

VirusTotal for Investigators

Brandon Levene, Juan Infantes, Jose Martin,
Julio Canto
VirusTotal

This session will demonstrate methods for using VirusTotal data to deep dive into malware campaigns. We will begin by exploring the design and implementation of the newest tools introduced to the VirusTotal arsenal: VTGrep and Graph. The workshop will then progress into discussion around how best to leverage the data available to VT users. By better understanding the breadth and depth of malicious campaigns, researchers and law enforcement can better investigate and mitigate impact. Recently introduced improved relational metadata as well as expanded retroactive and proactive hunting capabilities allow investigators to dive deep into malware within a global data source.

Objective:

Users will learn:

1. How to use VirusTotal Graph to visualize malware campaigns.
2. How to use VirusTotal Intelligence to identify interesting malware metadata.
3. How to use Yara for proactive and retroactive visibility.

Goals

- Discussion and Practical Application of Tools
 - Static Data Pivots
 - Faceted Search
 - VTGrep
 - VTGraph
 - YARA + VirusTotal Externals
- Highlight APIv3 Functionality



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

- 1) One Click Pivots and Visual Similarity Pivoting
- 2) VTGrep technical dive and functionality
- 3) VTGraph Technical dive and functionality
- 4) Yara guided rule dev, key modules, and practical examples
- 5) APIv3 New Go Tool (commandline) and functions
- 6) TEASERS

www.virustotal.com/gui/



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

<https://www.virustotal.com/subscription/event/klsas19/join>

00

VirusTotal Introduction

Introduction to VTE Functionality

What is VirusTotal Intelligence?

- VirusTotal Intelligence has been called the “Google of malware”
- VTI provides the ability to search through VT’s dataset using:
 - Binary properties
 - Detection verdicts/signatures
 - Static properties
 - Behavior patterns
 - Metadata
- Access via web interface or APIs



01

Faceted Search

Query Builder

File Type ▾ Detections or more ▾

Min. File size KB ▾ Max. File size KB ▾

Antivirus label contains...

Behavior report contains... File metadata contains...



Existing Search Modifiers:

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence>

Madlibs style guided query builder

Assumes all terms are AND

Faceted SEarches support OR queries as well!

Tips

<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Practice: <https://www.virustotal.com/wargame/>

Supports logical “AND” “OR” “NOT”

Respects order of operations: ()

Ranges can be denoted with + or -



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Practice makes perfect: <https://www.virustotal.com/wargame/>

Example 1

Find Windows Executables that communicate over HTTP



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

- Find Windows Executables that exhibit HTTP behaviors
 - (type:peexe OR type:pedll) behavior:http

Example 1

Key Search Terms:
type behavior

Find Windows Executables that communicate over HTTP



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

- Find Windows Executables that exhibit HTTP behaviors
 - (type:peexe OR type:pedll) behavior:http

Example 2

Find poorly detected Executables that use “fre.php” in their URI



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example 2

Find poorly detected Executables that use “fre.php” in their URI



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

Poorly Detected => Positives Ratio

Executables => Type

Uses => Behavior

- type:peexe behavior:fre.php p:10-

Example 2: Solution [Lokibot]

Find poorly detected Executables that use “fre.php” in their URI

p:10- type:peexe behavior:fre.php



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Show Results:

<https://www.virustotal.com/gui/search/p%253A10-%2520type%253Apeexe%2520behavior%253Afre.php/files>

Example 3

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



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Show Results:

<https://www.virustotal.com/gui/search/p%253A10-%2520type%253Apeexe%2520behavior%253Afre.php/files>

Example 3

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



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

Named => name:

With Macros => tag (static facet of file analysis)

From: => Submitter

Detections => p (or positives)

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

Example 3: Solution

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

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



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

<https://www.virustotal.com/gui/search/name%253A%2522invoice%2522%2520tag%253Amacros%2520p%253A5%252B%2520submitter%253AUS/files>

Key Terms:

Named => name:

With Macros => tag (static facet of file analysis)

From: => Submitter

Detections => p (or positives)

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

Example 4

Find files from domains containing “dropbox.com” or “box.com” with 10 or more detections



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

From Domains => itw

Detections => p

Example 4: Solution

Find files from domains containing “dropbox.com” or “box.com” with 10 or more detections

(itw:dropbox.com or itw:box.com) p:10+



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/\(itw%253Adropbox.com%2520or%2520itw%253Abox.com\)%2520p%253A10%252B/files](https://www.virustotal.com/gui/search/(itw%253Adropbox.com%2520or%2520itw%253Abox.com)%2520p%253A10%252B/files)

Key Terms:

From Domains => itw

Detections => p

- (itw:dropbox.com or itw:box.com) p:10+

Notice this shows all files, what if we want Windows Executables only?

Example 4a

Find Windows Executables from domains containing “dropbox.com” or “box.com” with 10 or more detections



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

Windows Executables => type

From Domains => itw

Detections => p

- (type:peexe OR type:pedll) (itw:dropbox.com or itw:box.com)
p:10+

Example 4a: Solution

Find Windows Executables from domains containing
“dropbox.com” or “box.com” with 10 or more
detections

(type:peexe OR type:pedll) (itw:dropbox.com OR itw:box.com) p:10+



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/\(type%253Apeexe%2520OR%2520type%253Apedll\)%2520\(itw%253Adropbox.com%2520or%2520itw%253Abox.com\)%2520p%253A10%252B/files](https://www.virustotal.com/gui/search/(type%253Apeexe%2520OR%2520type%253Apedll)%2520(itw%253Adropbox.com%2520or%2520itw%253Abox.com)%2520p%253A10%252B/files)

Key Terms:

Windows Executables => type

From Domains => itw

Detections => p

- (type:peexe OR type:pedll) (itw:dropbox.com or itw:box.com) p:10+

Example 4b

Find all files OTHER than Windows Executables from domains containing “dropbox.com” or “box.com” with 10 or more detections



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

Windows Executables => type

From Domains => itw

Detections => p

- (NOT type:peexe OR NOT type:pedll) (itw:dropbox.com or itw:box.com) p:10+

Example 4b: Solution

Find Windows Executables from domains containing
“dropbox.com” or “box.com” with 10 or more
detections
(NOT type:peexe AND NOT type:pedll) (itw:dropbox.com or
itw:box.com) p:10+



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/\(NOT%20type%253Apeexe%2520OR%2520NOT%2520type%253Apedll\)%2520\(itw%253Adropbox.com%2520or%2520itw%253Abox.com\)%2520p%253A10%252B/files](https://www.virustotal.com/gui/search/(NOT%20type%253Apeexe%2520OR%2520NOT%2520type%253Apedll)%2520(itw%253Adropbox.com%2520or%2520itw%253Abox.com)%2520p%253A10%252B/files)

Key Terms:

Windows Executables => type

From Domains => itw

Detections => p

- (NOT type:peexe AND NOT type:pedll) (itw:dropbox.com or itw:box.com) p:10+
- Technically the OR between the types is superfluous, because logic

Example 5

Find DLLs with Turla signature hits
first seen after March 1st, 2019



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Note we want to evaluate ALL engines for this signature string

Key Terms:

DLLs => type

signature hits => engines

First Seen = > fs

- engines:Turla type:pedll fs:2019-03-01+

If seeking from a specific AV scanner partner refer to the Full Vendor List:

a_squared
ad_aware
aegislab
agnitum
ahnlab
ahnlab_v3
alibaba
alyac
antivir
antivir7

antiy_avl
arcabit
authentium
avast
avast_mobile
avg
avira
avware
baidu
bitdefender
bkav
bytehero
cat_quickheal
clamav
cmc
commtouch
comodo
crowdstrike
cybereason
cylance
cyren
drweb
egambit
emsisoft
endgame
esafe
escan
eset_nod32
f_prot
f_secure
fortinet
gdata
ikarus
invincea
jiangmin
k7antivirus
k7gw
kaspersky
kingsoft
malwarebytes
max
mcafee
mcafee_gw_edition
microsoft
microworld_escan
nano_antivirus
nod32

norman
nprotect
paloalto
panda
pctools
prevx
prevx1
qihoo_360
rising
sentinelone
sophos
sunbelt
superantispyware
symantec
symantecmobileinsight
tencent
thehacker
totaldefense
trendmicro
trendmicro_housecall
trustlook
vba32
vipre
virobot
webroot
whitearmor
yandex
zillya
zonealarm
zoner

Example 5

Find DLLs with Turla signature hits first seen after March 1st, 2019

engines:Turla type:pedll fs:2019-03-01+



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

<https://www.virustotal.com/gui/search/engines%253ATurla%2520type%253Apedll%2520fs%253A2019-03-01%252B/files>

Key Terms:

DLLs => type

signature hits => engines

First Seen = > fs

■ engines:Turla type:pedll fs:2019-03-01+

Full Vendor List:

a_squared
ad_aware
aegislab
agnitum
ahnlab
ahnlab_v3
alibaba
alyac
antivir

antivir7
antiy_avl
arcabit
authentium
avast
avast_mobile
avg
avira
avware
baidu
bitdefender
bkav
bytehero
cat_quickheal
clamav
cmc
commtouch
comodo
crowdstrike
cybereason
cylance
cyren
drweb
egambit
emsisoft
endgame
esafe
escan
eset_nod32
f_prot
f_secure
fortinet
gdata
ikarus
invincea
jiangmin
k7antivirus
k7gw
kaspersky
kingsoft
malwarebytes
max
mcafee
mcafee_gw_edition
microsoft
microworld_escan
nano_antivirus

nod32
norman
nprotect
paloalto
panda
pctools
prevx
prevx1
qihoo_360
rising
sentinelone
sophos
sunbelt
superantispyware
symantec
symantecmobileinsight
tencent
thehacker
totaldefense
trendmicro
trendmicro_housecall
trustlook
vba32
vipre
virobot
webroot
whitearmor
yandex
zillya
zonealarm
zoner

Example 6

Find all RTF files with metadata containing "Windows User" that are using a known/identified CVE and NOT macros



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

files => type

metadata => metadata

known/identified => engines or tag

- metadata:"Windows User" type:rtf (tag:cve or engines:exploit or engines:cve) NOT tag:macros

Example 6

Find all RTF files with metadata containing “Windows User” that are using a known/identified CVE and NOT macros

```
metadata:"Windows User" type:rtf (tag:cve  
or engines:exploit or engines:cve) NOT  
tag:macros
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/metadata%253A%2522Windows%2520User%2522%2520type%253A%2520rtf%2520\(tag%253A%2520cve%2520or%2520engines%253A%2520exploit%2520or%2520engines%253A%2520cve\)%2520NOT%2520tag%253A%2520macros/files](https://www.virustotal.com/gui/search/metadata%253A%2522Windows%2520User%2522%2520type%253A%2520rtf%2520(tag%253A%2520cve%2520or%2520engines%253A%2520exploit%2520or%2520engines%253A%2520cve)%2520NOT%2520tag%253A%2520macros/files)

Key Terms:

files => type

metadata => metadata

known/identified => engines or tag

- metadata:"Windows User" type:rtf (tag:cve or engines:exploit or engines:cve) NOT tag:macros

Example 7

Find all document types using an exploit/or known CVE with RU lang encoding



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

files => type

known/identified => engines or tag

lang encoding => lang

- type:document (tag:cve or engines:exploit or engines:cve)
lang:ru
 - Note: Lang is available for peexe/pedll and office file formats ONLY

Example 7

Find all document types using an exploit/or known CVE with RU lang encoding

```
type:document (tag:cve or engines:exploit  
or engines:cve) lang:ru
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/type%253Adocument%2520\(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve\)%2520lang%253Aru%2520fs%253A2019-03-01%252B%2520ls%253A2019-03-15-/files](https://www.virustotal.com/gui/search/type%253Adocument%2520(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve)%2520lang%253Aru%2520fs%253A2019-03-01%252B%2520ls%253A2019-03-15-/files)

Key Terms:

files => type

known/identified => engines or tag

lang encoding => lang

first seen => fs

- type:document (tag:cve or engines:exploit or engines:cve)
lang:ru
 - Note: Lang is available for peexe/pedll and office file formats ONLY

Example 8

Find all document types using an exploit/or known CVE with RU lang encoding first seen between March 1st and March 15th

```
type:document (tag:cve or engines:exploit  
or engines:cve) lang:ru
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Key Terms:

files => type

known/identified => engines or tag

lang encoding => lang

- type:document (tag:cve or engines:exploit or engines:cve)
lang:ru fs:2019-03-01+ fs:2019-03-15-
 - Note: Lang is available for peexe/pedll and office file formats ONLY

Example 8

Find all document types using an exploit/or known CVE with RU lang encoding first seen between March 1st and March 15th

```
type:document (tag:cve or engines:exploit
or engines:cve) lang:ru fs:2019-03-01+
fs:2019-03-15-
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

[https://www.virustotal.com/gui/search/type%253Adocument%2520\(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve\)%2520lang%253Aru%2520fs%253A2019-03-01%252B%2520fs%253A2019-03-15-](https://www.virustotal.com/gui/search/type%253Adocument%2520(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve)%2520lang%253Aru%2520fs%253A2019-03-01%252B%2520fs%253A2019-03-15-)

Key Terms:

files => type

known/identified => engines or tag

lang encoding => lang

- type:document (tag:cve or engines:exploit or engines:cve)
lang:ru fs:2019-03-01+ fs:2019-03-15-
 - Note: Lang is available for peexe/pedll and office file formats ONLY

02

Static Data Pivoting

Assessing the “Details” Tab

The screenshot shows the VirusTotal interface for a file. At the top, a red circle indicates that 48 engines have detected the file. The file's SHA-256 hash is f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf. The file size is 552.38 KB and it was submitted on 2018-10-25 at 11:56:39 UTC. The file type is Win32 EXE. The 'Basic Properties' section lists various hashes and the file's magic bytes. The 'History' section shows the file's submission and analysis dates. The 'Names' section lists the file's name as Kidneys.exe.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
Basic Properties						
MD5	f0b2e393c18182c7bd48ce1f6e6c6765					
SHA-1	b6ea6907e036324b9595ef7d6a3f7ee05d37c5b					
SHA-256	f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf					
Authentihash	3d8871749d75f76677de18bfe87887aeafaf09460dafdeed13cdbc3183b968f					
Imphash	d0472d140aa0003beaf55821a63a5b03					
SSDEEP	6144yHo/cB8XBBAQ1rsU1XHBOOnVgdiv94pSpuOEz7HLYE/k4VQ/SXkillm:yt					
File type	Win32 EXE					
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit					
File size	552.38 KB (565637 bytes)					
Signature Info						
History						
Creation Time	2017-08-10 09:02:38					
First Seen In The Wild	2010-11-20 23:29:33					
First Submission	2018-06-16 21:32:54					
Last Submission	2018-10-25 11:56:39					
Last Analysis	2018-10-25 11:56:39					
Names						
f0b2e393c18182c7bd48ce1f6e6c6765.vir						
Kidneys						
Kidneys.exe						



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Let's look at a Trickbot Sample:

f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf

<https://www.virustotal.com/gui/file/f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf/detection>

Example: Pivot on Imphash

48 / 67
Community Score

48 engines detected this file

f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf
f0b2e393c18182c7bd48ce1f6e6c6765.vir

