Modern MacOS Threat Hunting



Karl Hiramoto
@karlhiramoto
karl.hiramoto@virustotal.com
October 2023



Let’s get to know each other!

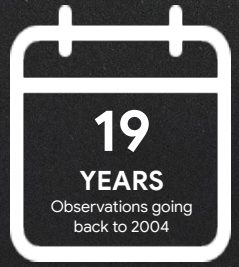
- Do you do threat hunting on a regular basis?
- Are you familiar with Yara?
- Are you familiar with VTI?

00

VirusTotal Introduction

World-largest threat observatory

- Massive amounts of data, **instantaneous searching**
- **Any kind** of threat observable (files, URLs, domains, IPs)
- **Multi-angular detection** (AVs, whitelists, sandboxes, etc.)
- Unparalleled history, going back to 2004
- Diverse, global, **crowdsourced**, real-time, **actionable**



50B+ files

Any file type: peexe, php, apk, powershell, ios, mac, lnk, etc.

1.5B+ Sandbox reports

2M Analyses per day

232 COUNTRIES submitting files

3M+ MONTHLY USERS sourcing data

6B+ URLs

6M+ URL analyses per day

5B+ Domains

170B+ pDNS Resolutions

45/71

70+ Antivirus
90+ URL blocklists
20+ Sandboxes
30+ Crowdsourced
YARA, SIGMA, IDS repos
~ 100K Crowdsourced rules

01

Let’s start hunting with VirusTotal Intelligence!

How we actually start? - a suggested approach

while (1):

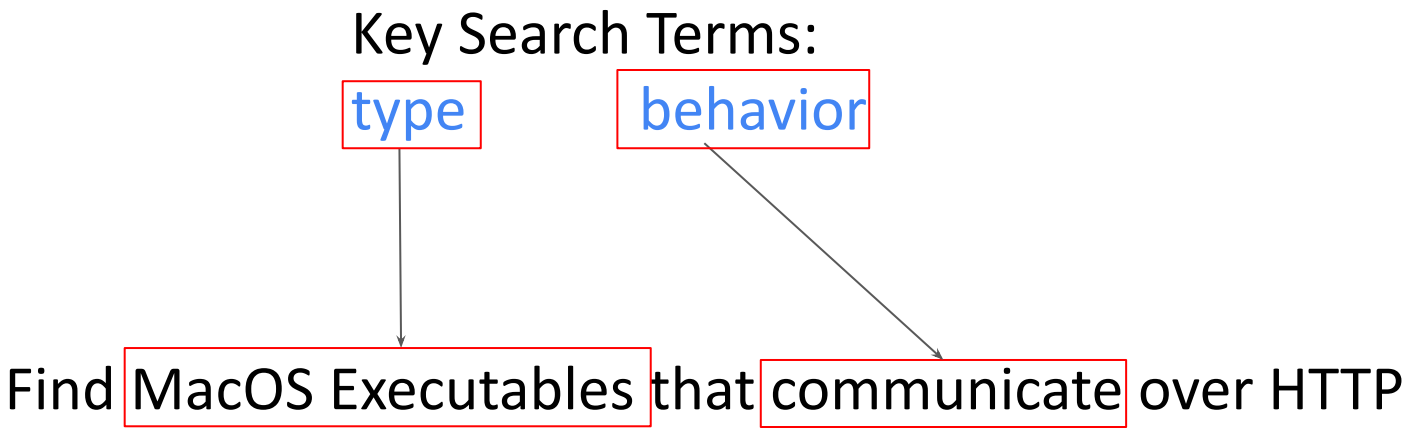
- Get context for a set of IOCs
- Identify the “interesting” ones
- Find anomalies and/or commonalities
- Pivot
- Update your set of IOCs

Tips

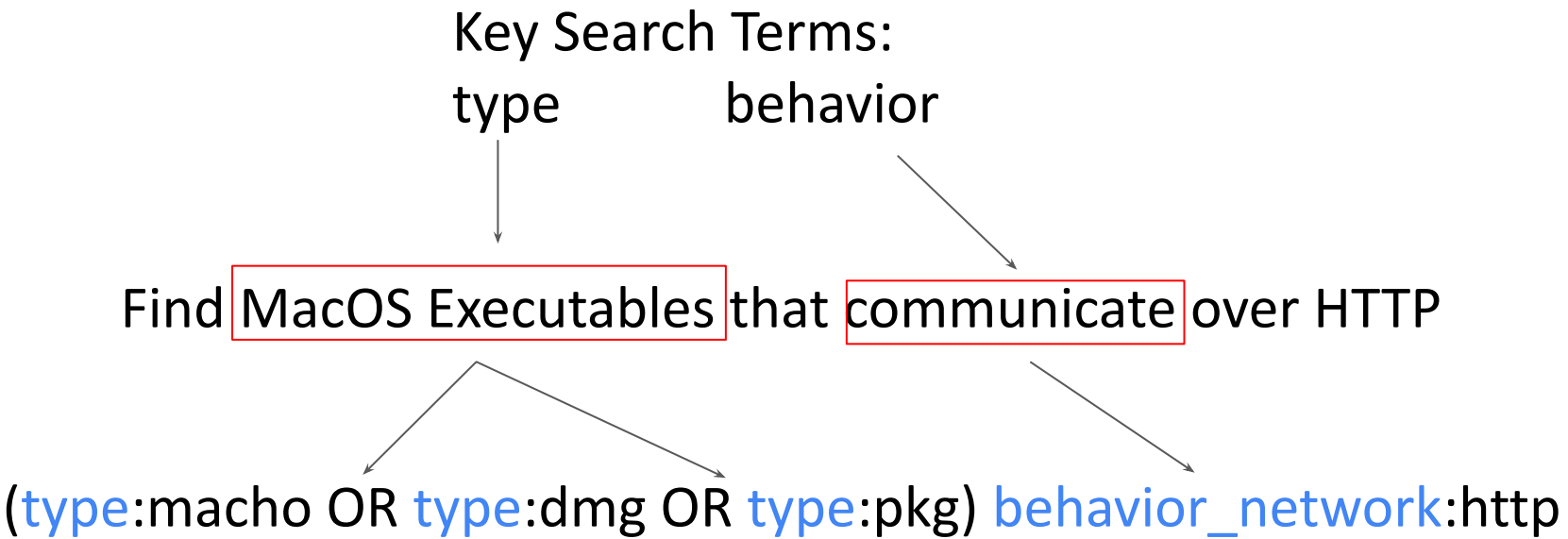
https://support.virustotal.com/

- Supports logical “AND” “OR” “NOT”
- Respects order of operations: ()
- Ranges can be denoted with + or -

Example 1


Key Search Terms:
type
behavior
Find MacOS Executables that communicate over HTTP

