



FALCON 302

LEARNER GUIDE

VERSION 02.2024

CROWDSTRIKE

U
CROWDSTRIKE
UNIVERSITY

TABLE OF CONTENTS

3	Overview
4	Threat Hunting Steps
7	Triggers and Pivots
16	Threat Sources
17	Intel 101
19	Resolution Tip
20	Threat Hunt Maturity Assessment
21	CrowdStrike S.E.A.R.C.H.
22	S.E.A.R.C.H.Tips
29	Hunting Methods
35	Visualizations
36	Advanced Hunting in EDR Data
40	Intelligence Models
42	MITRE ATT&CK
45	Morphological Analysis
47	ATT&CK Navigator
50	Threat Hunt Automation
53	Hunting Resources



OVERVIEW

What is threat hunting?

Threat hunting is a discipline where skilled defenders hunt actively for the faintest signs of advanced attacks. It augments automated detection techniques such as machine learning and behavioral analytics with human experience and intuition, to see and stop advanced, stealthy attacks.

Benefits

Done properly, threat hunting leverages human experience to see and stop advanced attacks that might otherwise linger unseen for days, weeks, or months. It shortens dwell time, and is key to reliably stopping breaches.

CROWDSTRIKE TAKE ON THREAT HUNTING



CROWDSTRIKE TAKE ON “THREAT HUNTING”

Generally, CrowdStrike refers to “Threat Hunting” as:

Proactively identifying threats in your network, on which toolsets may not otherwise alert.

- Automated solutions – even CrowdStrike Falcon – are not 100% effective against patient, persistent, and skilled adversaries
- Security buzzword – can mean different things to different people
- Can have an overlap with Incident Response
- Input: Threat Hunting typically requires threat intelligence to guide the hunt
- Output: Results of a hunt lead to updated threat intelligence and new hypotheses forming
- Threat hunting is a never-ending cycle of searching and learning

THREAT HUNTING STEPS



The process of proactive cyber threat hunting typically involves three steps: a trigger, an investigation and a resolution.

1. Trigger

Point threat hunters to a specific area of the network for investigation when potential malicious activity is detected.

2. Investigation

Threat hunters use EDR technology to deep dive into potential malicious compromise of a system.

3. Resolution

Communicating malicious activity intelligence to operations and security teams so they can respond to the incident and mitigate threats.

REACTIVE VS. PROACTIVE HUNTING

Reactive Hunting

After threat detection



- When you have notification of a detection or that there is already an anomaly in your network
- Can come from a sensor or routine analysis of logs, netflow, etc
- Can come from a third party notification

Proactive Hunting

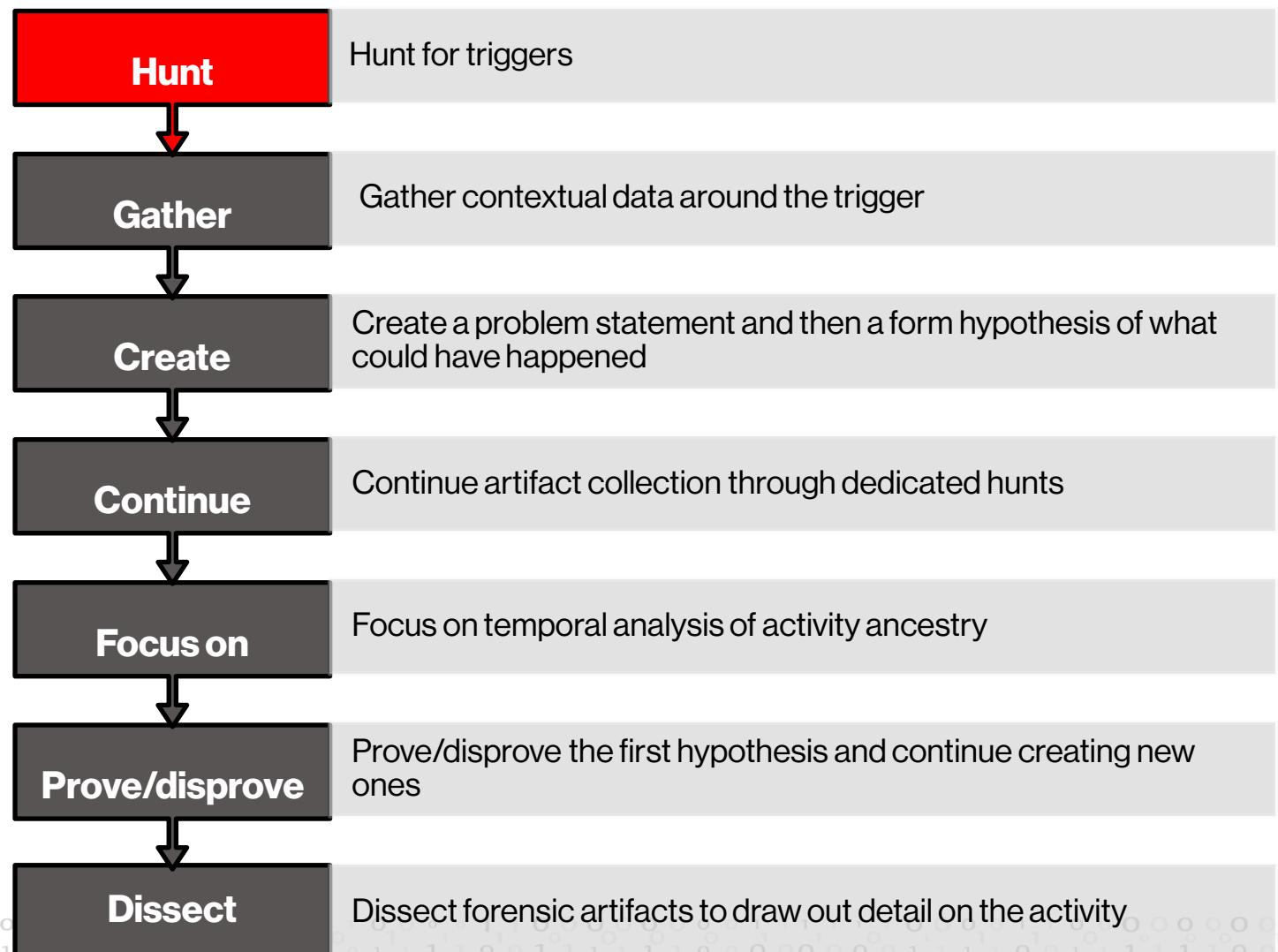
Before threat detection



- No known attacks or compromises
- Searching for “just in case” scenarios and zero-day exploits
- Something you found in the news or intel but no indication it happened to you

CROWDSTRIKE THREAT HUNTING

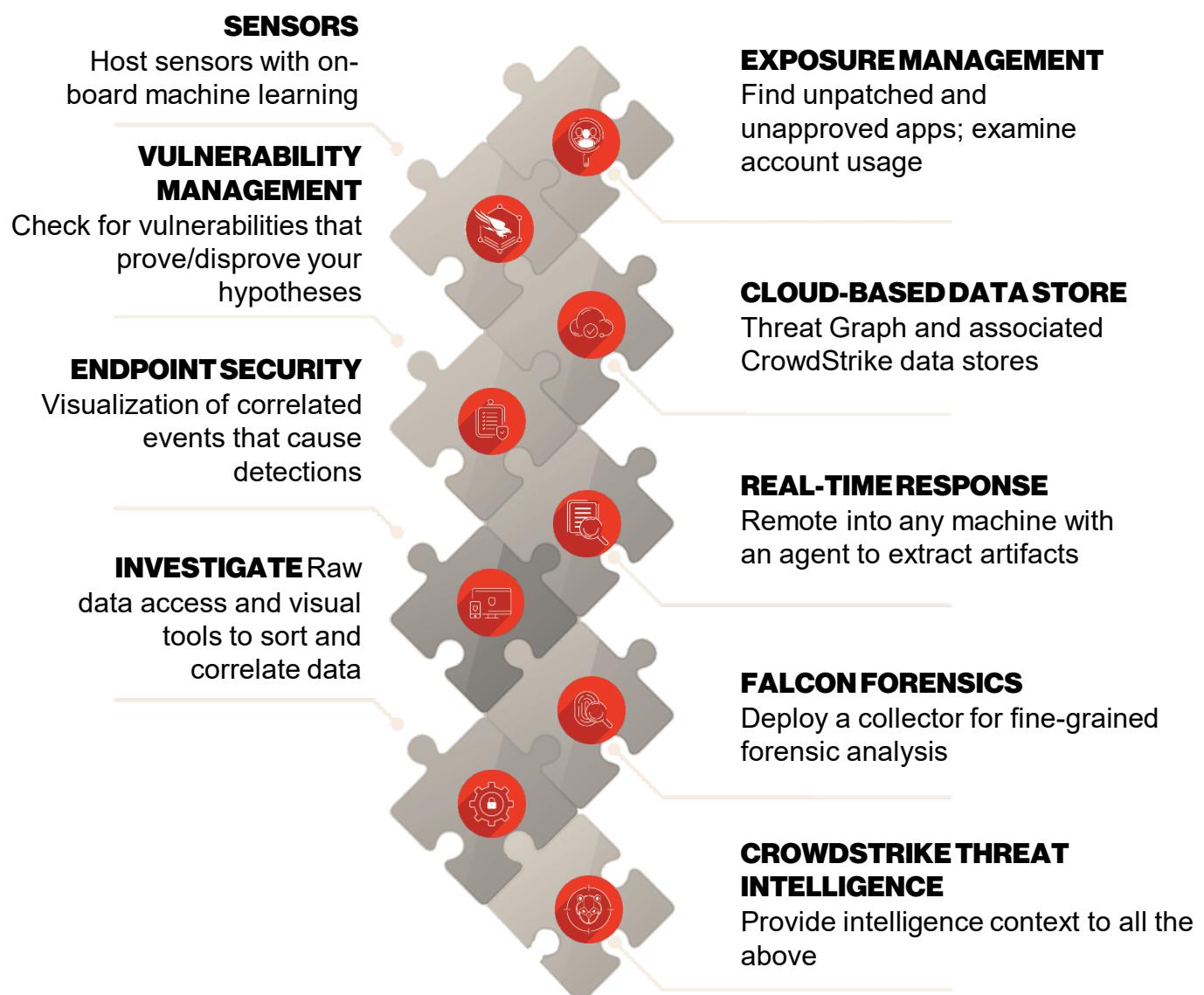
Tips for Hunting with Falcon



CROWDSTRIKE THREAT HUNTING



The following sections of the Falcon platform pertain to a threat hunter.



TRIGGERS AND PIVOTS

INDICATORS (IOCs)

- Hashes
- IP addresses
- Domain names

be24561427d754c0c1...

23.229.209.5

falconsplayingpoker.com

Triggering indicator SHA256 on library/DLL loaded

Description
This file meets the machine learning-based on-sensor AV protection's high confidence threshold for r

Tactic via technique
Machine Learning via Sensor-based ML

Hash action	Global prevalence	Local pre
None	Common	Low

Associated MD5
8658fcbb619b53454f14665dba30ebe

Associated file
\Device\HarddiskVolume1\Temp\c.exe

BEHAVIORS (IOAs)

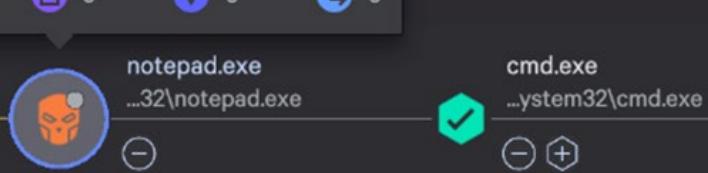
- Executables running from Temp directories
- Abnormal parent/child relationships
- Non-network processes making connections

Keep Access via Defense Evasion

Process name: notepad.exe
Start: Aug. 29, 2023 13:03:27
Duration: 00:07:04.123

Process Actions

9 (Wi-Fi), 81 (Network), 0 (File), 0 (Clipboard), 0 (Registry)



FALCON TRIGGERS

CROWDSTRIKE

FALCON TRIGGERS - INVESTIGATE (EVENT SEARCH)

Routine threat hunt query

```

1 #event_simpleName-ProcessRollup2 ParentBaseFileName=~cmd\.exe/i
2 |groupBy([fileName, CommandLine])
3 | sort(_count, order-desc)

```

Fields	#	%
.count	18	100%
CommandLine	41	100%
fileName	15	100%

Results

FileName	CommandLine
conhost.exe	\?\\Windows\\system32\\conhost.exe @ffffffffff -ForceV1
PING.EXE	ping contagioudump.blogspot.com
timeout.exe	timeout 1
PING.EXE	ping www.reallybaddomain.com
cmd.exe	C:\\Windows\\system32\\cmd.exe /c C:\\Windows\\system32\\reg.exe query hklm\\software\\microsoft\\windows\\softwareinventorylogging
reg.exe	C:\\Windows\\system32\\reg.exe query hklm\\software\\microsoft\\windows\\softwareinventorylogging /v collectionstate /reg:64
flic.exe	ffe -cid 3A84673e94cc4070880DC8446883f64-91 -replay-dir upload_bucket -replay-cloud prod
flic.exe	ffe -cid 3A84673e94cc4070880DC8446883f64-91 -config C:\\default_windows.yml -no-sensor -offline -verbose
powershell.exe	PowerShell -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand UABvNlcaZQByAFMaNB1AGwAbAAgAC0ATgB8
powershell.exe	PowerShell -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand UABvNlcaZQByAFMaNB1AGwAbAAgAC0ATgB8
ffe	ffe -cid 3A84673e94cc4070880DC8446883f64-91 -no-sensor -offline -verbose
WMIC.exe	wmic /node:172.17.0.5 /user:administrator /password:Password!! process call create "powershell.exe -exec b -w h -ec \$"
WMIC.exe	wmic qfe

Query status: Done Hits: 1,863 Speed: 2.28 Gb/s EPS: 743.64k Work: 2 Completion: 100%

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY

FALCON TRIGGERS - RAW DATA

```
{
  "CommandLine": "C:\\temp\\c.exe",
  "ComputerName": "LNV1P22EN0",
  "ConfigBuild": "1007.3.0017506.1",
  "ConfigStateHash": "263646383",
  "ContextProcessId": "9233720866",
  "EffectiveTransmissionClass": "2",
  "Entitlements": "15",
  "EventOrigin": "1",
  "GrandparentCommandLine": "C:\\Windows\\system32\\svchost.exe -k DcomLaunch -p",
  "GrandparentImageFileName": "\\Device\\HarddiskVolume1\\Windows\\System32\\svchost.exe",
  "GrandparentProcessId": "14074983",
  "GrandparentProcessPatternIdList": "7140,7150,7410,7411,7412,7426",
  "ImageFileName": "\\Device\\HarddiskVolume1\\Temp\\c.exe",
  "LocalAddressIP4": "10.1.1.66",
  "ParentCommandLine": "C:\\Windows\\system32\\wbem\\wmiprvse.exe -secured -Embedding",
  "ParentImageFileName": "\\Device\\HarddiskVolume1\\Windows\\System32\\wbem\\WmiPrvSE.exe",
  "ParentProcessId": "9231672724",
  "ParentProcessPatternIdList": "218,7119,7141,7200,7201,7391,7402,7410,7411,7412,7647,7652,7654,7655,7675,7683",
  "PatternId": "10126",
  "PatternIdList": "171,218,3450,5765,7079,7093,7142,7143,7149,7200,7205,7214,7217,7223,7225,7249,7252,7254,7256,7357,7398,7410,7411,7412,7428,7429,7430,7475,7566,7607,7646,7661,7675,7792,7900,7904,7912,10199,10251,10378,51324,51325",
  "Tags": "41, 53, 184, 197, 812, 843, 862, 874, 1218, 1225, 1226, 180388736803, 180388736922, 180388737277, 180388737404, 180388737948, 10995116277909, 10995116277927, 10995116277930, 10995116278019, 10995116278036, 10995116278186",
  "TemplateInstanceId": "15726",
  "TemplateInstanceIdList": "2932,3429,7355,7411,15308",
  "aid": "62d90c0e240a42a7ad0391cb8f4e6691",
  "aip": "100.26.62.1",
  "cid": "3a84673e94cc4070b8bdcb48468b3f64",
  "event_platform": "Win",
  "event_simpleName": "TemplateDetectAnalysis",
  "id": "4d86e3f2-0f03-4338-b592-9cc0f50b3894",
  "name": "TemplateDetectAnalysisV11",
  "timestamp": "1697231862934"
}
```

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY

FALCON TRIGGERS

CROWDSTRIKE

FALCON TRIGGERS - EXPOSURE MANAGEMENT

The screenshot shows the Falcon Triggers - Exposure Management interface. At the top, there are tabs for Dashboards, Vulnerabilities (which is selected), Installed patches, Reports, Suppression rules, and Tickets. A search bar is at the top right. Below the tabs, it says "2.3K vulnerabilities found on 9 assets". The main table has columns for Hostname, Asset criticality, Device type, Vulnerabilities, Remediations, Critical (ExPRT Rating), Actively used exploits, and Actions. Two rows are highlighted with red circles: "INTECH-AD" (Unassigned, Domain Controller) with 1,066 vulnerabilities and "INTECH-EXCHANG" (Unassigned, Server) with 357 vulnerabilities.

