$find_evil

“Threat Hunting”

@khannaanurag

#whoami

- Ex-Lead Investigator – Symantec Incident Response
  - Incident Response, Digital Forensics, Threat Hunting
- Incident Response and Forensics, Pen Testing, Solution Architect, Security Consulting
- GSE # 97 + (GIAC and Others)
- MS - (Digital Forensics) & MBA - (Networks & IT)
- @khannaanurag khannaanurag@gmail.com

What’s in it for me?

- What is threat hunting?
- Why do we need threat hunting?
- How can I setup a threat hunting program?
- How do I define hunts and run them?

Misconceptions about threat hunting

- Definitive answer to the question - Are we breached?
- Can be fully automated
- Is expensive and resource intensive
- Will always find evil

What is threat hunting?

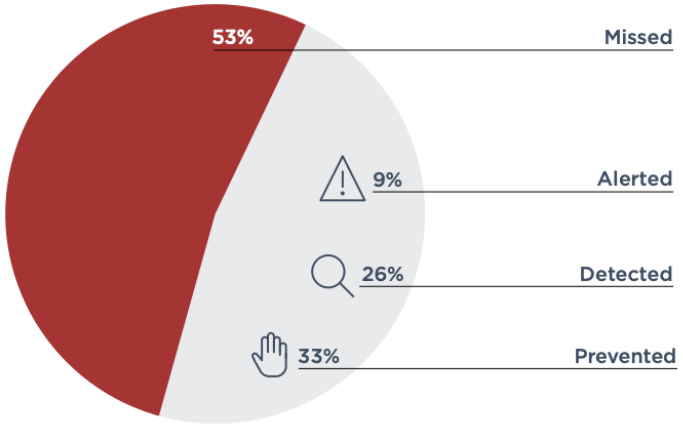
- **Proactive** , **focused** and **iterative** approach to **searching**, **identifying** and **understanding** adversaries internal to the defender's environment

- Identify, understand & characterize adversaries in order to **detect and evict** them from the environment **before they achieve their objectives**

Why hunt?

- Identify gaps in visibility, detection & response
- Improve detection
- Improve understanding of our environment
- Find previous unknown & undetected compromises
- Helps me find my own cases ☺

Can we detect adversaries in real time?



Attacks on enterprise environments

It is alarming that **alerts are only generated for 9% of attacks**

BLOAT

50-70

Average number of tools organizations report in their IT environment.

OVERLAP

35%

Average number of tools with overlapping capabilities.

MISCONFIGURATION

80%

Average number of tools left underutilized at default settings.

*** Mandiant – Security Effectiveness Report 2020**
https://content.fireeye.com/security-effectiveness/rpt-security-effectiveness-2020-deep-dive-into-cyber-reality