552.38 KB
Size

2018-10-25 11:56:39 UTC
1 month ago

overlay peexe

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Basic Properties

MD5	f0b2e393c18182c7bd48ce1f6e6c6765
SHA-1	b6ea6907e036324b9595ef7d6a3f7ee05d37c5b
SHA-256	f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf
Authenticating hash	3d8871749d75f76677de18bfe87887aeafaf09460dafdeed13cdbc3183b968f
Imphash	d0472d140aa0003beaf55821a63a5b03
SSDEEP	6144yHo/cB8XBBAQ1rsU1XHbOnVgdiv94pSpuOEz7HLYE/k4VQ/SXkilmy:
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	552.38 KB (565637 bytes)

Signature Info

History

Creation Time	2017-08-10 09:02:38
First Seen In The Wild	2010-11-20 23:29:33
First Submission	2018-06-16 21:32:54
Last Submission	2018-10-25 11:56:39
Last Analysis	2018-10-25 11:56:39

Names

- f0b2e393c18182c7bd48ce1f6e6c6765.vir
- Kidneys
- Kidneys.exe



imphash:"d0472d140aa0003beaf55821a63a5b03" (Anchor Trickbot)

<https://www.virustotal.com/gui/search/imphash%253A%2522d0472d140aa0003beaf55821a63a5b03%2522/files>

imphash:"d0472d140aa0003beaf55821a63a5b03"

FILES 8

COMMONALITIES

<input type="checkbox"/>	2aafd61ac7974a25c52faa0c66c88b472fb74f96964495799fb6c9028692c974 Kidneys.exe	51 / 68	552.38 KB	2019-03-13 14:30:17 first seen 2019-03-13 14:30:17 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fd Kidneys.exe	48 / 67	552.38 KB	2018-06-16 21:32:54 first seen 2018-10-25 11:56:39 last seen	2 submissions 2 submitters	
<input type="checkbox"/>	5eef1a0ff040799b65d7a6f4e45a3d478aabcee79b458b7aa4ce93678a81ea94 Kidneys.exe	42 / 68	552.38 KB	2018-09-20 13:27:45 first seen 2018-09-20 13:27:45 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	9e72e130898ab79c26c264775ec2eccc514a823212f8131af9a44477c38091 Kidneys.exe	47 / 66	552.38 KB	2017-08-10 09:15:21 first seen 2018-05-21 09:56:30 last seen	4 submissions 3 submitters	
<input type="checkbox"/>	ae6e8c24adf73a20e4dff0260dc6ec33042b423fcd921c350f355f61aaf70dce Kidneys.exe	47 / 67	552.38 KB	2017-08-11 13:18:48 first seen 2018-05-18 21:09:06 last seen	2 submissions 2 submitters	
<input type="checkbox"/>	923fcb901116fdecae68cfa461ab9c9064385fd2b9b206b3ba011e5008fe37b3 Kidneys.exe	46 / 66	552.38 KB	2018-01-15 21:12:21 first seen 2018-05-14 10:33:15 last seen	2 submissions 2 submitters	
<input type="checkbox"/>	51b7a2b25965251bcd2ad580b7037919158d431228af1417b3aad47fa19a332 Kidneys.exe	24 / 65	552.38 KB	2017-08-11 11:44:05 first seen 2017-08-11 11:44:05 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	c5eae65e0ce1325b79771f1a54bb2664e5e09139ced0eccd6e035cab1c7d09c45 Kidneys.exe	51 / 65	552.38 KB	2017-08-11 10:13:35 first seen 2017-08-11 10:13:35 last seen	2 submissions 1 submitters	

imphash:"d0472d140aa0003beaf55821a63a5b03" (Anchor Trickbot)

<https://www.virustotal.com/gui/search/imphash%253A%2522d0472d140aa0003beaf55821a63a5b03%2522/files>

Caveat: Imphash is NOT Always Reliable



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

- Example UPX packed files: section:upx1 section:upx0
- imphash:"7326001be3ced77b153640be93a8dff6"

Example:

175bafbcd5218e062619b16dd4c18279635ae3d621daa7aa559a3ca5882ebf1c

<https://www.virustotal.com/gui/search/imphash%253A%2527326001be3ced77b153640be93a8dff6%2522/files>

TLDR: You're actually matching the packer.

Similar-To (vhash)

similar-to:f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf

FILES 40+

<input type="checkbox"/>	719d15bc6874277ad6c62521064b9a8afeb7243acaa864e9cb1c1d53c7f6fed	PDFProfitLock.ext	peexe overlay	13 / 68	518.08 KB
<input type="checkbox"/>	4c8afd43ca299b2853928bd38f90fdc74291d2a3f8810a5b6574ef1cda71690e	PDFProfitLock.ext	peexe overlay	12 / 65	530.49 KB
<input type="checkbox"/>	2aafd61ac7974a25c52faa0c66c88b472fb74f96964495799fb6c9028692c974	Kidneys.exe	peexe overlay	53 / 69	552.38 KB
<input type="checkbox"/>	b988c65c1f015491a0049c1e8e5becf303644efc83826133354d2735a0395721	Uninstaller.exe	peexe	25 / 65	540 KB
<input type="checkbox"/>	be69330bb44534fe4feb56f4d855971172ba8a8b5f9c98f9feea7e1417a0cf34	AREMAIN9.EXE	peexe	4 / 68	552 KB



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

<https://www.virustotal.com/gui/search/similar-to%253Af579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf/files>

Lets check out our trickbot sample that we explored imphash with:

similar-to:f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf

Notice how many more results there are?

Visual Similarity

Supports:

- Windows Executables (embedded)
- PDF
- Office Documents



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Julio To Talk about how it works

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

-alternative mechanism:

resource:"77073160cc8d0c6443a55cf6514f3606d979ca8ce78a1a9cc20ec71c57e392d6"

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f7f27be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9efff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Visual Similarity: EXE



main_icon_dhash:b168c6a98ee460b2

FILES 20+						
<input type="checkbox"/>	13655185bac5e8ad856c3fd2ab93ba2af112a181f14ce66d22214b006b164ee8 Runtime Library peexe overlay	31 / 68	672.39 KB	2019-03-20 12:30:38 first seen 2019-03-20 12:30:38 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	de9d80a37b2179e2e994055c5f588156c16ed66568142b49e2aed36a6a65945 Runtime Library peexe overlay	43 / 65	556 KB	2019-03-17 19:10:51 first seen 2019-03-20 12:00:10 last seen	2 submissions 2 submitters	
<input type="checkbox"/>	a498aa74340381622ac341543e80de9f73beab9c7dd7cf68ea225aef6ff9efc Runtime Library peexe	42 / 68	2.96 MB	2019-03-15 15:54:58 first seen 2019-03-20 11:30:57 last seen	2 submissions 2 submitters	
<input type="checkbox"/>	5155f749eb8977650b92393e84d368cc76dee1908514bc42d5a423afbc7ba260 Runtime Library peexe overlay	29 / 65	668.5 KB	2019-03-20 11:18:44 first seen 2019-03-20 11:18:44 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	e780c9aa68787ad4d62e71c382f21b985a85112a2246b675d92e3d5277f5de Runtime Library peexe overlay	47 / 71	578.99 KB	2019-03-17 19:15:05 first seen 2019-03-20 11:02:11 last seen	2 submissions 2 submitters	



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

-alternative mechanism:

resource:"77073160cc8d0c6443a55cf6514f3606d979ca8ce78a1a9cc20ec71c57e392d6"

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f727be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9efff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Visual Similarity: PDF

Your Citibank, N.A. Account Has Been Suspended

We have temporarily suspended your Citibank, N.A. account for the funds transfer service.

Here are your account details:

<https://securemail.citibank.com/privacy/securereader?id=64124813498052&brand=95642159>.

Please contact Member Services to re-activate your suspended account.

Sincerely,

Member Services

Email ID: 431

<https://www.Citibank.com/>



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

PDF Preview Render

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f7f27be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9efff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Visual Similarity: PDF



main_icon_dhash:2313230300020000

FILES 20+						
<input type="checkbox"/>	944d60d78cea444fe42499abb7d2c6304296447c769e7cb583c369511d69cf5 WellsFargo Instr SUK 2702638.pdf	8 / 60	37.57 KB	2019-03-19 21:37:51 first seen 2019-03-19 21:37:51 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	26c093074ec4f0bf1ea5863c0e88cff700a445e81b249ea608f28c2d736c63d file_name	16 / 56	32.39 KB	2019-03-05 16:33:28 first seen 2019-03-19 09:45:34 last seen	20 submissions 12 submitters	
<input type="checkbox"/>	45ce591e001e8de4f5e1fd19ec8a29fb63ca3d47ed63cda604d806eaa96d29e	8 / 55	35.04 KB	2019-03-19 01:14:15 first seen 2019-03-19 01:14:15 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	6219dc8787ddb49b383e19d9da2b6758207e1d25dc32863722cdd1dcbcd8ba6	6 / 56	31.51 KB	2019-03-19 01:12:40 first seen 2019-03-19 01:12:40 last seen	1 submissions 1 submitters	
<input type="checkbox"/>	e876d50e96bcf114f116102d2eb7c7adf4030e0fa7729388af8e697d2a2e6d2a Citigroup Instr YAD 59365931.pdf	8 / 60	35.07 KB	2019-03-19 00:13:52 first seen 2019-03-19 00:13:52 last seen	1 submissions 1 submitters	



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Pivoting on the PDF Visual Similarity

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f7f27be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9efff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Visual Similarity: Office Documents



Protected Document

Loading content ...

Note: If you have problems viewing/loading secure document content please select "Enable Editing" and then "Enable Content" button.



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f7f27be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9eff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Visual Similarity: Office Documents



main_icon_dhash:0103001101000301

FILES 2

<input type="checkbox"/>	85f7ab110807cf0352ada5582611cc64af0e13ad8f32561d3e2c2763a70659c3	33 / 56	46.02 KB	2019-03-12 14:10:29 first seen 2019-03-12 14:10:29 last seen
	doc macros obfuscated run-file			
<input type="checkbox"/>	2db7425c7c9eff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45 ADP-Document-3810922.doc	43 / 60	46 KB	2018-07-19 16:31:07 first seen 2018-07-30 04:48:49 last seen
	doc attachment macros obfuscated run-file 🔒			



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbefe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

Emotet PDF:

<https://www.virustotal.com/gui/file/8c15b770e32ff70527a4e17e1173d3f2ff91f7f27be17268f2a814c72d863859/detection>

ADP Lure Doc:

<https://www.virustotal.com/gui/file/2db7425c7c9eff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

Signature Data

Signers

ALISA LTD

Name	ALISA LTD
Status	Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Valid	12:00 AM 02/22/2019
From	
Valid To	11:59 PM 02/21/2020
Valid	Code Signing
Usage	
Algorithm	sha256RSA
Serial	5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B
Number	



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

LockerGoga:

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

<https://www.virustotal.com/gui/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection>

Signature Data

Signature Verification

 File signature could not be verified

File Version Information

Copyright	Copyright (C) ALISA LTD 2019
Product	Service zzbdrimp
Description	Background Tasks Host
Original Name	zzbdrimp
Internal Name	zzbdrimp
File Version	1.4.4.0
Date signed	8:40 PM 3/20/2019



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

LockerGoga:

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

<https://www.virustotal.com/gui/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection>

Signature Data

Pivot Options:

- Broad = signature:"ALISA LTD"
- Narrow = signature:"5D A1 73 EB 1A
C7 63 40 AC 05 8E 1F F4 BF 5E 1B"



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

LockerGoga:

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

<https://www.virustotal.com/gui/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection>

By Name of Signer:

Broad => signature:"ALISA LTD"

BY Cert Hash

Narrow => signature:"5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B"

Signature Data

signature:"5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B" OR signature:"ALISA LTD"

<input type="checkbox"/>	FILES 5			
<input type="checkbox"/>	88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f tgytutrc	41 / 66	1.21 MB	peexe overlay
<input type="checkbox"/>	c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15 tgytutrc	39 / 66	1.21 MB	peexe overlay revoked-cert signed
<input type="checkbox"/>	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26 zzbdriimp	47 / 71	1.19 MB	peexe overlay revoked-cert signed
<input type="checkbox"/>	ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f imtvknqq	43 / 70	1.19 MB	peexe overlay revoked-cert signed
<input type="checkbox"/>	eda26a1cd80aac1c42cdbba9af813d9e4bc81f6052080bc33435d1e076e75aa0 yxugwjud	43 / 67	1.2 MB	peexe overlay revoked-cert signed



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

LockerGoga:

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

<https://www.virustotal.com/gui/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection>

By Name of Signer:

Broad => signature:"ALISA LTD"

BY Cert Hash

Narrow => signature:"5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B"

Combine the Two:

<https://www.virustotal.com/gui/search/signature%253A%25225D%2520A1%252073%2520EB%25201A%2520C7%252063%252040%2520AC%252005%25208E%25201F%2520F4%2520BF%25205E%25201B%2522%2520OR%2520signature%253A%2522ALISA%2520LTD%2522/files>

Note: In this instance the signer and hash were only used together, so you'll get the same results with either query.

Signature Data

signature:"Copyright (C) ALISA LTD 2019"

<input type="checkbox"/>	FILES 5			
<input type="checkbox"/>	88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c9193995af496a0f	tgylutrc	45 / 71	1.21 MB
		peexe overlay		
<input type="checkbox"/>	c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	tgylutrc	44 / 71	1.21 MB
		peexe overlay revoked-cert signed		
<input type="checkbox"/>	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c8dd26	zzbdriimp	47 / 71	1.19 MB
		peexe overlay revoked-cert signed		
<input type="checkbox"/>	ba15c2726265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057193f	imtknqq	45 / 71	1.19 MB
		peexe overlay revoked-cert signed		
<input type="checkbox"/>	eda26a1cd80aac1c42cbbba9af813d9c4bc8116052080bc33435d1e076e75aa0	yxugvjwad	46 / 70	1.2 MB
		peexe overlay revoked-cert signed		



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

LockerGoga:

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

<https://www.virustotal.com/gui/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection>

There is another option as well that leverages the structure within the PE itself with contains additional signature information:

signature:"Copyright (C) ALISA LTD 2019"

[https://www.virustotal.com/gui/search/signature%253A%2522Copyright%2520\(C\)%2520ALISA%2520LTD%25202019%2522/files](https://www.virustotal.com/gui/search/signature%253A%2522Copyright%2520(C)%2520ALISA%2520LTD%25202019%2522/files)

Metadata? MetaData? Meta-Data? Meta Data?

ExifTool File Metadata ⓘ

AppVersion	16.0
Author	cobalt
CharCountWithSpaces	34
Characters	30
CodePage	Windows Latin 1 (Western European)
CompObjUserType	Document Microsoft Word 97-2003
CompObjUserTypeLen	32
CreateDate	2018:10:30 23:22:00
DocFlags	Has picture, 1Table, ExtChar
FileType	DOC
FileTypeExtension	doc
HeadingPairs	Titre, 1
HyperlinksChanged	No



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

I have no idea what the convention is for this word, ya'll know what I mean.

This is data generated from Exiftool.