CVE-2013-3900

This is a detailed view of a specific vulnerability entry for CVE-2013-3900. It includes sections for Status (with Critical ExPRT rating and Exploit status), Description (mentioning WinVerifyTrust function), Vulnerability type, References, and a smaller table for remediations.

COPYRIGHT © 2024 CROWDSTRIKE, INC.

CROWDSTRIKE

FALCON TRIGGERS - REMOVABLE MEDIA

The screenshot shows the Falcon Triggers - Removable Media dashboard. At the top, there are tabs for Investigate (selected), Parameters, and Live. A search bar is at the top right. The main area shows a table of files written to removable media, with columns for FileName, #event_simpleName, ComputerName, TargetFileName, and Time. One row, "Stuff we need to keep between us.xls", is circled in red.

FileName	#event_simpleName	ComputerName	TargetFileName	Time
Stuff we need to keep between us.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume19\Stuff we need to keep between us.xls	2023-11-13 18:58:58
Your contact list.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume19\Your contact list.xls	2023-11-13 18:58:58
Yet another set of books.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume19\Yet another set of books.xls	2023-11-13 18:58:58
Your Customer List.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume19\Your Customer List.xls	2023-11-13 18:58:58
The Wall 10 Year Plans.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume19\The Wall 10 Year Plans.xls	2023-11-13 18:58:58
Marketing Forecast.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Marketing Forecast.doc	2023-11-13 18:58:58
Secret Memo.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Secret Memo.doc	2023-11-13 18:58:58
How to tame your dragon.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\How to tame your dragon.doc	2023-11-13 18:58:58
Secret memo 2.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Secret memo 2.doc	2023-11-13 18:58:58
My plans for world domination.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\My plans for world domination.doc	2023-11-13 18:58:58
More Plans.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\More Plans.doc	2023-11-13 18:58:58
Special Memo.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Special Memo.doc	2023-11-13 18:58:58
Plans.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Plans.doc	2023-11-13 18:58:58
Potty training dragons.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Potty training dragons.doc	2023-11-13 18:58:58
Strategic Plans.doc	MSDocxFileWritten	thematrix	\Device\HarddiskVolume19\Strategic Plans.doc	2023-11-13 18:58:58
Salaries.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Salaries.xls	2023-11-13 18:58:43
Second Set of Books.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Second Set of Books.xls	2023-11-13 18:58:43
Payroll.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Payroll.xls	2023-11-13 18:58:43
Expense Account numbers.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Expense Account numbers.xls	2023-11-13 18:58:43
Something wicked this way comes.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Something wicked this way comes.xls	2023-11-13 18:58:43
Internal Accounts.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\Internal Accounts.xls	2023-11-13 18:58:43
External Accounts.xls	MSXlsxFileWritten	thematrix	\Device\HarddiskVolume18\External Accounts.xls	2023-11-13 18:58:43

COPYRIGHT © 2024 CROWDSTRIKE, INC.

FALCON TRIGGERS



FALCON TRIGGERS - QUARANTINED FILES

Screenshot of CrowdStrike Falcon interface showing quarantined files. The interface includes a search bar, activity ID, customer ID, and notification icons.

Quarantined Files

Search: Activity@2fc7569b Customer ID Notifications

Status	File Name	Hostname	User
Quarantined	FHT200 samples setup.exe	APPSVR-61883	Administrator
Released	benignmalware 03593.exe	APPSVR-92010	Administrator
Cleaned	benignmalware 07802.exe	APPSVR-47417	Administrator
Deleted	benignmalware 12076.exe	APPSVR-71463	Administrator
Delete Pending	benignmalware 33889.exe	APPSVR-71023	Administrator
Release Pending	benignmalware 55887.exe	APPSVR-52746	Administrator

1,283 quarantined files found

Selected 0 of 1283

Date of Quarantine	File Name	Hostname	User	Status	Actions
Oct. 4, 2023 01:55:03	puttyX-85252.exe	APPSVR-85252	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 4, 2023 01:55:59	tricky-85252.exe	APPSVR-85252	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 2, 2023 04:36:36	puttyX-71796.exe	APPSVR-71796	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 2, 2023 04:36:32	benignmalware-7179...	APPSVR-71796	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 2, 2023 22:26:21	benignmalware-7613...	APPSVR-76134	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 3, 2023 00:45:18	straypuppy-76134.exe	APPSVR-76134	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 3, 2023 00:47:27	puttyX-76134-build9...	APPSVR-76134	Administrator	Quarantined	<input type="button"/> <input type="button"/>
Oct. 3, 2023 00:45:20	tricky-76134.exe	APPSVR-76134	Administrator	Quarantined	<input type="button"/> <input type="button"/>

Quarantined File Details

HOSTNAME	APPSVR-47417
FILE NAMES	\Device\HarddiskVolume1\detonate\tricky-47417.exe
USERNAME	Administrator
SHA 256	e4ab0baec6cb0115d67d5ff23b2556d57b2239e7d2eda9a357998d2e8af0f146
DATE QUARANTINED	Dec. 27, 2023 15:27:28
DATE UPDATED	Dec. 27, 2023 22:45:33

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ENTERPRISE TRIGGERS

- Every enterprise is unique – threat hunters must know their enterprise in detail
- Leads can be found in dozens (or even hundreds) of locations in a typical enterprise
- Security appliances are often the best starting points
- Dead-box forensics
- Help Desk tickets

pfirewall - Notepad

```

FileVersion: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpwin icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - SEND

```

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ENTERPRISE TRIGGERS



ENTERPRISE TRIGGERS - SECURITY APPLIANCE LOGS

A screenshot of a CrowdStrike security appliance logs interface. A red arrow points from the log output area to the search parameters at the bottom.

```

root@translator-pc: /home/linuxhint
ication: Potentially Bad Traffic [Priority: 2] {TCP} 127.137.226.20:30664 -> 10
.0.0.3:21
03/08-00:06:00.305306 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.216.124.47:30721 -> 10
.0.0.3:21
03/08-00:06:00.306572 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.67.48.199:30740 -> 10.
0.0.3:21
03/08-00:06:00.339271 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.181.171.161:30883 -> 1
0.0.0.3:21
03/08-00:06:00.375746 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.128.45.45:30908 -> 10.
0.0.3:21
03/08-00:06:00.481597 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.123.161.199:31411 -> 1
0.0.0.3:21
03/08-00:06:00.505607 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.124.255.205:31492 -> 1
0.0.0.3:21
03/08-00:06:00.573812 [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classifi
cation: Potentially Bad Traffic] [Priority: 2] {TCP} 127.243.142.70:31720 -> 10
.0.0.3:21

```

Filters: No filter ▾ Reset filter Parameters LocalAddressIP4 31.44.184.33 RemoteAddressIP4 31.44.184.33 aip Shared time -06:00 Chicago Last 30d Live

Parameters: LocalAddressIP4 31.44.184.33 RemoteAddressIP4 31.44.184.33 aip Company

Apply parameters

IP search summary

COPYRIGHT © 2024 CROWDSTRIKE, INC.

ENTERPRISE TRIGGERS - PACKET CAPTURE

A screenshot of a NetworkMiner tool interface showing a packet capture of Cobalt Strike callbacks. A red arrow points from the file list to the packet details pane.

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

capture-encrypted.pcap

No.	Time	Source	Destination	Protocol	Length	Info
4	2019-07-25 17:10:59,811275	10.7.25.101	31.44.184.33	HTTP	421	GET /visit.js HTTP/1.1
6	2019-07-25 17:10:59,995695	31.44.184.33	10.7.25.101	HTTP	219	HTTP/1.1 200 OK
13	2019-07-25 17:11:00,017536	10.7.25.101	31.44.184.33	HTTP	412	POST /submit.php?id=58282 HTTP/1.1
15	2019-07-25 17:11:00,349544	31.44.184.33	10.7.25.101	HTTP	155	HTTP/1.1 200 OK

Frame 13: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits)
 ↓ Ethernet II, Src: Houdlette_3c:7a:ae (00:00:02:1c:47:a8), Dst: Netgear_b6:93:f1 (08:0e:2a:1b:93:f1)
 Internet Protocol Version 4, Src: 10.7.25.101 (10.7.25.101), Dst: 31.44.184.33 (31.44.184.33)
 Transmission Control Protocol, Src Port: 49754, Dst Port: 80, Seq: 1, Ack: 1, Len: 358
 Hypertext Transfer Protocol
 Data (358 bytes):
 ...Data (358 bytes)
 Data (358 bytes)
 Data (358 bytes)
 [Length: 358]

Selected 0 - Showing 50 of 85 in 8 seconds

Malware (14) Clean (0) PUA (0) Unknown (82)

SHA256	R...	Related Actors	Type	File Size	First seen	Label	Family	Actions
aed80eaaf9941a1c0f5a327f928...	-	-	PE32	6.58MB	Jun. 6, 2021 00:00...	Unknown	Unknown	
f65d1b2c63b2c2e0e6364474...	-	-	PE32	10.89MB	Jun. 6, 2021 00:00...	Unknown	Unknown	
062aaef7715e3c799cab632f7fc6c7...	-	-	PE32	3.34MB	Apr. 21, 2021 00:00...	Malware	CheatEngine	
3e92807057813912e7b25ef7fb80...	-	-	PE32	3.34MB	Apr. 20, 2021 00:00...	Unknown	Unknown	
58728368d543e500f7ea7951...	-	-	PE32	40.00MB	Apr. 20, 2021 00:00...	Unknown	Unknown	
0d470532a3f2261a35f435272ae...	-	-	JAVA_ARC	49.56MB	Mar. 15, 2021 00:00...	PUA	Unknown	
5a0ae577a429ab5e52446ecc2...	-	-	PE32	440.00KB	Feb. 14, 2021 00:00...	Malware	Virlock	
6f546d0077302f18bc316a655cc...	-	-	PE32	488.00KB	Feb. 10, 2021 00:00...	Malware	Virlock	
c2e297bf215bc616986be833e65...	-	-	PE64	8.35MB	Jan. 30, 2021 00:00...	Unknown	Unknown	
6b7f9526e0eb2b-d097356515...	-	-	PE32	512.00KB	Dec. 19, 2020 00:00...	Malware	Vigorif	
46908c6320f4e4c3c2535922a94...	-	-	PDF	1.21MB	Nov. 26, 2020 00:00...	Unknown	Unknown	
4d17d743944d5c8250d860f5ea...	-	-	PE32	1.43MB	Sep. 13, 2020 00:00...	Malware	CheatEngine	
2431b0fd76ce0e083a7608e9d9...	-	-	PE32	1.44MB	Sep. 6, 2020 00:00...	Unknown	Unknown	
74bb01c8d3a123d7d50f4269ee8dc...	-	-	PE32	2.58MB	Sep. 5, 2020 00:00...	Malware	CheatEngine	

https://alcon.crowdstrike.com/search-engine/malquery/search

Packet capture of Cobalt Strike callback to the C2

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ENTERPRISE TRIGGERS



ENTERPRISE TRIGGERS - ENDPOINT FORENSICS

Screenshot of CrowdStrike Falcon Endpoint Forensics interface showing a Hash Search results page. A red arrow points from the left side of the interface towards the search results table.

Hash Search

MDS or SHA256: (Space Delimited) File Name: Command Line: Host Name: User Name(s):

4e3b5c5f42afbc601982cd49577 Time range: Since Mar 30, 2021 Submit Hide Filters

PE File Info

File Name	Application	Application Version	File Description	File Version	Vendor	SHA256
b.exe						4e3b5c5f42afbc601982cd49577
c						4e3b5c5f42afbc601982cd49577
c.exe						4e3b5c5f42afbc601982cd49577
conttransware-						4e3b5c5f42afbc601982cd49577

Hash Written History (SHA256-only)

File Name	# of Computers	First Written On	First Written Date	Last Written On	Last Written Date	SHA256
b.exe	31	EMI-WRKSTNY920K	2023-04-06	EMI-WRKSTNY920K	2021-05-17 18:16:37	4e3b5c5f42afbc601982cd49577
c	66	EMI-WRKSTNY920K	2023-04-06	EMI-WRKSTNY920K	2021-05-17 19:34:35	4e3b5c5f42afbc601982cd49577
c.exe	17	EMI-WRKSTNY920K	2023-04-06	EMI-WRKSTNY920K	2021-05-17 19:34:35	4e3b5c5f42afbc601982cd49577

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ENTERPRISE TRIGGERS - HELP DESK TICKETS

HELP DESK TICKET

Name:	Jeanne Ferrer
Workstation:	EMI-WRKSTNY920K
Time/Date:	534pm – 13 Oct 2024
Issue:	User clicked on a link in an email without thinking about it and now system is unresponsive and fan is loud.
Actions:	Referred to IR/TH team.

Auto (Event List) All Queries +00:00 UTC

1 ComputerName="EMI-WRKSTNY920K"

Showing fields from 200 events Fetch more

Filter fields

Columns	#	%	...
@timestamp	200	100%	...

Fields ↓

Fields	#	%	...
#data_source_group	1	100%	+
#data_source_name	1	100%	+
#error	1	100%	+
#repo	1	100%	+
#type	1	100%	+
@error	1	100%	+
@error_msg	200	100%	+
@error_msg[0]	200	100%	+
@error_msg[1]	1	100%	+
@event_parsed	1	100%	+
@id	200	100%	+

Results

Timestamp	Raw String
2023-10-13 21:24:00.000	#event_simpleName: EndOfProcess #repo: base_sensor #type: falcon-raw-data @id: sGWS3qtGFB5q6igAJkocsP6_12_245_... @ingestimestamp: 1697232244869 @rawstring: {'ComputerName': 'EMI-WRKST...'}

COPYRIGHT © 2024 CROWDSTRIKE, INC.

NEWS TRIGGERS

News articles on cybersecurity issues, CVE announcements, and cyber threat intelligence reports are often the starting point for specific hunts.

