



# Putting Big Data to Work in DFIR

Jason Mical, Global Cybersecurity Evangelist

July 17, 2020





## Go Beyond the Constraints of Traditional **Security Analytics, Logging, and Monitoring Tools**

### **Purpose-built**

Collect 20X the volume of machine data and meet the crushing demand of automation and algorithms consuming it, no re-architecting required

### **Put More Data to Work, Now**

Enrich and combine machine data with other datasets to go beyond isolated views and unlock the compounding value of your data

### **Game-Changing Economics**

Use more data, unlock new business use cases, all while shrinking operational costs and infrastructure footprint

# Challenges of Pivoting from Investigating to Hunting

What are the top factors contributing to lengthy investigations?



## Poor Visibility

**78%** report lack of visibility into IT security infrastructure



## Impact to Respond

**67%** report information overload



## Low Fidelity Alerts

**68%** report too many alerts to chase



## Isolated Threat Data

**51%** report inability to capture actionable intelligence



## Slow Investigations

**56%** report inability to prioritize threats

# LET THE ANALYSTS ANALYZE WHAT MATTERS MOST.

Analysts' time should not be spent curating information from disparate tools and wading through high noise, low signal alerts.

Automatic enrichment up-levels analysts' work and allows for increased experimentation and innovative analysis



**It's time to close the gap between  
detection and response**

# The Devo Approach: Empower Analysts with a Workflow to Focus on What Matters

## Detection

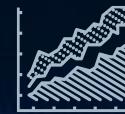


Reduce false positives and alert fatigue

## Investigation



Increase confidence by operationalizing threat data



Speed triage and investigation

## Response



Give analysts the right evidence at the right time

**The Right Alerts, Data, and Context at Analysts' Fingertips**

# Introducing Devo Security Operations

# Bringing it all Together

Devo Security  
Operations

## Entity Analytics

Reliably identify and investigate high-impact threats by shifting focus to entities

## High Signal Alerting

Improve signal-to-noise ratio and find hidden signal with advanced detection

## Auto-enrichment

Accelerate and simplify investigations through multi-layered auto-enrichment

## Threat Data Service

Leverage and share findings with the community through the Threat Data Service

## DFIR Evidence Toolkit

Quickly dive into the DFIR Toolkit with all the applicable evidence

## Hunting Workbench

Easily hunt across all data and context

Devo Data  
Analytics  
Platform

## Log Management

Improve visibility with a centralized, scalable platform for all data

# Analysts at the Heart of SOC Technology Design

Security Operations Overview Dashboard

## Alerts

Most Critical & Not Triaged Alerts

24/4 Critical  
199/199 High

Alert types stacked by ATT&CK MITRE techniques

Top alerts by MITRE ATT&CK

MITRE ATT&CK tactic	Count
Credential Access	299
Initial Access	217
Command and Control	167
Lateral Movement	124
Credential Access and Persistence	112
Exfiltration	105
Discovery	102
Impact	72
Adversary Opsec	28
Privilege Escalation	24

## Analytics

FW traffic during last hour pew pew map

Google Imagery ©2020 NASA, TerraMetrics Terms of Use

## Investigations

Top investigations, sorted by age

Created	Modified	Investigation name	Importance	Killchain	Assignee
3 months	8 days	PowerShell Exec 10.52.60.69	Medium	Execution	Jason Mica
about 2 months	21 days	PowerShell Privilege Escalation	Medium	Privilege Escalation	Fred
about 2 months	9 days	New investigation	Medium	Defense Evasion	John
about 1 month	9 days	Using IP in URL	High	Discovery	Cesar Jimenez
26 days	about 2 hours	PowerShell exec bypass 10.52.60.69	Medium	Credential Access	Fred
23 days	9 days	PowerShell investigation	Medium	Weaponization	Miguel Ang
22 days	22 days	Remote Desktop Session Detected	Medium	Pivoting	Cesar Jimenez
		Detected a dangerous	Medium		Samuel

10 rows | < | 1 - 10 of 31 | > | >|

## Alerts conversion by type

Converted (Green)  
Not converted (Blue)

## Investigations labels word cloud

# Alert Triage

©  
2  
0  
1  
8  
D  
e

Security Operations | Filters | Home > Incident Response > Triage | BACK

Keywords Alert priority Alert type Entity Select... Filter value +

Alert status City Select... Country Select... ATT&CK Tactic Privilege Escalation ATT&CK Technique Exploitation for Privilege Es... X

Showing results for Alerts FILTER

Advanced Filters ^

Alerts

IP 10.52.60.69 Host 10.52.60.69 User null ADD TO INVESTIGATION

50 Sightings for 10.52.60.69	Description	Details	Tactic	Technique	Status	City	Country	Triggered time
Counter: 50	Power Shell Exec Bypass	Suspicious PowerShell download command executed	Privilege Escalation	Exploitation for Privilege Escalation	Unread	Tokyo	JP	14-02-2020 07:10
First seen: about 2 months ago								
Last seen: about 2 hours ago								
User: Devo Security Process								

5 rows < < < > >| ADD TO INVESTIGATION

SUBMIT TO SIGHTING NOW

Description	Details	Tactic	Technique	Status	City	Country	Triggered time
Remote Desktop Execution	Remote Desktop Services Execution from Multiple Sources to Entity Destination	Lateral Movement	Remote Desktop Protocol	Unread			14-02-2020 08:01
Remote Desktop Protocol Scan	Remote Desktop Services Scan from one Entity to Multiple Destinations	Lateral Movement	Remote Desktop Protocol	Unread			14-02-2020 08:01

5 rows < < < > >| ADD TO INVESTIGATION

IP 10.52.60.69 10.11.24.38 ADD TO INVESTIGATION

Priority	Type	Description	Details	Tactic	Technique	Status	City	Country	Triggered time
12	High Detection	Remote Desktop Execution	Remote Desktop Services Execution from Multiple Sources to Entity Destination	Lateral Movement	Remote Desktop Protocol	Unread			14-02-2020 08:01
12	High Detection	Remote Desktop Protocol Scan	Remote Desktop Services Scan from one Entity to Multiple Destinations	Lateral Movement	Remote Desktop Protocol	Unread			14-02-2020 08:01

5 rows < < < > >| ADD TO INVESTIGATION

IP 10.52.60.69 10.20.222.52 ADD TO INVESTIGATION

Complete replay of all activity that occurred prior,  
during and after alert

# Live Victim associations with automated entity enrichment to determine impact

x Graph

QUERY FILTERS    GRAPH VISUALIZATION

**Relationships**  
Incoming   Outgoing  
Limit: 150   Depth: 1  
Impact:

**Entities**  
Entity type: system   Property:  ADD  
ip = 10.52.60.69   host = 10.52.60.69  
user = null

**Query to trigger**

```
filters : {  
    outgoingRelationshipsToAdd : []  
  "baseEntity" : "system"  
  "limit" : 150  
  "depth" : 1  
  filterProperties : {  
    ip : "10.52.60.69"  
  }  
}
```

**FILTER ▶**

**Entity details**

locationLat:	47.6062
customerDomain:	security_intelligence
os:	Windows 7
firstSeen:	30-06-2020 07:00
ip:	10.52.60.69
osConfidence:	50
lastSeen:	02-07-2020 07:00
locationCountry:	US
locationLon:	122.3321
locationCity:	Seattle
bytesOut:	187.25 KB
bytesIn:	183.18 KB
degreeIncoming:	1
degreeOutgoing:	29
type:	System
expanded:	true