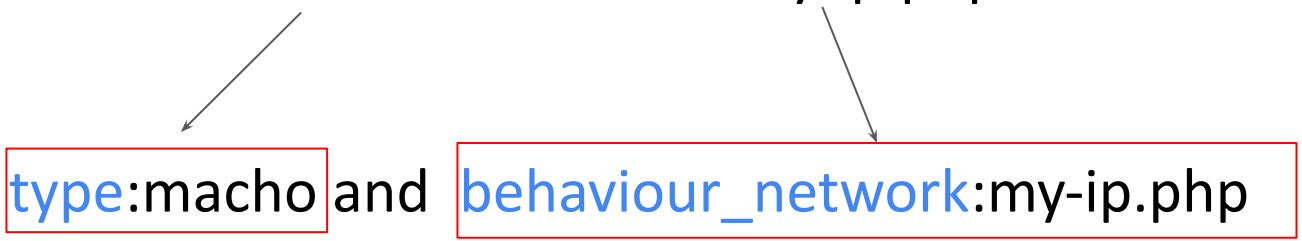
Example 1



VirusTotal

Example 2

Find Executables that use “my-ip.php” in their URI



VirusTotal

Example 3:

Files named “invoice” from the US with macros and greater than 5 detections

name:"invoice" tag:macros p:5+ submitter:US

VirusTotal

Popular modifiers

1. p:3+ and type:macho and tag:arm
2. content:osacompile
3. (type:macho or type:pkg or type:dmg or tag:mac-app) and p:2+ and submitter:UA
4. submitter:UA type:email p:1+ fs:2023-05-01+
5. tag:arm tag:multi-arch and fs:2023-10-01+
6. tag:cve-2023* and tag:macho
7. tag:attachment tag:cve-2017-0199 tag:docx tag:exploit
8. filename:"nl txt" AND tag:text AND ls:"2023-01-01T00:00:00+" AND ls:"2023-01-31T23:59:00-"

VirusTotal

Example: File magic

- magic:"Mach-O 64-bit arm64 executable"
- magic:"Mach-O 64-bit x86_64 executable"
- magic:"Mach-O universal binary"

Example: Mac systems turned into proxy exit nodes by AdLoad

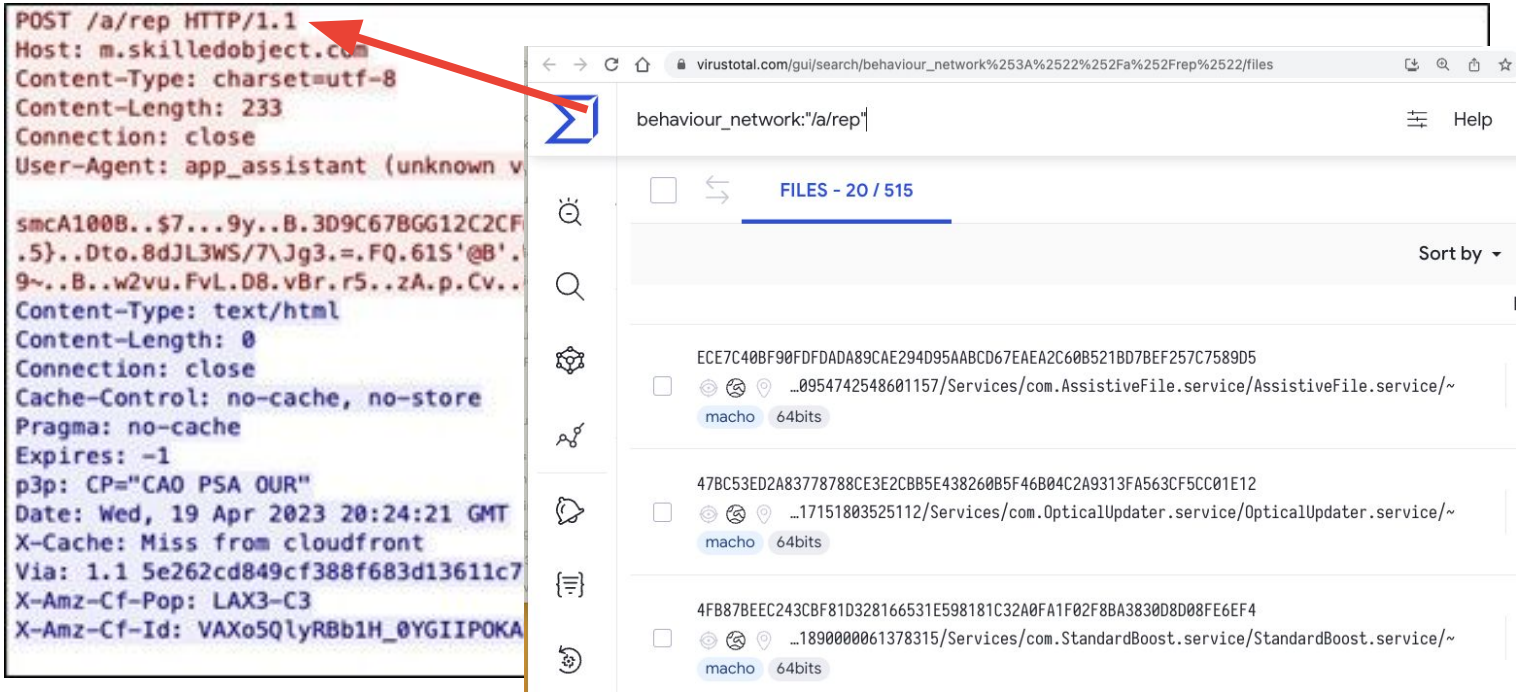
Executive summary

AdLoad malware is still infecting Mac systems years after its first appearance in 2017. AdLoad, a package bundler, has been observed delivering a wide range of payloads throughout its existence. During AT&T Alien Labs' investigation of its most recent payload, it was discovered that the most common component dropped by AdLoad during the past year has been a proxy application turning MacOS AdLoad victims into a giant, residential proxy botnet.

https://cybersecurity.att.com/blogs/labs-research/mac-systems-turned-into-proxy-exit-nodes-by-adload