CROWDSTRIKE

NEWS ARTICLE EXAMPLE

Russian Hackers Are Trying to Brute-Force Hundreds of Networks

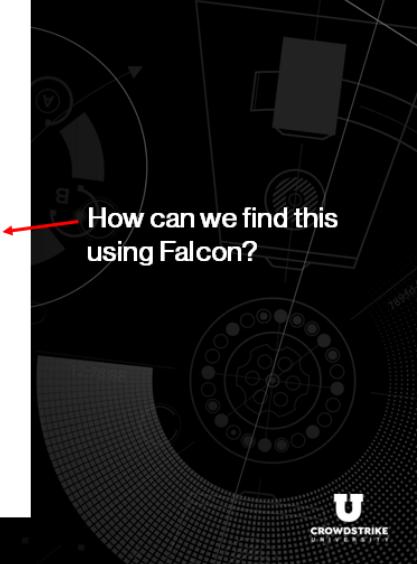
While SolarWinds rightly drew attention earlier this year, Moscow's Fancy Bear group has been on a password-guessing spree this whole time.

THE DISCOVERY of Russia's devastating SolarWinds spy campaign put the spotlight on the sophisticated supply chain hijacking techniques of Moscow's foreign intelligence hackers. But it's now apparent that, throughout that SolarWinds spying and its fallout, another group of Kremlin hackers has kept up their usual daily grind, using basic but often effective techniques to pry open practically any vulnerable network they could find across the US and the global internet.

On Thursday the NSA, the FBI, the DHS's Cybersecurity and Infrastructure Security Agency, and the UK's National Cybersecurity Centre issued a joint advisory warning of hundreds of attempted brute-force hacker intrusions around the world, all carried out by Unit 26165 of Russia's GRU military intelligence agency, also widely known as Fancy Bear or APT28. The hacking campaign has targeted a broad swath of organizations, including government and military agencies, defense contractors, political parties and consultancies, logistics companies, energy firms, universities, law firms, and media companies. In other words, practically every sector of interest on the internet.

The hacking campaign has used relatively basic techniques against those targets, guessing usernames and passwords en masse to gain initial access. But cybersecurity agencies warn that the Fancy Bear campaign has nonetheless successfully breached multiple entities and exfiltrated emails from them—and that it's not over. "This lengthy brute force campaign to collect and exfiltrate data, access credentials and more, is likely ongoing, on a global scale," the NSA's director of cybersecurity Rob Joyce wrote in a statement accompanying the advisory.

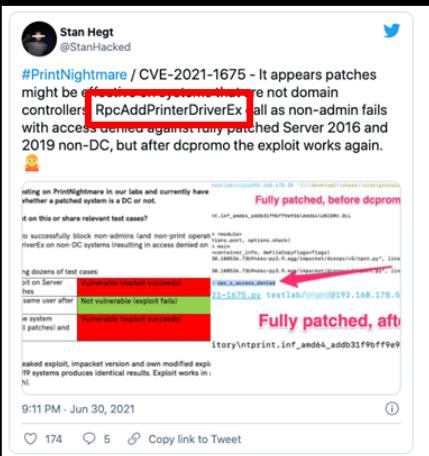
How can we find this using Falcon?



COPYRIGHT © 2024 CROWDSTRIKE, INC.

CROWDSTRIKE

SOCIAL MEDIA EXAMPLE



Stan Hegel (@StanHacked) 

#PrintNightmare / CVE-2021-1675 - It appears patches might be fully deployed on systems that are not domain controllers. RpcAddPrinterDriverEx, as well as non-admin fails with access denied against fully patched Server 2016 and 2019 non-DC, but after dcpromo the exploit works again.

Fully patched, before dcprom
Fully patched, after dcprom

9:11 PM · Jun 30, 2021  174  5  Copy link to Tweet

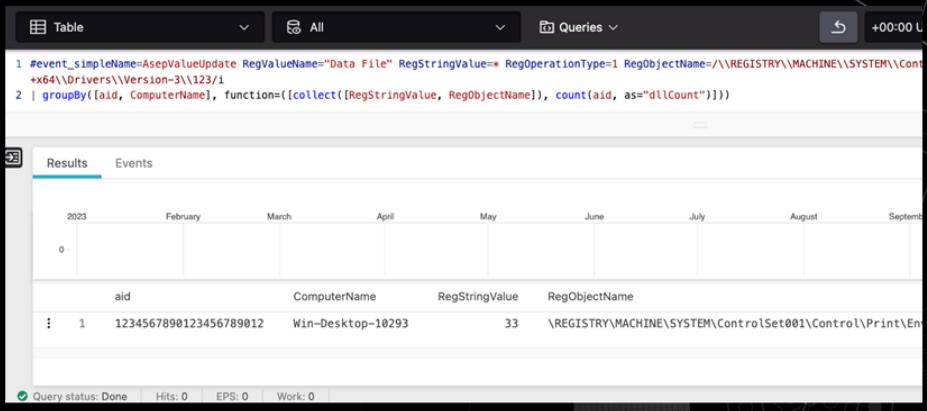


Table All Queries +0:00 U

```
1 #event_simpleName=AsepValueUpdate RegValueName="Data File" RegStringValue== RegOperationType=1 RegObjectName=/\REGISTRY\_MACHINE\SYSTEM\ControlSet001\Control\Print\En
+64\Drivers\Version-3\123/1
2 | groupBy([aid, ComputerName], function=[collect([RegStringValue, RegObjectName]), count(aid, as="d\Count")])
```

Results Events

aid	ComputerName	RegStringValue	RegObjectName
1	Win-Desktop-10293	33	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Print\En

Query status: Done Hits: 0 EPS: 0 Work: 0

COPYRIGHT © 2024 CROWDSTRIKE, INC.

NEWS TRIGGERS

CROWDSTRIKE

CVE EXAMPLE

[Printer-Friendly View](#)

CVE-ID	CVE-2021-3613 Learn more at National Vulnerability Database (NVD)
<ul style="list-style-type: none"> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information 	
Description	
<p>OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe).</p>	
References	
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> • MISC:https://openvpn.net/vpn-server-resources/openvpn-connect-for-windows-change-log/ • URL:https://openvpn.net/vpn-server-resources/openvpn-connect-for-windows-change-log/ 	
Assigning CNA	
OpenVPN Inc.	
Date Record Created	
20210622 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.	
Phase (Legacy)	
Assigned (20210622)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
<p>This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.</p> <p>SEARCH CVE USING KEYWORD: <input type="text"/> <input type="button" value="Submit"/></p> <p>You can also search by reference using the CVE Reference Maps.</p> <p>For More Information: CVE Request Web Form (select "Other" from dropdown)</p>	

COPYRIGHT © 2024 CROWDSTRIKE, INC.

 CROWDSTRIKE UNIVERSITY

How can we find this using Falcon?

CROWDSTRIKE

CYBER INTELLIGENCE EXAMPLE

Alert

WIZARD SPIDER Adds SMB Port Scanning in New Version of Conti Ransomware

CSA-201317 October 13, 2020 14:10:41

CrowdStrike Intelligence has identified notable changes in the latest variants of WIZARD SPIDER's Conti ransomware. WIZARD SPIDER's development and deployment of Conti is still ongoing, even with the recent return of Ryuk ransomware (CSA-20205). The simultaneous operation of both ransomware families in BGH campaigns suggests WIZARD SPIDER may have multiple sub-groups within their organization, each responsible for the development and deployment of their ransomware.

The following modifications to Conti have been observed since the publication of CSIT-20129 and CSA-201103:

- The encrypted file extension is unique for each victim and is typically five seemingly random characters, such as .DKVJ1, .JLMK9, or .TUWUQ.
- Ransom note file names are changed regularly and no longer identify the ransomware by name, e.g., README.txt or R3ADM3.txt.
- Scanning the local network to identify hosts with the TCP port 445 (SMB) open.
- The command-line arguments used to deploy the ransomware were changed to support additional functionality.
- Process termination functionality was reintroduced.
- Additional obfuscation of Windows API calls by resolving imported function addresses from precomputed MurMurHash² hash values during execution.
- Removal of the PE resource section; all configuration values are now stored within the executable's .data section.

How can we find this using Falcon?

PIVOTS

CROWDSTRIKE

IDENTIFY THE TRIGGER AND PIVOT

The screenshot shows a detailed analysis of a process named EXCEL.EXE. A green circle highlights the 'Run period' section, labeled 'Trigger'. A red circle highlights the 'User' section, labeled 'Pivot'. A red arrow points from the 'Pivot' section to a machine learning alert below, which also contains the command line "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\ygritte\AppData\Local\Temp\2\7z006FB6A4\KnightsWatch_Salaries.xls".

Trigger: EXCEL.EXE
Run period: Oct. 23, 2023 16:08:17

Pivot: User: CSULABS\ygritte

Context: Oct. 23, 2023 16:09:21

Machine Learning via Sensor-based ML

Description: A file written to the file system meets the on-sensor machine learning high confidence threshold for malicious files. Detection is based on a high degree of entropy, packing, anti-malware evasion, or other similarity to known malware.

Triggering indicator: Command line
"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\ygritte\AppData\Local\Temp\2\7z006FB6A4\KnightsWatch_Salaries.xls"

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

IDENTIFY THE TRIGGER AND PIVOT

The screenshot shows a network graph with various processes like explorer.exe, cmd.exe, and notePad.exe. A green circle highlights the 'cmd.exe' node, labeled 'Trigger'. A red circle highlights the 'CSULABS\jsnow' node, labeled 'Pivot'. A red arrow points from the 'Pivot' node to a detailed view of the PING.EXE process, which shows a command line "ping -t contagioudump.blogspot.com".

Trigger: cmd.exe
...Contagio.bat*

Pivot: CSULABS\jsnow

Context: PING.EXE
...mp.blogspot.com

PING.EXE

- Process: PING.EXE
- Execution details: Host name: CASTLEBLACK, Command line: ping -t contagioudump.blogspot.com, File path: \Device\HarddiskVolume1\Windows\System32\PING.EXE, Executable SHA256: 741ad992403c78a8a7dbd97c74fda06594a24 7e9e2fa05a40bb6945403a90056
- Actions: Actions ▾

COPYRIGHT © 2024 CROWDSTRIKE, INC.



THREAT SOURCES

Threat Sources	Description
External Actors	Ping sweeps RDP password guessing
Insider Threats	File share access attempts Unauthorized use of removable media Clicking of links in emails Download attachments from emails
Supply Chain	Lateral movement originating from inside Privilege escalation Malware deployment from inside Command and control from specified device Odd/new outbound IP connections after an update

NTEL 101

CROWDSTRIKE

THREAT DATA AND THREAT INTELLIGENCE

TACTICAL THREAT INTEL

Current adversarial actions in the form of detections & incidents and real-time, actionable threat intelligence. Generally, the main source of threat hunting leads.

OPERATIONAL THREAT INTEL

Understanding relatively-near-term historic data and predicting what may happen in the near future (days/weeks). Helps answer "what's next?"

STRATEGIC THREAT INTEL

Communicating malicious activity intelligence to operations and security teams so they can respond to the incident and mitigate threats

INTEL 101

Intel resource in Falcon	Description
Counter Adversary Operations > Intelligence Reports & Feeds	<ul style="list-style-type: none"> Periodic reports on adversary activities, as well as frequently updated feeds of CEF, NetWitness, Snort/Suricata, and YARA rules
Actors	<ul style="list-style-type: none"> Go to Threat intelligence > Research > Actors to find actor profiles and the intelligence CrowdStrike has gathered for each of them
Counter Adversary Operations > Indicators	<ul style="list-style-type: none"> The Indicators page enables you to query the database of CrowdStrike Intelligence indicators of compromise (IOCs)
Falcon Sandbox	<ul style="list-style-type: none"> Simplifies analysis of files and URLs that are suspicious or malicious into one automated workflow Rapid access to associated indicators of compromise (file hashes, domains, and IP addresses) that you can use to fine tune your organization's security infrastructure Provides report analyzing suspicious and malicious files and URLs to help validate whether a file is dangerous
Falcon Malquery	<ul style="list-style-type: none"> Falcon MalQuery also provides rich context describing malware This includes IOCs, such as hashes, a verdict whether the file is malware, the malware family, and if CrowdStrike has attributed the threat to an actor, links to the actor profile
Falcon Intelligence Recon	<ul style="list-style-type: none"> Counter Adversary Operations > External monitoring > Recon Falcon Intelligence Recon uncovers if adversaries are targeting your organization and whether any of your data is being mentioned, sold, or impersonated on the dark web, social media, forums, and other services
Global Search	<ul style="list-style-type: none"> The global search is available in every page of the Falcon platform

3RD PARTY INTEL

Intelligence Reach

- Your intelligence team isn't the only part of the company collecting intelligence.
- Critical to compare methods, timing, sources, and information.
- Intel Reach is the best way to VALIDATE intelligence your team has collected.

CROWDSTRIKE

COLLABORATION EXAMPLES



InfraGard – FBI partnership with private sector; enacted to share information; 4/5 Fortune 500 companies have a rep



NCFTA – Pittsburgh-based non-profit for “identifying, mitigating, and neutralizing cyber crime threats globally.”



Interpol – 192-member police organization; IGCI (Singapore) research & development between LE and private sector



NCIJTF (CyWatch) – 20+ LE/ID/DoD members; coordinates, integrates, and shares information to support cyber crime investigations



Cyber Threat Alliance – members submit data, scored and totaled to keep in good standing; can extract other user's data; uses STIX



CISA – Cybersecurity & Infrastructure Security Agency has the Cyber Information Sharing and Collaboration Platform (CISCP); unclassified information exchange through trusted public-private partnerships

2021 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

RESOLUTION

CROWDSTRIKE

RESOLUTION



As we work a threat hunt, we provide resolution at multiple layers:



Proving/Disproving individual hypotheses as issues are identified



Operationalizing intelligence to construct an on-going narrative



Formalizing output for others at the end

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY

RESOLUTION PRO TIP

TIPS

- Standardize note taking and documentation
- Notes may need to be shared internally, with LE, with lawyers, with insurance, etc

Threat Hunting Notes

Name	Ryan F
Date	2020-05-01
Hunting Topic / Objective	Threat hunt based on MITRE ATT&CK's APT31 evaluation
Timeframe	Last 7 days
Toolsets Used	CrowdStrike Falcon and SIEM PaloAlto logs

1. Search of Falcon Events for rundll32 utilization with Temp file paths.
 - a. Query: event_simpleName=ProcessRollup2 FileName=rundll32.exe "Temp"
 - b. Added filter NOT "ccm"
2. Further investigated the following data:
 - a. Systemname = ABC123 CommandLine=rundll32.exe C:\Windows\Temp\xi32.dll,start

THREAT HUNT MATURITY ASSESSMENT

5

- Some threat hunting automation
- Cyber Threat Intelligence is used to scope threat hunting

4

- Scheduled threat hunting is routinely conducted
- Cyber Threat Intelligence is used for operationalization
- APT metrics are tracked

3

- Threat hunt hypotheses are informed by threat intelligence
- Clearly defined transition from threat hunting to incident handling

2

- Threat hunting is performed ad hoc during an incident
- IOC understanding derived from ad hoc OSINT collection

1

- Organization has minimal understanding or use of threat hunting



THREAT HUNT MATURITY ASSESSMENT



Gold Standard

- Threat hunters dedicated to threat hunting
- Daily, automated threat hunting with routine ad hoc assistance
- Threat hunt findings support fine tuning of other cyber security initiatives
- Detailed metrics kept on successes and failures
- Cyber Threat Intelligence effectively used to guide hypotheses creation
- CTI supports hunting which then supports CTI
- Threat hunt findings incorporated into CTI products
- Routine reporting disseminated to key stakeholders (successes, failures, metrics, intel, etc)

CROWDSTRIKE S.E.A.R.C.H.