EmpireMonkey:

d57f128afb4843b6f0072fadda8dd14046b31703098e365bc5a226e117090d44

Metadata? MetaData? Meta-Data? Meta Data?

metadata:"Normal.dotm" and metadata:"cobalt"

The screenshot shows a VirusTotal search results page. At the top, it says 'FILES 36'. Below this, there are three file entries:

- File 1: ID 6cc84b3a58eea27e84f489b9bde5ac81fb0f05db6cd9327b26ffb776ad53288, filename PO-2815.doc, size 147 KB, detection 25 / 59. Tags: doc, copy-file, create-file, create-ole, environ, hide-app, macros, obfuscated.
- File 2: ID 728bbbea8797c5e00a8737ebf6bebfff3d84f9c86f144963a2940025329c28b, filename complaint-143.doc, size 91.5 KB, detection 35 / 56. Tags: doc, create-file, create-ole, environ, macros, run-dll, run-file.
- File 3: ID 59a24d9ac0ed2f2bea3883d7b943ab1229acfe3f9f350f2dee6deb14c559920b, filename document.doc, size 35.5 KB, detection 15 / 60. Tags: doc, create-ole, environ, hide-app, macros, obfuscated, open-file, write-file. A 'Download' button is visible.

The VirusTotal logo is in the bottom right corner.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

I have no idea what the convention is for this word, ya'll know what I mean.

This is data generated from Exiftool.

EmpireMonkey:

d57f128afb4843b6f0072fadda8dd14046b31703098e365bc5a226e117090d44

metadata:"Normal.dotm" and metadata:"cobalt"

<https://www.virustotal.com/gui/search/metadata%253A%2522Normal.dotm%2522%2520and%2520metadata%253A%2522cobalt%2522/files>

Metadata? MetaData? Meta-Data? Meta Data?

metadata:"Background Tasks Host"

<input type="checkbox"/>	FILES 5		
<input type="checkbox"/>	88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f	44 / 69	1.21 MB
<input type="checkbox"/>	tgylutrc		
	peexe overlay		
<input type="checkbox"/>	c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	42 / 69	1.21 MB
<input type="checkbox"/>	tgylutrc		
	peexe overlay revoked-cert signed		
<input type="checkbox"/>	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26	47 / 71	1.19 MB
<input type="checkbox"/>	zzbdrimp		
	peexe overlay revoked-cert signed		



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

I have no idea what the convention is for this word, ya'll know what I mean.

This is data generated from Exiftool.

Example 2: LockerGoga,

<https://www.virustotal.com/gui/file/88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f/detection>

metadata:"Background Tasks Host"

<https://www.virustotal.com/gui/search/metadata%253A%2522Background%2520Tasks%2520Host%2522/files>

Imports and Exports

Imports

- + ADVAPI32.dll
- + KERNEL32.dll
- + RPCRT4.dll
- + ntdll.dll

Exports

- DhcpNewPktHook
- DhcpServerCalloutEntry
- DnsPluginCleanup
- DnsPluginInitialize
- DnsPluginQuery
- ExtensionApiVersion
- InitializeChangeNotify
- PasswordChangeNotify
- SpLsaModelInitialize
- WinDbgExtensionDllInit



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example: Mimikatz

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Imports and Exports

imports:NdrMesTypeFree2 imports:MesHandleFree imports:RtlStringFromGUID imports:GetOEMCP

FILES 20+	
<input type="checkbox"/>	<p>b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4 mimilib.dll</p> <p>pedll 64bits assembly</p>
<input type="checkbox"/>	<p>f6413029e7a43d7eb5d44772efb413553e8896c2b287dd41de2fa380c58e611c mimilib.dll</p> <p>pedll</p>
<input type="checkbox"/>	<p>4a5ebda8ec96e7d3f1a976d748e7e42f95e46f9d46c360b886d13ee4212a6fa0 mimilib.dll</p> <p>pedll</p>



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example: Mimikatz

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Imports=> imports:NdrMesTypeFree2 imports:MesHandleFree

imports:RtlStringFromGUID imports:GetOEMCP




Exports => exports:"InitializeChangeNotify" exports:"PasswordChangeNotify"

exports:"SpLsaModelInitialize"

Imports and Exports

exports:"InitializeChangeNotify" exports:"PasswordChangeNotify" exports:"SpLsaModelInitialize"

FILES 20+

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4    30 / 63 120.5 KB
mimilib.dll 
pedll 64bits assembly

8615af1d78a23a4be6cf8775052bf1b4fb122e48c81bf415a251d2cf9102f4c0
w1and1g.dll 8 / 67 68.5 KB
pedll 64bits assembly

f6413029e7a43d7eb5d44772efb413553e8896c2b287dd41de2fa380c58e611c
mimilib.dll 37 / 69 104.5 KB
pedll



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example: Mimikatz

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Imports=> imports:NdrMesTypeFree2 imports:MesHandleFree
imports:RtlStringFromGUID imports:GetOEMCP

Exports => exports:"InitializeChangeNotify" exports:"PasswordChangeNotify"
exports:"SpLsaModelInitialize"

03

VTGrep

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

VTGrep (aka Content Search)

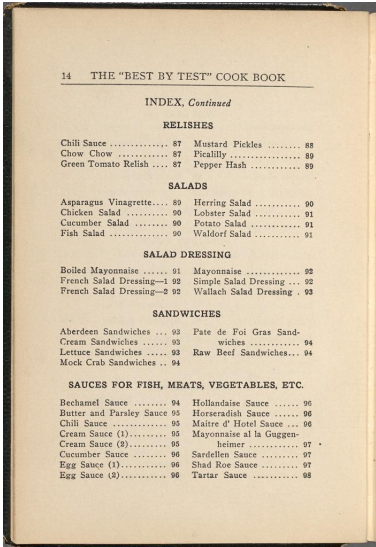
Use the “content:” search modifier to search for arbitrary hex or string patterns within files on VirusTotal



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

VTGrep (aka Content Search)

- VTGrep is an index of 32bit substrings to sample IDs (SHA256)
- It returns all the samples with the given content in less than 60 seconds
- It supports most YARA's string conditions
 - Wildcards, UTF-8, HEX, offsets, AND, OR, ...
 - No regexps, though :-(
- Great for prototyping Retrohunts
- It uses Google infrastructure to serve 1PB of compressed data (all samples uploaded to VT in a year)
 - Includes unpacked, OCR, macros, VBA code streams...



14 THE "BEST BY TEST" COOK BOOK

INDEX, *Continued*

RELISHES

Chili Sauce 87 Mustard Pickles 88
Chow Chow 87 Picallily 89
Green Tomato Relish 87 Pepper Hash 89

SALADS

Asparagus Vinagrette... 89 Herring Salad 90
Chicken Salad 90 Lobster Salad 91
Cucumber Salad 90 Potato Salad 91
Fish Salad 90 Waldorf Salad 91

SALAD DRESSING

Boiled Mayonnaise 91 Mayonnaise 92
French Salad Dressing—1 92 Simple Salad Dressing ... 92
French Salad Dressing—2 92 Wallach Salad Dressing . 93

SANDWICHES

Aberdeen Sandwiches ... 93 Pate de Foi Gras Sand-
wiches 94
Cream Sandwiches 93 wiches 94
Lettuce Sandwiches 93 Raw Beef Sandwiches... 94
Mock Crab Sandwiches . 94

SAUCES FOR FISH, MEATS, VEGETABLES, ETC.

Bechamel Sauce 94 Hollandaise Sauce 96
Butter and Parsley Sauce 95 Horseradish Sauce 96
Chili Sauce 95 Maitre d' Hotel Sauce ... 96
Cream Sauce (1) 95 Mayonnaise a la Guggen-
heim 97
Cream Sauce (2) 95
Cucumber Sauce 96 Sardellen Sauce 97
Egg Sauce (1) 96 Shad Roe Sauce 97
Egg Sauce (2) 96 Tartar Sauce 98



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

VTGrep: Example 1, ASCII Strings



The screenshot shows the VirusTotal interface for a file. The 'CONTENT' tab is selected, and the 'STRINGS' sub-tab is active. The following strings are listed:

```
cmd.exe %s%s"  
D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb  
kernel32.dll  
ADVAPI32.dll  
KERNEL32.dll  
kernel32.dll  
mscoree.dll
```

The VirusTotal logo is visible in the bottom right corner of the interface.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Trickbot: 5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

There appears to be a PDB! I love PDBs.





“Program database (**PDB**) is a proprietary file format (developed by Microsoft) for storing debugging information about a program (or, commonly, program modules such as a DLL or **EXE**). **PDB** files commonly have a **.pdb** extension. A **PDB** file is typically created from source files during compilation.”

Wouldn't it be cool if we could find more samples that contain this PDB string? Maybe the attackers left something behind!

VTGrep: Example 1, ASCII Strings

content:D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb

FILES 7

<input type="checkbox"/>	96e484009a93c796c2a405b5375b5b054abd3b5579d9f493d4f97a31aecf8b6b	45 / 68	698 KB
	peexe 		
<input type="checkbox"/>	5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399	46 / 66	390 KB
	testtab.png		
	peexe  		
<input type="checkbox"/>	3e0b63b51df79e2f40b7a775d1d353d68594eef3617afd56804ac00775754d89	54 / 69	394 KB
	peexe 		



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Trickbot: 5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

Oho there appears to be a PDB! I love PDBs.

“Program database (**PDB**) is a proprietary file format (developed by Microsoft) for storing debugging information about a program (or, commonly, program modules such as a DLL or **EXE**). **PDB** files commonly have a **.pdb** extension. A **PDB** file is typically created from source files during compilation.”

Wouldn't it be cool if we could find more samples that contain this PDB string? Maybe the attackers left something behind!

We can!

Two ways:

- 1) Click on the string in the “Content” tab to generate a query in Hex
 - a) `content:{443a5c4d7950726f6a656374735c7365636f6e64576f726b5c416e63686f725c57696e33325c52656c656173655c616e6`

- a) 3686f72496e7374616c6c65725f7838362e706462}
- 2) For an ASCII string search
 - a) content:D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb

These methods are functionally identical.

Bonus:

we can actually find more of this by shortening the string to not be SO specific:

- content:D:\MyProjects\secondWork\Anchor\Win32\Release

VTGrep: Example 2 Wildcards

```
content:D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Wildcarding

Trickbot: 5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb

What if we weren't sure about that D:\ path or the target compile platform

```
{???3a5c4d7950726f6a656374735c7365636f6e64576f726b5c416e63686f725c57696e  
????5c52656c656173655c}
```

We'll truncate it a bit more to remove the very specific build path:

```
?:\MyProjects\secondWork\Anchor\Win??\Release\
```

where ? represents a single character value

VTGrep: Example 2, Wildcards

```
content:{??3a5c4d7950726f6a656374735c7365636f6e64576f726b5c416e63686f725c57696e????5c52656c656173655c}
```

FILES 17			
<input type="checkbox"/>	18d347001057c68c4f2ad1d2f5af73e2dfa69aa46466fa43b40d7da360b79c01 1fe7f68f073ebf9162f1a46a5d45d43c.virus	41 / 69	140.5 KB
	pedli		
<input type="checkbox"/>	a38567922a6424b4821569805aa74cd28e124985cfd0d1838cc797568f6ba90c c2.dll	20 / 68	134.5 KB
	pedli		
<input type="checkbox"/>	96e484009a93c796c2a405b5375b5b054abd3b5579d9f493d4f97a31aecf8b6b	45 / 68	698 KB
	peexe		
<input type="checkbox"/>	191c372af20a9affa1f9acb522cb7af2e0b3cd0d38e4a88c1c2224a75ac35ded netnsgwv.dll	30 / 67	133 KB
	pedli		
<input type="checkbox"/>	5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399 testtab.png	46 / 66	390 KB
	peexe		



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Wildcarding

Trickbot: 5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

D:\MyProjects\secondWork\Anchor\Win32\Release\anchorInstaller_x86.pdb

What if we weren't sure about that D:\ path or the target compile platform

```
{??3a5c4d7950726f6a656374735c7365636f6e64576f726b5c416e63686f725c57696e  
????5c52656c656173655c}
```

We'll truncate it a bit more to remove the very specific build path:

```
?:\MyProjects\secondWork\Anchor\Win??\Release\
```

where ? represents a single character value

VTGrep: Example 3, Unicode

The screenshot shows the VirusTotal VTGrep interface. At the top, there are tabs for DETECTION, DETAILS, RELATIONS, CONTENT, SUBMISSIONS, and COMMUNITY. Below these, there are tabs for STRINGS and HEX. The main content area displays a list of strings extracted from a file. One string is highlighted in red: "%s",AfxGetHttpRequestMgr %s. To the right of the list, there are controls for sorting (down arrow, 1/9), a star icon, and buttons for ALL, ASCII, and WIDE. A blue 'WIDE' button is also shown below the zoomed-in string view. The VirusTotal logo is in the bottom right corner.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Unicode

Bookworm: b2737192ea1c912daa3ca4c43224fb6afcc878c5e3303e86a459de06df7af33f

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

"%s",AfxGetHttpRequestMgr %s => string of interest... but its in Unicode

Full String

content:{22002500730022002c00410066007800470065007400480074007400700052006500710075006100730074004d0067007200200025007300}

<https://www.virustotal.com/gui/search/content:%7B22002500730022002c00410066007800470065007400480074007400700052006500710075006100730074004d0067007200200025007300%7D/files>

Common strings at the beginning and end will typically be skipped:

Fixed

content:{410066007800470065007400480074007400700052006500710075006100730074004d00670072}

<https://www.virustotal.com/gui/search/content%253A%257B410066007800470065007400480074007400700052006500710075006100730074004d00670072%257D>

VTGrep: Example 3, Unicode

content:{22002500730022002c00410066007800470065007400480074007400700052006100710075006500730074004d0067007200}

FILES 4			
<input type="checkbox"/>	b2737192ea1c912daa3ca4c43224fb6afcc878c5e3303e86a459de06df7af33f HYPERTRM.dll	47 / 69	1.04 MB
<input type="checkbox"/>	b3ed50daf7b7285122573eec71fdba744a796b6d55a861efd96bb5cd7520b32d virussign.com_4dfa2f7a5138b9b158ecf9bbc65906e0.vir	35 / 61	931.5 KB
<input type="checkbox"/>	dc0e869bfbdbdeb1d4300e5ed57f347c53698107f30e4753ed4b1078ac1f99008 b50e5fa05e9e995067226403d245afef	27 / 66	1.04 MB
<input type="checkbox"/>	33b8bf2c05a88afaf175fe58c0e2f87158f21110a050f48620bba057a137c18 97e4973c618813ba75014fe4d7f4dbcd379a9795	45 / 67	931.5 KB



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Unicode

Bookworm: b2737192ea1c912daa3ca4c43224fb6afcc878c5e3303e86a459de06df7af33f

<https://www.virustotal.com/gui/file/5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399/detection>

"%s",AfxGetHttpRequastMgr %s => string of interest... but its in Unicode

We can just click on the string :-)

Full String

content:{22002500730022002c00410066007800470065007400480074007400700052006500710075006100730074004d0067007200200025007300}

<https://www.virustotal.com/gui/search/content:%7B22002500730022002c00410066007800470065007400480074007400700052006500710075006100730074004d0067007200200025007300%7D/files>

Fixed

content:{410066007800470065007400480074007400700052006500710075006100730074004d00670072}

<https://www.virustotal.com/gui/search/content%253A%257B410066007800470065007400480074007400700052006500710075006100730074004d00670072%257D>

VTGrep: Example 4, Logical “AND”

```
logout.log      CPU: %s(%d)  RAM: %lld Mb
WS2_32.dll      cmd /c %s
logout.log      %s %s: %s
ntdll.dll       %s %s: %s
cbomb.dat       GET /%s
data.dat        Host:%s
```



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Example:

Rietspoof:

f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96 (bot)

These strings seem to be relatively common on their own... Can we combine them somehow?

VTGrep: Example 4, Logical “AND”

```
content:"logout.log" AND content:"data.dat" AND content:"RAM: "
```

FILES 9+

<input type="checkbox"/>	f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96 iSatSrv.exe	41 / 71	2.29 MB
	peexe overlay signed		
<input type="checkbox"/>	ac46be54c303002d74df6c975083c706b3e1cb8a92e75516579cd0fe65ce918 iSatSrv.exe	30 / 65	192.06 KB
	peexe overlay revoked-cert signed		
<input type="checkbox"/>	3bc3552b1701280d0fa1c534901c0b926fef61314a1e76eaa7f9623054225633 windmhp.exe	30 / 65	200.21 KB
	peexe overlay revoked-cert signed		



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Note: The “AND” is implied by spaces and is present by convention in this example. It is not necessary to specify AND between terms.

Example:

Rietspoof:

f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96 (bot)

These strings seem to be relatively common on their own... Can we combine them somehow?

Yup we can!