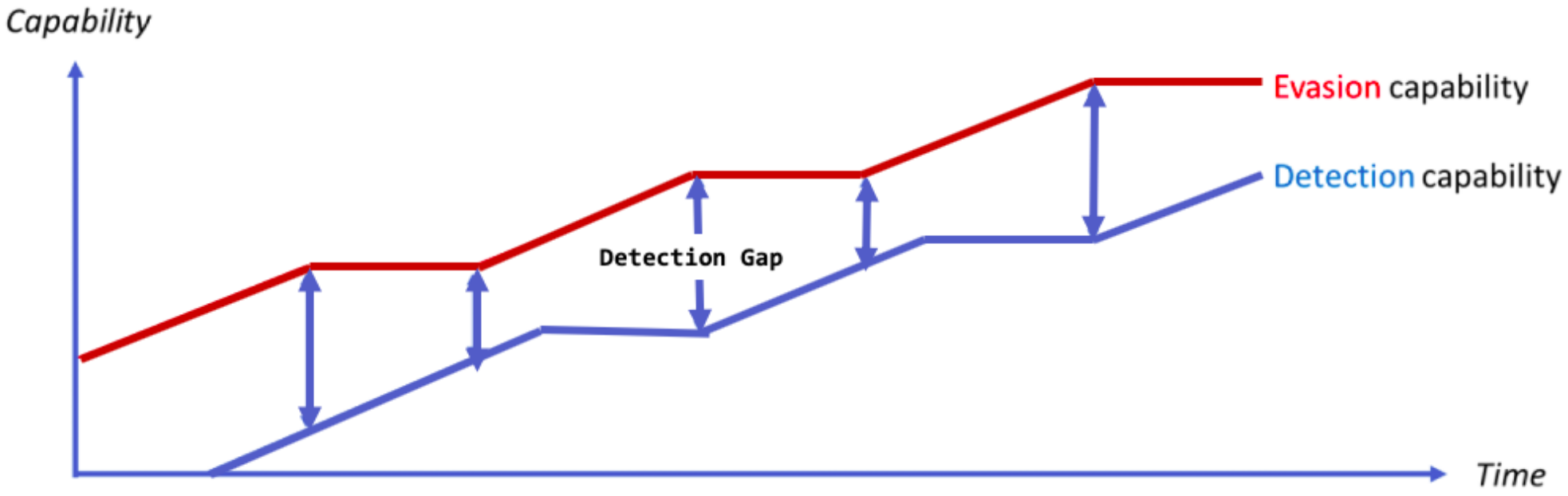
Reduce time of detection/dwell time

95 days*

2017	2018	2019
86 days	85 days	95 days

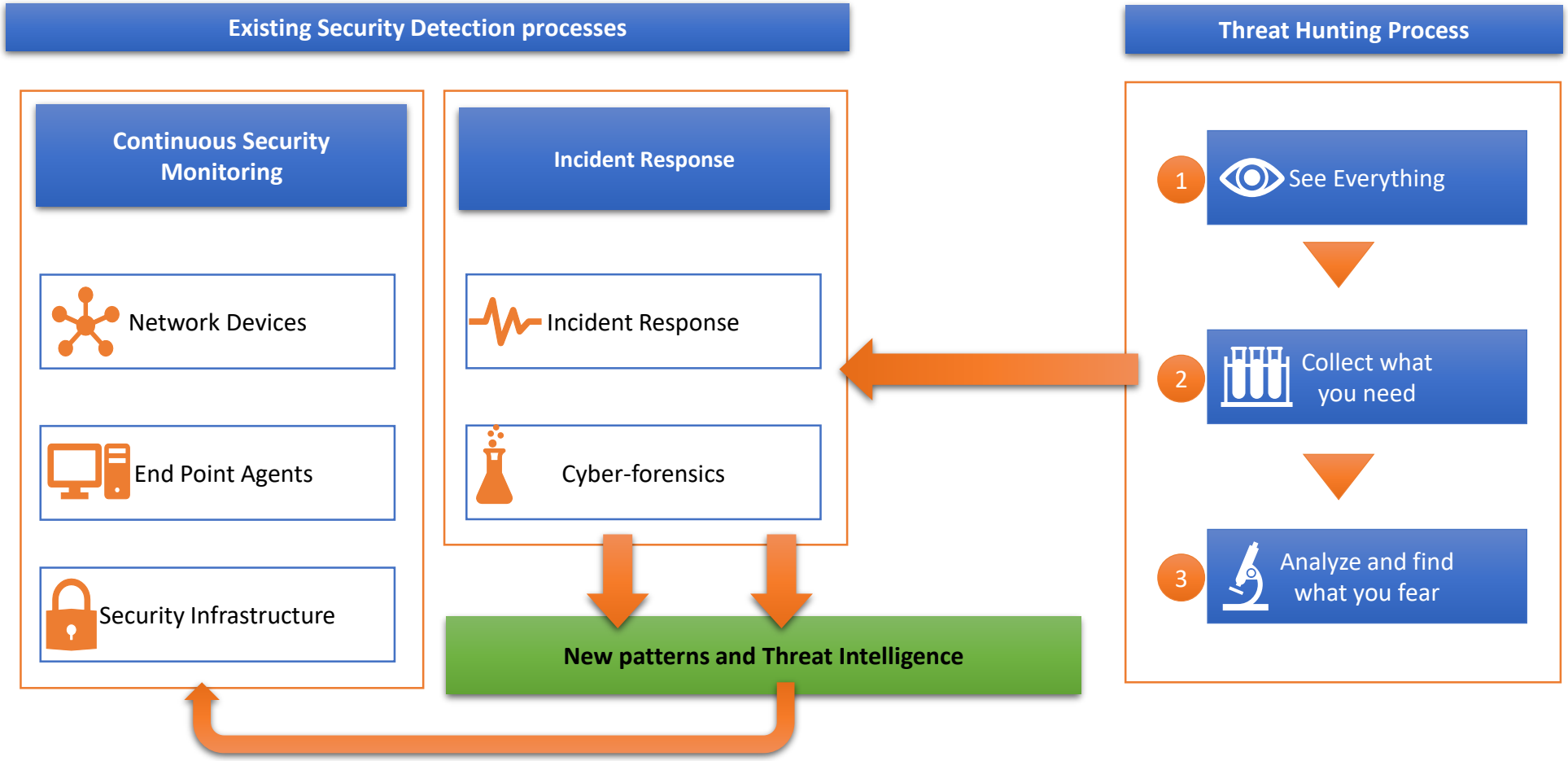
*Global Median dwell time – CrowdStrike
https://go.crowdstrike.com/rs/281-OBQ 266/images/Report2019CrowdStrikeServices.pdf