CROWDSTRIKE

S.E.A.R.C.H.



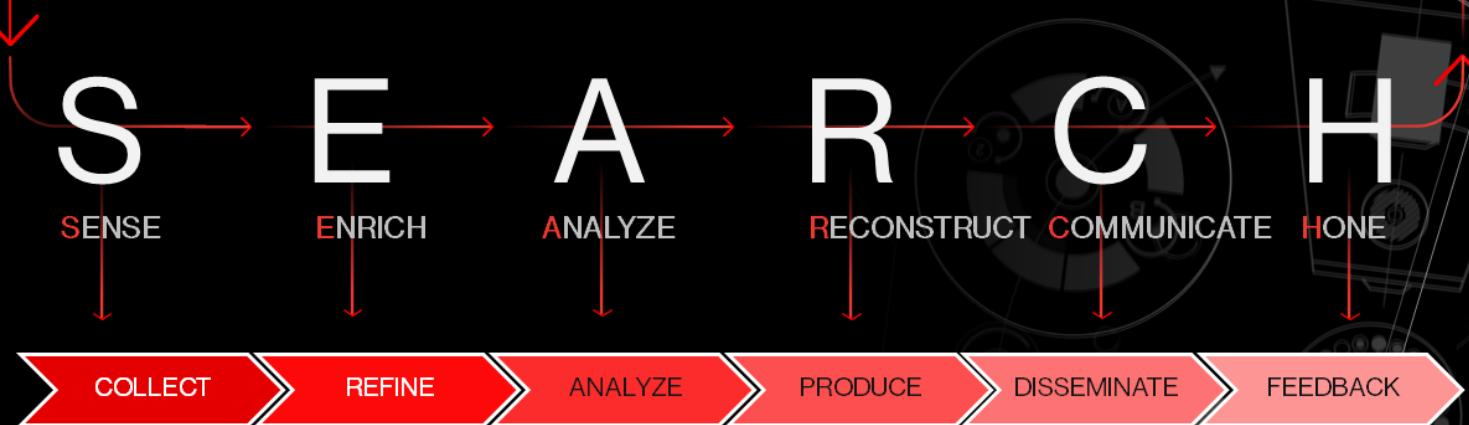
- CrowdStrike Falcon OverWatch team's proven hunt methodology
- Precise balance of people, processes, and technology
- The OverWatch team performs at a world-class level because of this framework
- We can't completely rebuild S.E.A.R.C.H. for our own use – but we can take away some key ideas, tools, and processes

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

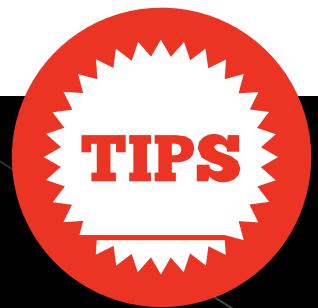
OVERWATCH SEARCH THREAT HUNTING METHODOLOGY



COPYRIGHT © 2024 CROWDSTRIKE, INC.



S.E.A.R.C.H. TIPS



CROWDSTRIKE

HOW TO COLLECT (SENSE) BETTER

Ensure all endpoints have a Falcon agent installed

Endpoints should be named smartly – be able to find an endpoint quickly

Place endpoints in appropriate groups

Create appropriate policies for the groups

Create exclusions to reduce false positives

Ensure sensor update policies are set correctly

COPYRIGHT © 2024 CROWDSTRIKE, INC.



STARTING POINTS

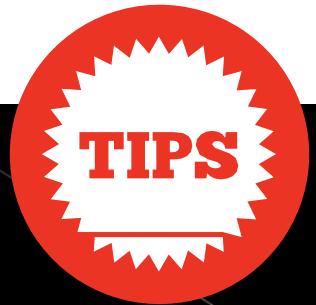
Time	ComputerName	UserName	ParentProcessId	TargetProcessId	RawProcessId	Score	Exec	Dwld	Encode
2023-10-31 18:16:04	thematrix	Administrator	21711268768	21712475174	1016	2	0	0	0
2023-10-31 18:14:33	thematrix	morpheus	21652053992	21654635160	2228	2	0	0	0
2023-10-31 17:44:26	thematrix	thematrix\$	17368246597	17410287733	2156	0	0	0	0
2023-10-31 17:44:24	thematrix	thematrix\$	17368246597	17408087189	6520	0	0	0	0

COPYRIGHT © 2024 CROWDSTRIKE, INC.



S.E.A.R.C.H. TIPS

CROWDSTRIKE



HOW TO REFINE (ENRICH) BETTER

Most of the enrichment is already done for you by the ThreatGraph

Pay attention to newly released threat intelligence reporting

Use the Actor Intelligence and Indicators portals to the greatest extent possible

Learn to use ALL of the Investigate pages

Practice your OSINT skills – use Falcon OSINT when you can

Build your Event Search query skills, Learn YARA, understand Sandbox reports – use Falcon proficiently

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ENRICH

- OverWatch identifies over 23 million hunting leads per day
- CONTEXT is EVERYTHING – must prioritize!
- ThreatGraph provides context to the events, building visualization between data points
- Hunting relies as much on threat intelligence as it does the raw data
- This is the biggest, most important part of the entire process!

S.E.A.R.C.H. TIPS



ENRICHMENT

Now what?

- Username?
 - Automated or hands-on?
Parent process?
 - Other endpoints with
C:/Temp?
 - Timeline this machine?

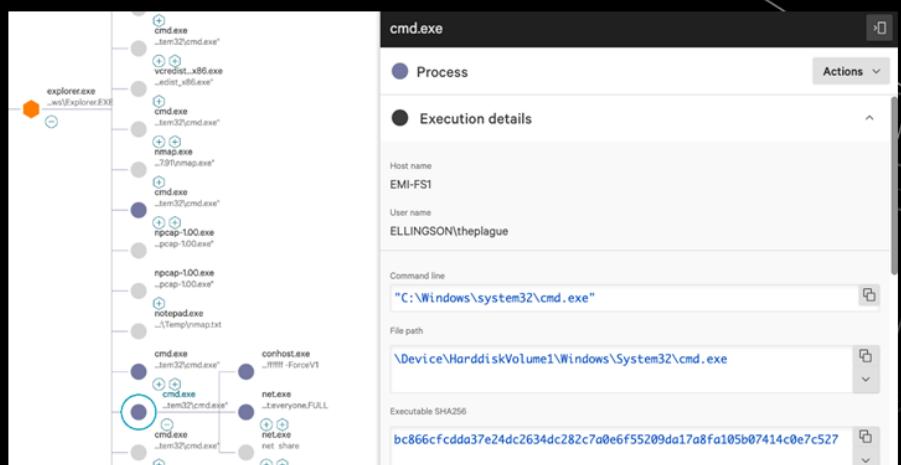
...so many ways to pivot!

COPYRIGHT © 2024 CROWDSTRIKE, INC.



PIVOTING

- No ONE right way to pivot
 - Experience and intuition
 - Remember your threat hunt goals
 - Find impacted hosts
 - Actor attribution



- Inspect
- Show in context
- Pivot - Host Search
- Show +/- 10-minute window of events
- Show Associated Event Data (from TargetProcessId)
- View Process Explorer for the responsible process**
- Show +/- 10-minute window of events (Mac)
- Show Network Connection Data
- Show Process DNS Information
- Show other computers accessed by this username

COPYRIGHT © 2024 CROWDSTRIKE, INC.



S.E.A.R.C.H. TIPS

CROWDSTRIKE

HOW TO ANALYZE BETTER

Learn structured analytics
(attend CST 346)

As a solo analyst – develop
your own methodologies and
stick to them

As a team – learn each
other's methodologies and
use them to refine your own

Study the particulars of
various tactics and
techniques – MITRE
ATT&CK is perfectly setup
for this

Develop capabilities to
merge automated analysis
with human-derived analysis

Review findings a
month/year later – what did
you get right and what did
you get wrong?

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ANALYZE

- Statistical models are great, but human analysis is required too
- Blending advanced machine learning with human intuition provides the best analysis
- Use of structured analytics greatly assists deep understanding

COPYRIGHT © 2024 CROWDSTRIKE, INC.



S.E.A.R.C.H. TIPS

CROWDSTRIKE

TIPS

HOW TO PRODUCE (RECONSTRUCT) BETTER

Have company-approved report formats and stick to them

Practice writing technical reports – develop your ability to tell a story concisely

Understand how to take screen shots from Falcon – it has already created the visuals for you

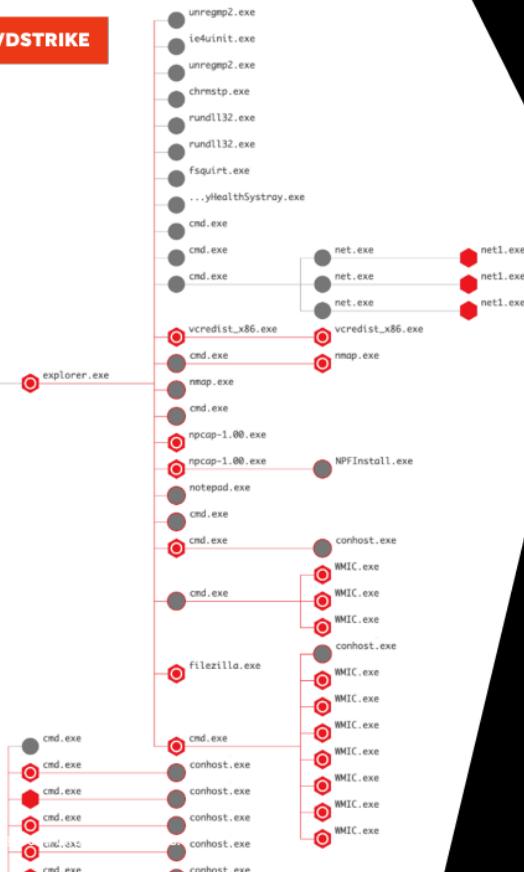
Include temporal analysis as often as possible

Peer review EVERYTHING!

Appoint someone to be the last “eyes” on the report – consumers shouldn’t be surprised by changes in language and format

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY



RECONSTRUCT

- Tying data together is critical to understanding the threat
- Automated ThreatGraph querying provides useful visualization of events
- Cloud performance built to withstand multiple simultaneous, sophisticated queries
- Temporal analytic views inherent in many Insight and Investigate pages

U
CROWDSTRIKE
UNIVERSITY

S.E.A.R.C.H. TIPS

CROWDSTRIKE



HOW TO PRODUCE (COMMUNICATE) BETTER

Know your consumers – who are they and what information do they NEED?

Understand the level of detail each of your customers need

Develop hand-off procedures within the team for large/important hunts and incidents

Keep metrics – they tell a story that managers understand

Have reporting timing policies – at what point do you inform IR? Inform legal? Report to execs?

Decide what stays internal and what should be shared with the community

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

EMI-FS2ENG at 20

Critical

0/10

Description

Objectives in this incident: Follow Through, Recovery

Techniques: Data Encrypted for Impact, Sensor Management, Instrumentation, Remote Services.

Involved hosts and end users: EMI-FS2ENG, Test

COMMUNICATE

- OverWatch analysis is incorporated into many parts of Falcon
- We won't fully benefit from all of OverWatch's insight without an OverWatch subscription
- But, Falcon includes other ways that our team members can share and communicate in the portal

EMI-FS2ENG		
Host	Assets	Vulnerabilities
OS	IP address	
Windows Server 2019	100.26	



S.E.A.R.C.H. TIPS

CROWDSTRIKE



HOW TO THREAT HUNT BETTER

Study your own team's reporting – actually use your lessons learned

Study open source reporting – use others' lessons learned

Include up-to-date threat intelligence – this is a moving target

Continually refine your processes – WRITE IT DOWN.

Consider outside consulting to evaluate your team

If you manage – get your team to cons and training

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY

CROWDSTRIKE

HONE

- Continuous improvement of tools and processes
- Threat intelligence must be:
 - Up-to-date
 - Deeply analytic
 - Contextual
 - Accessible
- Training is key:
 - Table-top exercises
 - CTF events
 - Emerging forensic techniques

COPYRIGHT © 2024 CROWDSTRIKE, INC.

U
CROWDSTRIKE
UNIVERSITY



HUNTING METHODS



HUNTING METHODS

SEARCHING

Pattern matching based on hypothesis

STACKING (FREQUENCY ANALYSIS)

Outliers based on counting of occurrences

TIME-BASED

Hunting based on timetriggers

MACHINE LEARNING

Using data science or ML to identify leads

VISUALIZATION

Visual representation to identify leads

COPYRIGHT © 2024 CROWDSTRIKE, INC.



THREAT HUNTING METHODOLOGIES TIPS

TIPS

There are many types of hunting – automated hunts often involve machine learning; manual hunts usually start with a hypothesis and use searches of data stores.

Good utilization of the hypotheses cycle is critical; pattern-matching and stacking queries are essential for proving/disproving the hypotheses.

Organizations with a mature hunting capability use routine procedures before, during, and after the hunt; have an SOP for your hunts.

Problem statements are opportunities for hypotheses development; we create concise problem statements to frame the issue for better understanding.

HUNTING METHODS

Hypotheses Generation



HYPOTHESES “MAKING AN EDUCATED GUESS”



COPYRIGHT © 2024 CROWDSTRIKE, INC.



- Must be TESTABLE
 - To be testable, must include at least one variable
 - Hunters must know where the data is and have the ability to access it
- Must clearly state an end result or product that is reachable
- Often starts with the identification of a problem
 - Creation of a **PROBLEM STATEMENT** helps us narrow down the exact answer we need

HUNTING METHODS

Frequency Analysis



FREQUENCY ANALYSIS - CQL EXAMPLE

```
#event_simpleName=ProcessRollup
| groupBy(CommandLine)
```

CommandLine	_count ↑
C:\Windows\system32\DllHost.exe /Processid:{F9717507-6651-4EDB-BFF7-AE615179BCCF}	44
taskhostw.exe	43
"C:\Windows\system32\backgroundTaskHost.exe" – ServerName:App.AppXmtcan0h2tbfy7k9kn8hbx6dmzz1zh0.mca	41
/0000000c	40
C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}	34
"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler	29
C:\Windows\system32\svchost.exe -k netsvcs -p -s wuauserv	25
C:\Windows\system32\TSTheme.exe -Embedding	25
C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc	17
C:\Windows\servicing\TrustedInstaller.exe	16
C:\Windows\System32\svchost.exe -k netsvcs -p -s NetSetupSvc	16
"C:\Windows\system32\SearchFilterHost.exe" 0 680 684 692 8192 688	16
taskhostw.exe KEYROAMING	15
C:\Windows\system32\compttelrunner.exe -m:aeinv.dll -f:UpdateSoftwareInventoryW	15
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc	12

1 2 3 4 5 6 7 ... 18

HUNTING METHODS

Frequency Analysis

CROWDSTRIKE

FREQUENCY ANALYSIS - CQL EXAMPLE

```
groupBy([ComputerName, FileName], function=collect([DomainName, MD5HashData, SHA256HashData], limit=100))
```

ComputerName	FileName
SE-SWH-RDP	taskhostw.exe
FC-JBE-RDP	svchost.exe
SE-TMA-RDP	GoogleUpdate.exe
SE-SLT-RDP	taskhostw.exe
SE-JBE-WIN10-C0	svchost.exe

DomainName	MD5HashData	SHA256HashData
settings-win.data.microsoft.com	8bd7b88da6bca54df9b595e4d9281beb	de85f29a8bc7219f10a4ac88654c3901abc329d75851
download.windowsupdate.com	4dd18f001ac31d5f48f50f99e4aa1761	2b105fb153b1bcd619b95028612b3a93c60b953eef61
geo.prod.do.dsp.mp.microsoft.com		
login.live.com		
cp601.prod.do.dsp.mp.microsoft.com		
fe2.update.microsoft.com		
fe3.delivery.mp.microsoft.com		
kv601.prod.do.dsp.mp.microsoft.com		
edged1.me.gvt1.com	94c4c8130e96785dd19b70a0fc10881f6	41793f27b823dbc1593df93b3181d0ae08ccbfe16ea1
update.googleapis.com		
clients2.google.com		
settings-win.data.microsoft.com	8bd7b88da6bca54df9b595e4d9281beb	de85f29a8bc7219f10a4ac88654c3901abc329d75851
settings-win.data.microsoft.com	9528a99e77d6196d0d09833146424113	dd191a5b23df92e12a8852291f9fb5ed594b76a28a5i
slscr.update.microsoft.com		
time.windows.com		
login.live.com		
tsfe.trafficshaping.dsp.mp.microsoft.com		
fs.microsoft.com		
fe3.delivery.mp.microsoft.com		

COPYRIGHT © 2024 CROWDSTRIKE, INC.

