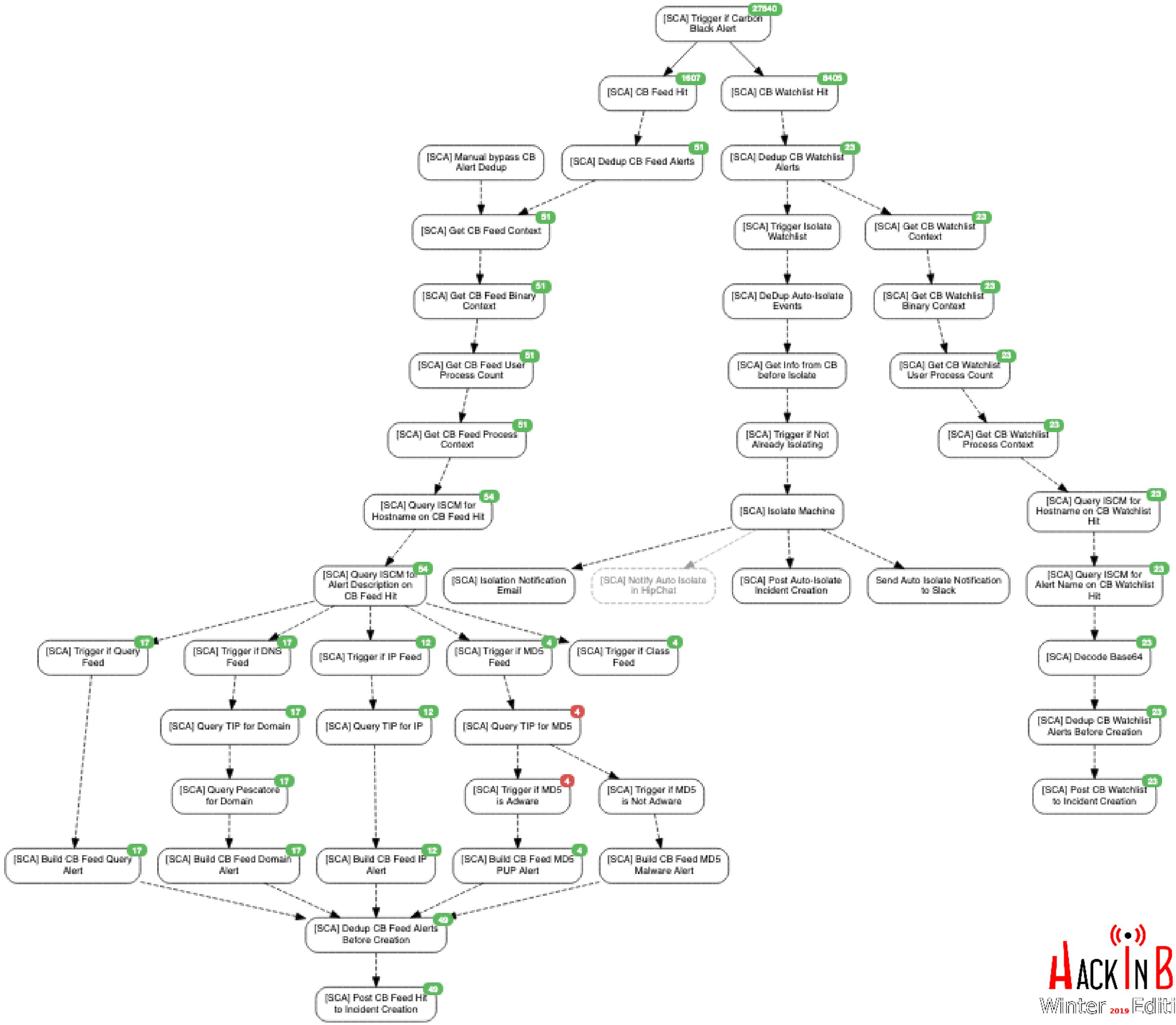
Isolate

NO

Collect previous alerts related to this incident