```
content:"logout.log" AND content:"data.dat" AND content:"RAM: "
```

```
(content:{52 41 4d 3a 20} AND content:{64 61 74 61 2e 64 61 74} AND content:{6c 6f 67 6f 75 74 2e 6c 6f 67})
```

VTGrep: Example 5, Logical “OR”

FirstStageDropper.dll is responsible for injecting **SecondStageDropper.dll** into another process to execute it. While the shellcode payload only contains code to search for and bypass EMET, **FirstStageDropper.dll** also contains code for Kaspersky and Bitdefender. In case of EMET, it searches the loaded modules for **emet.dll** and **emet64.dll**, for Kaspersky it searches for **klshk.dll**, and for Bitdefender it searches for **avcuf32.dll** and **avcuf64.dll**. It also collects and sends encrypted user system and process information data together with a unique hardcoded ID to the attacker's server. The data is sent to URLs that contain **“/home/”** and **“/log/”** directories and for encryption it uses the Rijndael algorithm. As the attacker server did not respond at the time of our analysis, we guess a command is sent back to execute the **SecondStageDropper.dll**.



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Chainshot:

<https://unit42.paloaltonetworks.com/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/>

Can we use the data from this report to find samples of Chainshot?

Yup we can!

VTGrep: Example 5, Logical “OR”

```
content:FirstStageDropper.dll OR content:SecondStageDropper.dll
```

FILE	STATUS	SIZE
<input type="checkbox"/> feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713 ...fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713.sample	pedll 64bits assembly cve-2018-5002 exploit	29 / 70 194.5 KB
<input type="checkbox"/> 3485c9b79dfd3e00aef9347326b9ccfee588018a608f89ecd6597da552e3872f	pedll 64bits assembly cve-2018-5002 exploit overlay	44 / 69 194.5 KB
<input type="checkbox"/> a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23 c:\foo.bar	pedll	48 / 70 370 KB



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Chainshot:

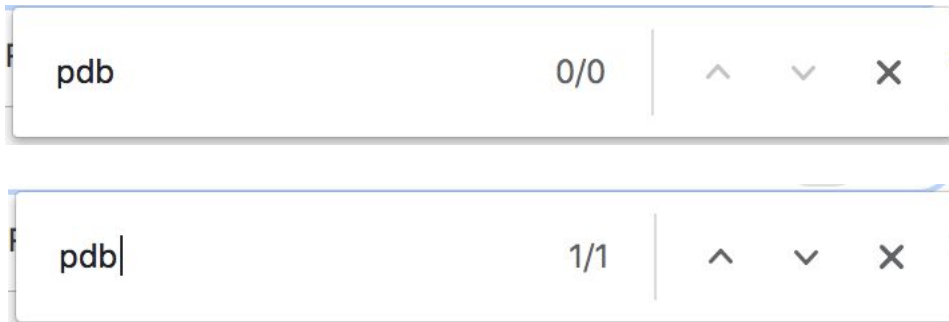
<https://unit42.paloaltonetworks.com/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/>

Can we use the data from this report to find samples of Chainshot?

Yup we can!

- CHAINSHOT Dropper Stages
 - content:{4669727374537461676544726F707065722E646C6C}
OR
content:{5365636F6E64537461676544726F707065722E646C6C}
 - content:FirstStageDropper.dll OR
content:SecondStageDropper.dll

VTGrep: Example 6, Combine Logical Operators



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Rietspoof (loader)

No PDB: f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96

PDB: 9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986

<https://www.virustotal.com/gui/search/f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96%250A9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986/files>

It looks like Rietspoof's loader occasionally has a PDB left in it... Sometimes it doesn't. Can we account for that?

VTGrep: Example 6, Combine Logical Operators

```
(content:{52 41 4d 3a 20} AND content:{64 61 74 61 2e 64 61 74} AND content:{6c 6f 67 6f 75 74 2e 6c 6f 67}) OR content:"G:\Work\Dr.Dre\hivez\new\load
```

FILE	STATUS	SIZE
<input type="checkbox"/> 9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986 a27dbbfaa2a384ba9cc3e0ceb0a86c6e.virus	peexe overlay signed	40 / 68 167.21 KB
<input type="checkbox"/> f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96 iSatSrv.exe	peexe overlay signed	41 / 71 2.29 MB
<input type="checkbox"/> acf46be54c303002d74df6c975083c706b3e1cb8a92e75516579cd0fe65ce918 iSatSrv.exe	peexe overlay revoked-cert signed	30 / 65 192.06 KB
<input type="checkbox"/> 3bc3552b1701280d0fa1c534901c0b926fef61314a1e76eaa7f9623054225633 windmhlp.exe	peexe overlay revoked-cert signed	30 / 65 200.21 KB



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Rietspoof (loader)

No PDB: f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96

PDB: 9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986

It looks like Rietspoof's loader occasionally has a PDB left in it... Sometimes it doesn't. Can we account for that?

By combining logical operators, we can!

```
(content:{52 41 4d 3a 20} AND content:{64 61 74 61 2e 64 61 74} AND content:{6c 6f 67 6f 75 74 2e 6c 6f 67}) OR content:"G:\Work\Dr.Dre\hivez\new\loader\Release\loader.pdb"
```

VTGrep: Example 7, Search at offset with range

"MZP" {00} [0-10000] "virus" @0

The screenshot shows the VirusTotal interface with a search query: `content:{4d5a5000 [0-10000] 76 69 72 75 73}@0`. The search results list several files, including `Virus.Win32.Expiro.a`, `Virus.Win32.Ultratt.8166.b`, and `Virus.Win32.HLLP.Taris.b`. A match context window is open, displaying the following file content:

```
00000000: 4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 MZP.....
00000010: B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 .....@.....
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....
00000040: BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90 .....!..L!..
00000050: 54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73 This program mus
00000060: 74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57 t be run under W
00000070: 69 6E 33 32 00 0A 24 37 00 00 00 00 00 00 00 00 in32..s7.....
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0001C90: 00 50 FF 95 F3 1C 41 00 93 8D BD D5 19 41 00 8D .P...A.....A..
0001CA0: 85 9F 19 41 00 57 53 FF 95 EF 1C 41 00 87 FE AB ...A.WS...A....
0001CB0: 87 FE 32 C0 AE 75 FD 80 3F 55 74 02 EB E7 C3 8D ...2..u..?Ut....
0001CC0: BD F0 18 41 00 E8 08 00 00 00 32 C0 AE 75 FD 80 ...A.....2..u..
0001CD0: 3F FF 75 F1 C3 33 D8 57 53 FF 95 97 19 41 00 91 ?..u..3.WS...A....
0001CE0: 83 0C 53 53 6A 12 51 FF 95 9B 19 41 00 B1 F9 C3 ..SSJ.Q.....A....
0001CF0: 41 56 50 20 4D 6F 6E 69 74 6F 72 00 41 6D 6F 6E AVP Monitor.Amon
0001D00: 20 41 6E 74 69 76 69 72 75 73 20 4D 6F 6E 69 74 Antivirus Monit
0001D10: 6F 72 00 41 56 47 20 43 6F 6E 74 72 6F 6E 6C 20 43 or.AVG.Control.C
```



`content:{4d5a5000 [0-10000] 7669727573}@0`

VTGrep: Example 8, Unpacked, OCR, macros, ...

The screenshot displays the VirusTotal VTGrep interface. On the left, three search results are listed, each with a content snippet and a file list. Arrows point from these snippets to the right-hand side of the interface.

- The first snippet is `content:"M4BUBc_ / Asc"`. It points to a file in the "Compressed Parents" table.
- The second snippet is `content:"Dim AWYbM5aiAlICElynkc7xb4gRO"`. It points to a macro stream in the "Macros And VBA Code Streams" section.
- The third snippet is `content:"JACKY ROSEN"`. It points to a preview of a document containing the text "JACKY ROSEN".

The "Compressed Parents" table shows:

Scanned	Detections	Type	Name
2019-04-01	28 / 59	ZIP	603f7b0eb76af3a55738036dacc8d417e9 1169d3e231c51d0e91fd77bfaacc0

The "Macros And VBA Code Streams" section shows a macro stream for `OzqB.bas` with the following code:

```
Dim AWYbM5aiAlICElynkc7xb4gRO, IzN7nY_rsfELZ1LTLQSQkF  
Dim CT_yz5LLbZKqdnTbJz6YERkrFkR1QvA1U8CgFSJT1zXj_C_1  
Dim F3tB3I5Z1vsq14Pg2_XZmFu3zvCC7nQNGA42vrvNoHRoYcJ1
```

content:"M4BUBc_ / Asc"
content:"Dim AWYbM5aiAlICElynkc7xb4gRO"
content:"JACKY ROSEN"



VTGrep: Pro tips

Prefer rare substrings.
Avoid long common substrings.
Particularly at the extremes.

Aaaah! Something went wrong here...

Results may not be exact due to extremely common substrings ([tips](#)) `ques`

No results found due to unselective query.
Try avoiding extremely common substrings ([tips](#)):

`"ques"`

`content:{00 00 00 00}` `content:{CAFE 00 00 00 00 CAFE}`
`content:{CAFE 00 00 00 00 00 CAFE}` `content:{CAFE 00 00 ?? 00 00 CAFE}`
`content:"http://www.virustotal.com"` `content:"virustotal.co"`



04

VTGraph

<https://support.virustotal.com/hc/en-us/articles/360000298637-VirusTotal-Graph>
<https://www.virustotal.com/graph/>

VTGraph

A visualization tool built on top of VirusTotal's data set. It understands the relationship between files, URLs, domains and IP addresses and it provides an easy interface to pivot and navigate over them



<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#content-search>

Start with f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

A [Near] Daily Occurrence: Emotet Droppers

39 / 60

39 engines detected this file

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b
SEP #979GW.doc
83.88 KB Size | 2018-11-23 00:26:16 UTC | 3 days ago
doc macros run-file

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

2018-11-23T00:26:16

Ad-Aware	VB:Trojan.Valytia.2557	AegisLab	Trojan.MSOffice.SLoad.4lc
AhnLab-V3	DOC/Downloader	ALYac	Trojan.Downloader.Doc.gen
Antiy-AVL	Trojan[Downloader]MSOffice.Agent.lhl	Arcabit	HEUR.VBA.Trojan.e
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
Avira	W97M/Agent.0547520	Baidu	VBA.Trojan-Downloader.Agent.dqq
BitDefender	VB:Trojan.Valytia.2557	Cyren	Trojan.PMHE-3
DrWeb	W97M.DownLoader.3108	Emsisoft	Trojan-Downloader.Macro.Generic.J (A)
Endgame	Malicious (High Confidence)	eScan	VB:Trojan.Valytia.2557
ESET-NOD32	VBA/TrojanDownloader.Agent.LHK	F-Prot	W97M/Downldr.gen
F-Secure	VB:Trojan.Valytia.2557	Fortinet	VBA/Agent.SABFtr.dldr



T1/SOC/ANALYST POV

Or

EmotetDoc: f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

A [Near] Daily Occurrence: Emotet Droppers

The screenshot shows the VirusTotal analysis interface for a file. The 'Basic Properties' section includes MD5, SHA-1, SHA-256, SSDEEP, File type (MS Word Document), Magic (CDF V2 Document), and File size (83.88 KB). The 'OLE Compound File Info' section lists 'Commonly Abused Properties' such as 'Makes use of macros' and 'May try to run other files, shell commands or applications.' A red box highlights the 'Macros And VBA Code Streams' section, which contains a file named 'clHiZVoci.cls'. The 'History' section shows submission and analysis dates. The 'Names' section lists several files, including 'SEP #979IGW.doc', 'O2_13_11_18.doc', 'PAY #397267OYCKGII.doc', 'BIZ #460536H.doc', and 'c:\interc-1\alligate\spool\proctwork\075062-1.vir\0.doc'. The 'ExifTool File Metadata' section is also visible.



T1/SOC/ANALYST POV

Or

EmotetDoc: f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

A [Near] Daily Occurrence: Emotet Droppers

The screenshot displays the VirusTotal interface for a specific file. The 'RELATIONS' tab is active, showing a central node connected to several categories: 8 itw uris, 4 itw domains, 10+ contacted uris, 10+ contacted ips, and 1 contacted domains. Below this, there are two tables: 'Contacted URLs' and 'Contained In Graphs'.

Contacted URLs Table:

Scanned	Detections	URL
2018-11-14	2 / 67	http://31.148.221.34/
2018-11-14	4 / 66	http://24.234.221.236:7080/
2018-11-15	4 / 66	http://81.149.110.194:8443/
2018-11-14	5 / 69	http://75.110.190.86/
2018-11-21	6 / 67	http://222.214.218.192:4143/
2018-11-14	2 / 69	http://58.65.180.67:443/
2018-11-14	3 / 66	http://68.102.169.43:8080/
2018-11-15	4 / 66	http://71.71.128.201:8080/
2018-11-13	0 / 67	http://184.149.17.62:8080/
2018-11-20	5 / 67	http://95.141.175.240:443/

Contained In Graphs Table:

IP	Autonomous System	Country
31.148.221.34	42244 - Hosting Operator eServer.ru ...	CZ
24.234.221.236	22773 - Cox Communications Inc.	US
81.149.110.194	2856 - BTnet UK Regional network	GB
75.110.190.86	19108 - Suddenlink Communications	US
222.214.218.192	4134 - Chinanet	CN
58.65.180.67	23674 - Micronet Broadband (Pvt) Ltd.	PK
68.102.169.43	22773 - Cox Communications Inc.	US
71.71.128.201	11426 - Time Warner Cable Internet ...	US

ITW UrIs Table:

Scanned	Detections	URL
2018-11-20	11 / 66	http://www.xianjiaopi.com/v41964HPAY/US/
2018-11-20	12 / 67	http://agrariszakkepzes.hu/OIM9mt5a/
2018-11-20	14 / 68	http://agrariszakkepzes.hu/OIM9mt5a
2018-11-13	6 / 67	https://www.linkub.com/blog/wp-content/0044444BN/com/Business/
2018-11-13	4 / 67	http://www.linkub.com/blog/wp-content/0044444BN/com/Business
2018-11-20	9 / 68	http://bandarbola.net/4KMA/PAYMENT/Personal



T1/SOC/ANALYST POV

Or

EmotetDoc: f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Pivot on Domain ITW Domain

www.xianjiaopi.com

DETAILS RELATIONS COMMUNITY

Graph Summary

URLs

Scanned	Detections	URL
2018-11-20	10 / 66	http://www.xianjiaopi.com/6kYDYzhpWoYlQ67g/BI Z/lhreSparkasse/
2018-11-20	10 / 67	http://www.xianjiaopi.com/6kYDYzhpWoYlQ67g/BI Z/lhreSparkasse
2018-11-20	11 / 66	http://www.xianjiaopi.com/41964H/PAY/US/
2018-11-20	12 / 67	http://www.xianjiaopi.com/733683H/BIZ/Commercia l
2018-11-20	12 / 67	http://www.xianjiaopi.com/DTWn8HR8e
2018-11-16	6 / 66	http://www.xianjiaopi.com/wp-

Passive DNS Replication

Date resolved	IP
2018-11-16	61.188.39.55

Files Referring

Scanned	Detections	Type	Name
2018-11-23	18 / 60	PDF	5bb9e4dc5f0c1b6269fd2f8dd4c05831891 ddb93b71af85c9b031eda95c00cc7
2018-11-15	19 / 58	PDF	FILE-1305716.pdf
2018-11-06	4 / 58	PDF	FILE-095144.pdf

VirusTotal

Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators

IR POV

search for the Emotet C2: itw: www.xianjiaopi.com (expand graph too?) [Graph is a different perspective]

virustotal.com/graph

These campaigns are typically pretty broad, let's figure out the full scope, you can miss stuff when relying on just one view!

- Private graph for internal investigations

Pivot on Domain

www.xianjiaopi.com



Downloaded Files

Scanned	Detections	Type	Name
2018-11-24	40 / 58	MS Word Document	jnrUFoMW.doc.part
2018-11-23	40 / 60	MS Word Document	ACC2363.doc
2018-11-25	40 / 59	MS Word Document	/data/cfs/malshare/9c8fc9d92225f9077f56 91e458c7d730
2018-11-23	38 / 60	MS Word Document	Customer No 1247823.doc

Communicating Files

Scanned	Detections	Type	Name
2018-11-20	42 / 58	MS Word Document	DOC_574023.doc
2018-10-27	41 / 59	MS Word Document	Untitled-278017836827.doc
2018-10-19	42 / 59	MS Word Document	FORM-05649935773192.doc
2018-10-17	43 / 60	MS Word Document	zbtcheckin_tracker_092018
2018-10-11	41 / 58	MS Word Document	Untitled-9877364339.doc



Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators
IR POV

search for the Emotet C2: itw: www.xianjiaopi.com (expand graph too?) [Graph is a different perspective]
virustotal.com/graph

These campaigns are typically pretty broad, let's figure out the full scope, you can miss stuff when relying on just one view!

- Private graph for internal investigations

Pivot on URI

The screenshot shows the VirusTotal interface with the URI `www.xianjiaopi.com/41964H/PAY/US/ x` entered in the search bar. The results show a list of 5 files:

File Name	Score	Size
cc4b92e40ce2beab7cf1dbedf349f086d01facb7b31e94f43ac698e7e5367473 DOC-62408603968.doc	40 / 59	75.5 KB
4088a57ed9bfac03cda27aa33200f516c0600538dc8d01eb419d20a89ef1767 Rechnung_2018_11_5633028508.doc	35 / 59	72.75 KB
f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b SEP #979IGW.doc	39 / 60	83.88 KB
42e713e46dbc93170ae2513db3d5dd169552df74d9c042ef98564f666fe0e88d O2_12_11_18.doc	39 / 60	82.5 KB
64aa4b8f1436b02328018a92c0c78118d9465054e7f558b9be4db077cca5dc53 2018_11Informationen_betreffend_Transaktion.doc	34 / 59	76.13 KB



Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators

IR POV

search for the Emotet C2: `itw: www.xianjiaopi.com` (expand graph too?) [Graph is a different perspective]

virustotal.com/graph

These campaigns are typically pretty broad, let's figure out the full scope, you can miss stuff when relying on just one view!

- Private graph for internal investigations

Expand With Graph

VTGRAPH

www.xianjiaopi.com

www.xianjiaopi.com

Basic Properties

Name www.xianjiaopi.com

Creation date 2014-01-10 13:09:20

Last update 2017-12-12 03:04:13

Relations

Downloaded files +10

Urls +10

Expand using new Intelligence search

Comments

Urls

Downloaded files

Resolutions

61.188.39.55

Referrer files

Communicating files

www.xianjiaopi.com

Save Download Share

VirusTotal

Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators

IR POV

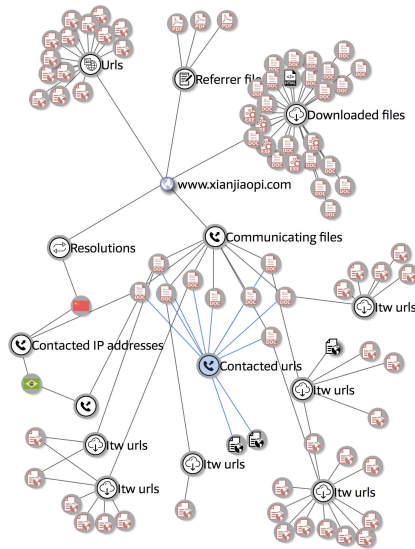
search for the Emotet C2: itw: www.xianjiaopi.com (expand graph too?) [Graph is a different perspective]

virustotal.com/graph

These campaigns are typically pretty broad, let's figure out the full scope, you can miss stuff when relying on just one view!

- Private graph for internal investigations

Expand With Graph



Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators
IR POV

search for the Emotet C2: itw: www.xianjiaopi.com (expand graph too?) [Graph is a different perspective]
[virustotal.com/graph](https://www.virustotal.com/graph)

These campaigns are typically pretty broad, let's figure out the full scope, you can miss stuff when relying on just one view!

- Private graph for internal investigations

Try it Yourself!



Let's escape from slide hell for a little bit!

<https://www.virustotal.com/graph/>

Image source: <https://www.youtube.com/watch?v=lug0OAUdz7M>

- Single Point Expansion: Gameradon [**Power of Visual Pivot**]
 - 195[.]62.53.126
 - <https://www.virustotal.com/graph/g17f21463fdf54396a0bf05fff61385788cb4951a3b694c1c895fc1105b725dab>
- OSINT Reporting
 - Option 1: Farseer,
<https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/>
 - Option 2: Babyshark,
<https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/>
 - <https://www.virustotal.com/graph/g1766a5d086d84a6d859f1c598620f704925844d218584cdb81e6c5736348528>

3

- Option 3: GreyEnergy Overlaps with Sofacy,
<https://securelist.com/greyenergys-overlap-with-zebrocy/89506/>
- Option 4: Bronze Union (APT27/LuckyMouse),
<https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox>
 - <https://www.virustotal.com/graph/gde1e0f5c8a3d41ef8f456d40df09c3b978e1e5f380034dfcad8adf4b9be2ca1a>
- Option 5: AutoIT Zebrocy,
<https://www.vkremez.com/2019/01/lets-learn-progression-of-apt-28-autoit.html>
 - <https://www.virustotal.com/graph/g7781518d548f4726aa4d70d9189b5a6d12d01c88fc494fc78d187056974da55>
- Messy/Large Campaigns - Emotet
 - 459397a134b2b4a201c2855bbb2ed4d1eeda9cc7637d7c65201e0a78217a8780
C060ca7e926c137d2a9b90d0182b288b86117430f8a7614a1bff92b722ee1fa6
 - Source:
https://paste.cryptolaemus.com/emotet/2019/03/14/emotet-malware-loCs_03-14-19.html
 - Emotet dropping Trickbot,
<https://www.malware-traffic-analysis.net/2019/03/13/index.html>
- Manual Expansion Using VTI Queries
 - Chainshot:
<https://unit42.paloaltonetworks.com/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/>
 - VTI Query - content:FirstStageDropper.dll OR
content:SecondStageDropper.dll

05

YARA

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

[https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals.](https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals)

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

What is YARA?

YARA is an acronym for: YARA: Another Recursive Acronym, or Yet Another Ridiculous Acronym. Pick your choice.

-- [Victor M. Alvarez \(@plusvic\)](#)

- Tool to assist malware researchers identify and classify malware
- Identify malware in string or binary patterns
- YARA rule = strings + condition
- Useful to catalog threat actors and associated IOCs



YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

What is a YARA Rule?

```
sample-rule {  
  strings:  
    $a = "malicious_string" ← INDICATOR  
    $b = {56 54 59} ← S  
  
  condition:  
    $a or $b ← LOGIC  
}
```



By default strings are considered ASCII

Crafting a Custom YARA Rule

Malware family: **Coblint**

- PE file
- Typically < 30kb in size
- Specifically Named for an embedded DLL string
- *OPTIONAL*: Imphash Might be shared
- *OPTIONAL*: Interesting Function Calls

Crafting a Custom YARA Rule (2)

Sample #1

STRINGS	HEX
KERNEL32.dll IPHLPAPI.DLL ADVAPI32.dll WININET.dll urlmon.dll int.dll	
<code><assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'></code>	
<code><requestedExecutionLevel level='asInvoker' uiAccess='false' /></code>	
<code><trustInfo xmlns="urn:schemas-microsoft-com:asm.v3"></code>	
<code>xml version='1.0' encoding='UTF-8' standalone='yes'</code>	
This program cannot be run in DOS mode.	
ReflectiveLoader@YGKPAX@Z	
InitializeCriticalSection	
</requestedPrivileges>	
DeleteCriticalSection	
ObtainUserAgentString	
<requestedPrivileges>	
EnterCriticalSection	
LeaveCriticalSection	
InternetQueryOptionA	

Sample #2

STRINGS	HEX
KERNEL32.dll IPHLPAPI.DLL ADVAPI32.dll WININET.dll urlmon.dll int.dll	
<code><assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'></code>	
<code><requestedExecutionLevel level='asInvoker' uiAccess='false' /></code>	
<code><trustInfo xmlns="urn:schemas-microsoft-com:asm.v3"></code>	
<code>xml version='1.0' encoding='UTF-8' standalone='yes'</code>	
This program cannot be run in DOS mode.	
ReflectiveLoader@YGKPAX@Z	
InitializeCriticalSection	
</requestedPrivileges>	
DeleteCriticalSection	
ObtainUserAgentString	
<requestedPrivileges>	
EnterCriticalSection	
LeaveCriticalSection	
InternetQueryOptionA	



Sample 1: 9540c062e1aefdb78e1f3f0b40c7f9d7f1a7c7fe90f2748e369a7d2e6fe4a6bb

Sample 2: 2f7b5219193541ae993f5cf87a1f6c07705aaa907354a6292bc5c8d8585e8bd1

Crafting a Custom YARA Rule (4)

Both Samples

Imports

- + ADVAPI32.dll
- + IPHLPAPI.DLL
- + KERNEL32.dll
- + WININET.dll
- + urlmon.dll

Basic Properties ⓘ	
MD5	616199072a11d95373b3c38626ad4c93
SHA-1	57201d6d3a8b1585f585e7d3927542c281b1494
Authentihash	46a3defc737d9160d0cf201aa0c02c2946c716415051798930424abc80d92fe0
Imphash	9fd476779121c8ccabe0e029935bcbcb
SSDEEP	192:/puE9/Cgv6sln1TeqopZ7quwnd7eV8pP:RZHiRpdqkB48pP
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File size	10.5 KB



Crafting a Custom YARA Rule (5)

```
strings:  
    // interesting strings  
    $s1 = "int.dll"  
    $s2 = "ReflectiveLoader"  
    $s3 = "ObtainUserAgentString"
```

Crafting a Custom YARA Rule (8)

```
import "pe"
rule apt_win_cobint_dll : Cobalt_Group
{
  strings:

  // interesting strings
  $s1 = "int.dll"
  $s2 = "ReflectiveLoader"
  $s3 = "ObtainUserAgentString"

  condition:
    uint16(0)==0x5a4d
    and (
      all of them
    or
      pe.imphash()== "9fd476779121c8ccabe0e029935bcbbb"
    )
    and filesize < 30KB
}
```



Strings are assumed to be ASCII by default.

if you want to indicate strings are unicode, use the wide modifier

If you want to include both ASCII and Unicode strings, use the two modifiers, ascii unicode, after your closing quote.

Retrohunt Results

100 %

Finished

blevene_Chron-1538937604 1 month ago

import "pe" rule apt_win_cobint_dll : Cobalt_Group { meta: description = "Identify potential CobInt downloader DLL Trojan sa...

16 matches



```
1 import "pe"
2 rule apt_win_cobint_dll : Cobalt_Group
3 {
4   meta:
5     description = "Identify potential CobInt downloader DLL Trojan samples, unique to CobaltGroup/Fin8"
6     author = "blevene @upperCase, Chronicle Security"
7     version = "1.0"
8     date = "09-94-2018"
9     TLP = "GREEN"
10    reference = "https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-still-active-despite-leaders-arrest/"
11    hash = "a7c1877112d25517333ea9b6bb46a056f1685c3f7055a45bb9f4f9abad74fdea"
12
13   strings:
14     // interesting strings
15     $s1 = "int.dll" ascii
16     $c2 = "ReflectiveLoader" ascii
```



Hunter/Researcher POV

Demo hunt UI = forward looking <https://www.virustotal.com/intelligence/hunting/>
Retrohunt = retrospective

Search old Notifications UI for "Cobalt_Group" to get CobInt notifications. Retrohunt should be done as well.

If people are interested show rule for pivoting on:

DHS Cosmos Backdoor:

820ca1903a30516263d630c7c08f2b95f7b65dffceb21129c51c9e21cf9551c6

Embedded Resource Pivoting:

a76c79a4146cfd5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3 (ursnif)

=> rsrc image pivot => Yara Rule

Retrohunt Results

RETROHUNT NOTIFICATIONS



fb386b74513964f463d530fb44e424f6013521344308b7870260f85a9df29c e4c39cfeaf03a0043455548a27a32fa.vir pedll apt_win_cobint_dll	44 / 67	10.5 KB	2018-07-06 15:33:08 first seen 2018-10-26 23:40:45 last seen	3 submissions 3 submitters
977b0c1c833941a35fd88d9f4972ced3e5957174a5e1958f5344b4ae4dc05a0 pedll apt_win_cobint_dll	42 / 65	10.5 KB	2018-09-19 18:15:27 first seen 2018-09-19 18:15:27 last seen	1 submissions 1 submitters
a2d959c5f209c454409b8cd90922c937cde4750068e7ede4995bfad20e32418 payload.dll pedll overlay apt_win_cobint_dll	45 / 67	11.01 KB	2018-01-25 20:59:40 first seen 2018-08-27 14:41:45 last seen	5 submissions 3 submitters
44c14518d39aa2f1ce1271e1425ad62c801186d9f5bf4d56e3e55cec50586087 mz apt_win_cobint_dll	0 / 62	8.12 KB	2018-08-14 15:33:16 first seen 2018-08-14 15:33:16 last seen	1 submissions 1 submitters
1bd96d83b6db67080e23c4d7d792a94455146d07bae00b02f8ee23a61c605967 rundll32.exe bin pedll overlay apt_win_cobint_dll	48 / 67	24 KB	2017-12-26 12:48:24 first seen 2017-12-26 12:48:24 last seen	2 submissions 1 submitters
b2c6208b6636dea33243f0d19979013772add75e477d8fd00f07371d505354 invoice-xox.dll pedll apt_win_cobint_dll	44 / 66	10.5 KB	2018-09-19 15:44:40 first seen 2018-10-02 01:43:30 last seen	2 submissions 2 submitters
9540c062e1aefdb78e1f3f0b40c7f9d711a7c7fe90f2748e369a7d2e6fe4a6bb 6b16c35bbaa2a74ed053c94e01062f0c.vir pedll apt_win_cobint_dll	44 / 68	28 KB	2018-09-04 19:45:49 first seen 2018-10-03 23:01:45 last seen	2 submissions 2 submitters
0640eb2242aa77ecc5a95fe0ce7d0f5e7712586883786b50c33a1aea799a2af2 2710000.dll pedll apt_win_cobint_dll	46 / 66	10.5 KB	2018-07-05 14:10:19 first seen 2018-10-25 21:58:06 last seen	3 submissions 3 submitters



Livehunt Results

LIVEHUNT NOTIFICATIONS

cobalt_group



44fb5685527f8af9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d

int.dll

pedll apt_win_cobint_dll cobalt_group presentation_cobint

47 / 66

11 KB

2018-11-20 10:58:12 date matched
2018-03-26 14:10:37 first seen

3 submissions
2 submitters



44fb5685527f8af9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d

int.dll

pedll apt_win_cobaltgroup apt_win_cobintunpacked cobalt_group

47 / 66

11 KB

2018-11-20 10:58:10 date matched
2018-03-26 14:10:37 first seen

3 submissions
2 submitters



44fb5685527f8af9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d

int.dll

pedll apt_win_cobaltgroup apt_win_cobint_dll cobalt_group

47 / 66

11 KB

2018-11-20 10:58:10 date matched
2018-03-26 14:10:37 first seen

3 submissions
2 submitters



LiveHunt Results

https://www.virustotal.com/gui/hunting/notifications/cobalt_group

But, CobInt doesn't use int.dll anymore!