CROWDSTRIKE

FREQUENCY ANALYSIS - CQL EXAMPLE

Example Search

```
#event_simpleName=NetworkConnectIP4 RemoteAddressIP4!=10.1.0.0/8
RemoteAddressIP4!=127.0.0.1
| join({#event_simpleName=ProcessRollup2}, field=[ContextProcessId],
key=TargetProcessId, include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort, CommandLine])
| sort(_count, order=asc, limit=20000)
```

COPYRIGHT © 2024 CROWDSTRIKE, INC.

HUNTING METHODS

Temporal Analysis



TEMPORAL ANALYSIS

- Examination of events in a chronological order
- Modeling of a variable's behavior in a data set over time
- Statistical analysis differentiation over time intervals

Process executions 601 items

Filename Command line Excluded filename(s) Excluded command line(s) Exclude common processes Apply

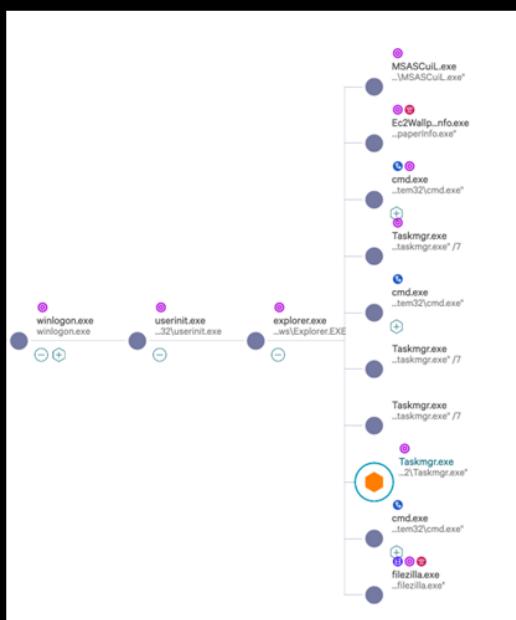
View in Advanced event search Export

Time (UTC)	Computer...	Username	Filename	PID	Process ID	Command...	MDS	Parent file...	Par...	Parent pr...	Parent co...
2024-01-04T19:58:48Z	EMI-WRKSTN...	EMI-WRKSTN...	SearchProtocolHos...	5264	4626275776	"C:\Windows\...	ae2b338f1629...	SearchIndexe...	4348	20651518	C:\Windows\s...
2024-01-04T19:58:48Z	EMI-WRKSTN...	EMI-WRKSTN...	SearchFilterHost.exe	928	4627266771	"C:\Windows\...	4281c1c543de...	SearchIndexe...	4348	20651518	C:\Windows\s...
2024-01-04T19:50:49Z	EMI-WRKSTN...	EMI-WRKSTN...	CSFalconService.exe	7028	4624597880	"C:\Program F...	0a19e2bbfffa8...	CSFalconServ...	8468	4297332924	*C:\Program F...
2024-01-04T19:47:43Z	EMI-WRKSTN...	michael_rivas	dllhost.exe	4028	4623582852	C:\Windows\s...	2d29c0afcc8...	svchost.exe	940	12002012	C:\Windows\s...
2024-01-04T19:47:38Z	EMI-WRKSTN...	michael_rivas	backgroundTaskH...	7252	4622507671	"C:\Windows\...	00bdae44f0...	svchost.exe	940	12002012	C:\Windows\s...
2024-01-04T19:47:13Z	EMI-WRKSTN...	michael_rivas	dllhost.exe	10552	4621513393	C:\Windows\s...	2d29c0afcc8...	svchost.exe	940	12002012	C:\Windows\s...

COPYRIGHT © 2024 CROWDSTRIKE, INC.



TEMPORAL ANALYSIS - TIME CHART



Event t...	Proces...	Command line	Status	Duration
Jan. 4, 2024 13:57:45	Proces...	...gr.exe ...:\Windows\System32\Taskmgr.exe*	Not ru...	1m 14s
Jan. 4, 2024 13:57:45	Event t...	Image file name	Target file name	SHA256
Jan. 4, 2024 13:57:56	DLL / e2\Windows\System32\version.dll	--	--
Jan. 4, 2024 13:57:56	DLL / e2\Windows\System32\dbgcore.dll	--	--
Jan. 4, 2024 13:57:56	DLL / e2\Windows\System32\dbghelp.dll	--	--
Jan. 4, 2024 13:57:56	DLL / me2\Windows\System32\verifier.dll	--	--
Jan. 4, 2024 13:57:56	DLL /lume2\Windows\System32\psapi.dll	--	--

COPYRIGHT © 2024 CROWDSTRIKE, INC.



HUNTING METHODS

Temporal Analysis



TEMPORAL ANALYSIS - TIME CHART

```
timechart(function=[avg ConfigStateHash, as=avgConfigStateHash], avg ConnectTime, as=avgConnectTime)]
```



COPYRIGHT © 2024 CROWDSTRIKE, INC.

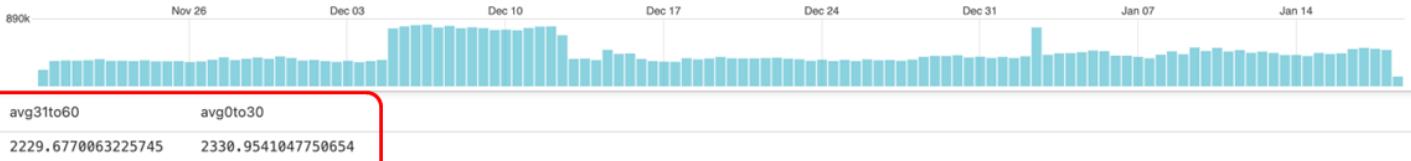


TEMPORAL ANALYSIS - INTERVALS

```
// Run this query over the last 60 days.
#event_simpleName = ProcessRollup2
| case {
  test(@timestamp < (start()+(30*24*60*60*1000))) | eventSize(as=eventSize31to60);
  * | eventSize(as=eventSize0to30);
}
| stats([avg(as=avg31to60, field=eventSize31to60), avg(as=avg0to30, field=eventSize0to30)])
```

Results Events

Save ▾



COPYRIGHT © 2024 CROWDSTRIKE, INC.



HUNTING METHODS

Machine Learning

CROWDSTRIKE

UNDERSTANDING THE THREAT GRAPH

		Actual Values	
		Positive	Negative
Predicted Values	Positive	True Positive (TP)	False Positive (FP)
	Negative	False Negative (FN)	True Negative (TN)

- **True Positive:** The model correctly predicted a file was malicious
- **True Negative:** The model correctly predicted that a file was not malicious
- **False Positive:** The model incorrectly predicted that a file was malicious (and it wasn't)
- **False Negative:** The model incorrectly predicted that a file wasn't malicious (and it was)

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

MACHINE LEARNING IN FALCON

```
#repo: detections
#type: falcon-raw-data
@id: ikILLPL2zEx5DPxRcMIC0fRT_26_64_1704403577
```

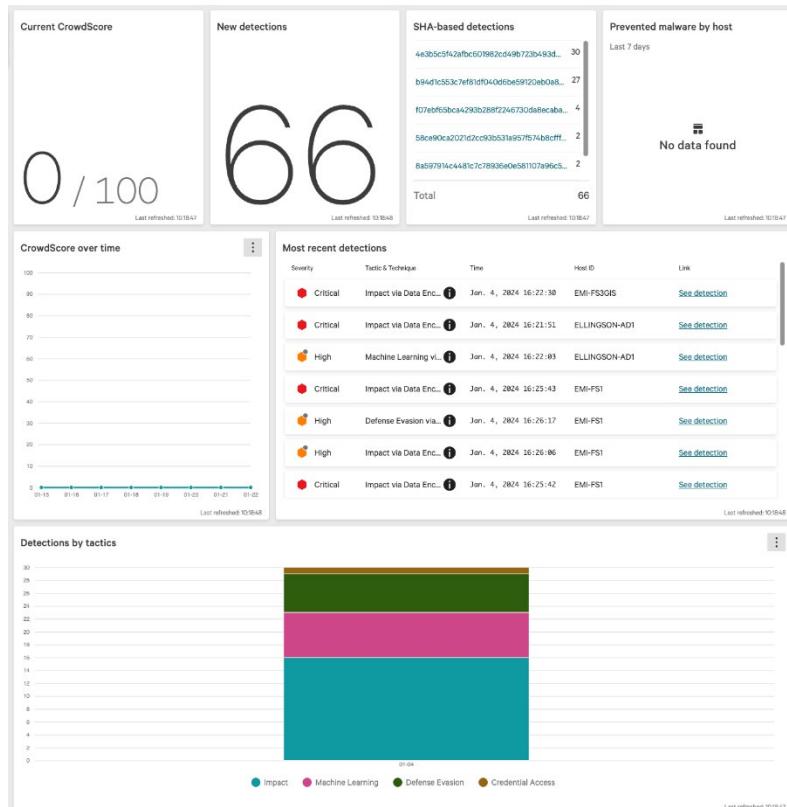
```
PatternDispositionValue: 33024
PatternId: 10378
ProcessEndTime: 0
ProcessId: 4493377033
ProcessStartTime: 1704403540
SensorId: 0e05b927e42346848b12caa677140742
Severity: 4
SeverityName: High
SHA1String: 0000000000000000000000000000000000000000000000000000000000000000
SHA256String: 4e3b5c5f42afbc601982cd49b723b493da0928d753548c7ed5e25927a597835b
Tactic: Defense Evasion
tactic: Defense Evasion
Technique: Disable or Modify Tools
technique: Disable or Modify Tools
timestamp: 2024-01-04T21:26:17Z
UserName: theplague
UTCTimestamp: 1704403577000
```

COPYRIGHT © 2024 CROWDSTRIKE, INC.



VISUALIZATIONS

Falcon is mainly built on visualizations of ThreatGraph data



Visual aids in Falcon

Iconography – Use of Icons to highlight key items of the process node activity

Colorization – Different colors used for things such as detection criticality

Proximal context - showing the inter-relationships between the different nodes in the detection tree, such as Parent/Child and Sibling relationships

Aggregation - bringing it all together in a common viewpoint, i.e. the process Tree views

Total detections count	Rooted on	Hostname	Last detection	Critical	High	Medium	Low	Informational
5 detections	c.exe	EMI-FS1	Jan. 4, 2024 16:26:17	2	3	0	0	0
3 detections	c.exe	EMI-FS4CONT	Jan. 4, 2024 16:23:02	0	3	0	0	0
5 detections	c.exe	EMI-FS3GIS	Jan. 4, 2024 16:22:59	2	3	0	0	0
3 detections	c.exe	EMI-FS2ENG	Jan. 4, 2024 16:22:54	0	3	0	0	0
4 detections	c.exe	ELLINGSON-AD1	Jan. 4, 2024 16:22:37	1	3	0	0	0
1 detection	cmd.exe	EMI-FS4CONT	Jan. 4, 2024 16:22:27	1	0	0	0	0
1 detection	vsadmin.exe	EMI-FS4CONT	Jan. 4, 2024 16:22:26	1	0	0	0	0

Falcon reports, dashboards, and other visualizations contain contextual pairings of charts, timelines, matrices, diagrams, lists, and more. This detection view is both a list and a timeline.

Advanced Hunting in EDR Data

TRIAGE – THE IMPORTANCE OF PROCESS TREES

- Critical to understand the process tree:
 - Process relationships
 - Start times, stop times, and duration of processes
- Temporal analysis of process events (Timelining) around a given event

COPYRIGHT © 2024 CROWDSTRIKE, INC.

Process trees with no detections

Connect to Host

Draw Process Explorer

View Process Explorer for the responsible process

Show +/- 10-minute window of events (Mac)

Show Responsible Process Data

Show Network Connection Data

Show Process DNS Information

Show other computers accessed by this username

Event pivots

2024-01-04 16:27:42.000 #event_simpleName: EndOfProcess
 #repo: base_sensor
 #type: falcon-raw-data
 @id: j10vuKgv7L8jbrL1uPCiEv6U_16_166_1
 @ingesttimestamp: 1704403667572
 @rawstring: {"ComputerName":"EMI-WRKSTN929J","ConfigStateHash":"3968429268","Cont0","ContextTimeStamp":"1704403659.798","Cont1","Entitlements":1,"ExitCode":0}

Advanced Hunting in EDR Data

Endpoint Detection & Response Data

Important data retention periods:

- Detections, Incidents, and other visual aids generally available for 90 days
- EDR data is available for your organization's retention agreement – generally 7 or 30 days
- End point/Falcon agent information is available for 45 days
- Build advanced queries to find context
- For advanced threat hunting, it is often best to incrementally piece together your query

Example Search

```
aid=a4c18e8bf47a4003924cf55978533e72 #event_simpleName=NetworkConnectIP4
RemoteIP!=10.1.0.0/16 RemoteIP!=127.0.0.1
| join({#event_simpleName=ProcessRollup2}, field=[ContextProcessId],
key=TargetProcessId, include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort, CommandLine])
```

EDR SEARCHES

Pivoting and Filtering

Example Search

```
aid=a4c18e8bf47a4003924cf55978533e72
#event_simpleName=NetworkConnectIP4
RemoteIP!=10.1.0.0/16 RemoteIP!=127.0.0.1
| join({#event_simpleName=ProcessRollup2},
field=[ContextProcessId], key=TargetProcessId,
include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort,
CommandLine])
```

Threat hunting is largely an exercise of anomaly detection and pivoting

We find something, we pivot our hunt to follow the leads

Reduction in noise or the amount of data to analyze is critical for efficiency

In CQL Event Search, it can come in several forms:

field!=value field!=value)

field!= [value, value, value]

Prebuilt timelines in Advanced event search

Show +/- 10-minute window of processes

Show +/- 10-minute window of events

Show Sibling Processes

Show Associated Event Data (from ContextProcessId)

Show Associated Event Data (from TargetProcessId)

Connect to Host

Draw Process Explorer

View Process Explorer for the responsible process

Show +/- 10-minute window of events (Mac)