Reduce the detection gap

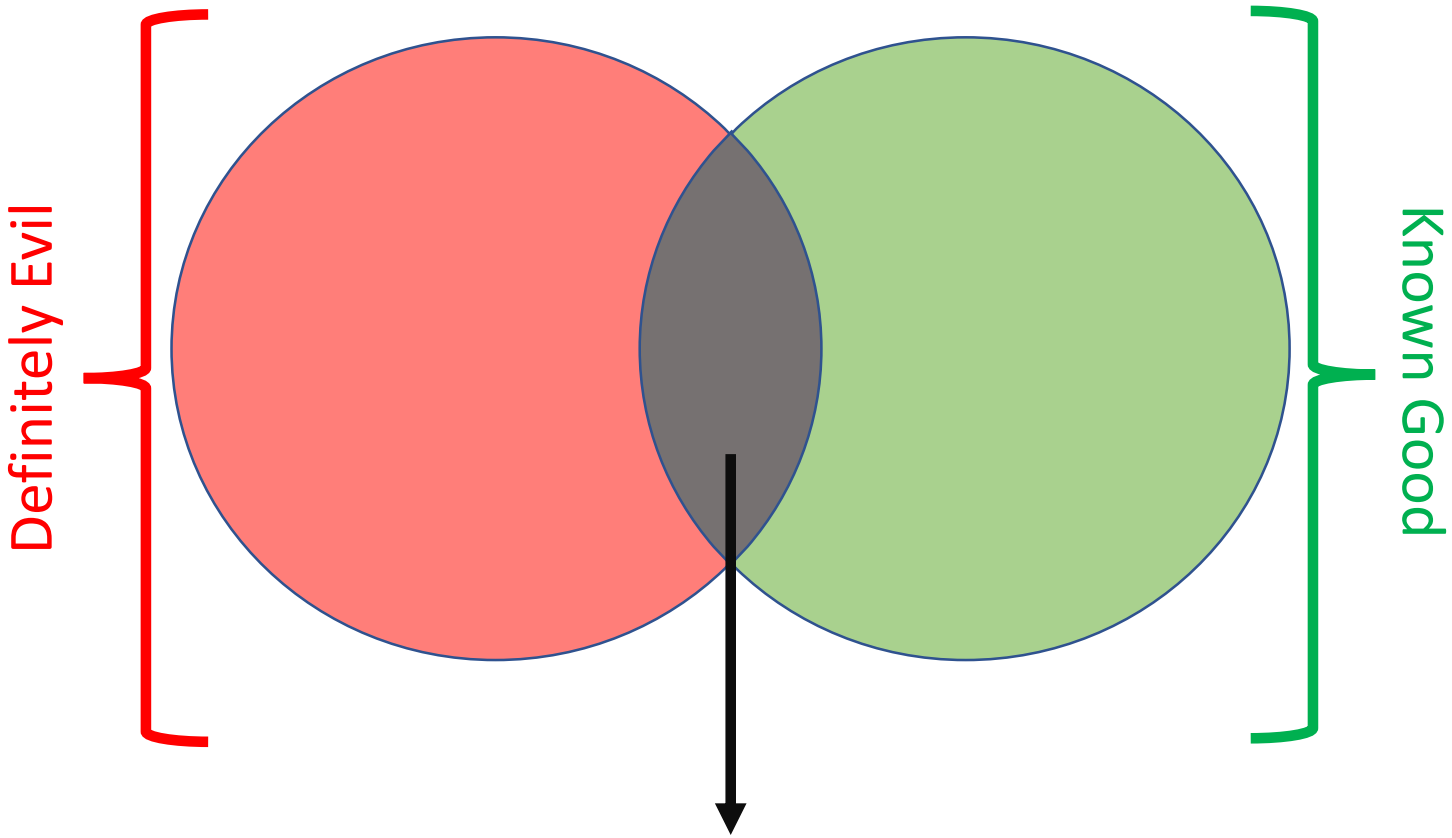


TaHiTI Hunting Methodology
https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf

Where does threat hunting fit in?