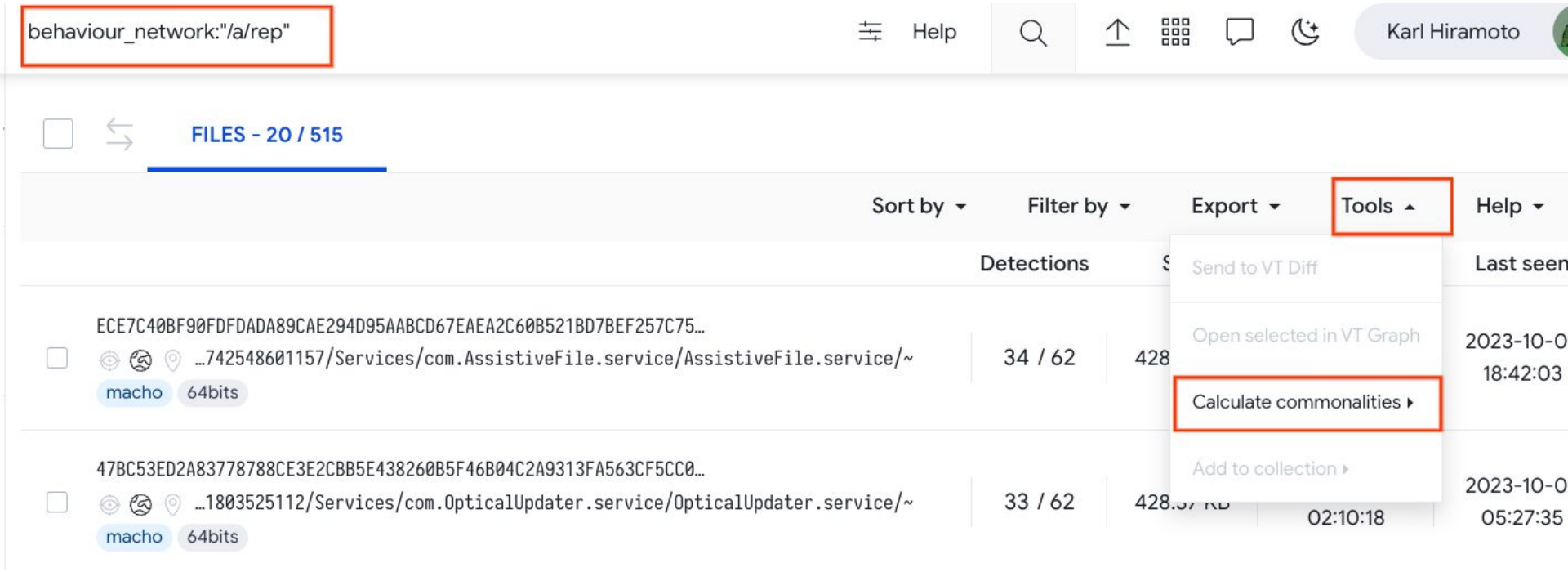
VirusTotal

Example: AdLoad HTTP Request



- behaviour_network:"/a/rep" or behaviour_network:"app_assistant"