Timeline: May 3 - Jul 21, 2020

# Association expansion with automated additional symptoms observed

x Graph

QUERY FILTERS    GRAPH VISUALIZATION

**Relationships**  
Incoming   Outgoing

Limit: 150   Depth: 1

Impact:

**Entities**  
Entity type: system   Property  
ADD

ip = 10.52.60.69   host = 10.52.60.69  
user = null

**Query to trigger**

```
filters : {  
    outgoingRelationshipsToAdd : []  
    "baseEntity" : "system"  
    "limit" : 150  
    "depth" : 1  
    filterProperties : {  
        "ip" : "10.52.60.69"  
    }  
}
```

COPY   FILTER ▶

May 3 - May 9, 2020   May 4 - 10, 2020   May 11 - 17, 2020   May 18 - 24, 2020   May 25 - 31, 2020   Jun 1 - 7, 2020   Jun 8 - 14, 2020   Jun 15 - 21, 2020   Jun 22 - 28, 2020   Jun 29 - Jul 5, 2020   Jul 6 - 12, 2020   Jul 13 - 19, 2020

# Tag artifacts for case creation

Security Operations | BACK

1 Select the items to add to the investigation

Power Shell Exec Bypass  
Suspicious PowerShell download command executed  
Detected a suspicious PowerShell download or execution command  
"C:\Windows\system32\WindowsPowerShell\v1.0\powershellExe" ... from 10.52.60.69

Privilege Escalation  
Exploitation for Privilege Escalation  
Detection 23/25

IP 10.52.60.69

New Domain Located  
A Client has browsed to a newly registered domain never seen by this network  
10.52.60.69 visited a Newly Observed Domain 109.232.105.106 which resolves to 185.156.177.222 from this /x0lbn9efhz . Newly registered domains are not normally directly accessed by users, and have a high probability of being...

Suspicious CNCConnection  
Detected possible CnC connection based on signature  
Detected possible malware campaign from 10.52.60.69 to 42.62.11.210 / casaangeli.it . Connections to CnC with payloads hosted on compromised wordpress...

Remote Desktop Protocol Scan  
Remote Desktop Services Scan from one Entity to Multiple Destinations  
RDP service scan from 10.0.0.100 to 10.52.60.69 and at least 8 Entities

New Domain Observed Client  
A Client has browsed to a newly registered domain never seen by this network  
10.52.60.69 visited a Newly Observed Domain casaangeli.it which resolves to 42.62.11.210 from this /wp-content/themes/Crevison/irvice\_cnn.html . Newly registered domains are not normally directly accessed by users, and have a high probability of being...

Remote Desktop Execution

2 Select New or Add to an existing investigation

New investigation  
Toggle to add to an existing investigation

CREATE INVESTIGATION CANCEL

Security Operations DFIR powered by Devo

# Case Management

Security Operations | Incident Response | Investigations

Home > Incident Response > Investigations ← BACK

Investigation filters 09-01-2019 08:21 > 29-01-2020 12:21 JASONS OPEN CASES RESET FILTERS TO HOME

Importance Low Medium High Investigation Name  Assigned to  Status

Advanced Filters FILTER

**Investigations**

Importance	Investigation name	Assigned to	Status	ATT&CK Tactic	Labels	Keywords	Last Updated	Creation Time
High	Powershell Exec 10.52.60.69	Jason Mical	Open	Execution	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">powershell</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">10.52.60.69</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">mimikatz</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Lateral movement</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">RDP Scanning</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">powershell</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">execution</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">mimikatz</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">lateral movement</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">RDP scanning</span>	26-02-2020 11:10	04-12-2019 06:53
High	RDP exploit 10.52.60.69	Jason Mical	Open	Execution	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">RDP</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Bluekeep</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">RDP</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">execution</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">bluekeep</span>	30-01-2020 15:39	03-12-2019 19:45
High	Info Stealing Detected	Jason Mical	Open	Credential Access	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Mimikatz</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">credential dumping</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">credential dumping</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Mimikatz</span>	29-01-2020 10:42	29-01-2020 10:28
High	Possible compromised host	Jason Mical	Open	Privilege Escalation	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Credential Access</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Persistence</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Credential Access</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Persistence</span>	27-01-2020 10:55	27-01-2020 07:28
High	rdp attack	Jason Mical	Open	Command & Control	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">rdp</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">rdp</span>	15-01-2020 11:27	15-01-2020 11:27
High	Possible CnC connection	Jason Mical	Open	Command & Control	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">42.62.11.210</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">casaangeli.it</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">CnC</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">Web Service</span>	23-12-2019 07:47	19-12-2019 05:36

10 rows < < 1-6 of 6 > >

# Investigation Workbench

© 2018 Devo

Security Operations

Home > Incident Response > Investigations > Investigation Details

CLOSE SAVE

Name\*: PowerShell Exec 10.52.60.69

Importance: Low Medium High

Status: Open

Assigned to: Jason Mical

ATTACK Tactic\*: Execution (TA0002)

Details: looks like a client is becoming a server with powershell exec

Labels: powershell (radio button), 10.52.60.69 (radio button), mimikatz (radio button), Lateral movement (radio button), RDP Scanning (radio button), 42.62.11.210 (radio button), casaangeli.it (radio button)

Keywords: powershell (radio button), execution (radio button), mimikatz (radio button), lateral movement (radio button), RDP scanning (radio button)

Created 04-12-2019 06:53 Last updated 02-07-2020 04:02

EVIDENCE INVESTIGATION TIMELINE

COMMENTS

INVESTIGATION COMMENTS

Jason Mical about 1 month ago: Memory Dump captured

Jason Mical about 1 month ago: RDP Scan from Victim to Multiple Destinations- possible lateral movement

Jason Mical about 1 month ago: Powershell has been found executing with the encoded and hidden parameters

Jason Mical about 1 month ago: Mimikatz has been detected based on the dlls loaded into this process

Fred about 1 month ago: "srcIP": "42.62.11.210"

Search: Search

5 rows < < 1-5 of 6 > >

ASSOCIATIONS

Jason Mical (jason.mical@devo.com)

Start writing your new comment here...

ADD

The screenshot displays the 'Investigation Workbench' interface. On the left, a sidebar contains navigation links for Home, Incident Response, Investigations, and Investigation Details. Below these are sections for Name, Importance (Low, Medium, High), Status (Open), Assigned to (Jason Mical), ATTACK Tactic (Execution), Details (looks like a client is becoming a server with powershell exec), Labels (powershell, 10.52.60.69, mimikatz, Lateral movement, RDP Scanning, 42.62.11.210, casaangeli.it), and Keywords (powershell, execution, mimikatz, lateral movement, RDP scanning). At the bottom of the sidebar are creation and update timestamps. The main content area is divided into EVIDENCE and INVESTIGATION TIMELINE tabs. The EVIDENCE tab is currently active, showing sections for DETECTIONS, OBSERVATIONS, MODELS, and ANALYTICS. The INVESTIGATION TIMELINE tab shows a list of comments. A sidebar on the right lists related investigations, queries, enrichment, entities, files/analysis, and associations. A search bar is at the top right, and pagination controls are at the bottom right.

# Investigation Timeline

Security Operations

Home > Incident Response > Investigations > Investigation Details - Trojan Found in Hunt

CLOSE SAVE

EVIDENCE INVESTIGATION TIMELINE

Timeline for about 1 month

RESTORE ZOOM ?