Let’s detect the gray

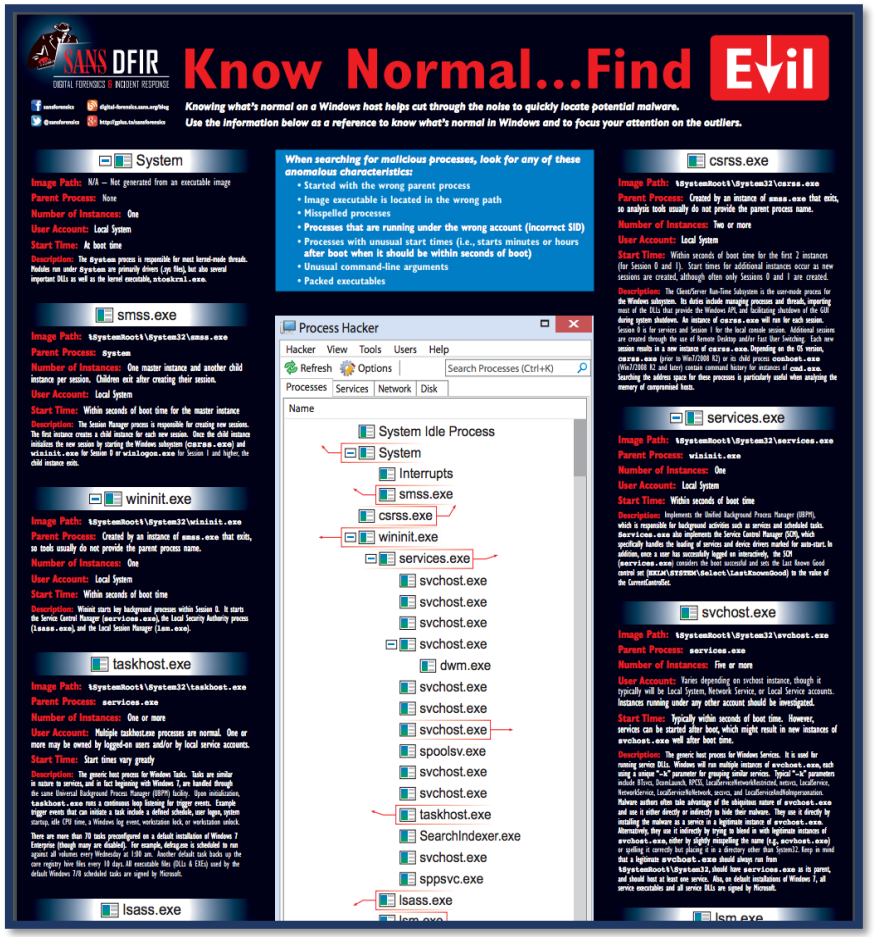


Unknown
Depends on the context

What do you need?

- Experienced analysts
- Visibility, Logs & Data
- Tools & Techniques
- Know Normal
- Threat Intelligence

- Triage & Response



How to hunt?

1. Form a Hypothesis
2. What to search
3. How to search
4. Enrichment & Intel
5. Automate

“The Who, What, Where, When, Why and How of Effective Threat Hunting,“ March 2016, https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

1. Forming Hypothesis

- What is the question you are trying to answer?
- Based on observations & experience

"Generating Hypotheses for Successful Threat Hunting" – SANS Whitepaper

https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art11.html

2. What to search?

- Flow records
- OS Logs
- Alerts
- Network logs
- Master File Tables
- Memory dumps
- Registry hives
- Event logs
- Process listing
- System artifacts
- DNS logs
- System files

and many more…

DATA – DATA – DATA!

Depends on your environment and the question you are trying to answer .

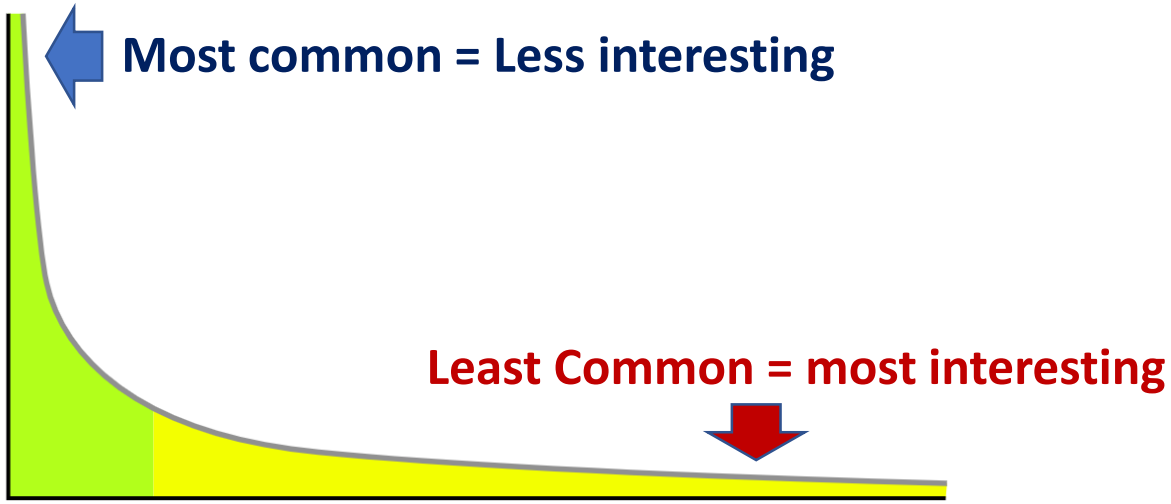
3.1 How to search? 👀

- Ask the Endpoint - Live Analysis
  - Endpoint Agents
- Collect & Analyze evidence - Offline Analysis
  - Endpoint scripts, Kansa, OS Query, PSHunt, Kape
- Analysis Platforms
  - Elastic, Splunk, Excel, CLI

Automated periodic collection and analysis of data can be performed.