Example: AdLoad Comoonalities

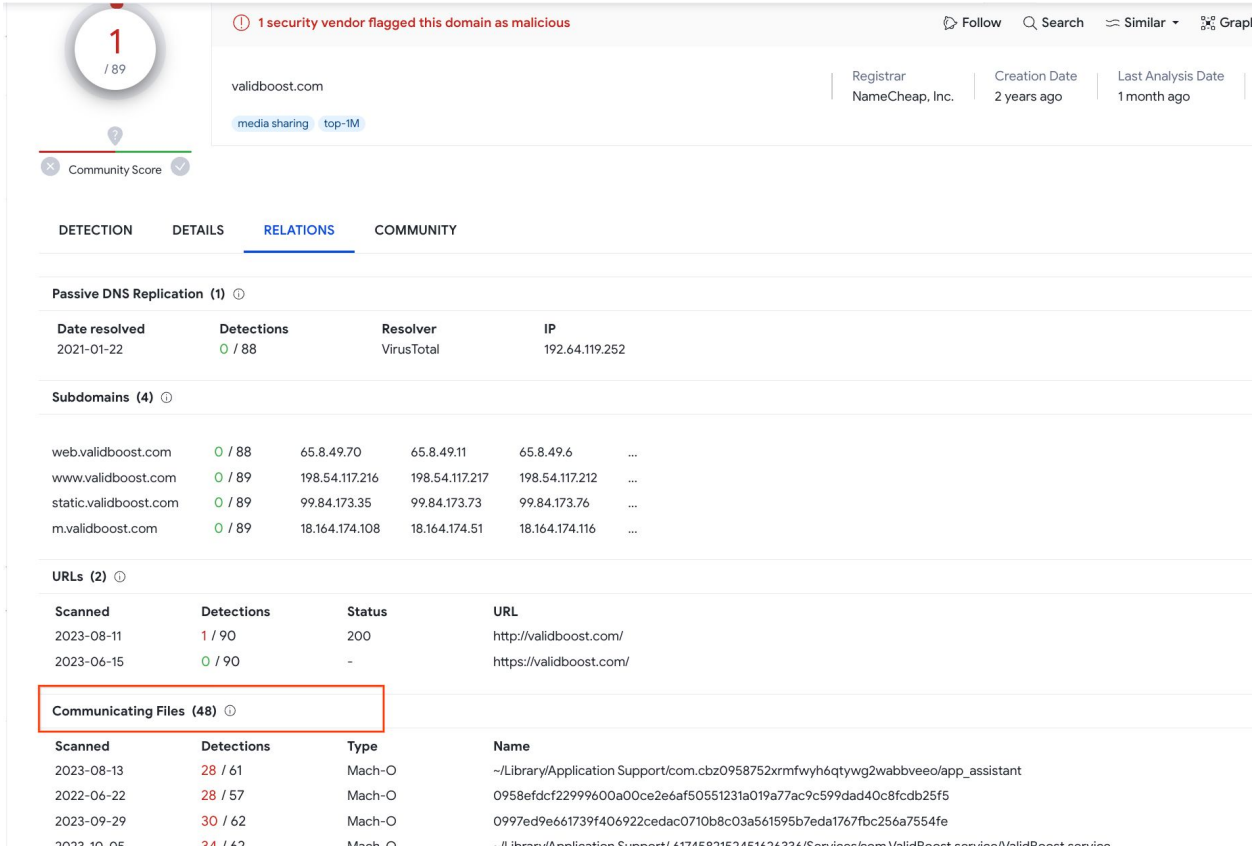


Example: Comoonalities URLS and Domains

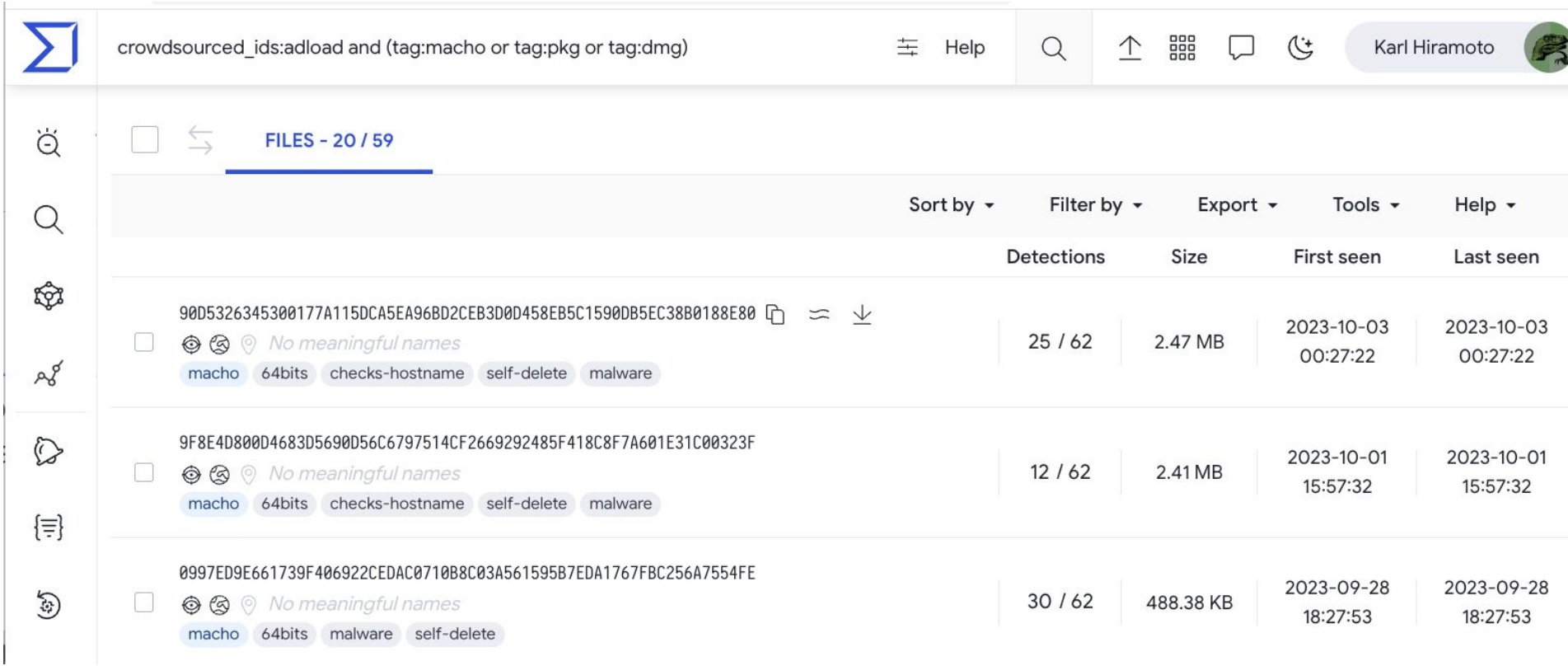
3 items	http://x1.i.lencr.org/
2 items	http://m.activitycache.com/a/rep
2 items	http://m.compellingstate.com/a/rep
2 items	http://m.configboost.com/a/rep
2 items	http://m.essencecuration.com/a/rep
2 items	http://m.extendedsample.com/a/rep
2 items	http://m.operativeunit.com/a/rep
2 items	http://m.portsage.com/a/rep
2 items	http://m.rotatorbox.com/a/rep
2 items	http://m.configprogress.com/a/rep
2 items	http://m.elemntstate.com/py/gwill
2 items	http://m.flexibleorigin.com/a/rep
2 items	http://m.exploreanalog.com/a/rep
2 items	http://m.assistiverecord.com/a/rep
2 items	http://api.ipify.org/

13 items	typecharacter.com
13 items	m.validboost.com
13 items	m.typecharacter.com
13 items	5.courier-push-apple.com.akadns.net
12 items	m.originalmodule.com
12 items	d3mno0637j48br.cloudfront.net
12 items	m.operativemachine.com
12 items	skilledobject.com
12 items	m.skilledobject.com
12 items	validboost.com
12 items	d4qfcokgjy4q2.cloudfront.net
12 items	m.extendedsprint.com
12 items	icanhazip.com
11 items	originalmodule.com
11 items	d5x2tcx9f5urn.cloudfront.net
11 items	d1czzonvly6iby.cloudfront.net
11 items	d36mqntu5jayw3.cloudfront.net
11 items	extendedsprint.com
11 items	m.typeinitiator.com
11 items	api.apple-cloudkit.fe.apple-dns.net
11 items	ianadata.vip.icann.org