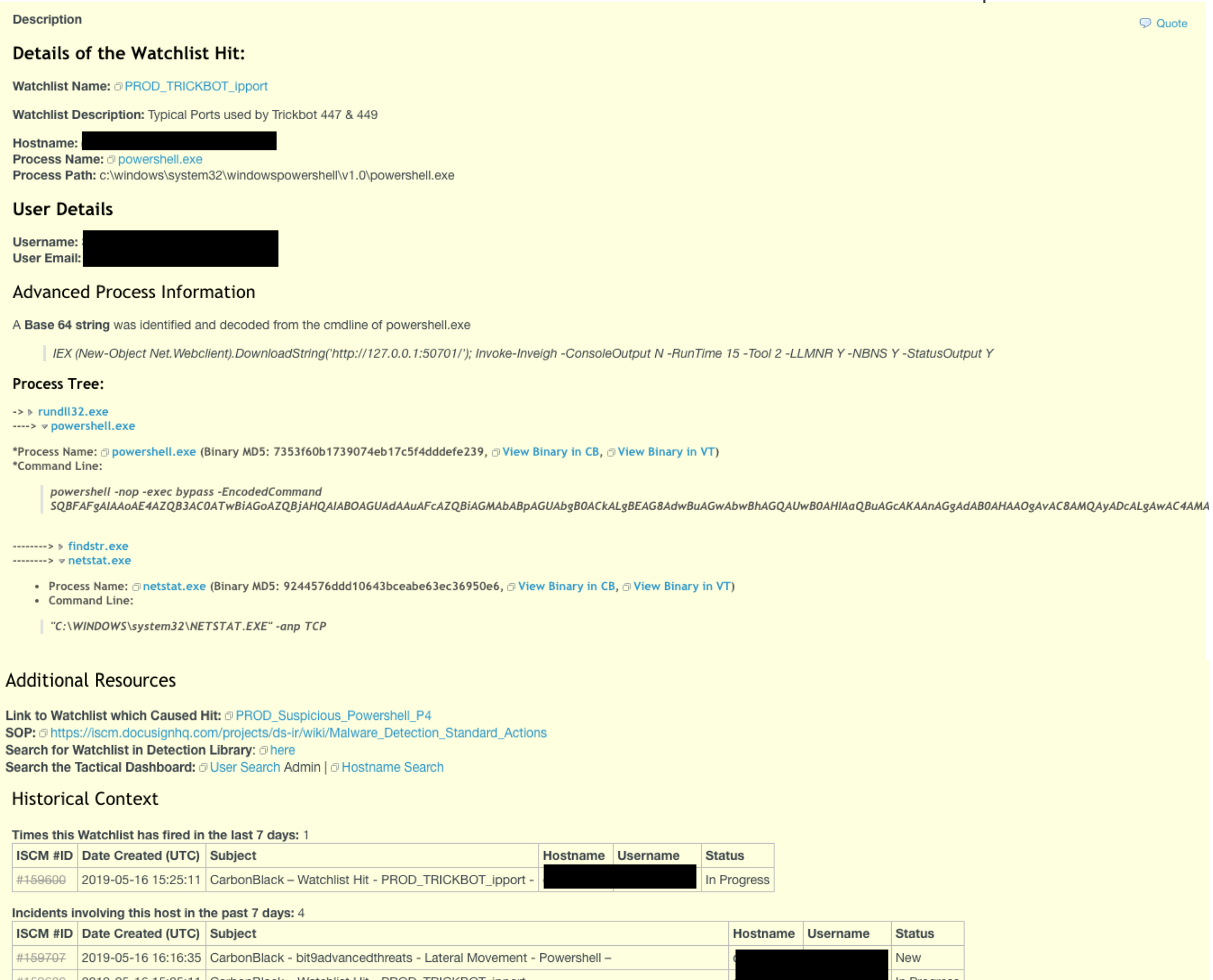
Query Threat Intelligence Platform to enrich incident