Show Responsible Process Data

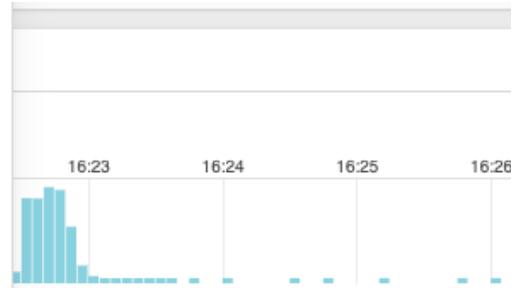
Show Network Connection Data

Show Process DNS Information

Show other computers accessed by this username

2024-01-04 16:28:34.000

ComputerName": "EMI-FS3GIS", "ConHostId": "816", "ConHostProcessId": "1007.3.0017706.1", "ConfigStateHash": "2136042914", "ContextProcessBehaviorBitfield": "2", "ContextProcessStartHashData": "7fd065bac18c5278777ae44908104442098954", "Entitlements": "15", "EventOrigin": "468750", "LocalAddressIP4": "10.1.1.144", "MaxThreadCount": "94", "ProcessStartTime": "1704387096.252", "RawProcessId": "1080", "TargetProcessId": "63204105", "UserName": "LOCAL SERVICE", "UserToken": "b935ff485a87c28b1b452f4ad6", "aip": "100", "event_platform": "Win", "event_simpleName": "EndOfProcessV15", "event_time": "2024-01-04T16:28:34.000Z", "event_type": "Process", "host_ip": "10.1.1.144", "host_name": "EMI-FS3GIS", "host_processor_cores": "4", "host_processor_model": "Intel(R) Core(TM) i5-13400H CPU @ 2.50GHz", "host_processor_threads": "8", "host_ram_size": "16GB", "host_uefi": "UEFI", "host_vendor": "Dell", "host_windows_version": "Windows 11 Pro"}, {"ComputerName": "EMI-FS3GIS", "ConHostId": "816", "ConHostProcessId": "1007.3.0017706.1", "ConfigStateHash": "2136042914", "ContextProcessBehaviorBitfield": "2", "ContextProcessStartHashData": "7fd065bac18c5278777ae44908104442098954", "Entitlements": "15", "EventOrigin": "468750", "LocalAddressIP4": "10.1.1.144", "MaxThreadCount": "94", "ProcessStartTime": "1704387096.252", "RawProcessId": "1080", "TargetProcessId": "63204105", "UserName": "LOCAL SERVICE", "UserToken": "b935ff485a87c28b1b452f4ad6", "aip": "100", "event_platform": "Win", "event_simpleName": "EndOfProcessV15", "event_time": "2024-01-04T16:28:34.000Z", "event_type": "Process", "host_ip": "10.1.1.144", "host_name": "EMI-FS3GIS", "host_processor_cores": "4", "host_processor_model": "Intel(R) Core(TM) i5-13400H CPU @ 2.50GHz", "host_processor_threads": "8", "host_ram_size": "16GB", "host_uefi": "UEFI", "host_vendor": "Dell", "host_windows_version": "Windows 11 Pro"}]



```
, "Entitlements": 15, "EventOrigin": "468750", "LocalAddressIP4": "10.1.1.144", "ProcessBehaviorBitfield": "2", "ProcessStartHashData": "7fd065bac18c5278777ae44908104442098954", "UserName": "LOCAL SERVICE", "UserToken": "b935ff485a87c28b1b452f4ad6", "aip": "100", "event_platform": "Win", "event_simpleName": "EndOfProcessV15", "event_time": "2024-01-04T16:28:34.000Z", "event_type": "Process", "host_ip": "10.1.1.144", "host_name": "EMI-FS3GIS", "host_processor_cores": "4", "host_processor_model": "Intel(R) Core(TM) i5-13400H CPU @ 2.50GHz", "host_processor_threads": "8", "host_ram_size": "16GB", "host_uefi": "UEFI", "host_vendor": "Dell", "host_windows_version": "Windows 11 Pro"}, {"ComputerName": "EMI-FS3GIS", "ConHostId": "816", "ConHostProcessId": "1007.3.0017706.1", "ConfigStateHash": "2136042914", "ContextProcessBehaviorBitfield": "2", "ContextProcessStartHashData": "7fd065bac18c5278777ae44908104442098954", "Entitlements": "15", "EventOrigin": "468750", "LocalAddressIP4": "10.1.1.144", "MaxThreadCount": "94", "ProcessStartTime": "1704387096.252", "RawProcessId": "1080", "TargetProcessId": "63204105", "UserName": "LOCAL SERVICE", "UserToken": "b935ff485a87c28b1b452f4ad6", "aip": "100", "event_platform": "Win", "event_simpleName": "EndOfProcessV15", "event_time": "2024-01-04T16:28:34.000Z", "event_type": "Process", "host_ip": "10.1.1.144", "host_name": "EMI-FS3GIS", "host_processor_cores": "4", "host_processor_model": "Intel(R) Core(TM) i5-13400H CPU @ 2.50GHz", "host_processor_threads": "8", "host_ram_size": "16GB", "host_uefi": "UEFI", "host_vendor": "Dell", "host_windows_version": "Windows 11 Pro"}]
```

EDR SEARCHES

CROWDSTRIKE

PRE-BUILT TIMELINES IN ADVANCED EVENT SEARCH

aid=f3d98bb935ff485a87c28b1b452f4ad6 | newstamp := @timestamp/1000 | querystamp := 1704403711000/1000 | test newstamp > querystamp-600
| test newstamp < querystamp+600 | table([@timestamp, #event_simpleName, ContextProcessId, TargetProcessId, ParentProcessId, ImageFileName, CommandLine, RegObjectName, RegValueName, TargetFileName, RemoteAddressIP4, RPort, LPort], limit=20000)

The screenshot shows the CrowdStrike Falcon Advanced Event Search interface. At the top, there's a search bar with the query: aid=f3d98bb935ff485a87c28b1b452f4ad6 | newstamp := @timestamp/1000 | querystamp := 1704403711000/1000 | test newstamp > querystamp-600 | test newstamp < querystamp+600 | table([@timestamp, #event_simpleName, ContextProcessId, TargetProcessId, ParentProcessId, ImageFileName, CommandLine, RegObjectName, RegValueName, TargetFileName, RemoteAddressIP4, RPort, LPort], limit=20000). Below the search bar is a timeline visualization with red arrows pointing to specific time points. To the right of the timeline is a table titled 'Events' showing 13 rows of event data. On the left, there's a 'Filter fields' sidebar. At the bottom right, there's a logo for CrowdStrike.

HUNTING EDR FOR ENTERPRISE TRIGGERS

Hunt

- Linux sensors Updated
- Mac sensors Updated
- Detection activity Updated
- Detection resolutions Updated
- Indicator activity New
- Command line and ASEP activity Updated
- Executables running from Recycle Bin Updated
- Executables running from temp directories Updated
- Files written to removable media - windows Updated
- Files written to removable media - mac Updated
- Firewall set rules Updated
- Powershell hunt Updated
- Scheduled tasks registered Updated

Auto (Event List)

Showing fields from 13 events Fetch more

Filter fields

Columns	#	%	...
@timestamp	3	100%	...
Fields ↓	#	%	...
#data_source_group	3	100%	+
#data_source_name	1	100%	+
#repo	1	100%	+
#type	1	100%	+
#id	13	100%	+
@ingesttimestamp	3	100%	+
@rawstring	13	100%	+
@sourcetype	1	100%	+
@timestamp.nanos	1	100%	+
@timezone	1	100%	+
assignment_type	2	100%	+
cid	1	100%	+
config_id_stage	1	100%	+
created_by	2	100%	+
created_timestamp	3	100%	+
description	2	100%	+
enabled	1	100%	+
groups	2	100%	+

Recent Saved

Search... Q

falcon/investigate

- admin_dd_helper Event List
- aid_base Table
- aid_master Table
- aid_policy Table
- annotation_data_parse Event List
- appinfo Table
- cid_name Table
- cli_and_asep_activity Table
- exec_running_from_recycle_bin Table
- exec_running_from_temp_dir Table
- failed_login_to_falcon_console Table

Prebuilt queries saved in the UI

INTELLIGENCE MODELS

The Cyber Kill Chain model identifies what the adversaries must complete in order to achieve their objective.

CROWDSTRIKE

LOCKHEED'S SEVEN WAYS TO USE THE CYBER KILL CHAIN®

- 1. Prioritize Sensor Alerts
 - Detections mapped to latter stages of the kill chain should have higher priority
 - Should be automatically associated with other threat info in a threat platform
- 2. Prioritize Escalation
 - Detections of adversary activity that map to certain points in the kill chain should require escalated response – up to executive notification – this is a function of the SOP
- 3. Prioritize Investment
 - Create a two-dimensional graph outlining mitigation tools available to IR, mapped to each stage of the kill chain
- 4. Measure Effectiveness
 - Analysis of mitigated attacks should concentrate on the stage at which the attack was discovered and stopped, then build capability to stop earlier
- 5. Measure Resilience
 - Analyze mitigated attacks to assess if later stages would have caught it, if the stage at which it was actually stopped would have failed
- 6. Measure Analytic Completeness
 - Analyze the entire chain – even if the attack was stopped; understand what the actor would have done
- 7. Identify and Track Campaigns
 - Create a scorecard to provide insight into defensive effectiveness against an actor or across all actors

COPYRIGHT © 2021 CROWDSTRIKE, INC.

How Falcon applies the Cyber Kill Chain

WIZARD SPIDER
Russian Federation, Eastern Europe

All actors Summary Kill chain MITRE ATT&CK Matrix Reports

Details			Actor activity		
Last seen date: Sep 2016	Status: Inactive	Actor type: eCrime	Sandbox reports 0	Endpoint detections 0	Vulnerabilities 2
Last seen date: Nov 2022	Motivator: Criminal	Origin: Russian Federation Eastern Europe			
Target industries:	Cryptocurrency, Academic, Aviation, Extraterritorial Consulting and Professional Services, Industries and Engineering, Oil and Gas, Defense, Manufacture, Hospitality, National Government, Real Estate, Travel, Opportunistic, Logistics, NGO, Entertainment, Utilities, Consumer Goods, Pharmaceutical, Financial Services, Agriculture, Transportation, Legal, Retail, Government, Technology, Automotive, Law Enforcement, Media, Telecommunications, Financial Management & Hedge Funds, Aerospace, Sports Organizations, Healthcare, Insurance, Food and Beverage, Chemicals, Laundry				
Target countries:	Serbia, South Africa, Switzerland, Sweden, Hungary, China, Italy, Canada, Taiwan, Spain, Netherlands, Mexico, Luxembourg, Brunei, Darussalam, United States, Belgium, Bangladesh, Colombia, Germany, Chile, Vietnam, Pakistan, Norway, Nicaragua, Ireland, Indonesia, Turkey, United Kingdom, South Korea, Singapore, New Zealand, Japan, India, Dominican Republic, Saudi Arabia, Germany, Honduras, France, Bahamas, Australia, Austria, Argentina				
Common identifiers:	TatBrikk, Ryuk, FIN7, TrickBot, GOLD				

Kill chain

Services Used

- Cobalt open botnet
- Kellogg open botnet (ZOMBIE SPIDER)
- RIG exploit kit
- CrifP2P open botnet
- Emotet malware distribution service (MALAMAF SPIDER)
- TrickBot malware distribution service (LUKAR SPIDER)

Services Offered

The extent of which tools WIZARD SPIDER provides access to, or how they maintain these relationships, is unknown. However, it is possible that they have worked with trusted criminal operators in TrickBot campaigns.

Customers

Evidence has emerged that indicate a relationship between WIZARD SPIDER access tools and STARDUST CHOLLIMA's post-exploitation implants. The full extent of this relationship remains unknown.

Victims

- TrickBot victims are currently targeted globally
- Anchor DNS has targets victims in the email sector
- Ryuk has impacted organizations in multiple sectors, including healthcare, government, manufacturing and commercial, and is used to target large businesses or organizations for high-revenue demands.
- Victims of Sodin remain unknown.

Crimes

- Accessing a computer without authorization for the purpose of commercial advantage and private financial gain
- Damaging a computer through the transmission of code and commands
- Committing a crime, fraud and related activity in connection with computers
- Threatening or demanding a demand or recompense by threatening or damaging a protected computer
- Extortion

Motivation

- Monetary theft from victim accounts, likely to have a network of money laundering and money muling
- Ransom payments using BitCoin (BTC)

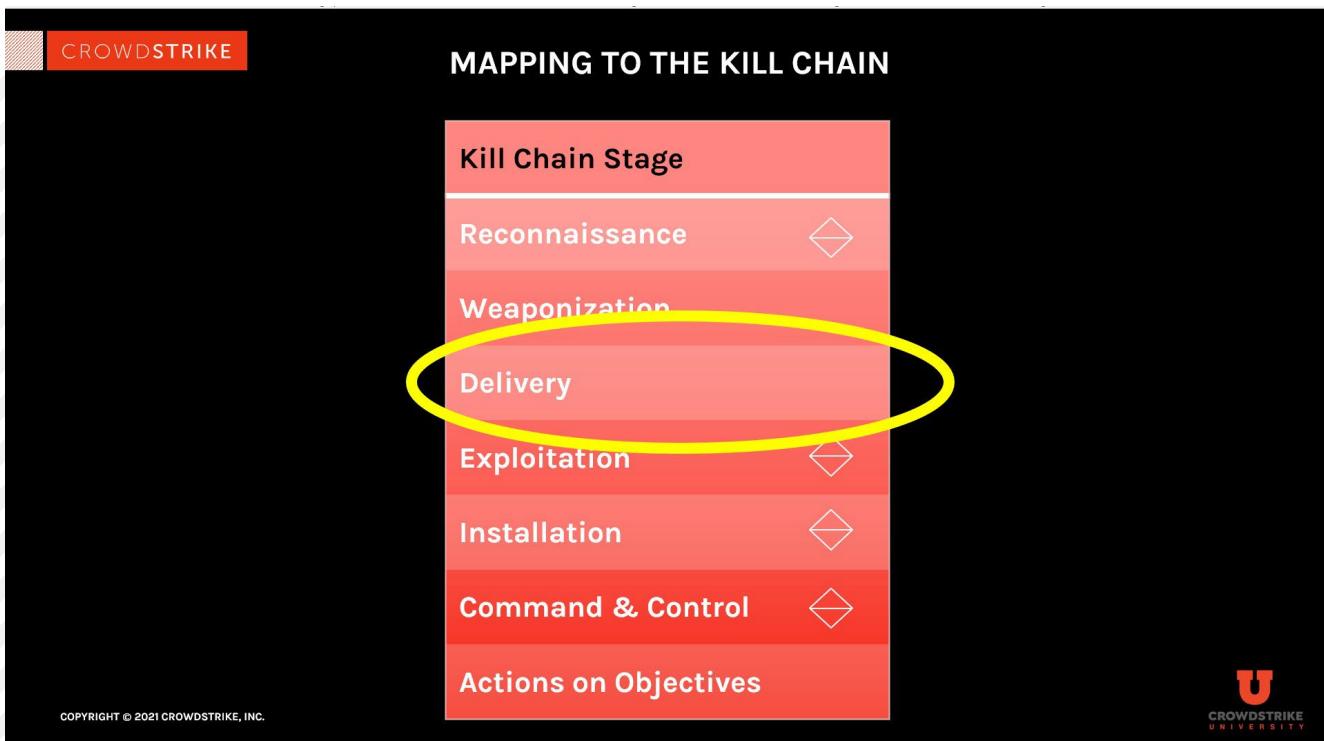
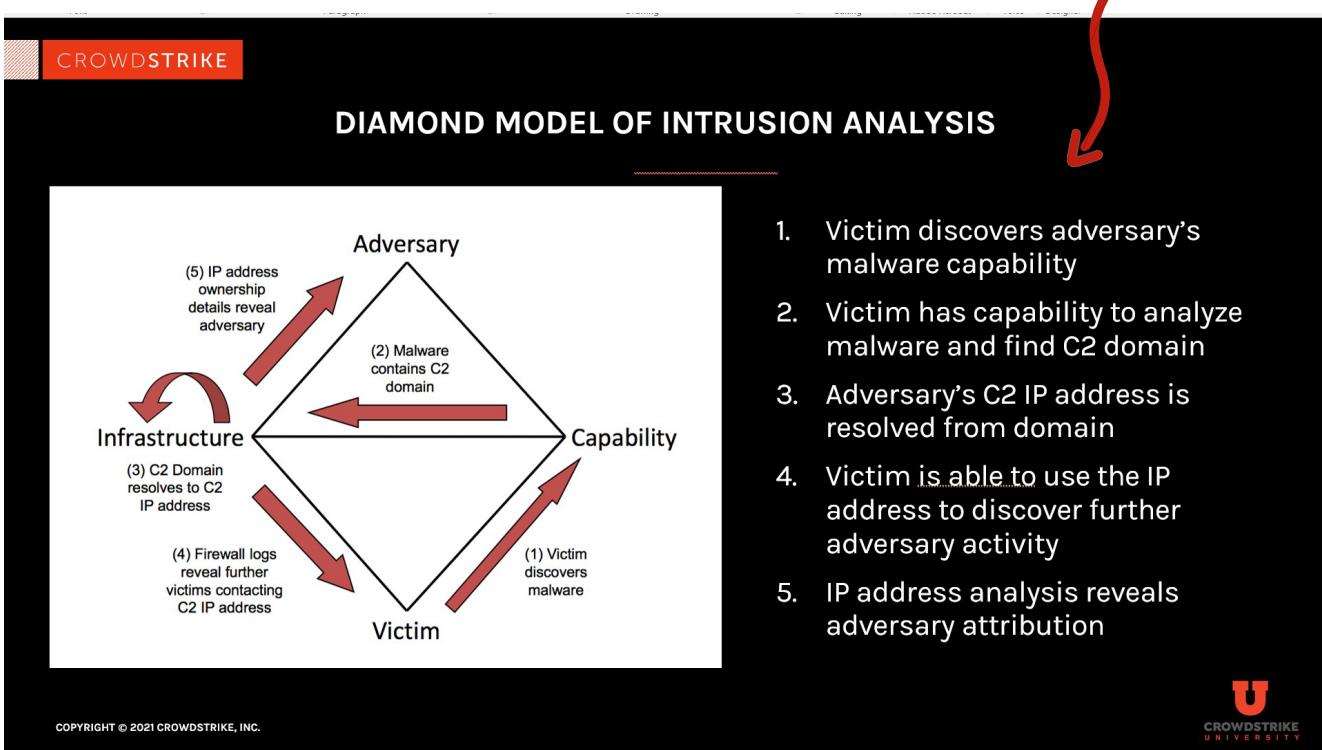
Technical Tradecraft