08 MAY

- 11:25:26 A query was added to the investigation by Jason Mical
- 11:21:59 A comment was added to the investigation by Jason Mical
- 09:47:37 A query was added to the investigation by Jason Mical

06 MAY

- 13:21:32 An entity was added to the investigation
- 13:21:00 2 entities were added to the investigation
- 13:09:20 A query was added to the investigation by Jason Mical
- (new)** The investigation was created

05 MAY

- 05:31:08 An alert of type DETECTION was triggered
  - Corelight Detect Big File Transfer
  - Corelight Detect Big File Transfer
  - High
  - Big file transfer in SAMBA (SMB) protocol
- 05:30:53 An alert of type DETECTION was triggered
  - Corelight Suspicious DNSRequest
  - Corelight Suspicious DNSRequest
  - High
  - DNS request with Shannon entropy >= 4
- 23:31:05 An alert of type DETECTION was triggered
  - Corelight Detect Big File Transfer
  - Corelight Detect Big File Transfer
  - High
  - Big file transfer in SAMBA (SMB) protocol

10 rows < < 1-10 of 203 > >

# Investigation Workbench- case notes

©  
2  
0  
1  
8  
D  
e

The screenshot shows the 'Comments' tab of an 'Investigation Details' page in the Security Operations platform. The left sidebar contains various navigation links such as Home, Incident Response, Investigations, Evidence, Comments, Detections, Observations, Models, Analytics, Related Investigations, Queries, Enrichment, Entities, Files / Analysis, and Associations. The main content area displays a list of comments from Jason Mical and Fred, with timestamps indicating they were made 'about 1 month ago'. Jason's comments describe capturing a memory dump, performing an RDP scan, and detecting PowerShell and Mimikatz activity. Fred's comment includes the IP address 'srcIP: "42.62.11.210"'. A search bar and a save button are visible at the top right.

Comments

Jason Mical about 1 month ago

Memory Dump captured

Jason Mical about 1 month ago

RDP Scan from Victim to Multiple Destinations- possible lateral movement

Jason Mical about 1 month ago

Powershell has been found executing with the encoded and hidden parameters

Jason Mical about 1 month ago

Mimikatz has been detected based on the dlls loaded into this process

Fred about 1 month ago

"srcIP": "42.62.11.210".

Start writing your new comment here...

# Investigation Workbench- Detections

©  
2  
0  
1  
8  
D  
e



+999



Security Operations

Home > Incident Response > Investigations > Investigation Details - Powershell Exec 10.52.60.69

CLOSE SAVE BACK

Evidence Investigation Timeline

Investigation Detections

**Critical** Suspicious PowerShell download command executed

Alert triggered about 1 month ago - 03-02-2020 23:00

Table : edr.crowdstrike.cannon.processrollup2 ATT&CK Tactic : Privilege Escalation ATT&CK Technique : Exploitation for Privilege Escalation

Details Detected a suspicious PowerShell download or execution command `commandline` "C:\Windows\system32\WindowsPowerShell..." from `hostname` 10.52.60.69

**High** Remote Desktop Services Scan from one Entity to Multiple Destinations

Alert triggered about 1 month ago - 03-02-2020 22:01

Table : ids.bro.rdp ATT&CK Tactic : Lateral Movement ATT&CK Technique : Remote Desktop Protocol

Details RDP service scan from `entity_sourceip` 10.52.60.69 to `entity_destinationip` 10.11.24.33 and at least `rdp_destination` 2 Entities

**Critical** Suspicious PowerShell download command executed

Alert triggered about 1 month ago - 03-02-2020 21:00

Table : edr.crowdstrike.cannon.processrollup2 ATT&CK Tactic : Privilege Escalation ATT&CK Technique : Exploitation for Privilege Escalation

Details Detected a suspicious PowerShell download or execution command `commandline` "C:\Windows\system32\WindowsPowerShell..." from `hostname` 10.52.60.69

**Critical** Suspicious PowerShell download command executed

Alert triggered about 1 month ago - 03-02-2020 21:00

Table : edr.crowdstrike.cannon.processrollup2 ATT&CK Tactic : Privilege Escalation ATT&CK Technique : Exploitation for Privilege Escalation

Details Detected a suspicious PowerShell download or execution command `commandline` "C:\Windows\system32\WindowsPowerShell..." from `hostname` 10.52.60.69

**High** Remote Desktop Services Scan from one Entity to Multiple Destinations

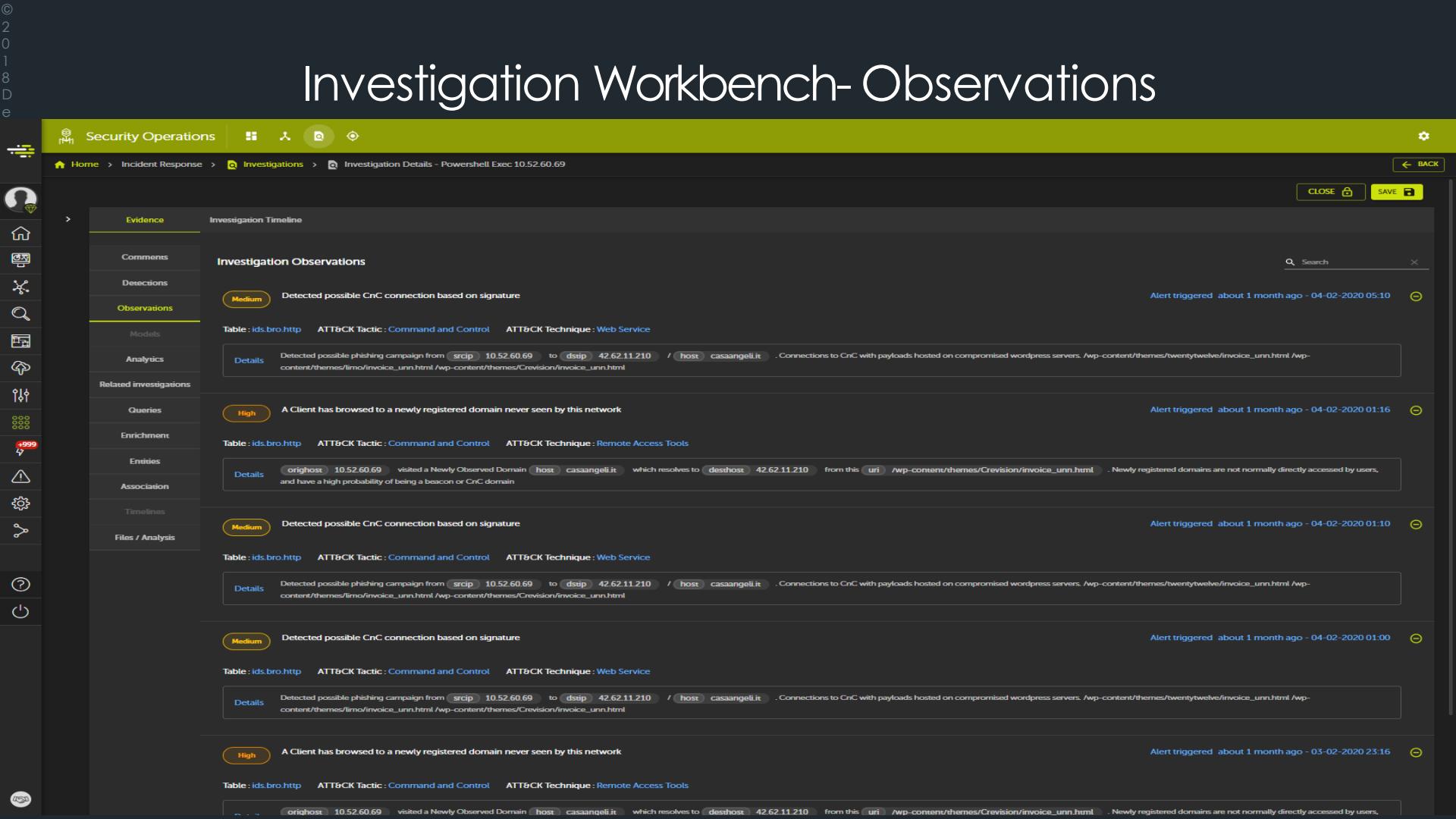
Alert triggered about 1 month ago - 03-02-2020 20:01