Create Incident


[SCA] Trigger if Carbon Black Alert
27840
[SCA] CB Feed Hit
1607
[SCA] CB Watchlist Hit
8405
[SCA] Manual bypass CB Alert Dedup
[SCA] Dedup CB Feed Alerts
51
[SCA] Dedup CB Watchlist Alerts
23
[SCA] Get CB Feed Context
51
[SCA] Trigger Isolate Watchlist
[SCA] Get CB Watchlist Context
23
[SCA] Get CB Feed Binary Context
51
[SCA] DeDup Auto-Isolate Events
[SCA] Get CB Watchlist Binary Context
23
[SCA] Get CB Feed User Process Count
51
[SCA] Get Info from CB before Isolate
[SCA] Get CB Watchlist User Process Count
23
[SCA] Get CB Feed Process Context
51
[SCA] Trigger if Not Already Isolating
[SCA] Get CB Watchlist Process Context
23
[SCA] Query ISCM for Hostname on CB Feed Hit
54
[SCA] Isolate Machine
[SCA] Query ISCM for Hostname on CB Watchlist Hit
23
[SCA] Query ISCM for Alert Description on CB Feed Hit
54
[SCA] Isolation Notification Email
[SCA] Notify Auto Isolate in HipChat
[SCA] Post Auto-Isolate Incident Creation
Send Auto Isolate Notification to Slack
[SCA] Query ISCM for Alert Name on CB Watchlist Hit
23
[SCA] Trigger if Query Feed
17
[SCA] Trigger if DNS Feed
17
[SCA] Trigger if IP Feed
12
[SCA] Trigger if MD5 Feed
4
[SCA] Trigger if Class Feed
4
[SCA] Decode Base64
23
[SCA] Query TIP for Domain
17
[SCA] Query TIP for IP
12
[SCA] Query TIP for MD5
4
[SCA] Dedup CB Watchlist Alerts Before Creation
23
[SCA] Query Pescatore for Domain
17
[SCA] Trigger if MD5 is Adware
4
[SCA] Trigger if MD5 is Not Adware
[SCA] Post CB Watchlist to Incident Creation
23
[SCA] Build CB Feed Query Alert
17
[SCA] Build CB Feed Domain Alert
17
[SCA] Build CB Feed IP Alert
12
[SCA] Build CB Feed MD5 PUP Alert
4
[SCA] Build CB Feed MD5 Malware Alert
[SCA] Dedup CB Feed Alerts Before Creation
49
[SCA] Post CB Feed Hit to Incident Creation
49

Scenario 2 – Malicious Code - Data Enrichment

Malicious Code or Suspicious Behavior



Description

Quote

Details of the Watchlist Hit:

Watchlist Name: PROD_TRICKBOT_ipport

Watchlist Description: Typical Ports used by Trickbot 447 & 449

Hostname: [redacted]
Process Name: powershell.exe
Process Path: c:\windows\system32\windowspowershell\v1.0\powershell.exe

User Details

Username: [redacted]
User Email:

Advanced Process Information

A **Base 64 string** was identified and decoded from the cmdline of powershell.exe

> *IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:50701/'); Invoke-Inveigh -ConsoleOutput N -RunTime 15 -Tool 2 -LLMNR Y -NBNS Y -StatusOutput Y*

Process Tree:

```
-> ▸ rundll32.exe
----> ▾ powershell.exe
```

*Process Name: powershell.exe (Binary MD5: 7353f60b1739074eb17c5f4dddefe239, View Binary in CB, View Binary in VT)
*Command Line:

```
powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMA
```

```
--------> ▸ findstr.exe
--------> ▾ netstat.exe
```

- Process Name: netstat.exe (Binary MD5: 9244576ddd10643bceabe63ec36950e6, View Binary in CB, View Binary in VT)
- Command Line:

```
"C:\WINDOWS\system32\NETSTAT.EXE" -anp TCP
```

Additional Resources

Link to Watchlist which Caused Hit: PROD_Suspicious_Powershell_P4
SOP: https://iscm.docusignhq.com/projects/ds-ir/wiki/Malware_Detection_Standard_Actions
Search for Watchlist in Detection Library: here
Search the Tactical Dashboard: User Search Admin | Hostname Search

Historical Context

Times this Watchlist has fired in the last 7 days: 1

ISCM #ID	Date Created (UTC)	Subject	Hostname	Username	Status
~~#159600~~	2019-05-16 15:25:11	CarbonBlack – Watchlist Hit - PROD_TRICKBOT_ipport -	[redacted]	[redacted]	In Progress

Incidents involving this host in the past 7 days: 4

ISCM #ID	Date Created (UTC)	Subject	Hostname	Username	Status
~~#159707~~	2019-05-16 16:16:35	CarbonBlack - bit9advancedthreats - Lateral Movement - Powershell –	[redacted]	[redacted]	New

What's in the incident?