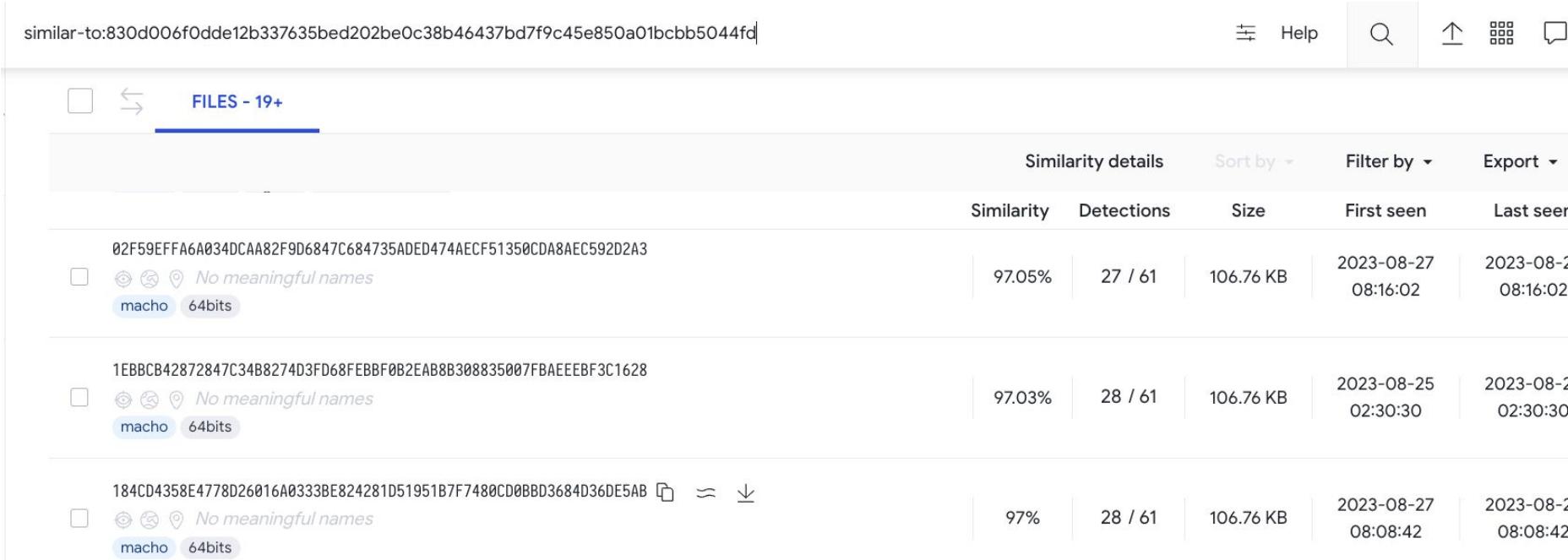
Relationships



Adload: IDS

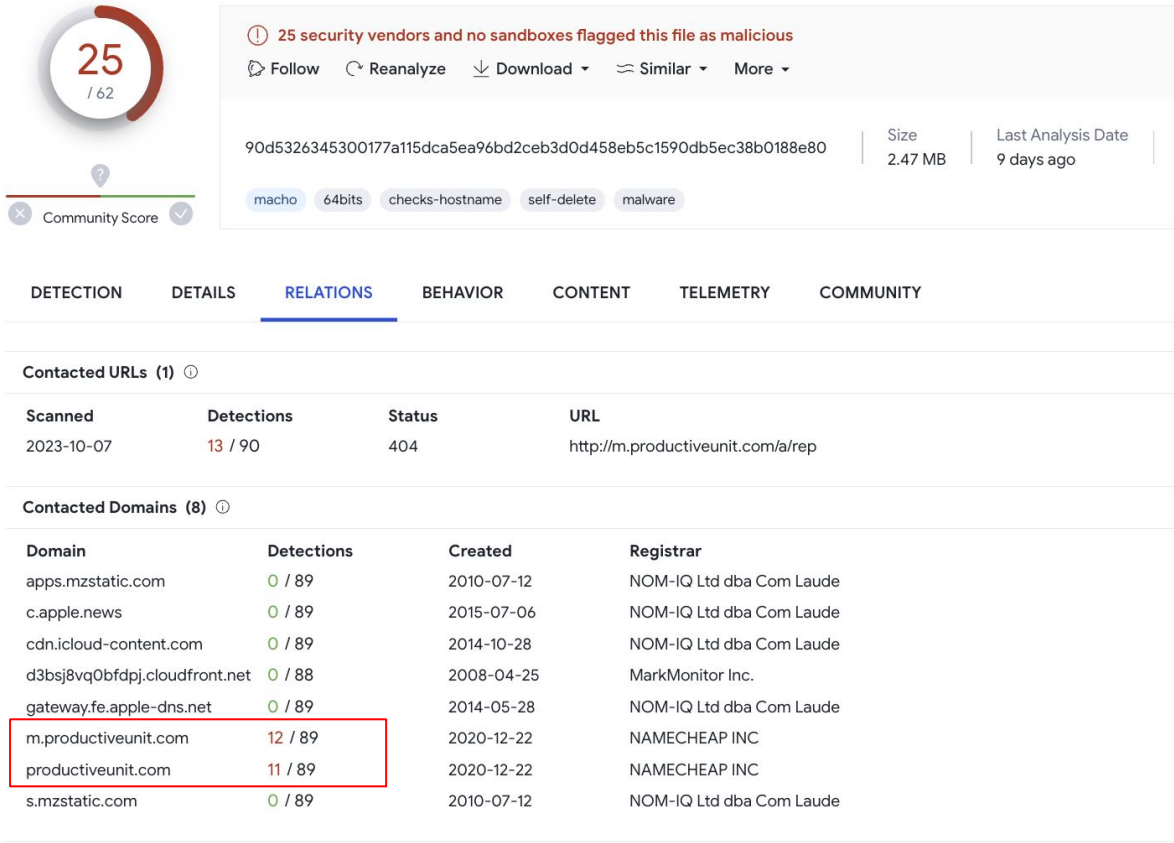

crowdsourced_ids:adload and (tag:macho or tag:pkg or tag:dmg)
Help
Karl Hiramoto
FILES - 20 / 59
Sort by
Filter by
Export
Tools
Help
Detections
Size
First seen
Last seen
90D5326345300177A115DCA5EA96BD2CEB3D0D458EB5C1590DB5EC38B0188E80
No meaningful names
macho
64bits
checks-hostname
self-delete
malware
25 / 62
2.47 MB
2023-10-03 00:27:22
2023-10-03 00:27:22
9F8E4D800D4683D5690D56C6797514CF2669292485F418C8F7A601E31C00323F
No meaningful names
macho
64bits
checks-hostname
self-delete
malware
12 / 62
2.41 MB
2023-10-01 15:57:32
2023-10-01 15:57:32
0997ED9E661739F406922CEDAC0710B8C03A561595B7EDA1767FBC256A7554FE
No meaningful names
macho
64bits
malware
self-delete
30 / 62
488.38 KB
2023-09-28 18:27:53
2023-09-28 18:27:53

Adload: similar-to



Infrastructure matters

Find relationships



VirusTotal

Infrastructure matters

Communicating Files (36)

Scanned	Detections	Type	Name
2023-08-04	30 / 61	Mach-O	600308845.txt
2023-09-13	29 / 61	Mach-O	/Library/Application Support/384759932502384436/org.384759932502384436_.384759932502384436/_9432131669907520018_
2022-09-09	28 / 61	Mach-O	1441fcf925fa263cc2dd6bd432b2e343e82535e8219e1c82d9f8063e7bc3c87f
2023-09-15	32 / 61	Mach-O	14ebe214e394204216e477083318c000c5e464a48689730e2d0024199b8b3064
2023-02-28	30 / 60	Mach-O	/Library/Application Support/com.5428436708794290304._5428436708794290304/_1205552142911415543
2023-08-06	29 / 61	Mach-O	2b1ef933aa02a34ac38e42308c76f259b050d32a2dce43ef54d161eb1dd1f11e
2023-08-04	33 / 61	Mach-O	42d7d8c9b33725e07460f97048241843d41722a5bacd7905ddba296154df568f
2023-10-05	34 / 62	Mach-O	/Users/Camila/Library/Application Support/.15314127506195013446/Services/com.SkilledObject.service/SkilledObject.service
2021-09-18	21 / 60	Mach-O	ee6ddd4d434abab88ba8571b511d9d95.virus
2023-01-31	28 / 62	Mach-O	/Library/Application Support/com.8400335054633276275._8400335054633276275/_1051750455036116408

Files Referring (9)

Scanned	Detections	Type	Name
2023-09-15	31 / 61	Mach-O	6a9c32032d69f507a088af3855852c8546640b016f3ff78e479246bc63c31394
2023-09-15	31 / 61	Mach-O	/Library/Application Support/com.135894973829846700 67.E9F6A8DC-F0F1-440A-BC1E-ADBE8DC3C6D3/_7708268185943189550
2023-09-13	31 / 60	Mach-O	_473416355257566537
2023-08-04	31 / 61	Mach-O	600308849.txt

VirusTotal

Example: Searching for persistence

- behaviour_processes:"/Library/StartupItems/" or behaviour_files:"/Library/StartupItems/"
- behaviour:"PlistBuddy"
- behaviour_processes:"RunAtLoad"

Adload

behaviour_processes:"Library/Application Support/"
behaviour_processes:"app_assistant"

Behaviour_files:"pcyx.ver"

crowdsourced_ids:adload and (tag:macho or tag:pkg or tag:dmg)

02

YARA FOR HUNTING AND MONITORING

Yara in a nutshell

- “Superb version” of grep tool
- Industry standard for sharing knowledge
- Main purpose:
  - Malware detection and classification
  - Finding suspicious activity
  - Searching for intellectual property
  - Forensic analysis
- Lots of useful documentation:

  https://yara.readthedocs.io/

```
rule ExampleRule
{
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 23 FB }

    condition:
        $my_text_string or $my_hex_string
}
```