Table : ids.bro.rdp ATT&CK Tactic : Lateral Movement ATT&CK Technique : Remote Desktop Protocol

Details RDP service scan from `entity_sourceip` 10.52.60.69 to `entity_destinationip` 10.11.24.33 and at least `rdp_destination` 2 Entities



# Investigation Workbench- Observations



# Investigation Workbench- Analytics

©  
2  
0  
1  
8  
D  
e

Security Operations

Home > Incident Response > Investigations > Investigation Details - Powershell Exec 10.52.60.69

CLOSE SAVE

Evidence Investigation Timeline

Comments

Detections

Observations

Models

Analytics

Related investigations

Queries

Enrichment

+999

Entities

Association

Timelines

Files / Analysis

Search

Alert triggered 14 days ago - 20-02-2020 23:01

Investigation Analytics

Medium Connections with a lot of data load must be monitored because they can be related to threats such as service denial or data exfiltration attacks.

Table : firewall.all.traffic ATT&CK Tactic :Exfiltration ATT&CK Technique :Data Transfer Size Limits

Details Unique connection between entity\_sourceip 192.168.8.218 and entity\_destinationip 31.13.83.51 with more than 50Mbits.

Alert triggered 15 days ago - 19-02-2020 23:01

Medium Connections with a lot of data load must be monitored because they can be related to threats such as service denial or data exfiltration attacks.

Table : firewall.all.traffic ATT&CK Tactic :Exfiltration ATT&CK Technique :Data Transfer Size Limits

Details Unique connection between entity\_sourceip 192.168.8.218 and entity\_destinationip 31.13.83.51 with more than 50Mbits.

Alert triggered 16 days ago - 18-02-2020 17:01

Medium Connections with a lot of data load must be monitored because they can be related to threats such as service denial or data exfiltration attacks.

Table : firewall.all.traffic ATT&CK Tactic :Exfiltration ATT&CK Technique :Data Transfer Size Limits

Details Unique connection between entity\_sourceip 192.168.8.218 and entity\_destinationip 31.13.83.51 with more than 50Mbits.

Alert triggered 17 days ago - 17-02-2020 17:01

Medium Connections with a lot of data load must be monitored because they can be related to threats such as service denial or data exfiltration attacks.

Table : firewall.all.traffic ATT&CK Tactic :Exfiltration ATT&CK Technique :Data Transfer Size Limits

Details Unique connection between entity\_sourceip 192.168.8.218 and entity\_destinationip 31.13.83.51 with more than 50Mbits.

Alert triggered 18 days ago - 16-02-2020 11:01

Medium Connections with a lot of data load must be monitored because they can be related to threats such as service denial or data exfiltration attacks.

Table : firewall.all.traffic ATT&CK Tactic :Exfiltration ATT&CK Technique :Data Transfer Size Limits

Details Unique connection between entity\_sourceip 192.168.8.218 and entity\_destinationip 31.13.83.51 with more than 50Mbits.

# Investigation Workbench- Forensic analysis of obfuscated commands

Security Operations

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Code tidy

Forensics

Multimedia

Recipe

From Base64

Alphabet A-Za-z0-9+=

Remove non-alphabet chars

Input

```
"C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -Noninteractive -NoLogo -windowstyle hidden -e AD7AAAAAAAIYCAA=AAAAAAAAAAAAAAAAAGMCAAARABoACCYAAAAAAIAAAAAAAAABsaWJzZWxpbnV4LnNvLjEAX0IUTV9kZXJ1Z21zdGvYVE1DbG9uZVRhYmxAf9fZ21vb19zdgFydrF9fA9f9fV1cmvnaxN0ZKJUTUnNsB251VGF1bGUAZmd1dgZpbGVjb24AaNjZ1ZwNvbgsZ2vZm1sZwNvbgsaWJjlnlvjYAZmzsdxNoAHN0cmNweQNbnsXrpblWfcgBFx3Byalw50z19jaGszM5YXrjaABzWfkZG1yAHN1dgxvY2fzZQ8tVnJ0b3djdAHN0cmSjbxAab3B0aW5kAHN0cnJjahHAZmZsdXnlo3xVubG9ja2VkaGrjZ2V0dGV4dABzdHByU3B5Agd1dHb3dwIkAGNsbs3NLzGlyAgDldGdyZ2lkAGVycm9yAHNpZ25hbAbtYnN0b3djcwBzaWdwmcwSjbwFzawBFxF3N0VwNrX2no19mYlwsAf9fb1hzbGf0AGlzd3Byalw50zAHJ1YWxsbs2MAYWJvcnQAX2v4AxQAc3Rc3BuAHByb2dyYm1faW52bNhgd1v619yW1AHN0cmZoaw11AF9fYXNzzXj0zhaWwAbgjYnxoaw11x3IAx19jdH1wVSnZKRfbwJF3Vyx21heAbpcwBzvBcHduYm0AY2fsb69jaAHN0cmx1bgbzadlx0eXnlAdBtZ1zZXQabG9jYm1xLY29udgBFx2Vycm5vX2xkvY2F0aW9uA11bWntcAbtZ1w1I3B5AHVuwcB69jaAHN0cmx1bgbzadlx0eXnlAdBtZ1zZXQabG9jYm1xLY29udgBFx2Vycm5vX2xkvY2F0aW9uA11bWntcAbtZ1w1I1bbNwQ8mY2xvc2UAc0ryd91bAbtYwxsbs2MAdGltZwdtAHjhA1Ng1ic2luwaQAdpZQAbmxwfGfuZ2luzm8Ab3B1bmRpccgFxF2N0eXB1X2f9gjAgl1dGvdugFb2zdgfja19hbGxvY2F0ZWRfcABvcRhmcAx19mcwVhzGluzwbzdGr1cnId2N3amwR0aAbPb2N0bAbfb2Jzdgfja19zWdR18xAm9fYnR25wcmldGzFy2hRAHf1G9wdf9s5b25mA9f2nhzdgF0AGZpbGVubwBzXRob3N0bmfTzQ8fb2zdgfja19tZw1vcn1fdXN1zABnXkrjD2QAnzdyaxR1Agl1dhRpbwVzRmeQBzalndhY3RpB24AX19tZw1jch1fY2hAHnpDZ21zbwVtYmVzAgNsbs2Nr2d1dHRpbfu9yR19tZw1jch1fY2hAHf1G9wdf9s5b25mcwAb1t0ak11AHByb2dywfa5b2Nhdb1v19zg9ydf9uWt1Ahjdj3Rbhj1zAF0Y3R5GVfdg91ch1C19s2MAX19jdH1wVz90b2xvd2Vyx2xvBvYnN0YwNrX2Fsb9jx2ZhaWx1Zf9oYw5kbGvyAF9fY3hhx2Zpbmfsaxp1af9f3cByalw50z19jaGsAX194c3RhdbNzXkR4XR0cgBtzW1tb321Af9vYnN0YwNrX2J1Z21uAGJpbmR0Zxh0Z9tYwluAf9fZnhzdGf0YXQAzndyaXr1x3vubG9ja2VKAH0cmNtcAB0Y2d1dHBNcnAAX1
```