```
import "pe"
rule apt_win_cobint_dll : Cobalt_Group
{
    strings:

    // interesting strings
    $s1 = "[a-zA-Z]{3}\.dll/ ascii"
    $s2 = "ReflectiveLoader"
    $s3 = "ObtainUserAgentString"

    condition:
        uint16(0)==0x5a4d
        and (
            all of them
        or
            pe.imphash()== "9fd476779121c8ccabe0e029935bcbbb"
        )
        and filesize < 30KB
}
```



Regex!

Basic Rule Dev 1: I want to use all the strings



<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

Rietspooft (bot):

8ea856534561e1fbfe8c13c8901cdc9c8f7eb6139e76ef5eea8f9137c2295199

<https://www.virustotal.com/gui/file/8ea856534561e1fbfe8c13c8901cdc9c8f7eb6139e76ef5eea8f9137c2295199/submissions>

---I'm going to have to do this in a notepad I think, the rule is too big to be visible in slides---

```
rule trojan_win_rietspooft_bot : commodity
{
    meta:
        description = "Identify Reitspooft Bot"
```

```
    author = "blevene@chronicle.security"
    date = "20-02-2019" //dd-mm-yyyy
    reference =
"https://www.bleepingcomputer.com/news/security/multi-stage-r
ietspooof-malware-drops-multiple-malicious-payloads/"
    hash01 =
"8ea856534561e1fbfe8c13c8901cdc9c8f7eb6139e76ef5eea8f9137c229
5199"

    strings:

        $ = "cbomb.dat" wide
        $ = "Secur32.dll" wide
        $ = "CreatePipe"
        $ = "PeekNamedPipe"
        $ = "WS2_32.dll"

    condition:
        uint16(0)==0x5a4d
        and all of them
}
```

Basic Rule Dev 2:
I need to employ more
selective logic for my
strings



<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

Rietspoof (loader)

No PDB: f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96

PDB: 9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986

---Again, going to have to do this in a Notepad---

```
rule trojan_win_rietspoof_loader : commodity
{
    meta:
        description = "Identify Reitspoof Loader Phase"
        author = "blevene@chronicle.security"
        date = "20-02-2019" //dd-mm-yyyy
        reference =
```

```
"https://www.bleepingcomputer.com/news/security/multi-stage-r  
ietspooof-malware-drops-multiple-malicious-payloads/"
```

```
hash01 =
```

```
"f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd191  
6c96"
```

```
hash02 =
```

```
"d7a15001a45c6157f0b2ed728a88cc9db09ed39e733310e76bd906ccdf52  
7a4e"
```

```
strings:
```

```
$s1 = "CPU: %s(%d) "
```

```
$s2 = "data.dat"
```

```
$s3 = "Host:%s"
```

```
$s4 = "logout.log"
```

```
$s5 = "RAM: "
```

```
$s6 = "WScript"
```

```
//old PDB
```

```
$pdb =
```

```
"G:\\Work\\Dr.Dre\\hivez\\new\\loader\\Release\\loader.pdb"
```

```
condition:
```

```
uint16(0)==0x5a4d
```

```
and ( all of ($s*) or $pdb)
```

```
}
```

Modules

Modules are the method YARA provides for extending its features. They allow you to define data structures and functions which can be used in your rules to express more complex conditions.



YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

Important => <https://yara.readthedocs.io/en/v3.9.0/modules.html>

Writing your own modules =>

<https://yara.readthedocs.io/en/v3.9.0/writingmodules.html#writing-modules> (Its in C)

Modules: PE

```
import "pe"

rule single_section
{
    condition:
        pe.number_of_sections == 1
}

rule control_panel_applet
{
    condition:
        pe.exports("CPLApplet")
}

rule is_dll
{
    condition:
        pe.characteristics & pe.DLL
}
```



YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

<https://yara.readthedocs.io/en/v3.9.0/modules/pe.html>

“The PE module allows you to create more fine-grained rules for PE files by using attributes and features of the PE file format. This module exposes most of the fields present in a PE header and provides functions which can be used to write more expressive and targeted rules.”

Modules: Hash

```
import "pe"
import "hash"
rule trojan_win_ursnif_resource : Commodity
{
    meta:
        description = "Identify Ursnif/Gozi/ISFB samples seen on 10/26/2018"
        author = "blevene@chronicle.security"
        hash01 =
"a76c79a4146cfd5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3"
        condition:
            uint16(0)==0x5a4d
            and filesize < 600KB
            and for any i in (0..pe.number_of_resources - 1):
                (hash.sha256(pe.resources[i].offset, pe.resources[i].length) ==
"059f9bf1cded9a989daeeecd2df32db54318347d3975f343aaf8d123d0ca517d")
}
```



YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

<https://yara.readthedocs.io/en/v3.9.0/modules/hash.html>

The Hash module allows you to calculate hashes (MD5, SHA1, SHA256) from portions of your file and create signatures based on those hashes.

Bonus, we are a looping!

<https://yara.readthedocs.io/en/v3.9.0/writingrules.html#iterating-over-string-occurrences>

Sample:

<https://www.virustotal.com/gui/file/a76c79a4146cfd5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3/detection>

Modules: Math

```
rule trojan_win_atmos : Commodity
{
    meta:
        hash1 =
"16ce22397e8261714a272d82627bb3a55b65d7f4e65e0d54acfb3c5ed37e68cc"
        author = "blevene"
        date = "2016-11-10"
        description = "Identify Atmos samples, Zeus/Citadel Variant"
        reference =
"https://www.kaspersky.com/blog/atmos-yet-another-zeus-variant-is-threatening-businesses/5476/"

    condition:
        uint16(0) == 0x5a4d
        and math.entropy(pe.sections[1].raw_data_offset,
pe.sections[1].raw_data_size) > 7.8
        and for any i in (0..pe.number_of_sections -1):
            (pe.sections[i].name == ".sock")
}
```



YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

<https://yara.readthedocs.io/>

<https://github.com/InQuest/awesome-yara>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>.

<https://support.virustotal.com/hc/en-us/articles/360000347157-VT-Intelligence#search-modifiers>

`math.entropy(offset, filesize)` => Returns the entropy for *size* bytes starting at *offset*

“The Math module allows you to calculate certain values from portions of your file and create signatures based on those results.”

Bonus: Looping in Yara!

<https://yara.readthedocs.io/en/v3.9.0/writingrules.html#iterating-over-string-occurrences>

atmos = Zeus Variant

<https://www.virustotal.com/gui/file/16ce22397e8261714a272d82627bb3a55b65d7f4e65e0d54acfb3c5ed37e68cc/detection>

Practical Applications 1

Mimikatz



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example:

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4
(mimikatz)

<https://github.com/gentilkiwi/mimikatz>

Practical Applications 1

Mimikatz, Option 1 Strings Only



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example:

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4
(mimikatz)

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Ref: <https://github.com/gentilkiwi/mimikatz>

---Will do in a notepad---

Option 1, strings only

```
rule hacktool_win_mimikatz_dll_option1_strings : hacktool
{
  meta:
    description = "Identify stock Mimikatz DLL. Example rule."
    author = "blevene@chronicle.security"
    date = "03/15/2019" //mm/dd/yyyy
    hash =
```

"b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4"
strings:

```
//exports
$e1 = "InitializeChangeNotify" ascii fullword
$e2 = "PasswordChangeNotify" ascii fullword
$e3 = "SpLsaModelInitialize" ascii fullword
```

```
//imports
$i1 = "NdrMesTypeFree2" ascii fullword
$i2 = "MesHandleFree" ascii fullword
$i3 = "RtlStringFromGUID" ascii fullword
$i4 = "GetOEMCP" ascii fullword
```

condition:

```
/* option 1:
all of them
*/
/*option 2:
all of ($e*) and all of ($i*)
*/
```

}

Practical Applications 1

Mimikatz, Option 2 PE Exports



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example:

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4
(mimikatz)

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Ref: <https://github.com/gentilkiwi/mimikatz>

---Will do in a notepad---

```
import "pe"
rule hacktool_win_mimikatz_dll_option2_exportonly : hacktool
{
  meta:
    description = "Identify stock Mimikatz DLL. Example rule."
    author = "blevene@chronicle.security"
    date = "03/15/2019" //mm/dd/yyyy
    hash =
      "b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4"
```

condition:

```
pe.exports("InitializeChangeNotify")  
and pe.exports("PasswordChangeNotify")  
and pe.exports ("SpLsaModelInitialize")
```

```
}
```

Practical Applications 1

Mimikatz, Option 3 PE Imports



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

Example:

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4
(mimikatz)

<https://www.virustotal.com/gui/file/b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4/detection>

Ref: <https://github.com/gentilkiwi/mimikatz>

---Will do in a notepad---

```
import "pe"
rule hacktool_win_mimikatz_dll_option3_importonly : hacktool
{
  meta:
    description = "Identify stock Mimikatz DLL. Example rule."
    author = "blevene@chronicle.security"
    date = "03/15/2019" //mm/dd/yyyy
    hash =
      "b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4"
```


condition:

```
pe.imports("RPCRT4.dll", "MesHandleFree")  
and pe.imports("RPCRT4.dll", "NdrMesTypeFree2")  
and pe.imports("ntdll.dll", "RtlStringFromGUID")  
and pe.imports ("KERNEL32.dll", "GetOEMCP")
```

```
}
```

Practical Applications 2

DustSquad "Octopus" Implant



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

2d5f3edc4132f463cb6efe6379fda46e00fb7225f51a9fb69d2b11161c43faa6
2af44715d4f0655bd50d30d46b01336b7f7743ade6b78e2e7650a8d60dc35858
caaf10e6f65d630130c04453160596eada9a5b78167c934e9ea3e8baffa2c345

<https://www.virustotal.com/gui/search/2d5f3edc4132f463cb6efe6379fda46e00fb7225f51a9fb69d2b11161c43faa6%250A2af44715d4f0655bd50d30d46b01336b7f7743ade6b78e2e7650a8d60dc35858%250Acaaf10e6f65d630130c04453160596eada9a5b78167c934e9ea3e8baffa2c345/files>

---Will do in a notepad---

```
import "pe"
rule apt_win_octopus : DustSquad {
  meta:
    description = "Identify potential DustSquad 'octopus' implants"
    graph =
      "https://www.virustotal.com/graph/g4c327ce3e88e43f99191d7618b1b74e4eefee8ccd2e44451ae8aa49ac1a36e47"
```

```
date = "10-16-2018"
author = "blevene@chronicle.security"
hash01 =
"2d5f3edc4132f463cb6efe6379fda46e00fb7225f51a9fb69d2b11161c43faa6"
hash02 =
"2af44715d4f0655bd50d30d46b01336b7f7743ade6b78e2e7650a8d60dc35858"
hash03 =
"caaf10e6f65d630130c04453160596eada9a5b78167c934e9ea3e8baffa2c345"
```

strings:

```
//unicode strings
$u1 = "Download:" wide
$u2 = "Remove:" wide
$u3 = "Embaracdero" wide
$u4 = "php?check" wide
```

condition:

```
uint16(0)==0x5a4d
    and (
        all of them
    or
        pe.imphash()== "65ffe87ad21cc53609d3db7bc15603b0"
or
    vhash == "0360b6666d5c0d5d151c003232z5e002c025z8035z23z303cz1"
    )
    and filesize < 5MB
}
```

Practical Applications 3

LuckyCat “ExileRat” Implant



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

3eb026d8b778716231a07b3dbbdc99e2d3a635b1956de8a1e6efc659330e52de
<https://www.virustotal.com/gui/file/3eb026d8b778716231a07b3dbbdc99e2d3a635b1956de8a1e6efc659330e52de/detection>

---Will do in a notepad---

```
rule apt_win_exilerat : LuckyCat
{
    meta:
        description = "Identify ExileRat as described by Talos"
        author = "blevene@chronicle.security"
        date = "04-02-2019" //dd-mm-yyyy
        reference =
            "https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html"
        hash01 =
            "3eb026d8b778716231a07b3dbbdc99e2d3a635b1956de8a1e6efc659330e52de"

    strings:
```

```
//filewrites
$f1 = "prepare to write file %s, %d, %d"
$f2 = "end write file %s, %d"

//pdb
$pdb= "D:\\proj\\proj.vs2015\\scout\\Release\\scout.pdb"

//hardcoded IPs
$ip1 = "27.126.188.212"
$ip2 = "192.100.106.207"
```

condition:

```
uint16(0)==0x5a4d
and (
    all of ($f*)
    or $pdb
    or 1 of ($ip*)
)
```

```
}
```

Practical Applications 4

Lazarus “RisingSun” Implant



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

37b04dcdcfca885df0f392524db7ae7b73806ad8a8e76fbc6a2df4db064e71
<https://www.virustotal.com/gui/file/37b04dcdcfca885df0f392524db7ae7b73806ad8a8e76fbc6a2df4db064e71/detection>

---Will do in a notepad---

```
rule apt_win_RisingSun : Lazarus
{
    meta:
        description = "Identify RisingSun Implant which McAfee Aleeges is
related to Lazarus' Duuzer"
        author = "blevene@chronicle.security"
        date = "12-12-2018" //dd-mm-yyyy
        reference =
"https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.p
df"
        hash01 =
```

"37b04dcdcfdaaa885df0f392524db7ae7b73806ad8a8e76fbc6a2df4db064e71"

strings:

\$ = "Accept-Language: en-us;q=0.8;q=0.6,en-us;q=0.4,en;q=0.2" wide

\$ = "charset={[A-Za-z0-9\\-_]+}" wide

\$ = "Content-Length: {[0-9]+}" wide

\$ = "Location: {[0-9]+}" wide

\$ = "q(\"[^\"]*\")(('[^']*'))" wide

\$ = "Set-Cookie:\\b*{.+?}\\n" wide

\$ = "%s%d&page=result%s%d" ascii

\$uri = "%s%d&page=" ascii

condition:

uint16(0)==0x5a4d

and #uri > 3

and all of them

}

Practical Applications 5

CobaltGang "ShapesMacro" Dropper



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

2a8c62c4e167f9f52c2c5a4fe5be96df53d1f6015dd793747391775e34d16fbf
<https://www.virustotal.com/gui/file/2a8c62c4e167f9f52c2c5a4fe5be96df53d1f6015dd793747391775e34d16fbf/detection>

---Will do in a notepad---