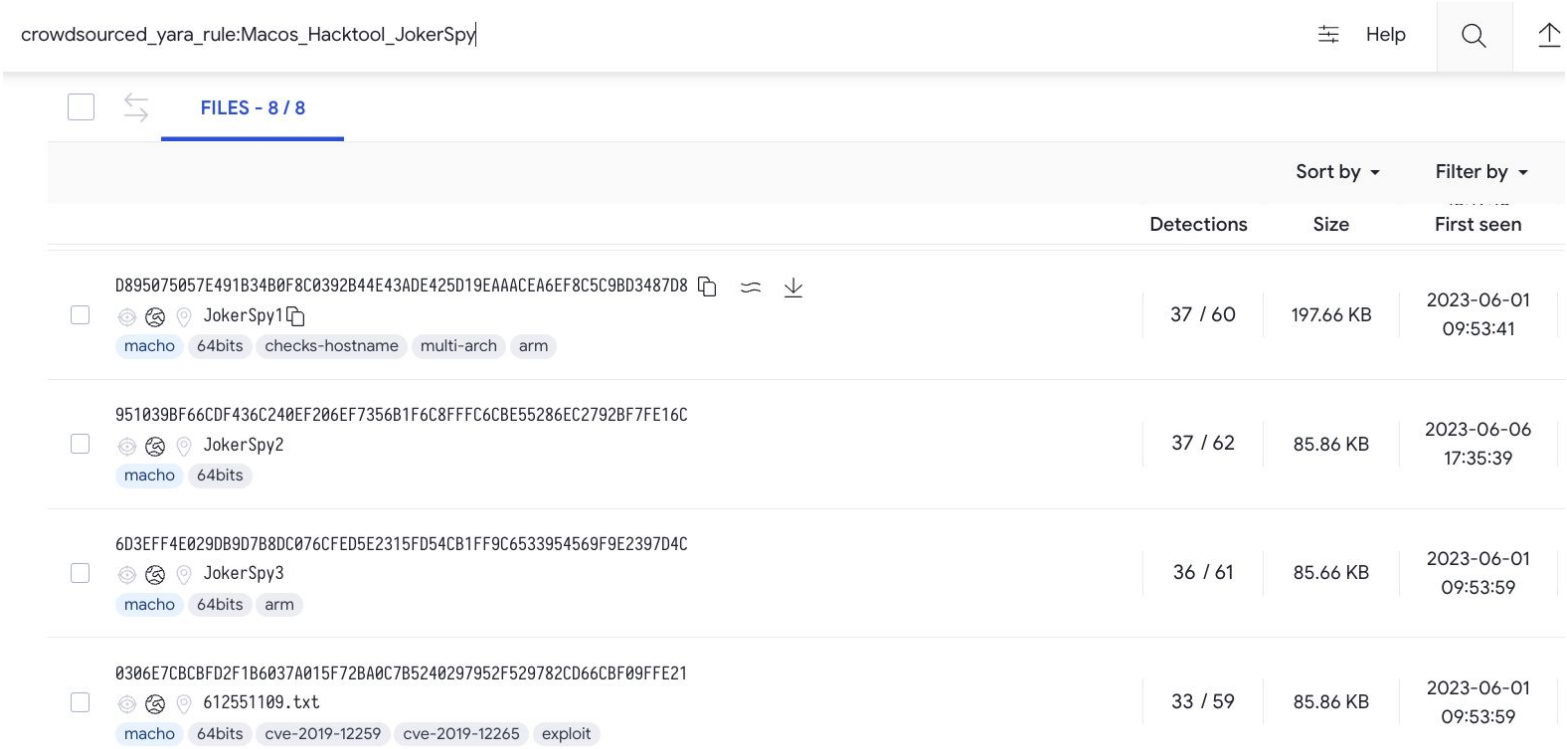
Let’s check how YARAs look like

```
rule Macos_Hacktool_JokerSpy_58a6b26d {
    meta:
        author = "Elastic Security"
        id = "58a6b26d-13dd-485a-bac3-77a1053c3a02"
        fingerprint = "71423d5c4c917917281b7e0f644142a0570df7a5a7ea568506753cb6eabef1c0"
        creation_date = "2023-06-19"
        last_modified = "2023-06-19"
        threat_name = "Macos.Hacktool.JokerSpy"
        reference_sample = "d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8"
        severity = 100
        arch_context = "x86"
        scan_context = "file, memory"
        license = "Elastic License v2"
        os = "macos"
    strings:
        $str1 = "ScreenRecording: NO" fullword
        $str2 = "Accessibility: NO" fullword
        $str3 = "Accessibility: YES" fullword
        $str4 = "eck13XProtectCheck"
        $str5 = "Accessibility: NO" fullword
        $str6 = "kMDItemDisplayName = *TCC.db" fullword
    condition:
        5 of them
}
```