Output

```
h5v..^+-zmoZ)Y€..€..«J..y!..€^..Wzyl^qX0jE
€x§µeÜrø^xÜ.€
0.whÄEr.ebus§x.ü.....c.....&.....libselinux.so.1._ITM_deregisterTMCloneTable._gmon_start_.ITM_registerTMCloneTable.fgetfilecon.lgetfilecon.libc.so.6.fflush
ush.strcpy.gmtime r.._printf chk.fnmatch.readdir.setlocale.mbrtowc.strncmp.optind.strchr.fflush unlocked.dgettext.stpcpy.getpwuid.closedir.getgrgid.error.signal.mbstowcs.sigprocmask._stack_chk_fail._lxstat.isprint.realloc._exit.strspn.program_invocation_name.strftime._assert_fail.localtime._r._ctype_get_mb_cur_max.isatty.getpwmam.callc.strlen.sigemptyset.memset.localeconv._errno_locatio
n.memcmp.memcpy.unsetenv._setjmp._fprintf_chk.sigaddset.getgrnam.wcswidth.stdout.lseek.memcpy._fclose.e.strtoul.malloc.timegm.raise.mbsinit.nl_langinfo.opendir._ctype_b_loc.getenvn._obstack_allocat
ed_p_optarg._freeling.stderw.cwidht.ioctl._obstack_begin_1._obstack_newchunk._snprintf_chk.readlin
k.getopt_long._fxstat.fileno.gethostname._obstack_memory_used.getcwd.fwrite.gettimeofday.sigaction._memcp
y_chk.sigismember.clock_gettime._fpending.strchr.iwcntrl.mktimer.program_invocation_short_name._wcstombs._ctype_toupper_loc._ctype_tolower_loc._obstack_alloc_failed_handler._cxa_finalize._sprin
tf_chk._xstat.getxattr.memmove._obstack_begin.bindtextdomain._fxstatat.fwrite_unlocked.strcmp.tcget
pgrp_-
```

# © 2 0 1 8 D e Investigation Workbench- Pivot to forensic utility to capture live artifacts

The screenshot displays the Investigation Workbench interface. At the top, there is a navigation bar with icons for Security Operations, Home, Incident Response, Triage, and Alerts - Power Shell Exec Bypass (25). Below the navigation bar is a search bar with fields for 'From' (2020/07/01 07:41), 'To' (Forever), and 'APPLY INTERVAL'. The main area shows a table of search results:

eventdate	aip	CommandLine	FileName	ImageFileName	MD5HashData	RawProcessId	SHA1HashData	
2020-07-01 15:10:49.556	10.52.6	Pages	powershell.exe" -exec bypass -NonInteractive ...	powershell.exe	C:\Windows\system32\WindowsPowerShellv1.0\powershell.exe	0906e49c252cde958db247fe205b1bb	13159	e978f868350d50ebe88342ab8b4357a4dc01753f

A tooltip for the 'Pages' column indicates the following options:

- Virus Total Lookup
- Virus Total Lookup
- whois
- domain and registration information
- DNS Lookup
- public IP investigation information
- Threat Intelligence Analysis
- ThreatConnect Threat Data Analysis platform
- Fidelis CyberSecurity
- Launch CommandPost
- Host Forensic Analysis
- EnCase Enterprise

The sidebar on the left contains various icons for navigation and system functions, including Home, Incident Response, Triage, Alerts, Threat Intelligence, DNS, WHOIS, Virus Total, Fidelis CyberSecurity, Host Forensic Analysis, and a Help icon.

# Acquire forensic Image from identified victim

© 2  
0  
1  
8  
D  
e

EnCase Acquisition (Dongle Removed)

Case Evidence x

View: Entries | Acquire | Device | Refresh

\$Recycle.Bin  
S-1-5-21-2850218695-3419610912-3  
Path  
Tmp  
Users  
Administrator  
AppData  
Desktop  
carol.ortega  
Public  
Windows  
inf  
Prefetch  
System32

Table  
Selected 929/930

Name	Rej	Fol	Ign	File Ext	Logical Size	Category	Signature Analysis
1 @Please_Read_Me@.txt				txt	933	Document	Match Text
2 @WanaDecryptor@.exe				exe	245,760	Executable	Match Windows Executable
3 \$IC3VP2A.bat.WNCRY				WNCRY	824	None	Unknown

Fields Report

Find Compressed View

000 Q: What's wrong with my files? A: Oops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted. If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely! Let's start decrypting! Q: What do I do? A: First, you need to pay service fees for the decryption. Please send \$300 worth of bitcoin to this bitcoin address: 44413AM4VN2dhxYgXeQepoHkHSQuy6NgaEb94. Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software. Run and follow the instructions! (You may need to disable your antivirus for a while.) Q: How can I trust? A: Don't worry about decryption. We will decrypt your files surely because nobody will trust us if we cheat users. \* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.

Condition Filter EnScript Decode Tag

Decode QuickView  
View Types  
Text  
Do not Show  
High ASCII  
Low ASCII  
Hex  
Unicode  
ROT 13 Encoding  
Base64 Encoding  
UUE Encoding  
Quoted-Printable  
HTML  
HTML (Unicode)  
Picture  
Picture  
Base64 Encoding  
UUE Encoding P  
Integers  
Dates  
Windows

Name	Value
High ASCII	
Unicode	

# Capture Live memory from victim

© 2018 DE

EnCase Acquisition (Dongle Removed)

Case Evidence X

View Tools EnScript Add Evidence

Evidence X

Acquire Device Refresh

Table

Add Local Device

Detect Tableau Hardware

Only Show Write-blocked

Detect Legacy FastBloc

Enable DCO Removal

Enable Physical Memory

Enable Process Memory

Selected 0/81

Local Devices

Name	Label	Access	Sectors	Size	Process ID	Write Blocked	Read	Parse Link Files	Has DCO
2	C	Wind...	233,850,8...	111.5 ...		FALSE	TRUE	TRUE	FA...
3	Process Memory	Mem...				FALSE	FALSE	FALSE	FA...
4	ntoskrnl.exe	Mem...		128 TB	4	FALSE	FALSE	FALSE	FA...
5	smss.exe	Mem...		128 TB	352	FALSE	FALSE	FALSE	FA...
6	csrss.exe	Mem...		128 TB	444	FALSE	FALSE	FALSE	FA...
7	csrss.exe	Mem...		128 TB	528	FALSE	FALSE	FALSE	FA...
8	wininit.exe	Mem...		128 TB	552	FALSE	FALSE	FALSE	FA...
9	winlogon.exe	Mem...		128 TB	592	FALSE	FALSE	FALSE	FA...
10	services.exe	Mem...		128 TB	664	FALSE	FALSE	FALSE	FA...
11	lsass.exe	Mem...		128 TB	680	FALSE	FALSE	FALSE	FA...
12	svchost.exe	Mem...		128 TB	884	FALSE	FALSE	FALSE	FA...
13	svchost.exe	Mem...		128 TB	948	FALSE	FALSE	FALSE	FA...
14	svchost.exe	Mem...		128 TB	380	FALSE	FALSE	FALSE	FA...
15	svchost.exe	Mem...		128 TB	532	FALSE	FALSE	FALSE	FA...
16	svchost.exe	Mem...		128 TB	800	FALSE	FALSE	FALSE	FA...