TrickBot Operations

- TLS, command and control communications
- XORAES/SHA256 encryption
- Uses Monero Cryptonight

INTELLIGENCE MODELS

The Diamond Model is “Used to describe an EVENT where an ADVERSARY takes a step towards an intended goal by using a CAPABILITY over INFRASTRUCTURE against a VICTIM producing a result.”



MITRE ATT&CK

Organizations can use the ATT&CK Framework to measure their detection and response capabilities.

CROWDSTRIKE

FALCON AND THE MITRE ATT&CK FRAMEWORK

@timestamp	@rawstring
2023-11-03 16:39:15.000	<pre>#event_simpleName: AssociateTreeIdWithRoot #repo: base_sensor #type: falcon-raw-data @id: 68jEW8ayiKAI5xymI70X2vp_0_8_1699029555 @ingestTimestamp: 1699029558172 @rawstring: {"AllowlistingFilterId": "", "ComputerName": "REYNHOLM-AD" @source: PlatformEvents @sourcetype: xdr/xdr-base-parsers:falcon-raw-data @timestamp: 1699029555000 @timestamp_nanos: 0 @timezone: Z Agent IP: 34.232.243.230 aid: b998bb0a5f5f48e9974c1b7914ba26da aip: 34.232.243.230 AllowlistingFilterId: cid: 7209dc9105f47669659533a363d69ab ComputerName: REYNHOLM-AD ConfigBuild: 1007.3.0017506.1 ConfigStateHash: 337962162 ContextTimeStamp: 1699029555.279 DetectDescription: A process has created a memory dump of LSASS DetectName: LsassProcdump DetectScenario: Credential theft DetectSeverity: 70 EffectiveTransmissionClass: 3 Entitlements: 15 event_platform: Win EventOrigin: 5 GrandparentProcessBehavioralContext: id: ab505744-80af-4232-8c79-1e5744bfc980 LocalAddressIP4: 10.2.1.5 LocalIP: 10.2.1.5 ParentProcessBehavioralContext: PatternDisposition: 0 PatternId: 47 ProcessBehavioralContext: tactic: Credential Access targetprocessid: 31740200 technique: OS Credential Dumping timestamp: 169902955565 TreeId: 1746369 TreeRoot: 316394495</pre>

Detection event data is populated in the Falcon ThreatGraph immediately upon sensor identification of an IOA or Falcon Cloud identification of an IOC

Tactic and technique are included in the event data based on pre-mapped patterns

CrowdStrike's ThreatGraph is responsible for piecing together the elements for determinations and matching identified patterns to MITRE ATT&CK tactics and techniques.

COPYRIGHT © 2024 CROWDSTRIKE, INC.



MITRE ATT&CK

Using ATT&CK with an EDR involves mapping events observed by the endpoint agent to phases of adversary activity, assess associated risk, and prioritize IR.

Aug. 23, 2023 07:34:46

01:51.804

I/O related actors

Status

Process

Run period

Severity: High

Action taken: None

Objective: Gain Access

Tactic & technique: Credential Access via OS Credential Dumping

An unusual process accessed lsass. This might indicate an attempt to dump credentials. Investigate the process tree.

Technique ID: T1003

IOA name: ProcAccessLsass

Local process ID: 10212

Command line: "C:\Windows\System32\Taskmgr.exe"

File path: \Device\HarddiskVolume2\Windows\System32\Taskmgr.exe

Hash

58ce90ca2021d2cc93b531a957f574b8cff7f8edbe53b6494ff2aaef8887ea29

Activity: IOC Management, Sandbox, Cybersixgill, OPSWAT, VirusTotal

External prevalence: Last seen

Internal prevalence: Internal prevalence

See full detection

COPYRIGHT © 2024 CROWDSTRIKE, INC.



MITRE ATT&CK

CROWDSTRIKE

FALCON DETECTION METHOD

Process

Run period: Dec. 5, 2023 19:05:54 - Dec. 5, 2023 19:05:57 (00:00:03.374)

Severity: High	Actions taken: File quarantined	
Objective: Falcon Detection Method	Tactic & technique: Machine Learning via Cloud-based ML	
Specific to this detection: This file meets the File Analysis ML algorithm's high-confidence threshold for malware.		
Technique ID: CST0008	IOA name: --	Local process ID: 4988

Falcon Detection Method (FDM) – a matrix for tactics and techniques CrowdStrike considers malicious and worth investigating

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

TECHNIQUE ID

Process

Run period: Dec. 5, 2023 19:05:57 - Dec. 5, 2023 19:05:57 (00:00:00.115)

Severity: High	Actions taken: File quarantined	
Objective: Gain Access	Tactic & technique: Credential Access via OS Credential Dumping	
Specific to this detection: A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.		
Technique ID: T1003	IOA name: ProcMimikatz	Local process ID: 6256

MITRE ATT&CK™		
	Technique	Description
T1003	OS Credential Dumping	Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
.001	LSASS Memory	Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using the Alternate Authentication Material.
.002	Security Account Manager	Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the <code>sak</code> <code>sacl</code> command. Enumerating the SAM database requires SYSTEM level access.
.003	NTDS	Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights. By default, the NTDS file (NTDS.dit) is located in <code>\SystemRoot\NTDS\Stora.dit</code> of a domain controller.
.004	LSA Secrets	Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts. LSA secrets are stored in the registry at <code>HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets</code> . LSA secrets can also be dumped from memory.
.005	Cached Domain Credentials	Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.
.006	DCSync	Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API) to simulate the replication process from a remote domain controller using a technique called DC Sync.
Filesystem		Adversaries may gather credentials from information stored in the Proc filesystem or <code>/proc</code> . The Proc filesystem on Linux contains a great deal of information regarding the state of the running operating system. Processes running with root privileges can use this facility to scrape live memory of other running programs. If any of these programs store passwords in clear text or password hashes in memory, these values can then be harvested for either usage or brute force attacks, respectively.
Accessed and shadow		Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking. Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> to store user account information including password hashes in <code>/etc/shadow</code> . By default, <code>/etc/shadow</code> is only readable by the root user.

Precisely identifies the MITRE ATT&CK Framework technique
Sub-techniques are not yet enumerated in Falcon (work in progress)



MITRE ATT&CK

CROWDSTRIKE

USING ATT&CK INFO IN DETECTIONS

Assists understanding of what happened and what is next.

The screenshot shows a detection summary for a process launching mimikatz. Key details include:

- Run period:** Dec. 5, 2023 19:05:57 to Dec. 5, 2023 19:05:57, duration 00:00:00.115.
- Severity:** High.
- Objective:** Gain Access.
- Actions taken:** File quarantined.
- Tactic & technique:** Credential Access via OS Credential Dumping (T1003).
- Specific to this detection:** A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.
- Technique ID:** T1003.
- IOA name:** ProcMimikatz.
- Local process ID:** 6256.
- Description:** Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

In this example, we would pivot to looking for **lateral movement**. We can use the matrix to help build our hypotheses of which technique was most likely.

Credential Access	Discovery	Lateral Movement
17 techniques	32 techniques	9 techniques
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
Brute Force (4)	Application Window Discovery	Internal Spearphishing
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Forced Authentication	Cloud Service Dashboard	Replication Through Removable Media
Forge Web Credentials (2)	Cloud Service Discovery	Software Deployment Tools
Input Capture (4)	Cloud Storage Object Discovery	
	Container and Resource Discovery	

COPYRIGHT © 2024 CROWDSTRIKE, INC.

CROWDSTRIKE

DETECTION LINKS TO DOCUMENTATION

The screenshot shows a detection summary for a process launching mimikatz. Key details include:

- Run period:** Dec. 5, 2023 19:05:57 to Dec. 5, 2023 19:05:57, duration 00:00:00.115.
- Severity:** High.
- Objective:** Gain Access.
- Actions taken:** File quarantined.
- Tactic & technique:** Credential Access via OS Credential Dumping (T1003).
- Specific to this detection:** A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.
- Technique ID:** T1003.
- IOA name:** ProcMimikatz.
- Local process ID:** 6256.

Gain Access

Objective Description

Gaining access to your endpoints is a key phase in an adversary's attack strategy. A common way to get in is through social engineering or exploiting vulnerabilities. Once an adversary has initial access, they work to gain more access by escalating privileges on compromised accounts.

Common Tactics – Enterprise

Credential Access

The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques that steal legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the means to perform other attacks.

Show Related Techniques

Initial Access

The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. These techniques often exploit weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access if not detected and removed.

Show Related Techniques

Privilege Escalation

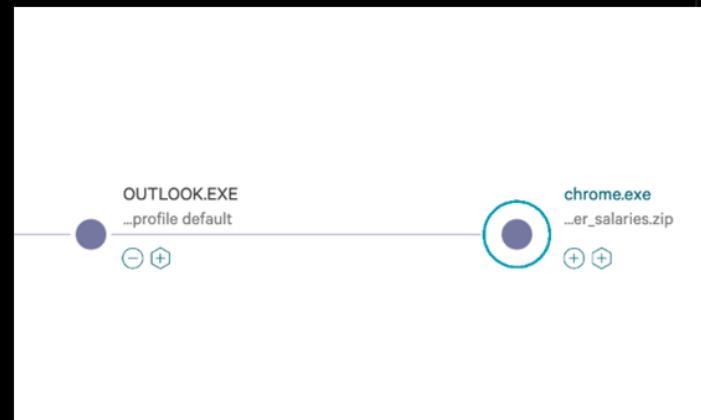
The adversary is trying to gain higher-level permissions.

COPYRIGHT © 2024 CROWDSTRIKE, INC.

MORPHOLOGICAL ANALYSIS

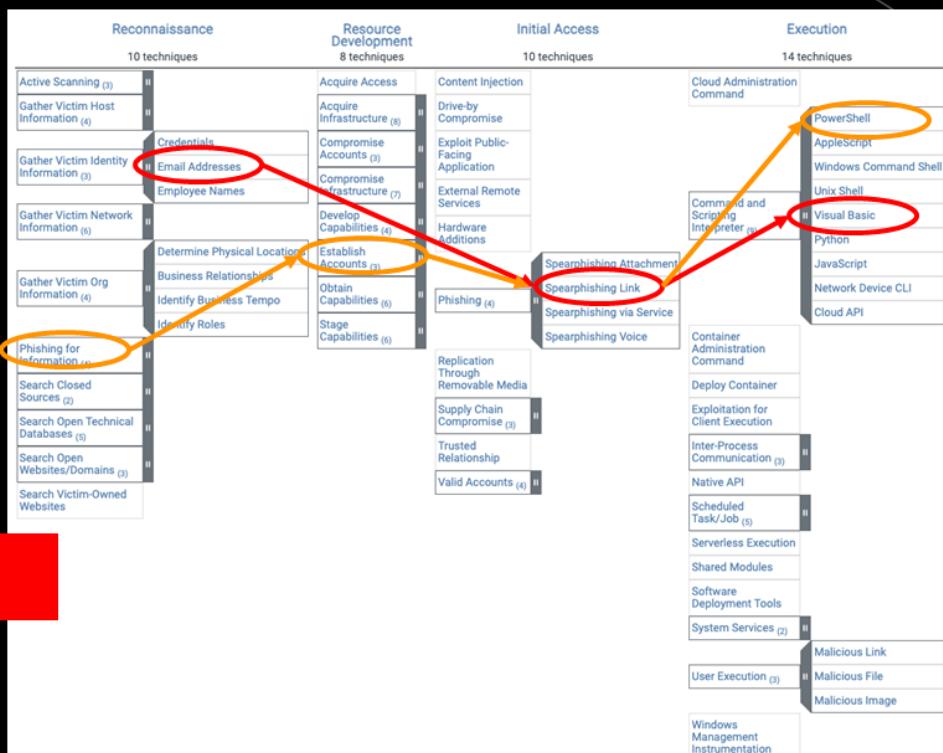
- While hunting, I found what appears to be a parent-child relationship indicative of a spearphishing attempt
- What do you think are the parent and child processes?
- Majority of analysts would likely say “Outlook to Chrome” - but why?
- You created a hypothesis based on past experience – and you used **morphological analysis** to do it!

POSSIBLE ATTACK PATHS



COPYRIGHT © 2024 CROWDSTRIKE, INC.

POSSIBLE ATTACK PATHS



COPYRIGHT © 2024 CROWDSTRIKE, INC.

MORPHOLOGICAL ANALYSIS

CROWDSTRIKE

MORPHOLOGICAL REASONING

Identifying a Complete Set of Relationships

Exploring all possible solutions and relationships to a complex, non-quantifiable issue; forces a new way of thinking.