crowdsourced_yara_rule:Macos_Hacktool_JokerSpy_58a6b26d

VirusTotal

Searching hits on crowdsourced yara



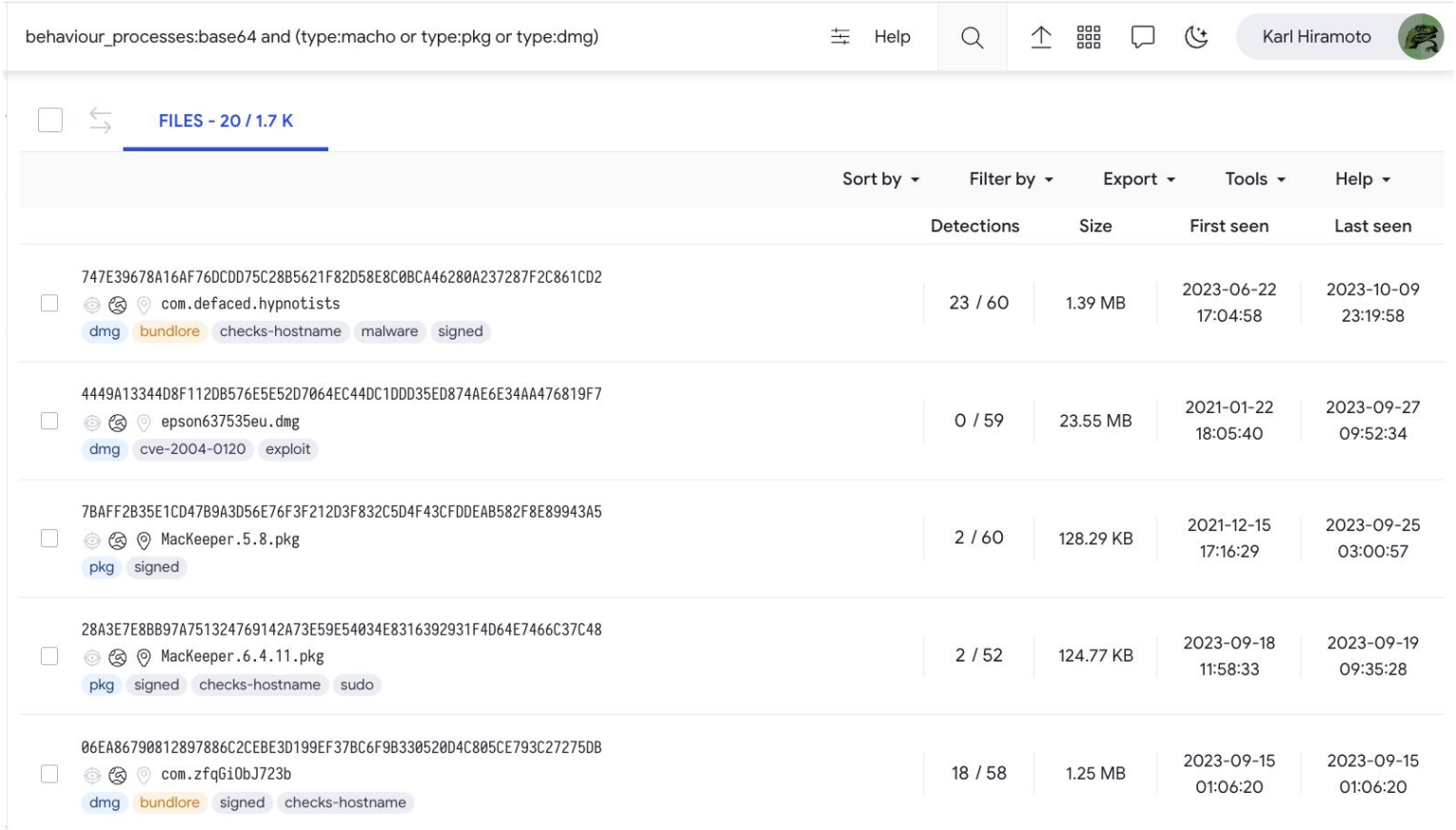
VirusTotal

Yara VT Module: import “vt”

```
rule mac_base64d
{
  meta:
    sigma_source = "https://github.com/SigmaHQ/sigma/blob/master/rules/macos/process_creat
    example1 = "f3e5c20b34731d6611e1a49def1c89d5c180db9bb465f8471ba84c1ad16b90e5"
    example2 = "ea502018cb3eeb56a930df29c7447857c6cca05d3431d2f575d2c62753bb81f1"
  strings:
    $koly = "koly"
  condition:
    ( $koly at (filesize-512) or
      vt.metadata.file_type == vt.FileType.PKG or
      vt.metadata.file_type == vt.FileType.MACH_O)
    and
    for any cmd in vt.behaviour.command_executions : (
        cmd icontains "base64 " and cmd icontains " -d"
    )
}
```

behaviour_processes:base64 and (type:macho or type:pkg or type:dmg)

VTI query equivalent



Yara with VT module

```
rule osascript
{
  meta:
    sigma_source = "https://github.com/SigmaHQ/sigma/blob/master/rules/macos/process_creation/p
    sha256 = "e69d82edc7e7b89d088db01ed62bb2896c0cb49abbfc0c61471c10609004f458"
  condition:
    for any cmd in vt.behaviour.command_executions : (
        cmd icontains "osascript"
        and cmd icontains " -e "
    )
}
```

behaviour_processes:"osascript -e "

Create new VTDiff session

VTDIFF helps threat analysts in creating YARA rules by automating the identification optimal patterns to detect groups of files (malware families, threat campaigns, threat actor toolset). These patterns can be used in Livehunt YARA rules, Retrohunt jobs and VT GREP content searches. Run through a quick VTDIFF tutorial here . In order to get best results when creating a new diff session, check the following guidelines:

- Write / paste file hashes for including.
- Work best when using 2 to 5 files.
- Avoid mixing different filetypes if possible (eg: 2 exe and 1 doc).
- Avoid mixing packed and unpacked files.

addload

Match

075cc08d19a93ea7dc6c9dae673fcf695cece9184f5447039d5a6dba4201919e
95befc341cf1633112536f7454b053768292db6c8cb7e94108dd9809401033c6
4cac93fe7748dfacc454d986b9769a90da49f5e812a33d1cb28161111f2fe9d8
915a2c85f4e244c9e05de0b46a94d28352eb41a19343a3fcf3abd94cccde701b
30e58260df259e477c9294675abd9005e850b52b516cfd40004636674cfa71d3

Exclude

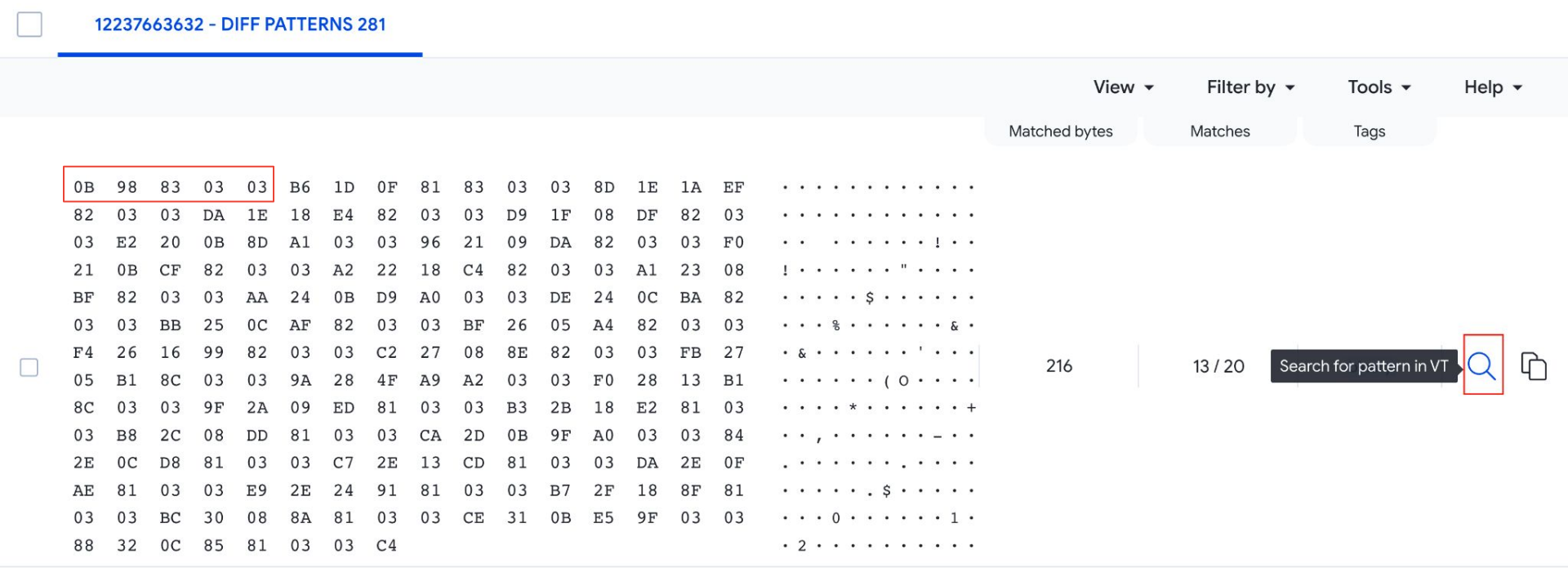
d1af8d88e10b45e7e3c80a4f0611c5e8f80fba70620663fff26d1589599f34ec
5e6598f993dcbe86d5f7b9fee66d35aca11690a5641d95879850a8cb13baf88b
4ab90662385798df4c39de96d58df1915429e9db8a5714d95dbfef2b66b5f263
97e72eba46c5c0f65a6c5e47c99f59827afa7f0253c3238e94e99104060ac6af
0322e140335431b1d49b3dc41ea97110534c6cf8eea3da218d6845885fff2ccd

The first text area allows you to specify the hashes whose common and optimal detection patterns should be identified. The second text area allows you to provide an exclusion list of hashes, no subportions of those files will ever be identified as detection patterns. The exclusion list allows you to optimize the patterns identified, to prevent false positives and to repeatedly iterate over the matches for a given session in order to improve the VTDIFF output. For certain less common file types the exclusion list is mandatory.