Signature Analysis

Match Text

Match Windows Exec

Unknown

Value

UUE Encoded P

Integers

Dates

Windows

< Back Next > Cancel

000 Q: What's wrong with m  
111 to access them anymore  
222 to decrypt all your file  
333 u need to pay service f  
444 13AM4VN2dhhXgXeQepoHHS  
555 is the decrypt softwar  
666 nile.)  
Q: How c  
777 because nobody will tru  
888 king <Contact Us> on th

# Centralized Evidence Locker

©  
2  
0  
1  
8  
D  
e

Security Operations

Home > Incident Response > Investigations > Investigation Details - Powershell Exec 10.52.60.69

CLOSE SAVE

Evidence

Comments

Detections

Observations

Models

Analytics

Related investigations

Queries

Enrichment

+999

Entities

Association

Timelines

Files / Analysis

Investigation Timeline

Upload Files

Upload Artifact

Drag & drop or browse your files

Files Selected

None

RESET LIST

UPLOAD

Files included in this investigation

Name	User	Size	Analyze	VIPER analysis	Other analysis	Creation date
2020-02-17-potentially_malicious_traffic.pcap	jason.mical@devo.com	7.51 KB	True	🟡	🟡	17-02-2020 08:35
injector.exe	Brian.martin@devo.com	79.5 KB	True	🟡	🟡	17-02-2020 09:27
2020-02-17-potentially_malicious_traffic.pcap	jason.mical@devo.com	7.51 KB	True	🟡	🟡	24-02-2020 07:34
SCAN_nmap_version_scan_EvilFingers.pcap	jason.mical@devo.com	153.16 KB	True	🟡	🟡	25-02-2020 17:19
SCAN_nmap_version_scan_EvilFingers.pcap	jason.mical@devo.com	153.16 KB	True	🟡	🟡	25-02-2020 17:20

5 rows ▾ |◀|◀|23-25 of 26|▶|▶|

# Evidence Locker- memory analysis

©  
2  
0  
1  
8  
D  
e

Security Operations

Home > Incident Response > Investigations > Investigation Details - Powershell Exec 10.52.60.69 (2)

Memory Analysis

Chose Endpoint: wannacry\_victim

Process scan

eventdate	instance	psscan_data_ExitTime	psscan_data_ImageFileName	psscan_data_Offset	psscan_data_Size
2020-03-17 13:26:29.240	wannacry_victim	2017-05-12T21:26:23	taskse.exe	32849176	536
2020-03-17 13:26:29.240	wannacry_victim	2017-05-12T21:25:53	@WanaDecryptor@	32938832	424
2020-03-17 13:26:29.240	wannacry_victim	2017-05-12T21:26:23	@WanaDecryptor@	33077848	576

Top rows shown: 3 of 3

Process Commandline Activity

eventdate	instance	cmdline_data_Args
2020-03-17 13:26:24.149	wannacry_victim	\SystemRoot\System32\smss.exe
2020-03-17 13:26:24.149	wannacry_victim	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystem
2020-03-17 13:26:24.149	wannacry_victim	winlogon.exe

Top rows shown: 19 of 19

Network Connections

Local_IP	Destination_IP	netscan_Owner	netscan_PID	netscan_State
127.0.0.1	239.255.255.250	cb.exe	1508	CLOSED
169.254.64.5	224.0.0.252	advanced_port_	5800	CLOSED
169.254.64.5	192.168.191.2	cb.exe	1508	CLOSED
169.254.64.5	192.168.191.31	cb.exe	1508	CLOSED

Connections

The treemap visualization shows the relative sizes of various active processes. The largest process is lsass.exe (approx. 67%), followed by spoolsv.exe (approx. 14.8%), wuaclt.exe (approx. 11.7%), and csrss.exe (approx. 8.3%). Other visible processes include smss.exe, winlogon.exe, and wsctf.

Process	Percentage
lsass.exe	~67%
spoolsv.exe	~14.8%
wuaclt.exe	~11.7%
csrss.exe	~8.3%
smss.exe	~3.93%
winlogon.exe	~3.93%
wsctf	~3.93%

# Evidence Locker- Binary Analysis

©  
2  
0  
1  
8  
D  
e



Security Operations    BACK

CLOSE    SAVE

### Viper Analysis for injector.exe

```
"root": { 5 items
  "idanalysis": string "979c9807-00f5-4657-8f79-06103549e9e8"
  "idinvestigation": string "1575467591036000"
  "type": string "VIPER"
  "response": [ 1 item
    {
      "links": [ 4 items
        "notes": string "/api/v3/project/default/malware/4a8d35ea25b9406aa2e1670287f67338020d74d85e98b9833ff73391f516ee47"
        "web": string "/project/default/file/4a8d35ea25b9406aa2e1670287f67338020d74d85e98b9833ff73391f516ee47"
        "analysis": string "/api/v3/project/default/malware/4a8d35ea25b9406aa2e1670287f67338020d74d85e98b9833ff73391f516ee47/analysis/"
        "tags": string "/api/v3/project/default/malware/4a8d35ea25b9406aa2e1670287f67338020d74d85e98b9833ff73391f516ee47/tag/"
      ]
      "data": [ 15 items
        "sha256": string "4a8d35ea25b9406aa2e1670287f67338020d74d85e98b9833ff73391f516ee47"
        "mime": string "application/x-dosexec"
        "sha512": string "807ed857453f69be1994a9294e8e2ac7fc5a170397df0e21156049856980ecfdfaec95b4620eb9d7199fcc61d9528afc5b1c4ba93e7e5c3f10648cc22da6fff2"
        "ssdeep": string "P336:ukM0ERRzsAC/OByQ4H0oYrwtkeQPP6QjQtarvewPKT:RhdVLpYt"
        "type": string "PE32+ executable (GUI) x86-64, for MS Windows"
        "shah": string "6d44f28f29a5b1b7f573ebc2136dc55822cale3"
        "size": string "81408"
        "name": string "injector.exe2315128859349912590.tmp"
        "crc32": string "F348136F"
        "id": string "156"
        "md5": string "1011522443c9e5d9321bb0100ff91503"
        "parent": null
        "created_at": string "2020-02-15 01:33:57.841659"
        "analysis_set": [ 2 items
          {
            "data": [ 4 items
              "id": int 329
              "results": string "[{"type": "info", "data": "Scanning mimikatz.exe4857736066583359363.tmp (ecc23612029589623e0ae27da942440a9b0a9c4df9681ec866613e64a247969d)"}]"
              "cmd_line": string "yara scan -t"
              "stored_at": string "2020-02-17 16:27:01.460116"
            ]
            "links": null
            "url": string "/api/v3/project/default/analysis/329/"
          }
          {
            "data": [ 4 items
              "id": int 330
              "results": string "[]"
              "cmd_line": string "triage"
              "stored_at": string "2020-02-17 16:27:01.460116"
            ]
            "links": null
            "url": string "/api/v3/project/default/analysis/330/"
          }
        ]
      ]
    }
  ]
}
```

Search

Creation date

Date
17-02-2020 08:35
17-02-2020 09:27
24-02-2020 07:34
25-02-2020 17:19
25-02-2020 17:20

5 rows    | <    < 21-25 of 26    > >|

COPY

CLOSE

CLOSE

# Evidence Locker- Pcap analysis

Security Operations DFR powered by Devo

Home > Incident Response > Investigations > Investigation Details - Powershell Exec 10.52.60.69

BACK CLOSE SAVE

### Other Analysis for 2020-02-17-potentially\_malicious\_traffic.pcap

**Evidence** **Investigation Time**

**Comments** **Upload**

**Detections**

**Observations**

**Models** SC

**Analytics** SC

**Related investigations** SC

**Queries** SC

**Enrichment** GE

**Entities**

**Association**

**Timelines**

**Files / Analysis**

**Name**

- 2020-02-17-p...
- injector.exe
- 2020-02-17-p...
- SCAN\_nmap\_v...
- SCAN\_nmap\_v...