3.2 How to search? 👀

- Querying
- Stack Counting
- Clustering
- Grouping
- Long Tail Analysis
- Unique Values



Long Tail Analysis

*https://www.fireeye.com/blog/threat-research/2012/11/indepth-data-stacking.html

*Image By User:Husky - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1449504

4. Enrichment & Intel 

- Intelligence - Using new Intel on old data
- Patterns & Anomalies
- Enrich data with helpful context
  - GeoIP Information, ASN Information
  - Domain creation dates
  - Known good
  - Signed vs unsigned binaries and more

5. Automate

- You hunt once and detect always
- Automation is the Key but may not be always possible

Hypothesis

- Let's consider a high-level hypothesis to understand how threat hunting may look like in the real world

Hunters Perspective

us

?

ous

Was any of this EVIL?

Hunters Perspective

Attack	We downloaded from a malicious website?
Delivery	We downloaded malware?
Execution	Malware executed on machine?
Persistence	Malware is persisting on my machine?
C2	My system connecting to malicious C2 Infra?

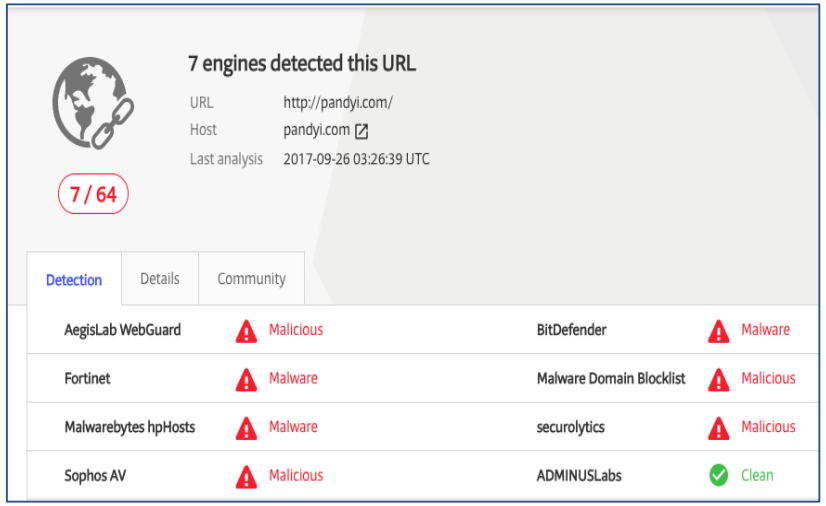
Hunt 1 : We downloaded from a malicious website?

What to search?

- DNS Cache
- Passive DNS
- Netstat entries
- Proxy Logs
- Firewall logs
- Network Logs

Enrichment

- Threat Intel Feeds
- ASN Info
- Domain Registration date
- Long Domain names
- Top 1M – Cisco Umbrella Popularity list*



How to search?

Analysis and Intelligence to detect uncommon and malicious download links.

*https://docs.umbrella.com/investigate-api/docs/top-million-domains

Count	Entry
420	www.google.com
230	netflix.com
100	wikipedia.org
98	crl.globalsign.net
25	ocsp.digicert.com
15	www.sublimetext.com
14	safebrowsing.google.com
8	notepad-plus-plus.org
3	update.googleapis.com
1	pandyi.com
1	ipv6.msftncsi.com
1	rediff.com

Subset of domain cache data

Count	Entry	Top 1m Rank
420	www.google.com	5
230	netflix.com	1
100	wikipedia.org	1324
98	crl.globalsign.net	690
25	ocsp.digicert.com	88
15	www.sublimetext.com	28549
14	safebrowsing.google.com	749
8	notepad-plus-plus.org	27688
3	update.googleapis.com	39
1	pandyi.com	NA
1	ipv6.msftncsi.com	64399
1	rediff.com	11838

Subset of domain cache data

Count	Entry	Top 1m Rank
420	www.google.com	5
230	netflix.com	1
100	wikipedia.org	1324
98	crl.globalsign.net	690
25	ocsp.digicert.com	88
15	www.sublimetext.com	28549
14	safebrowsing.google.com	749
8	notepad-plus-plus.org	27688
3	update.googleapis.com	39
1	pandyi.com	NA
1	ipv6.msftncsi.com	64399
1	rediff.com	11838

Subset of Domain Cache data

Hunters Perspective

Attack	We downloaded from a malicious website?
Delivery	We downloaded malware?
Execution	Malware executed on machine?
Persistence	Malware is persisting on my machine?
C2	My system connecting to malicious C2 Infra?