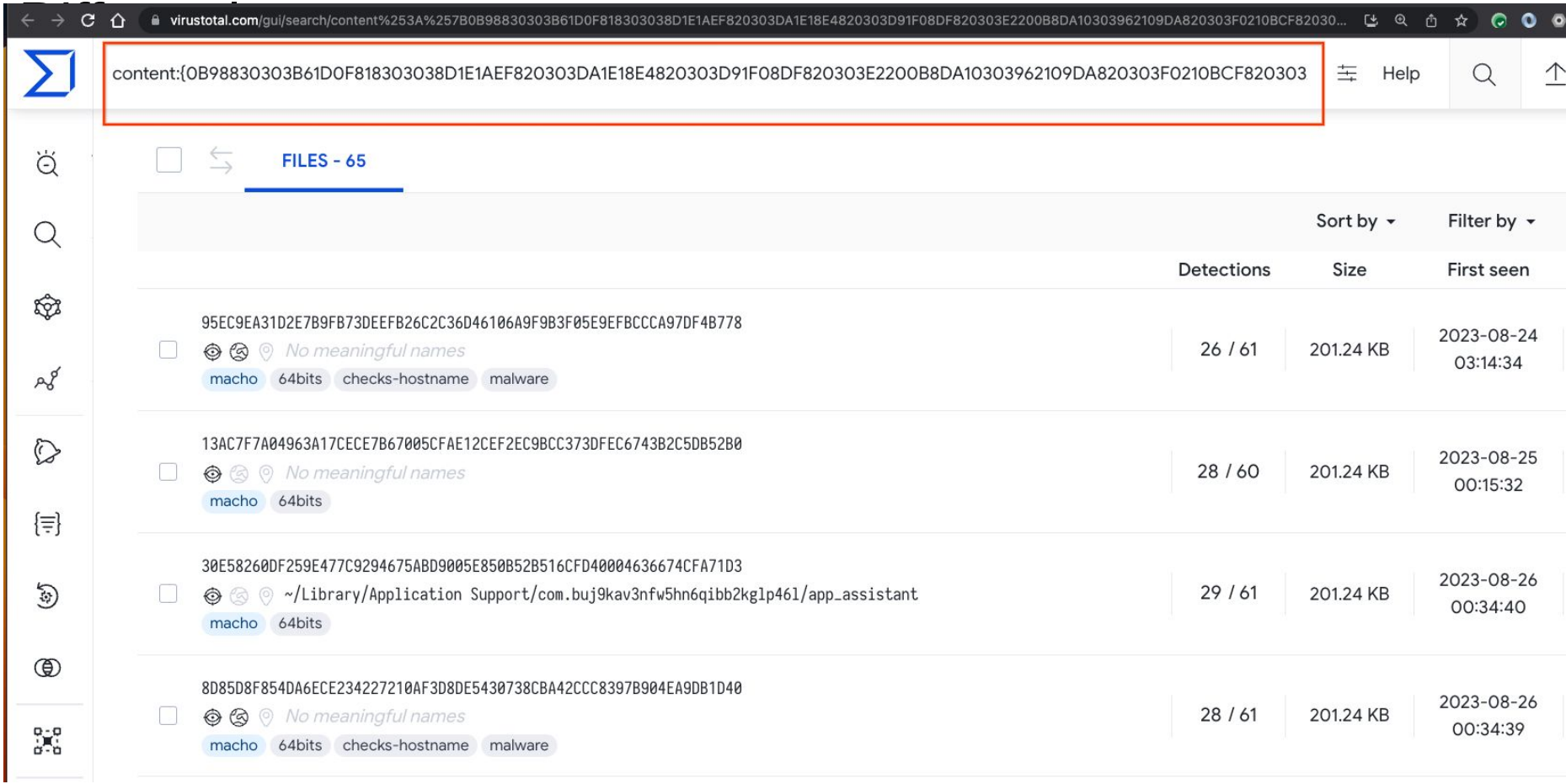
Cancel

Create

Diff result


12237663632 - DIFF PATTERNS 281
View
Filter by
Tools
Help
Matched bytes
Matches
Tags
0B 98 83 03 03 B6 1D 0F 81 83 03 03 8D 1E 1A EF
82 03 03 DA 1E 18 E4 82 03 03 D9 1F 08 DF 82 03
03 E2 20 0B 8D A1 03 03 96 21 09 DA 82 03 03 F0
21 0B CF 82 03 03 A2 22 18 C4 82 03 03 A1 23 08
BF 82 03 03 AA 24 0B D9 A0 03 03 DE 24 0C BA 82
03 03 BB 25 0C AF 82 03 03 BF 26 05 A4 82 03 03
F4 26 16 99 82 03 03 C2 27 08 8E 82 03 03 FB 27
05 B1 8C 03 03 9A 28 4F A9 A2 03 03 F0 28 13 B1
8C 03 03 9F 2A 09 ED 81 03 03 B3 2B 18 E2 81 03
03 B8 2C 08 DD 81 03 03 CA 2D 0B 9F A0 03 03 84
2E 0C D8 81 03 03 C7 2E 13 CD 81 03 03 DA 2E 0F
AE 81 03 03 E9 2E 24 91 81 03 03 B7 2F 18 8F 81
03 03 BC 30 08 8A 81 03 03 CE 31 0B E5 9F 03 03
88 32 0C 85 81 03 03 C4
216
13 / 20
Search for pattern in VT

Diff to content search



Wrapping up

while (1):

- Get context for a set of IOCs
- Identify the “interesting” ones
- Find anomalies and/or commonalities
- Pivot
- Update your set of IOCs

VirusTotal

Community

1. Submit new files
2. Comment on files
3. conact@virutotal.com to contribute crowdsourced:
    a. Add yara rule repositories
    b. Snort or Suricata Rules
    c. Sigma rules
    d. Any feedback, feature requests or bug reports.
4. https://www.virustotal.com/wargame/

VirusTotal

Happy Hunting

Karl Hiramoto
@karlhiramoto
karl.hiramoto@virustotal.com
October 2023