Category:	Imaginative Thinking
Complexity:	Medium
Collaboration:	Individual or Group

I = Initial energy form
 T = Transmission form
 S = Final Storage form

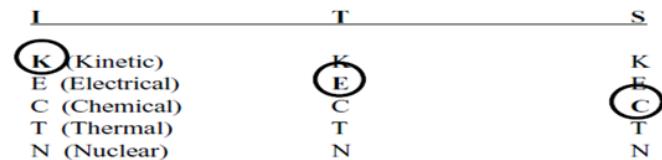


Figure 2: Energy Conversion Matrix (example)

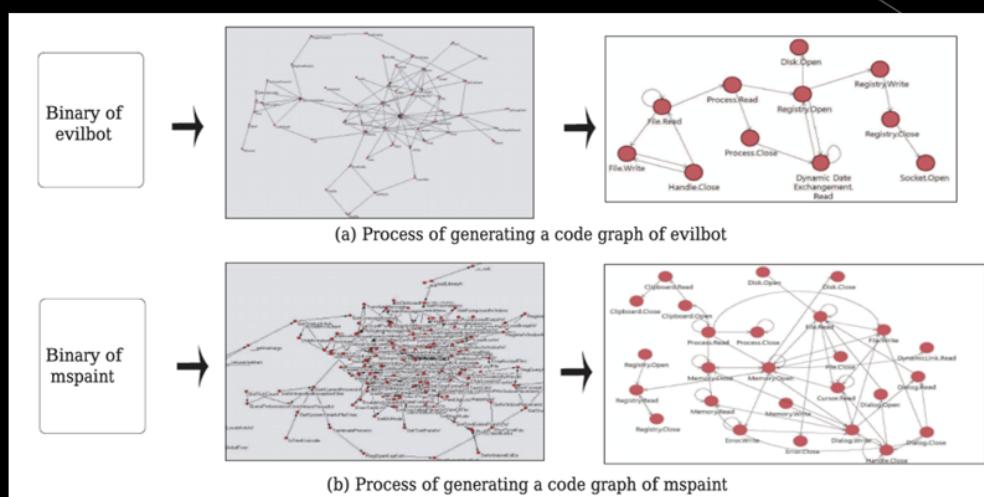
COPYRIGHT © 2024 CROWDSTRIKE, INC.



CROWDSTRIKE

“ZWICKY-STYLE” MORPHOLOGICAL REASONING

- Problem to be solved must be very concisely formulated
- All parameters that might be of importance must be analyzed
- Morphological box or multi-dimensional matrix, which contains all of the potential solutions of the given problem, is constructed
- All solutions contained in the morphological box are evaluated
- Best solutions are selected and are practically applied



Detecting Metamorphic Malwares using Code Graphs (Jan 2010)
 Jusuk Lee, Kyoochang Jeong, and Heejoo Lee
 Div. of Computer & Communication Engineering
 Korea University

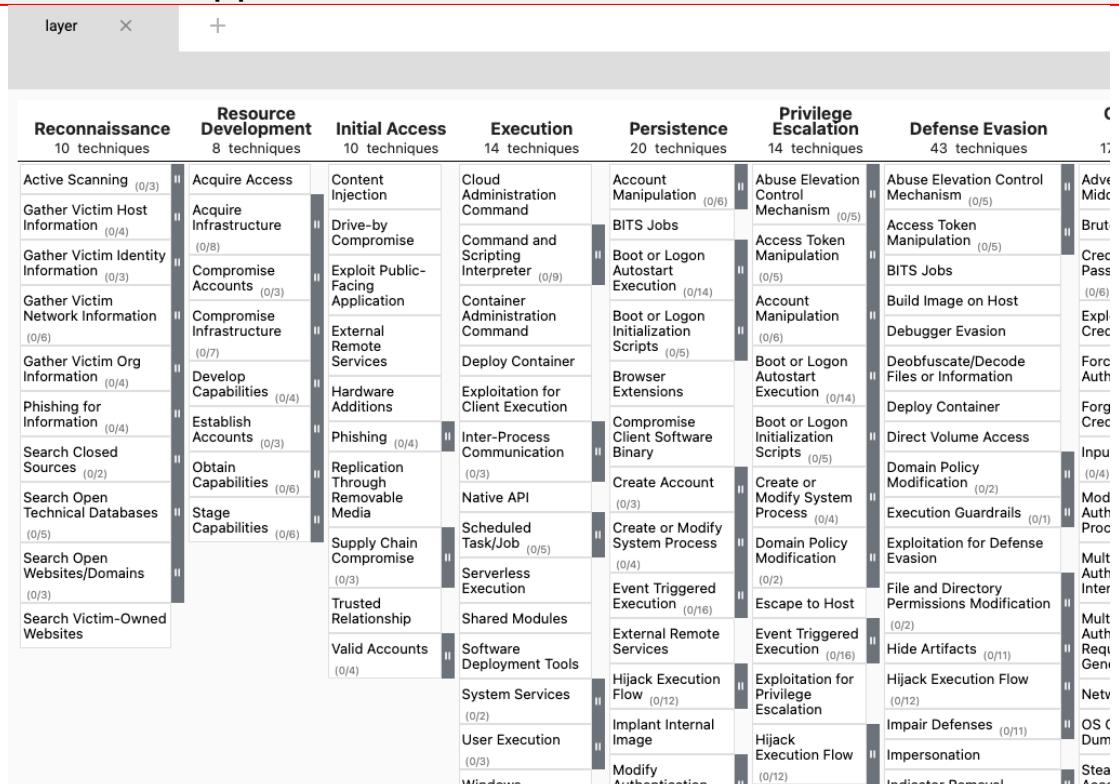
Concept Pioneered by Fritz Zwicky (1966)

COPYRIGHT © 2024 CROWDSTRIKE, INC.



ATT&CK NAVIGATOR

- Provides basic navigation and annotation on ATT&CK matrices
- Allows colorization, enumeration, comments, and the ability to define layers (custom views)
- Hosted webapp at GitHub, but also downloadable to run locally



Known Adversary TTP SET

This screenshot shows a more detailed and annotated view of the ATT&CK Navigator, likely representing a specific adversary profile (e.g., APT28).

The main interface displays a grid of TTPs categorized by layer:

- Initial Access**: 10 techniques
- Execution**: 10 techniques
- Persistence**: 19 techniques
- Privilege Escalation**: 14 techniques
- Defense Evasion**: 35 techniques
- Credential Access**: 16 techniques
- Discovery**: 27 techniques
- Lateral Movement**: 9 techniques
- Collection**: 15 techniques
- Command and Control**: 17 techniques

Annotations include colored boxes highlighting specific TTPs, such as "Exploitation for Client Execution" in green and "Hijack Execution Flow" in red. A sidebar on the right provides search and filtering capabilities for specific techniques and threat groups, including a search bar for "APT28" and sections for "Techniques (1)", "Threat Groups (2)", "Software (17)", "Mitigations (0)", "Campaigns (0)", "Assets (0)", and "Data Sources (0)".

ATT&CK NAVIGATOR

Aggregate Scoring



The ATT&CK Navigator is a great tool to visualize adversary TTPs

ATT&CK NAVIGATOR

Aggregate Scoring

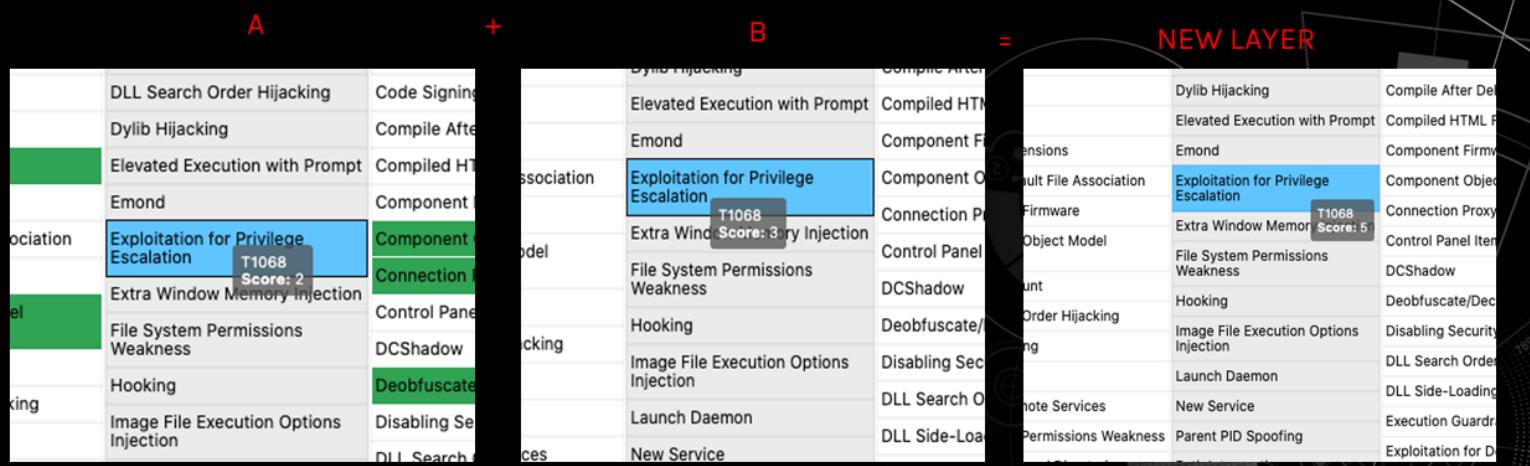
The screenshot shows the ATT&CK Navigator interface with several tabs at the top: FANCY BEAR, SKELETON SPIDER, new tab, and a plus sign. A red circle labeled 'a' highlights the FANCY BEAR tab. Another red circle labeled 'b' highlights the SKELETON SPIDER tab.

The main area is a configuration panel for creating a new layer:

- Create New Layer**: Create a new empty layer.
- Open Existing Layer**: Load a layer from your computer or a URL.
- Create Layer from other layers**: Choose layers to inherit properties from. A red circle labeled 'a+b' highlights the 'score expression' input field containing 'a+b'.
- coloring**: Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.
- comments**: Choose which layer to import comments from. Leave blank to initialize with no comments.
- states**: Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.
- filters**: Choose which layer to import filters - stages and platforms - from. Leave blank to initialize with no filters.
- legend**: Choose which layer to import the legend from. Leave blank to initialize with an empty legend.
- Create**: A button to create the new layer.

At the bottom, there's a section for creating a customized navigator:

- Create Customized Navigator**: Create a hyperlink to a customized ATT&CK Navigator.



THREAT HUNT AUTOMATION



THREAT HUNT AUTOMATION

Tools don't hunt – analysts do

- Tools are only as good as their developer and user
- Tools can only pivot in ways they are taught to pivot
- Tools can only use the context provided to them – they cannot inherently infer context on their own
- Even the best tools don't (yet) think like the human mind, we must supplement with human hunting



FALCON APIs

- Falcon has many APIs – but for this course we are concerned with Threat Graph APIs
- The official documentation has a wealth of information on how to set APIs up and utilize them
- All APIs are based on OAuth2

Endpoint Security APIs

Detection and Prevention Policy APIs

Incident, Detection, and Alert Monitoring APIs

Real Time Response APIs

Real Time Response Policy APIs

USB Device Control Policy APIs

Falcon Firewall Management APIs

Zero Trust Assessment APIs

Threat Graph API (key-based)

Windows On-Demand Scanning APIs

APIs can be used in scripting languages like Python or in programs like Postman
Requires support ticket to enable the APIs

THREAT HUNT AUTOMATION

CUSTOM IOAs

STATUS	RULE GROUP NAME	PLATFORM	RULES	POLICIES ASSIG...	LAST MODIFIED	MODIFIED BY	DESCRIPTION
Enabled	Example Group	Windows	1	0	Aug. 2, 2021...		Just an example...



With **Falcon Insight**:

- Monitor for unique circumstances and environments



With **Falcon Prevent** customers can also:

- Block and kill processes
- Add (or exclude) specific process executions or events
- Create rules for events that are NOT malicious

COPYRIGHT © 2024 CROWDSTRIKE, INC.



CUSTOM IOCs

- Hashes, domains, and IP addresses
 - Limit of 90,000 hashes
- Can be applied to ALL HOSTS or selected GROUPS
- Set your own severity
- Create individually or upload csv or json file

Indicator	Action	Mobile action	Date added	Last seen	Last modified	Host groups	Expiration date	Severity
No action	No action	Nov. 4, 2023 21...	Dec. 5, 2023 16...	Nov. 17, 2023 14...	FHT 240 2023 up...	—	—	High
Allow	No action	Jul. 27, 2023 19...	Jul. 27, 2023 19...	Jul. 27, 2023 19...	YI-PreProd	—	—	Low
Block	No action	Jul. 27, 2023 19...	Jul. 27, 2023 19...	Jul. 27, 2023 19...	YI-PreProd	—	—	Low
Block	No action	Jul. 27, 2023 19...	Jul. 27, 2023 19...	Jul. 27, 2023 19...	YI-PreProd	—	—	Low
No action	No action	Jul. 18, 2023 14...	Nov. 3, 2023 17...	Jul. 25, 2023 09...	FHT 240 2023 up...	—	—	Critical
No action	No action	May 11, 2022 00...	—	Jun. 8, 2022 00...	GoT - New Scenar...	—	—	Low
No action	No action	May 11, 2022 01...	—	Jun. 8, 2022 00...	GoT - New Scenar...	—	—	—
No action	No action	Jun. 13, 2022 14...	—	Jun. 14, 2022 18...	MT Mac	Jun. 13, 2022	—	Critical
No action	No action	Apr. 21, 2021 22...	—	Apr. 21, 2021 22...	All hosts	—	—	—
No action	No action	Apr. 21, 2021 22...	—	Apr. 21, 2021 22...	All hosts	—	—	—



THREAT HUNT AUTOMATION

CROWDSTRIKE

SCHEDULED SEARCH TABS

The screenshot shows a dark-themed interface with three main tabs at the top: "Scheduled searches" (highlighted in blue), "Search log", and "Audit log". A tooltip for "Scheduled searches" reads: "View your scheduled searches". A tooltip for "Search log" reads: "Log of all previous searches with number of hits". A tooltip for "Audit log" reads: "Audit trail – only accessible by admins". Below the tabs, there's a table listing one result: "Legacy Possible phishing ... 12 hours -- Nov. 14, 2023 20... Nov. 14, 2023 08... 0 results / 14 sear... 100% Active david.morgan@cr...".

COPYRIGHT © 2024 CROWDSTRIKE, INC.

CROWDSTRIKE

FALCON FUSION

- Granular definitions for automated actions for incidents, detections, etc
- Actions dependent on role-based access and subscriptions
- Some actions may require a connector from the CrowdStrike Store

The screenshot shows the "Fusion workflows" section of the Falcon interface. On the left, a sidebar lists "Endpoint security", "Exposure management", "Counter Adversary Operations", "Investigate", and "Fusion workflows" (which is circled in red). The main area shows a "Create a workflow" dialog with a "Workflow preview" section containing a flowchart. The flowchart starts with a "Trigger" box ("New endpoint detection"), followed by an "IF" condition ("Severity is equal to Critical"), and an "Action" box ("Create ServiceNow incident").

COPYRIGHT © 2024 CROWDSTRIKE, INC.

HUNTING RESOURCES

The hunting guide offers best practices for introductory threat hunting in Falcon, hunting queries, and focuses on IOCs. It also includes various search pages in Investigate

The screenshot shows a navigation sidebar on the left with sections like Sensor Deployment and Maintenance, Falcon Main View, Falcon Management, Unified Detection Monitoring, Endpoint Security (which is expanded to show Start Up and Scale Up, MITRE-Based Falcon Detections Framework, Indicator Graph Explorer), XDR, Endpoint Monitoring, Event Investigation, and Events Data Dictionary. The main content area shows the breadcrumb path: Falcon Documentation > Endpoint Security > Event Investigation > Hunting and Investigation. The title 'Hunting and Investigation' is displayed, along with a note about the new CrowdStrike Query language experience. The page was last updated on Dec. 13, 2023. A 'Print to PDF' button is in the top right.

RESOURCES

Access documentation in the Falcon platform by going to Support > Docs