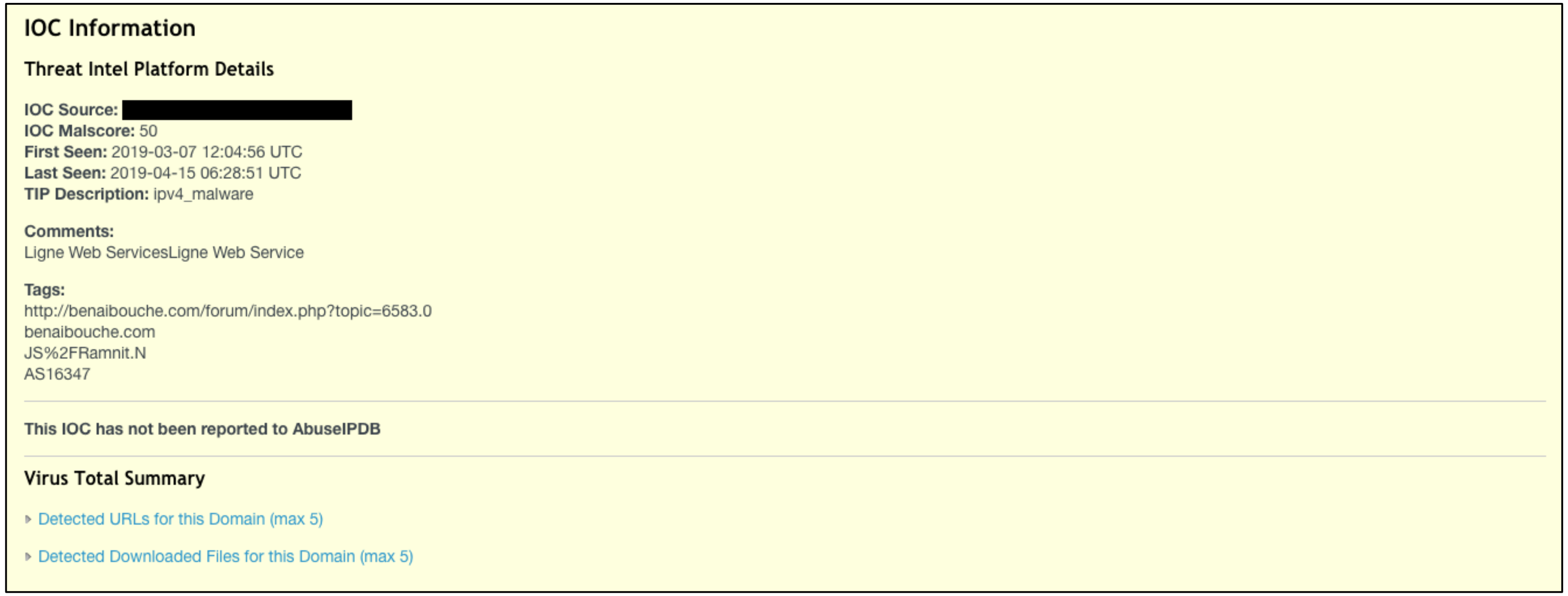
- Automated Base64 decode
- Process tree with links that points to HIDS
- Historical context based on alert/machine
- Threat Intel Enrichment (next slide)
- SOPs and Detection details (next slide)

Scenario 2 – Malicious Code - Data Enrichment

Malicious Code or Suspicious Behavior

Thereat Intelligence Enrichment

- Where the intelligence was collected from
- Malicious Score
- When it was initially/last seen
- VT details
  - Malicious URLs
  - Malicious downloads



IOC Information

Threat Intel Platform Details

IOC Source: [redacted]
IOC Malscore: 50
First Seen: 2019-03-07 12:04:56 UTC
Last Seen: 2019-04-15 06:28:51 UTC
TIP Description: ipv4_malware