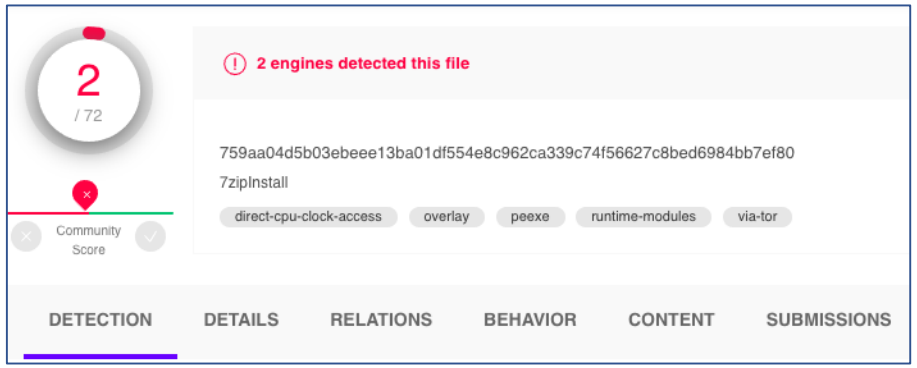
Hunt 2 : Malware executed on machine?

What to search?

- Running Process
- Command Line
- ShimCache
- UserAssist
- Prefetch
- Amcache
- Windows Logs

Enrichment

- Hash Lookups- Intel
- Path of Executable
- Knowing the normal
- SHA1 Lookups
- Signing Info



How to search?

Analysis and Intelligence to detect untrusted and malicious executed files.

```
Tasklistv$ cat *.csv | cut -f 1 -d , | sort | uniq -c | sort -nr
```

101	"svchost.exe"
35	"wsmprovhost.exe"
11	"conhost.exe"
9	"chrome.exe"
8	"csrss.exe"
7	"WmiPrvSE.exe"
6	"vmtoolsd.exe"
6	"powershell.exe"
4	"dwm.exe"
4	"System"
4	"System Idle Process"
4	"SearchIndexer.exe"
3	"taskhostw.exe"
2	"OfficeClickToRun.exe"
2	"LogonUI.exe"
1	"scvhost.exe"
1	"cmd.exe"
1	"avguix.exe"
1	"2183.exe"

List of running tasks – collected across an environment using Kansa

Tasklistv$ cat *.csv | cut -f 1 -d , | sort | uniq -c | sort -nr

101	"svchost.exe"
35	"wsmprovhost.exe"
11	"conhost.exe"
9	"chrome.exe"
8	"csrss.exe"
7	"WmiPrvSE.exe"
6	"vmtoolsd.exe"
6	"powershell.exe"
4	"dwm.exe"
4	"System"
4	"System Idle Process"
4	"SearchIndexer.exe"
3	"taskhostw.exe"
2	"OfficeClickToRun.exe"
2	"LogonUI.exe"
1	"scvhost.exe"
1	"cmd.exe"
1	"avguix.exe"
1	"2183.exe"

List of running tasks – collected across an environment using Kansa

Hunters Perspective

Attack	We downloaded from a malicious website?
Delivery	We downloaded malware?
Execution	Malware executed on machine?
Persistence	Malware is persisting on my machine?
C2	My system connecting to malicious C2 Infra?

Hunt 3 : Malware is persisting on my machine?

What to search?

- Registry Entries
- Startup Links
- Services
- Scheduled tasks
- WMI Event Consumers
- Several others

Enrichment

- Known Good
- Sigcheck*
- Date of creation
- Content
- Scripts referenced
- Hash Lookups

```
:\Users\admin\Downloads\Sigcheck\putty.exe:
        Verified:       Signed
        Signing date:   5:32 PM 9/22/2019
        Publisher:      Simon Tatham
        Company:        Simon Tatham
        Description:    SSH, Telnet and Rlogin client
        Product:        PuTTY suite
        Prod version:   Release 0.73
        File version:   Release 0.73 (with embedded help)
        MachineType:    64-bit
        VT detection:   0/71
        VT link:        https://www.virustotal.com/file/601cdbc
analysis/
```

How to search?