**root** : { 5 items  
  "idAnalysis" : string "1621db9d-afb5-4db6-9baf-fb74ef92fb12"  
  "idInVESTigation" : string "15754675910360000"  
  "type" : string "PCAP"  
  "response" : { 7 items  
    "connections" : 105 items  

- I 100 items  
  - 0 : { 7 items  
          "arrivalTime" : string "2018.01.08 20:21:34.423"  
          "packetInfo" : string "pcap Layer LAYER\_1"  
          "srcIP" : string "10.52.60.69"  
          "dstIP" : string "10.0.0.100"  
          "name" : string "pcap"  
          "payload" : NULL  
          "type" : string "eth"  
        }
  - 1 : { 7 items  
          "arrivalTime" : string "2018.01.08 20:21:34.525"  
          "packetInfo" : string "pcap Layer LAYER\_1"  
          "srcIP" : string "10.0.0.100"  
          "dstIP" : string "10.52.60.69"  
          "name" : string "pcap"  
          "payload" : NULL  
          "type" : string "eth"  
        }
  - 2 : { 7 items  
          "arrivalTime" : string "2018.01.08 20:21:34.529"  
          "packetInfo" : string "pcap Layer LAYER\_1"  
          "srcIP" : string "10.52.60.69"  
          "dstIP" : string "42.62.11.210"  
          "name" : string "pcap"  
          "payload" : NULL  
          "type" : string "eth"  
        }
  - 3 : { 7 items  
          "arrivalTime" : string "2018.01.08 20:21:34.582"  
          "packetInfo" : string "pcap Layer LAYER\_1"  
          "srcIP" : string "42.62.11.210"  
          "dstIP" : string "10.52.60.69"  
          "name" : string "pcap"  
          "payload" : NULL  
          "type" : string "eth"  
        }
  - 4 : { 7 items  
          "arrivalTime" : string "2018.01.08 20:21:34.583"  
        }

COPY CLOSE

Search UPLOAD

Creation date

Creation date
17-02-2020 08:35
17-02-2020 09:27
24-02-2020 07:34
25-02-2020 17:19
25-02-2020 17:20

5 Rows | < < 1-5 of 19 > > |

# Investigation Workbench- Automated Entity Enrichment

©  
2  
0  
1  
8  
D  
e

Security Operations | Home > Incident Response > Investigations > Investigation Details - Possible Exfiltration

Possible Exfiltration

Importance: Low, Medium, High

Status: Open

Assigned to: Raul Arriola

ATT&CK Tactic: Adversary OPSEC (TA0021)

Details, Labels, Keywords

Created 25-06-2020 03:59, Last updated 30-06-2020 02:18

INVESTIGATION ENRICHMENTS

Name	Description	Value	User	Actions
127.87.1.35	Obtain from Devo Sighting for value 127.87.1.35	<pre>{"root": { "value": "127.87.1.35", "first_seen": 1593082277, "last_seen": 1593082277, "count": 1, "tags": ""}}</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from GrayNoise Intelligence, LLC for ip 127.87.1.35	<pre>[{"error": 400, "description": "Invalid IP submitted"}, {"error": null} ]</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from DNS for ip 127.87.1.35	<pre>{"root": { "addresses": {} }}</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from Devo Enigma for ip 127.87.1.35	<pre>{"root": { ... } }</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from Devo MISP server for attribute = 127.87.1.35	<pre>{"root": { "response": { "Attribute": [] } }}</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from DomainTools IRR iris-investigate API for ip equals 127.87.1.35	<pre>{"root": { "response": { "limit_exceeded": false, "has_more_results": false, "message": "" } }}</pre>	Devo Security Process	⋮
127.87.1.35	Obtain from Devo MISP server for attribute = 127.87.1.35	<pre>{"root": { "response": { "Attribute": [] } }}</pre>	Raul Arriola	⋮

# Investigation Workbench- investigative searches

The screenshot displays a complex interface for security operations, specifically focusing on investigation details. On the left, a vertical sidebar lists navigation items such as Home, Incident Response, Investigations, Evidence, Comments, Detections, Observations, Models, Analytics, Related Investigations, Queries, Enrichment, Entities, Files / Analysis, and Associations. The main content area is titled "INVESTIGATION TIMELINE" and contains several sections for different users and their activities. Each section includes a timestamp (e.g., "about 1 month ago") and a "RUN QUERY" button. The queries themselves are displayed in code snippets, such as:

```
1 from edr.CommandLine where command_line like '%powershell.exe%' -exec bypass -NonInteractive -NoLogo -WindowStyle Hidden & e
AD78A4A4-0000-0000-0000-000000000000
1 from domains.all where domain = "casaangeli.it" and url -> "casaangeli.it"
1 from domains.all where domain -> "casaa"
1 from edr.carbonblock.ingress where command_line -> "mimikatz"
1 from ids.bro.rdp where origHost -> "10.52.68.69"
```