Comments:
Ligne Web ServicesLigne Web Service

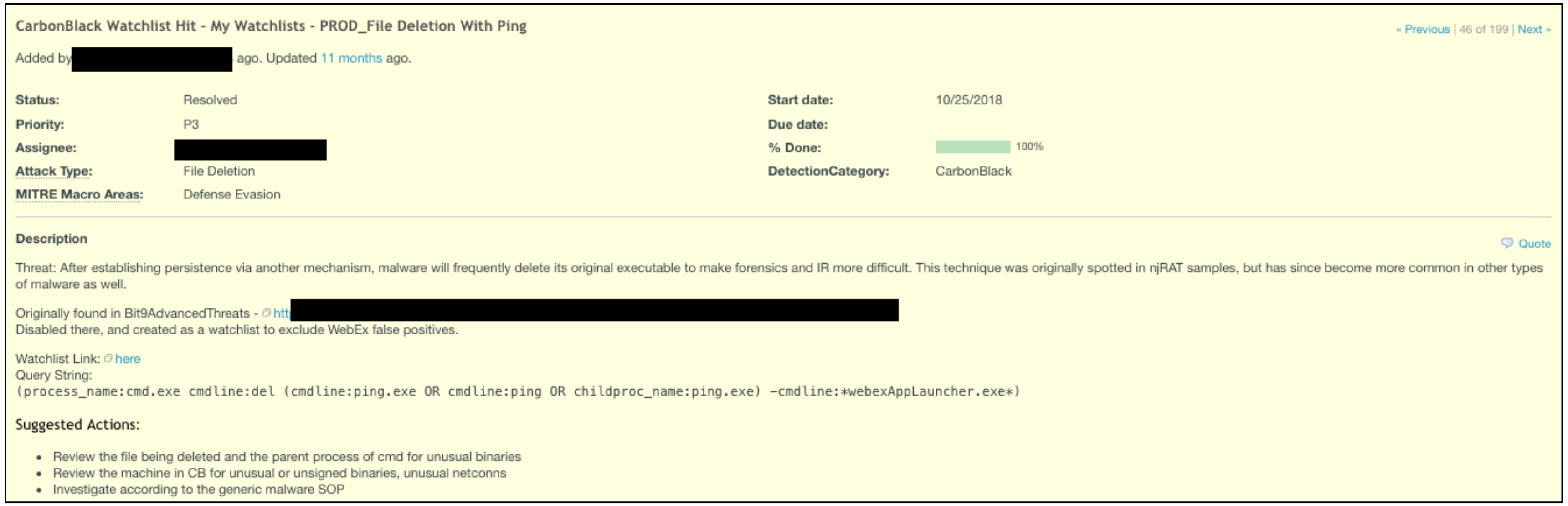
Tags:
http://benaibouche.com/forum/index.php?topic=6583.0
benaibouche.com
JS%2FRamnit.N
AS16347

This IOC has not been reported to AbuseIPDB

Virus Total Summary

▸ Detected URLs for this Domain (max 5)

▸ Detected Downloaded Files for this Domain (max 5)



CarbonBlack Watchlist Hit - My Watchlists - PROD_File Deletion With Ping

« Previous | 46 of 199 | Next »

Added by [redacted] ago. Updated 11 months ago.

Status:	Resolved	**Start date:**	10/25/2018
Priority:	P3	**Due date:**	
Assignee:	[redacted]	**% Done:**	100%
Attack Type:	File Deletion	**DetectionCategory:**	CarbonBlack
MITRE Macro Areas:	Defense Evasion		

Description

Quote

Threat: After establishing persistence via another mechanism, malware will frequently delete its original executable to make forensics and IR more difficult. This technique was originally spotted in njRAT samples, but has since become more common in other types of malware as well.

Originally found in Bit9AdvancedThreats - htt[redacted]
Disabled there, and created as a watchlist to exclude WebEx false positives.

Watchlist Link: here
Query String:

```
(process_name:cmd.exe cmdline:del (cmdline:ping.exe OR cmdline:ping OR childproc_name:ping.exe) -cmdline:*webexAppLauncher.exe*)
```

Suggested Actions:

- Review the file being deleted and the parent process of cmd for unusual binaries
- Review the machine in CB for unusual or unsigned binaries, unusual netconns
- Investigate according to the generic malware SOP

Documentation is important

- Type of alert
- MITRE Areas (useful to identify gaps in detections or logs)
- Description
- Suggested Actions
- False Positives
- Speed up response time

Conclusion / Takeaways

- You want to scale, you need to automate
- Do not give up
- Do not be afraid to develop in-house tools
- Cost saving
- Do not feel you have to do everything at once, keep automating and keep developing

THANK YOU

HackInBo®
Winter 2019 Edition
13ª EDIZIONE