Analysis and Enrichment to identify malicious ASEPs

*https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck

```
$grep Auto  AllServices.csv | awk -F "," '{print $3}' | sort | uniq -c | sort -nr
  26 C:\Windows\system32\svchost.exe -k netsvcs
  13 C:\Windows\system32\svchost.exe -k LocalService
  12 C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
  11 C:\Windows\system32\svchost.exe -k DcomLaunch
  10 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
  10 C:\Windows\System32\svchost.exe -k netsvcs
  10 C:\Windows\System32\svchost.exe -k NetworkService
   <REDACTED>
   2 C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted
   2 C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork
   2 C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe""
/service"
   1 C:\Windows\system32\svchost.exe -k appmodel
   1 C:\Windows\system32\svchost.exe -k WbioSvcGroup
   1 C:\Windows\system32\hasplms.exe  -run
   1 C:\WINDOWS\system32\svchost.exe -k rpcss
   1 C:\WINDOWS\system32\svchost.exe -k appmodel
   1 C:\Program Files (x86)\SLmail\s1smtp.exe
   1 C:\WINDOWS\system32\svchost.exe -k RPCSS
   1 C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
```

List of configured services – collected across an environment using kansa

```
$grep Auto  AllServices.csv | awk -F "," '{print $3}' | sort | uniq -c | sort -nr
  26 C:\Windows\system32\svchost.exe -k netsvcs
  13 C:\Windows\system32\svchost.exe -k LocalService
  12 C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
  11 C:\Windows\system32\svchost.exe -k DcomLaunch
  10 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
  10 C:\Windows\System32\svchost.exe -k netsvcs
  10 C:\Windows\System32\svchost.exe -k NetworkService
   <REDACTED>
   2 C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted
   2 C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork
   2 C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe""
/service"
   1 C:\Windows\system32\svchost.exe -k appmodel
   1 C:\Windows\system32\svchost.exe -k WbioSvcGroup
   1 C:\Windows\system32\hasplms.exe  -run
   1 C:\WINDOWS\system32\svchost.exe -k rpcss
   1 C:\WINDOWS\system32\svchost.exe -k appmodel
   1 C:\Program Files (x86)\SLmail\s1smtp.exe
   1 C:\WINDOWS\system32\svchost.exe -k RPCSS
   1 C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
```

List of configured services – collected across an environment using kansa

Possible Enrichment

Hash Values

+

Virus Total Lookups

Registry Run Key - Descending	Count
ctfmon.exe /n	150
C:\Windows\security\audit\svchost.exe	95
C:\Windows\system32\logon.scr	15
C:\WINDOWS\system32\ctfmon.exe	12
C:\Windows\security\svchost.exe	10
C:\Program Files (x86)\Softland\FBackup 5\bTray.exe	6
C:\Windows\System32\mctadmin.exe	6
C:\Windows\System32\ctfmon.exe ctfmon.exe	5
%SystemRoot%\system32\logon.scr	4
C:\Program Files\CCleaner\CCleaner64.exe /MONITOR	3
C:\Windows\system32\scrnsave.scr	3
"C:\Program Files (x86)\BitTorrent Sync\BTSync.exe" /MINIMIZED	2
"C:\Users\Administrator\AppData\Roaming\BitTorrent Sync\BTSync.exe" /MINIMIZED	2
C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_11_2_202_235_ActiveX.exe -update activex	2
C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup	2
C:\Windows\security\audit\cchost.exe	2

List of machine run keys – collected across an environment

Registry Run Key - Descending	Count
ctfmon.exe /n	150
C:\Windows\security\audit\svchost.exe	95
C:\Windows\system32\logon.scr	15
C:\WINDOWS\system32\ctfmon.exe	12
C:\Windows\security\svchost.exe	10
C:\Program Files (x86)\Softland\FBackup 5\bTray.exe	6
C:\Windows\System32\mctadmin.exe	6
C:\Windows\System32\ctfmon.exe ctfmon.exe	5
%SystemRoot%\system32\logon.scr	4
C:\Program Files\CCleaner\CCleaner64.exe /MONITOR	3
C:\Windows\system32\scrnsave.scr	3
"C:\Program Files (x86)\BitTorrent Sync\BTSync.exe" /MINIMIZED	2
"C:\Users\Administrator\AppData\Roaming\BitTorrent Sync\BTSync.exe" /MINIMIZED	2
C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_11_2_202_235_ActiveX.exe -update activex	2
C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup	2
C:\Windows\security\audit\cchost.exe	2

List of machine run keys – collected across an environment

Possible Enrichment

Hash Values

+

Virus Total Lookups

Hunters Perspective

Attack	We downloaded from a malicious website?
Delivery	We downloaded malware?
Execution	Malware executed on machine?
Persistence	Malware is persisting on my machine?
C2	My system is connecting to malicious C2 Infra?

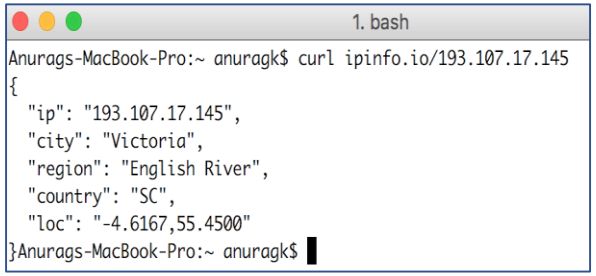
Hunt 4 : My system is connecting to malicious C2 Infra?