# Hunting workbench

Security Operations

Home > Investigator > Hunting BACK

Hunting filters RESET FILTERS

01-01-2019 00:00 > 05-03-2020 11:26

Target Tables: `edr.carbonblack.ingress`

Filters Criteria: `command_line` equals `mimikatz`

Results statistics: 01-01-2019 00:00 > 05-03-2020 11:26

edr.carbonblack.ingress 4 matching results

Hunting results

eventdate	Table	Data
10-12-2019 08:38:49.363	edr.carbonblack.ingress	<pre>action:actiontype:cb_server:aws_cbserver:computer_name:AWS-WEBSERVER:event_type:proc:filetype:filetype_name:link_process:https://10.0.0.100/#analyze/00000005-0000-1010-01d5-af6deadbb80/link_ path:c:\mimikatz\x64\mimikatz.exe:pid:4112:process_guid:00000005-0000-1010-01d5-af6deadbb80:process_path:c:\mimikatz\x64\mimikatz.exe:sensor_id:5:sha256:E32A750F0316199E83D59197088B25B12634969C type:ingress.event.procstart:direction:domain:ipv4:port:local_ip:local_port:protocol:remote_ip:remote_port:child_process_guid:created:link_child:command_line:C:\Mimikatz\x64\mimikatz.exe link_parent:https://10.0.0.100/#analyze/00000005-0000-1714-01d5-af6c4050e501:parent_create_time:1575992264000:parent_md5:5746BD7E255DD6A8AFA06F7C42C1BA41:parent_path:c:\windows\system32\cmd.exe username:AWS-WEBSERVER\Student:cross_process_type:is_target:link_target:requested_access:target_create_time:target_md5:target_path:target_pid:target_process_guid:blocked:emer_timestamp:log_i uid:S-1-5-21-2895370199-1438549402-3901547284-1000:tamper_type:parent_pid:5908 message:{"cb_server": "aws_cbserver", "command_line": "C:\Mimikatz\x64\mimikatz.exe", "computer_name": "AWS-WEBSERVER", "event_type": "proc", "expect_followon_w_md5": false, "filtering_known_dlls": true, "link_parent": "https://10.0.0.100/#analyze/00000005-0000-1010-01d5-af6deadbb80", "path": "c:\mimikatz\x64\mimikatz.exe", "pid": 4112, "process_guid": "00000005-0000-1010-01d5-af6deadbb80", "sensor_id": 5, "sha256": "E32A750F0316199E83D59197088B25B12634969C, "type": "ingress.event.procstart", "username": "AWS-WEBSERVER\Student"}, "parent_md5": "5746BD7E255DD6A8AFA06F7C42C1BA41", "parent_path": "c:\windows\system32\cmd.exe", "parent_pid": 5908}</pre>
13-12-2019 08:03:06.062	edr.carbonblack.ingress	<pre>action:actiontype:cb_server:aws_cbserver:computer_name:AWS-WEBSERVER:event_type:proc:filetype:filetype_name:link_process:https://10.0.0.100/#analyze/00000005-0000-0abc-01d5-b1c4df9c1c10/link_ path:c:\mimikatz\x64\mimikatz.exe:pid:2748:process_guid:00000005-0000-0abc-01d5-b1c4df9c1c10:process_path:c:\mimikatz\x64\mimikatz.exe:sensor_id:5:sha256:E32A750F0316199E83D59197088B25B12634969C type:ingress.event.procstart:direction:domain:ipv4:port:local_ip:local_port:protocol:remote_ip:remote_port:child_process_guid:created:link_child:command_line:C:\Mimikatz\x64\mimikatz.exe link_parent:https://10.0.0.100/#analyze/00000005-0000-141c-01d5-b1c4d622820f1:parent_create_time:1576248704000:parent_md5:5746BD7E255DD6A8AFA06F7C42C1BA41:parent_path:c:\windows\system32\cmd.exe username:AWS-WEBSERVER\Student:cross_process_type:is_target:link_target:requested_access:target_create_time:target_md5:target_path:target_pid:target_process_guid:blocked:emer_timestamp:log_i uid:S-1-5-21-2895370199-1438549402-3901547284-1000:tamper_type:parent_pid:5148 message:{"cb_server": "aws_cbserver", "command_line": "C:\Mimikatz\x64\mimikatz.exe", "computer_name": "AWS-WEBSERVER", "event_type": "proc", "expect_followon_w_md5": false, "filtering_known_dlls": true, "link_parent": "https://10.0.0.100/#analyze/00000005-0000-0abc-01d5-b1c4df9c1c10", "path": "c:\mimikatz\x64\mimikatz.exe", "pid": 2748, "process_guid": "00000005-0000-0abc-01d5-b1c4df9c1c10", "sensor_id": 5, "sha256": "E32A750F0316199E83D59197088B25B12634969C, "type": "ingress.event.procstart", "username": "AWS-WEBSERVER\Student"}, "parent_md5": "5746BD7E255DD6A8AFA06F7C42C1BA41", "parent_path": "c:\windows\system32\cmd.exe", "parent_pid": 5148}</pre>

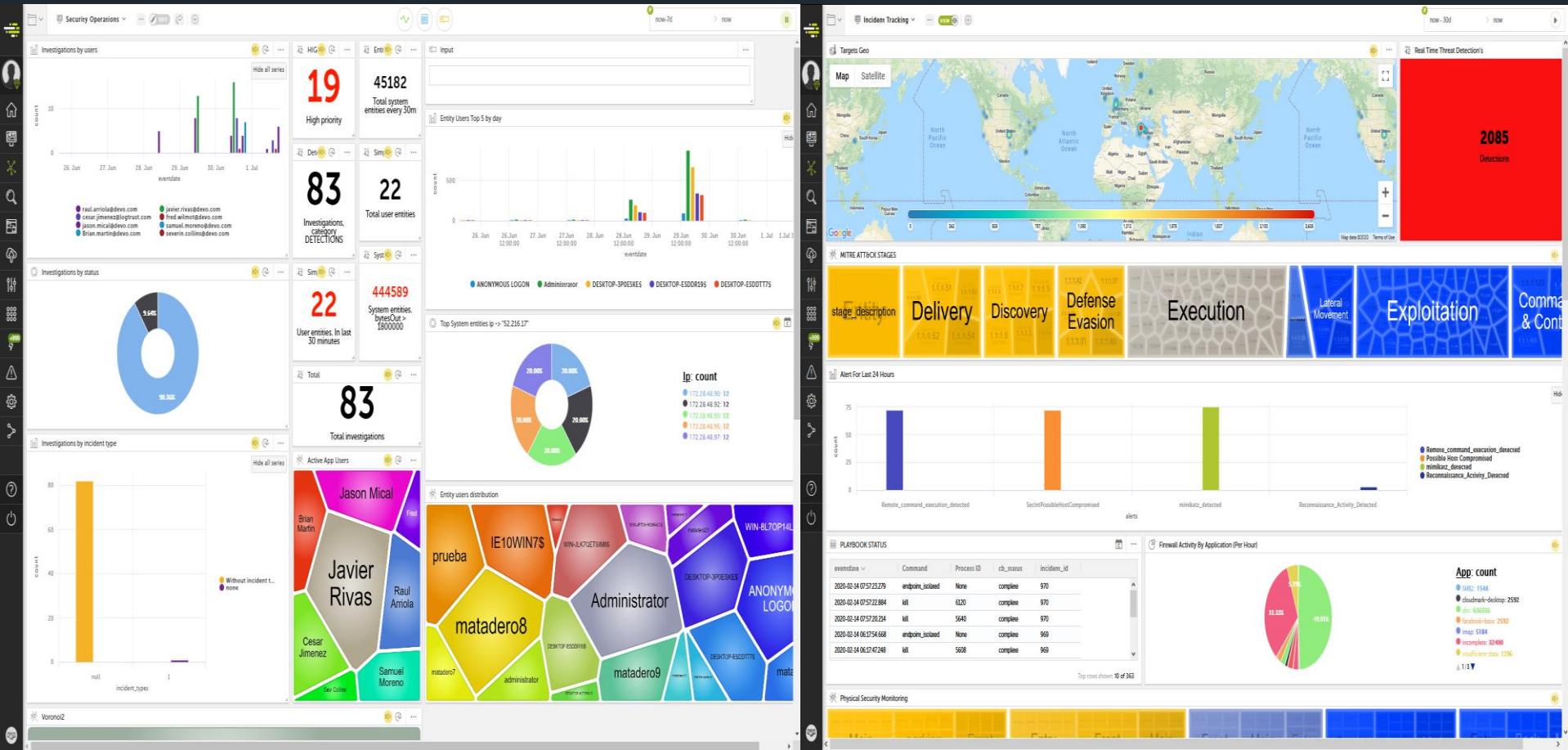
# Investigation Workbench- Related investigations

The screenshot shows the 'Investigation Details' page for a PowerShell execution event. The left sidebar includes icons for Home, Incident Response, Investigations, Evidence, Comments, Detections, Observations, Models, Analytics, Related investigations (highlighted), Queries, Enrichment, Entities, Association, Timelines, and Files / Analysis. The main content area has tabs for Evidence and Investigation Timeline. Under 'Related investigations', a table lists five entries:

Importance	Name	Assigned	Status	Last Update	Actions
Medium	data exfiltration	Jason Mical	Open	12-02-2020 07:50	
High	Using IP in URL	Cesar Jimenez	Open	04-02-2020 05:16	
High	powershellExe bypass 10.52.60.69	Fred	Open	18-12-2019 17:27	
High	RDP Malware	Samuel Sancho	Open	04-12-2019 06:22	
High	priv escalation T2004 Upload big binary file	Cesar Jimenez	Closed	03-12-2019 11:01	

Below the table, there is a search bar with placeholder text 'Investigation Select...' and a 'Search' button.

# Live Interactive Reporting/Dashboards



# Questions?

Learn more at **devo.com** or email us at [sales@devo.com](mailto:sales@devo.com)



THANK YOU