What to search?

- Firewall logs
- Web Proxy logs
- NetFlow
- Full packet Capture
- Bro logs
- Netstat entries
- DNS cache

Enrichment

- ASN Numbers
- Geo IP Information
- Intel Look up



How to search?

Analysis and Enrichment to identify malicious Communication using IPs

IPs & DNS both can be used, we talked about DNS in Hunt1

ct	Protocol	LocalAddress	ForeignAddress	State	ConPId	Process
1	TCP	10.199.2.132	65.52.108.219	ESTABLISHED	3064	WpnService
1	TCP	10.199.2.132	65.52.108.223	ESTABLISHED	3064	WpnService
4	TCP	192.168.35.105	192.168.35.101	ESTABLISHED	8832	[powershell.exe]
3	TCP	192.168.35.105	192.168.35.106	ESTABLISHED	8832	[powershell.exe]
3	TCP	192.168.35.105	192.168.35.102	ESTABLISHED	8832	[powershell.exe]
2	TCP	10.199.2.236	84.255.206.8	CLOSE_WAIT	5472	[microsoftedgecp.exe]
2	TCP	10.199.2.132	34.228.214.37	ESTABLISHED	1788	[chrome.exe]
1	TCP	10.199.2.132	172.217.6.35	ESTABLISHED	1788	[chrome.exe]
1	TCP	10.199.2.132	172.217.6.46	ESTABLISHED	6692	[chrome.exe]
1	TCP	10.199.2.128	23.43.62.56	ESTABLISHED	1444	[chrome.exe]
1	TCP	10.199.2.132	185.189.92.231	ESTABLISHED	2720	[avgsvca.exe]
2	TCP	10.199.2.132	23.205.213.149	CLOSE_WAIT	14308	[SearchUI.exe]
1	TCP	10.199.2.236	65.52.108.198	ESTABLISHED	2060	[Explorer.EXE]
1	TCP	10.199.2.236	65.52.108.191	ESTABLISHED	4640	[Explorer.EXE]
1	TCP	10.199.2.132	77.234.41.26	ESTABLISHED	2392	[ncl.exe]

65.52.108.219	WpnService	Microsoft Corporation
65.52.108.223	WpnService	Microsoft Corporation
84.255.206.8	[microsoftedgecp.exe]	T-2 Access Network
34.228.214.37	[chrome.exe]	Amazon.com, Inc
172.217.6.35	[chrome.exe]	Google LLC
172.217.6.46	[chrome.exe]	Google LLC
23.43.62.56	[chrome.exe]	Akamai Technologies Inc.
185.189.92.231	[avgsvca.exe]	AVAST Software s.r.o.
23.205.213.149	[SearchUI.exe]	Akamai Technologies Inc.
65.52.108.198	[Explorer.EXE]	Microsoft Corporation
65.52.108.191	[Explorer.EXE]	Microsoft Corporation
104.131.100.39	[ncl.exe]	DigitalOcean LLC

List of public IP Addresses systems are connecting to

65.52.108.219	WpnService	Microsoft Corporation
65.52.108.223	WpnService	Microsoft Corporation
84.255.206.8	[microsoftedgecp.exe]	T-2 Access Network
34.228.214.37	[chrome.exe]	Amazon.com, Inc
172.217.6.35	[chrome.exe]	Google LLC
172.217.6.46	[chrome.exe]	Google LLC
23.43.62.56	[chrome.exe]	Akamai Technologies Inc.
185.189.92.231	[avgsvca.exe]	AVAST Software s.r.o.
23.205.213.149	[SearchUI.exe]	Akamai Technologies Inc.
65.52.108.198	[Explorer.EXE]	Microsoft Corporation
65.52.108.191	[Explorer.EXE]	Microsoft Corporation
104.131.100.39	[ncl.exe]	DigitalOcean LLC

List of public IP Addresses systems are connecting to

Summary

- Threat hunting can leverage automation but **always need manual intervention**
- **Experience and skill of the threat hunter** is the most important ingredient of threat hunting
- Threat hunting requires **expert analysts**, **data & log repository** and an **analysis platform**

Interested to learn more?

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

Associated Certification: GIAC Certified Incident Handler (GCIH)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Associated Certification: GIAC Certified Forensic Analyst (GCFA)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

Associated Certification: GIAC Network Forensic Analyst (GNFA)

SEC555: SIEM with Tactical Analytics

Associated Certification: GIAC Certified Detection Analyst (GCDA)

SEC511: Continuous Monitoring and Security Operations

Associated Certification: GIAC Continuous Monitoring Certification (GMON)

Thanks for listening!

Anurag Khanna

khannaanurag@gmail.com

@khannaanurag