```
rule apt_win_shapesmacro_cobaltdropper : Cobalt_Gang
{
    meta:
        description = "Identify malicious office documents which abuse the
Shapes function"
        author = "blevene@chronicle.security"
        date = "20-12-2018" //dd-mm-yyyy
        reference =
"https://twitter.com/dissectmalware/status/1064977287915950080?lang=en"
        hash01 =
"2a8c62c4e167f9f52c2c5a4fe5be96df53d1f6015dd793747391775e34d16fbf"
```


strings:

\$office = { D0 CF 11 E0 A1 B1 1A E1 }

\$s1 = "ThisProject.ThisDocument.AutoOpen" wide nocase

\$s2 = "Shapes" ascii nocase

\$s3 = "Shell" ascii nocase

\$s4 = "TextFrame" ascii

\$s5 = "TextRange" ascii

\$s4 = "ThisProject" ascii

\$var = "var" ascii nocase

condition:

\$office at 0

and #var > 8

and all of (\$s*)

}

06

YARA Tools on VT

<https://www.virustotal.com/gui/hunting/retrohunt>

Retrohunt

+ New retrohunt job

100 %	Finished	blevene_Chron-1553198358 20 hours ago rule Office_Base64_BreakCatchWide :maidoc { meta: description = "Potential Emotet maidoc using base64 wide encoded break->catch" author ...	615 matches	↓
100 %	Finished	blevene_Chron-1553197869 20 hours ago import "pe" rule apt_win_cobint_dll : Cobalt_Group { meta: description = "Identify potential Cobint downloader DLL Trojan samples, unique to Co..."	1011 matches	↓
100 %	Finished	blevene_Chron-1553179894 1 day ago rule apt_win_EyeHawk : CN { meta: description = "Identify payload from RTF: 69f44ca082ed90c97d9c4ebaae589d7e41c69b02e582cc69886abf..."	5 matches	↓
100 %	Finished	blevene_Chron-1553117311 1 day ago rule astra_docs { meta: description="ver1 of astra_docs" author="JDP" strings: \$header = (d0cf11e0a1b11ae1) \$a1 = "PROTECTED CONTENT"...	12 matches	↓
100 %	Finished	blevene_Chron-1553115402 1 day ago import "pe" rule LockerGogaRansomware { meta: description = "LockerGoga Ransomware" author = "Christiaan Beek - McAfee ATR team" date ...	7 matches	↓
100 %	Finished	blevene_Chron-1553023105 2 days ago rule ransomware_win_lockergoga : ransomware { meta: description = "Identify LockerGoga ransomware, mostly clustered around Dutch and Dan..."	15 matches	↓



<https://support.virustotal.com/hc/en-us/articles/360000347157-VirusTotal-Intelligence>

<https://www.virustotal.com/gui/hunting/retrohunt>

Beside hunting for files in real time as they arrive to VirusTotal, you can also apply your YARA rules to files sent in the past with the Retrohunt feature. The concept is plain simple: just put your YARA rules in the provided text box, launch your Retrohunt job and you'll get a list of files matching your rules. The process can take a few hours, as it scans multiple terabytes of data, but you can provide an email address in order to be notified when the scanning finishes.


However, notice that none of the Malware Hunting-specific features will work with Retrohunt, including rules based on the number of positives, antivirus signatures, tags, file type and Cuckoo's behaviour reports. Only pure YARA rules will work.

LiveHunt

LIVEHUNT NOTIFICATIONS

Search notifications ? [filter] [refresh] [trash] [copy] [download]

<input type="checkbox"/>	6ec9d3a2302a7cd6b170b155a9a2f0eed3c264e25a2c829a5d8f7df2e44ee9dc log file.exe peexe assembly overlay apt_win_nedrat gazahackerteam [lock] [share]	45 / 65	3.58 MB	2019-03-22 16:17:17 date matched 2019-03-22 16:14:19 first seen	1 submissions 1 submitters	
<input type="checkbox"/>	7b081379d83e7bcfac3619f4b274f5d5e073b81618803f8feded0127bb8f6918 OPXVKAAL.EXE peexe av_emotet av_trojan_win_emotet emotet	12 / 64	748.5 KB	2019-03-22 16:13:33 date matched 2019-03-22 16:07:10 first seen	1 submissions 1 submitters	
<input type="checkbox"/>	ba8aaca4dfb35315e502e66aede7be7af535af42934024bd61391db8977f2ba DISM.EXE peexe overlay av_emotet av_trojan_win_emotet emotet [lock]	14 / 67	185.26 KB	2019-03-22 16:12:47 date matched 2019-03-22 16:08:55 first seen	1 submissions 1 submitters	
<input type="checkbox"/>	aca9e4365f5e563fc21779c81d54ec6037be9c8a2202b3bef0428c388389da6 etohaknairnik.exe peexe av_emotet av_trojan_win_emotet emotet [lock]	38 / 66	6.31 MB	2019-03-22 16:11:10 date matched 2019-03-22 16:03:47 first seen	1 submissions 1 submitters	



<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://www.virustotal.com/gui/hunting/notifications>

<https://www.virustotal.com/gui/hunting/rulesets>

Livehunt allows you to hook into the stream of files submitted to VirusTotal and get notified whenever one of them matches a certain rule written in the YARA language. Applying YARA rules to the files submitted to VirusTotal you should be able to get a constant flow of malware files classified by family, discover new malware files not detected by antivirus engines, collect files written in a given language or packed with a specific run-time packer, create heuristic rules to detect suspicious files, and, in general, enjoy the benefits of YARA's versatility acting on the huge amount of files processed by VirusTotal every day.

LiveHunt: VirusTotal Externals

AntiVirus Detection Externals

```
rule av_externals_example
{
  condition:
    signatures contains "Trojan"
    or
    eset_nod32 contains "Backdoor"
}
```



<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://www.virustotal.com/gui/hunting/notifications>

<https://www.virustotal.com/gui/hunting/rulesets>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#antivirus-externals>

In malware hunting your rules can take into account not only the contents of the file itself, but also the signatures generated by the different antivirus engines that scanned the file, which means that you can construct rules stating: *"give me the files containing the strings 'foo' and 'bar', and detected by more than two antivirus vendors"* or *"give me the files detected by antivirus X"* or *"give me new files that antivirus X detects as 'baz'"*.

LiveHunt: VirusTotal Externals

VirusTotal Tags

```
rule VT_Tags_example
{
  condition:
    tags contains "nsrl" or tags
contains "trusted"
}
```



<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://www.virustotal.com/gui/hunting/notifications>

<https://www.virustotal.com/gui/hunting/rulesets>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#tag-externals>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#file-types>

In malware hunting your rules can take into account not only the contents of the file itself, but also the signatures generated by the different antivirus engines that scanned the file, which means that you can construct rules stating: *"give me the files containing the strings 'foo' and 'bar', and detected by more than two antivirus vendors"* or *"give me the files detected by antivirus X"* or *"give me new files that antivirus X detects as 'baz'"*.

LiveHunt: VirusTotal Externals

VirusTotal Externals

```
rule VT_Tags_example
{
  condition:
    file_type contains "document"
    and file_name contains "invoice"
    and new_file
}
```



<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://www.virustotal.com/gui/hunting/notifications>

<https://www.virustotal.com/gui/hunting/rulesets>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#tag-externals>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#file-types>

In malware hunting your rules can take into account not only the contents of the file itself, but also the signatures generated by the different antivirus engines that scanned the file, which means that you can construct rules stating: *"give me the files containing the strings 'foo' and 'bar', and detected by more than two antivirus vendors"* or *"give me the files detected by antivirus X"* or *"give me new files that antivirus X detects as 'baz'"*.

LiveHunt: VirusTotal Externals Example 2

```
rule mueller_report_lures : current_event
{
    meta:
        description = "Identify mueller report lures"

    condition:
        (file_type contains "document" or file_type contains
"email") and new_file and

        ( file_name contains "mueller"
or file_name contains "mueller report"
or (file_name contains "mueller" and file_name
contains "report")
)
}
```



<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting>

<https://www.virustotal.com/gui/hunting/notifications>

<https://www.virustotal.com/gui/hunting/rulesets>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#tag-externals>

<https://support.virustotal.com/hc/en-us/articles/360000363717-VT-Hunting#file-types>

In malware hunting your rules can take into account not only the contents of the file itself, but also the signatures generated by the different antivirus engines that scanned the file, which means that you can construct rules stating: *"give me the files containing the strings 'foo' and 'bar', and detected by more than two antivirus vendors"* or *"give me the files detected by antivirus X"* or *"give me new files that antivirus X detects as 'baz'"*.

07

APIv3 - VTCLI

<https://asciinema.org/a/179696>

<https://developers.virustotal.com/v3.0/reference>

<https://github.com/VirusTotal/vt-cli>

Helpful Tool for APIv3

[https://github.com/VirusTotal/vt-cl
i](https://github.com/VirusTotal/vt-cli)



<https://asciinema.org/a/179696>

<https://developers.virustotal.com/v3.0/reference>

<https://github.com/VirusTotal/vt-cli>

APIv3 - Query File Information

```
blevene@blevene-imacpro ~$ vt file b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37
- file <b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37>:
  bundle_info:
    extensions:
      bin: 1
      jpg: 1
      xml: 14
    file_types:
      JPG: 1
      Microsoft Office: 1
      XML: 18
    highest_datetime: "1980-01-01 00:00:00"
    lowest_datetime: "1980-01-01 00:00:00"
    num_children: 20
    type: "DOCX"
    uncompressed_size: 149149
    vhash: "7905a57c5a030c4ad3a9e777cc1bd352"
  creation_date: 1553645460 # 2019-03-26 20:11:00 -0400 EDT
```



Displayed output is abbreviated in the slide (it doesn't all fit)

Truncated the results in the raw output as well, ya'll get the point, hopefully.

```
blevene@blevene-imacpro ~$ vt file
b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37
- file
<b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37>:
  bundle_info:
    extensions:
      bin: 1
      jpg: 1
      xml: 14
    file_types:
      JPG: 1
      Microsoft Office: 1
      XML: 18
    highest_datetime: "1980-01-01 00:00:00"
    lowest_datetime: "1980-01-01 00:00:00"
    num_children: 20
    type: "DOCX"
    uncompressed_size: 149149
```

vhash: "7905a57c5a030c4ad3a9e777cc1bd352"
creation_date: 1553645460 # 2019-03-26 20:11:00 -0400 EDT
downloadable: true
exiftool:
 AppVersion: "16.0"
 Application: "Microsoft Office Word"
 Characters: "3"
 CharactersWithSpaces: "3"
 Company: "VPS2day"
 CreateDate: "2019:03:27 00:11:00Z"
 Creator: "VPS2day"
 DocSecurity: "None"
 FileType: "DOCM"
 FileTypeExtension: "docm"
 HeadingPairs: "Title, 1"
 HyperlinksChanged: "No"
 LastModifiedBy: "VPS2day"
 Lines: "1"
 LinksUpToDate: "No"
 MIMEType: "application/vnd.ms-word.document.macroEnabled"
 ModifyDate: "2019:03:31 19:23:00Z"
 Pages: "1"
 Paragraphs: "1"
 RevisionNumber: "31"
 ScaleCrop: "No"
 SharedDoc: "No"
 Template: "Normal.dotm"
 TotalEditTime: "1.8 hours"
 Words: "0"
 ZipBitFlag: "0x0006"
 ZipCRC: "0x2a6675f6"
 ZipCompressedSize: "445"
 ZipCompression: "Deflated"
 ZipFileName: "[Content_Types].xml"
 ZipModifyDate: "1980:01:01 00:00:00"
 ZipRequiredVersion: "20"
 ZipUncompressedSize: "1900"
first_submission_date: 1554194217 # 2019-04-02 04:36:57 -0400 EDT
last_analysis_date: 1554194217 # 2019-04-02 04:36:57 -0400 EDT
last_analysis_results:
 <---TRUNCATED--->

APIv3 - URL Data w/Filter

```
blevene@blevene-iacpro ~/Malware_Stuff vt url -i first_submission_date virustotal.com  
- url <a354494a73382ea0b4bc47f4c9e8d6c578027cd4598196dc88f05a22b5817293>:  
  first_submission_date: 1276681241 # 2010-06-16 05:40:41 -0400 EDT
```



```
blevene@blevene-iacpro ~/Malware_Stuff vt url -i first_submission_date  
virustotal.com  
- url <a354494a73382ea0b4bc47f4c9e8d6c578027cd4598196dc88f05a22b5817293>:  
  first_submission_date: 1276681241 # 2010-06-16 05:40:41 -0400 EDT
```

APIv3 - Search VTI

```
✖ blevene@blevene-imagpro ~ vt search "metadata:VPS2day size:75KB+ size:100KB-" -I -n 25
b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810
2589053adc1f830c667dfd5ac4fadf0c8161b8a48ae2c30200cfc5e3b8bb7957
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37
f46ab59d7c9aee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb
2c5da5f76808b9f6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616
dc0b933d259b5ec516e5d361da3ae3cfff5bbba53e8895db485dc9a3f4a4b42c3
16590482d1729a5353599009da917e36cab70e497fbcf4a7e808c0ba6cbedc65
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee
```



Where -I is identifiers only (hashes) and -n is number of results

```
✖ blevene@blevene-imagpro ~ vt search "metadata:VPS2day size:75KB+
size:100KB-" -I -n 25
b331ae16014d6219f1e2e3a2e2d568e7836bfbb0e6b40ec081a3c71edd508a37
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810
2589053adc1f830c667dfd5ac4fadf0c8161b8a48ae2c30200cfc5e3b8bb7957
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37
f46ab59d7c9aee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb
```

2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616
dc0b933d259b5ec516e5d361da3ae3cff5bbba53e8895db485dc9a3f4a4b42c3
16590482d1729a5353599009da917e36cab70e497fbcf4a7e808c0ba6cbec65
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee

MORE WITH:

```
vt search 'metadata:VPS2day size:75KB+ size:100KB-' --identifiers-only=true  
--limit=25  
--cursor=NMvJrqPKAQDQfT7jSr1KeBeKydXSVWQmAzaDAYONiiFGM48Fpojy71m03vls  
zn-_blXffP3-KhEal9_f35_P56-tmtcFDSHu_0qH7jseq--N_q56lLdt9c77NP9e8nhOy3-n67  
wM80-uY6ppwTbV70fZE071ujFG2qa-LCzo_vD927tEqsQk5tP0u_Yotp1cQWaxlXNYFHa  
gShZUPw9B0nhyd_MyCkuWveSgPbfSqspxSjKCMdPaEGS5VkoZWVukdwfa0Pox0HuqG  
MreCKelHFJLa5JxW5H2ZpmX4yfAXBLHAn11zwrDg9QibBHh2adccCKgFh14RcFSbC_XP  
1nAygxZOEIRylkvzbt1OpEQGjtjyOndCcYY8jg7K-dFOLxDZNnlKJ5zyog6TzYLJ-78O7eWtxl  
ttTFBZj-6A2NuXj0TICARP1HM6AXLO8qy7usBTpeGupeLs3Fre76h_ALFyk2UeCrC5LNdL  
GjatmMOV9yPVC2wF11Wkq2Xe0hRMOme1SeUilK835phuoh1b54lutu7cXxvoag9FWO  
g9pdNvTNfJK7XgjimQ84r6SrjklxwaR6paB9PIT7PgWbSQjrKF_GN7GJHemTuH_zZ5XSJX  
OUjJnQF4TiZ5LXNqGZUuWufokJwkZ4aAd31XLDRawzlx_F0H-jRoSivWbNzDJmgzbWDJ  
Kwz-5D2U7qgzmcdmD6vSj9Wx4gL52lALzxPvWvS3TbP2XK6uF1wuzZH7S-UgQNz0qHr  
4bC5jhY5b-MNVIMDHRzO2UuicOj0IRVFXBR9mNifBMGKiz3gx8fDERVN8cM5kqfPbtNh  
XMzE-dzrlVZITJHAHTPtVfKsmoVGnfGjwoxcTwcxB3g0RMASONuS3bS-Oc-R4TRMXPxM  
OXzZSPwAH1xV2wnrqLBIGO-In5SEYTT6nk06-EVcGx5CrOqEWvbzzQ1u0oW_z4rc3h88  
T3gi3ygh1AWA7h9-QAgwT25iO5Ufq-15yOyp52uhn3iZaqhvUXVuEDCB9uLqS7QZQOx  
NyTK30vx8Yj1PZ02VelUI0WARzGncmzPb0oyOq5_P-13_h4UV00oZqG-clFqRumRNpczn  
byJW2ShUwHYtuDCkpwjsER4VIFR1SbNmJJIM5CvA3AOK1bVwEFSWhNyqN4uy6p33V  
B5c_Cu8AQmqo4Zjm7NCbK9h-BbCOiN3ZxVblqP3A1s__7PspKAm9Z8xj9djuIsRvEv-uzb  
Lshi_M-IOvJf9Jlnr8IVPxNiiSvAvGntIVXoR_A_IGWL-lcjWiYl2joW_yD5jX_-teXVRRlJr5-k_  
_7x_8DAAD_
```

APIv3 - Search and Download VTI

```
❌ blevene@blevene-imagpro ~/Malware_Stuff vt search "metadata:VPS2day size:75KB+ size:100KB-" -n 25 -d
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb [ok]
b331ae16014d6219f1e2e3a2e2d568e7836fbfb0e6b40ec081a3c71edd508a37 [ok]
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a [ok]
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa [ok]
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765 [ok]
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9 [ok]
2589053adc1f830c667dfd5ac4fadf0c8161b8a48ae2c30200cfc5e3b8bb7957 [ok]
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096 [ok]
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229 [ok]
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810 [ok]
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789 [ok]
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77 [ok]
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab [ok]
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37 [ok]
f46ab59d7c9aee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8 [ok]
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb [ok]
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb [ok]
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a [ok]
2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616 [ok]
dc0b933d259b5ec516e5d361da3ae3cfff5bbba53e8895db485dc9a3f4a4b42c3 [ok]
16590482d1729a5353599009da917e36cab70e497fbcf4a7e808c0ba6cbec65 [ok]
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778 [ok]
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2 [ok]
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee [ok]
9b713329c00f2a98883ea68144c621490804f1bd09aec8f3c1ef242229db914b6 [ok]
```



Where -d is download and -n is number of results

```
❌ blevene@blevene-imagpro ~/Malware_Stuff vt search "metadata:VPS2day
size:75KB+ size:100KB-" -n 25 -d
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb [ok]
b331ae16014d6219f1e2e3a2e2d568e7836fbfb0e6b40ec081a3c71edd508a37 [ok]
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a [ok]
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa [ok]
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765 [ok]
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9 [ok]
2589053adc1f830c667dfd5ac4fadf0c8161b8a48ae2c30200cfc5e3b8bb7957 [ok]
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096 [ok]
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229 [ok]
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810 [ok]
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789 [ok]
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77 [ok]
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab [ok]
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37 [ok]
f46ab59d7c9aee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8 [ok]
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb [ok]
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb [ok]
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a [ok]
```


2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616 [ok]
dc0b933d259b5ec516e5d361da3ae3cff5bbba53e8895db485dc9a3f4a4b42c3 [ok]
16590482d1729a5353599009da917e36cab70e497fbcf4a7e808c0ba6cbedc65 [ok]
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778 [ok]
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2 [ok]
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee [ok]
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6 [ok]

APIv3 - VTGrep

```
blevene@blevene-imagpro ~$ vt search "content:FirstStageDropper.dll OR content:SecondStageDropper.dll" -I  
feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713  
3485c9b79dfd3e00aef9347326b9ccfee588018a608f89ecd6597da552e3872f  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
43f7ae58e8e5471917178430f3425061d333b736974f4b2784ca543e3093204b  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
2d7cb5ff4a449fa284721f83e352098c2fdea125f756322c90a40ad3ebc5e40d  
a63437a044d3ad01c52b0b18016bfbdb8af2338067a4216be2dcaa04ec8ecee97  
bf38bea3f89a697b0be13413b0fb1db2154b3dc79fffbee238014e4adeb0b880
```



Where -I is identifiers only (hashes)

```
blevene@blevene-imagpro ~$ vt search "content:FirstStageDropper.dll OR  
content:SecondStageDropper.dll" -I  
feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713  
3485c9b79dfd3e00aef9347326b9ccfee588018a608f89ecd6597da552e3872f  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
43f7ae58e8e5471917178430f3425061d333b736974f4b2784ca543e3093204b  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
2d7cb5ff4a449fa284721f83e352098c2fdea125f756322c90a40ad3ebc5e40d  
a63437a044d3ad01c52b0b18016bfbdb8af2338067a4216be2dcaa04ec8ecee97  
bf38bea3f89a697b0be13413b0fb1db2154b3dc79fffbee238014e4adeb0b880
```

APIv3 - Upload A Rule

```
blevene@blevene-vmacpro ~$ vt hunting rulesets add TestBotSet ~/Documents/YaraRules/trojan_win_psiXbot.yar
- hunting_ruleset <5529739319771136>:
  creation_date: 1554219815 # 2019-04-02 11:43:35 -0400 EDT
  enabled: false
  limit: 100
  modification_date: 1554219815 # 2019-04-02 11:43:35 -0400 EDT
  name: "TestBotSet"
  notification_emails: []
  number_of_rules: 1
  rules: |
    import "pe"
    rule trojan_win_psiXbot : commodity
    {
      meta:
        description = "Identify PsiXBot dropped from Splevo Exploit Kit"
        author = "blevene@chronicle.security"
        date = "01-04-2019" //dd-mm-yyyy
        reference = "https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/"
        hash01 = "ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79df7ea4ae8"
        hash02 = "1b213a457a9d1949feb5aaca7402ee6a200cb711cc03e22e86f862007404ec5"

      strings:
        //not actually contained in import table
        $s1 = "acledit.dll"

        //ekjynhadfrderatafrhnmkioplplynhatoplhaterafdertayum
        $s1 = {656b0a796e861646566726465726174616672686e16d6b696f706c706c69796e6861696f706c68617465726166646572746179756e64}

      condition:
        uint16(0)==0x5a4d
        and
        {
          pe.imports("authz.dll")
          and pe.imports("clbcatq.dll")
        }
        or for any i in (0..pe.number_of_sections -1):
          (pe.sections[i].name == ".relok")
        }
        and 1 of them
    }
blevene@blevene-vmacpro ~$ vt hunting rulesets enable 5529739319771136
```



Full Console Output

```
blevene@blevene-vmacpro ~$ vt hunting rulesets add TestBotSet
~/Documents/YaraRules/trojan_win_psiXbot.yar
- hunting_ruleset <5529739319771136>:
  creation_date: 1554219815 # 2019-04-02 11:43:35 -0400 EDT
  enabled: false
  limit: 100
  modification_date: 1554219815 # 2019-04-02 11:43:35 -0400 EDT
  name: "TestBotSet"
  notification_emails: []
  number_of_rules: 1
  rules: |
    import "pe"
    rule trojan_win_psiXbot : commodity
    {
      meta:
        description = "Identify PsiXBot dropped from Splevo Exploit Kit"
        author = "blevene@chronicle.security"
        date = "01-04-2019" //dd-mm-yyyy
        reference =
"https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/"
        hash01 =
```

```
"ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffa4ae8"  
    hash02 =  
"1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5"
```

```
strings:
```

```
    //not actually contained in import table  
    $s1 = "acledit.dll"
```

```
    //ekjynhadefrderatafrhnamkioplpliyhaioplhaterafdertayunm  
    $u1 =
```

```
{656b6a796e6861646566726465726174616672686e616d6b696f706c706c69796e68  
61696f706c68617465726166646572746179756e6d}
```

```
condition:
```

```
    uint16(0)==0x5a4d
```

```
    and
```

```
        (
```

```
            (
```

```
                pe.imports("authz.dll")
```

```
                and pe.imports("clbcatq.dll")
```

```
            )
```

```
            or for any i in (0..pe.number_of_sections -1):
```

```
                (pe.sections[i].name == ".relok")
```

```
        )
```

```
    and 1 of them
```

```
}
```

```
blevene@blevene-imagpro ~ vt hunting rulesets enable 5529739319771136
```

APIv3 - Start a Retrohunt

```
x blevene@blevene-imagro ~$ vt retrohunt start ~/Documents/YaraRules/trojan_win_psixbot.yar
blevene_Chron-1554220302
blevene@blevene-imagro ~$ vt rh list
retrohunt_job <blevene_Chron-1554220302>:
  creation_date: 1554220302 # 2019-04-02 11:51:42 -0400 EDT
  eta_seconds: 21876
  num_matches: 0
  num_matches_outside_time_range: 0
  progress: 0.027419341
  rules: |
  import "pe"
  rule trojan_win_psixbot : commodity
  {
    meta:
      description = "Identify PsiXBot dropped from Splevo Exploit Kit"
      author = "blevene@chronicle.security"
      date = "01-04-2019" //dd-mm-yyyy
      reference = "https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/"
      hash01 = "ca30c42334fcc693320772b4ce1d2fe5f1d0110bc454ec6388d79dffa4ae8"
      hash02 = "1b213a457a9d1949feb5aac7402ee6a200cb871c6c93e2e86f862087404ec5"

  strings:
    //not actually contained in import table
    $s1 = "acledit.dll"

    //ekynhadefderatafrhnamkiopllynhaioplhaterafertayunn
    $s1 = [65b66a796e861646566726465726174616672686e616d8b696f786c786c69796e6861696f786c68817465726166646572746179756e68]

  condition:
    uint16(0)=0x5a4d
    and
      {
        {
          pe.imports("authz.dll")
          and pe.imports("clbcatq.dll")
        }
        or for any i in (0..pe.number_of_sections -1):
          (pe.sections[i].name == ".relok")
      }
    and 1 of them
    and filesize < 500KB
  }
  scanned_bytes: 2579372141
  start_date: 1554220307 # 2019-04-02 11:51:47 -0400 EDT
  status: "running"
```



Full Console Output

```
x blevene@blevene-imagro ~$ vt retrohunt start
~/Documents/YaraRules/trojan_win_psixbot.yar
blevene_Chron-1554220302
blevene@blevene-imagro ~$ vt rh list
- retrohunt_job <blevene_Chron-1554220302>:
  creation_date: 1554220302 # 2019-04-02 11:51:42 -0400 EDT
  eta_seconds: 21876
  num_matches: 0
  num_matches_outside_time_range: 0
  progress: 0.027419341
  rules: |
  import "pe"
  rule trojan_win_psixbot : commodity
  {
    meta:
      description = "Identify PsiXBot dropped from Splevo Exploit Kit"
      author = "blevene@chronicle.security"
      date = "01-04-2019" //dd-mm-yyyy
      reference =
"https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/"
      hash01 =
```

```
"ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffa4ae8"  
    hash02 =  
"1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5"
```

```
strings:
```

```
    //not actually contained in import table  
    $s1 = "acledit.dll"
```

```
    //ekjynhadefrderatafrhnamkioplpiynhaioplhaterafdertayunm  
    $u1 =
```

```
{656b6a796e6861646566726465726174616672686e616d6b696f706c706c69796e68  
61696f706c68617465726166646572746179756e6d}
```

```
condition:
```

```
    uint16(0)==0x5a4d
```

```
    and
```

```
        (
```

```
            (
```

```
                pe.imports("authz.dll")
```

```
                and pe.imports("clbcatq.dll")
```

```
            )
```

```
            or for any i in (0..pe.number_of_sections -1):
```

```
                (pe.sections[i].name == ".relok")
```

```
        )
```

```
    and 1 of them
```

```
    and filesize < 500KB
```

```
}
```

```
scanned_bytes: 2579372141
```

```
start_date: 1554220307 # 2019-04-02 11:51:47 -0400 EDT
```

```
status: "running"
```

APIv3 - Retrohunt Matches

```
blevene@blevene-imacpro ~$ vt retrohunt matches blevene_Chron-1554220302 -I -n 50
2644cd4a843e35b807271aeff9ec17a48a7b3214fc052b625dba89796822a240
a7490c93e8423909cf1c53571697b260c17e0b0661bfa538754d72daf965a156
1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5
68102340ddf132808aa231e8884b3426bc430136ac5119228217edd2adc0d83b
c8d2af690ee697a4cb2e3cf81c75227151ed6b96c763892858c47f87677c2807
0252e1e82ce3992e48b6dabc90f33188183ac5029b8d5049f47d087bdfb5bcab
6fb4b6a4e5367ce4bff82fdadb3b3ef64a393b9ee86e677ebaec658606310bd0
ef363c3be4fe16411dcfb52599c9242ef0377daa8742c1e672ace0055f3c88d8
15049d944375f2022a5b3f31dcd0ea9c02f517a6153d9cfc4d8c841d7efe2248
fd35b23d2c02bdd57245acf109fb6961bfaa205a91083983b80898ff2ab5c14d
3736b350803dbac08691679556a35216c318ddd5e10722c5279118d812e721c0
e66a2a247964480415d75b1f524f13f14081c737cdfdca39559a706bd808e8b7
8e13b9d80a746203d2a0e768491c62ee550402e17274e022453adcc7ef1ffbde
9c644b4cab4c4ccc485c2656c291a1089fffe9e0bc6f07d2c17db2bf578095d
ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8
253c4cbf357de49e240ba1695570e20667586dbdeccd820a2d94e773e85b1889
d0a48a5b3faf5e9a531b8fcf2c0be676b20975dfceec624109fec560c4a240aa
21c4e6dfb9017b6de79676649b69de5962883eba8315c0ceef6523bb16d11e72
e985706257e2c9f781723aee5007ccc3bfd16671302e0a53cda1164023cab94e
```



Where -I is the file identifier (sha256 only) and -n is number of results (to auto iterate over pages)

```
blevene@blevene-imacpro ~$ vt retrohunt matches blevene_Chron-1554220302 -I -n 50
```

```
2644cd4a843e35b807271aeff9ec17a48a7b3214fc052b625dba89796822a240
a7490c93e8423909cf1c53571697b260c17e0b0661bfa538754d72daf965a156
1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5
68102340ddf132808aa231e8884b3426bc430136ac5119228217edd2adc0d83b
c8d2af690ee697a4cb2e3cf81c75227151ed6b96c763892858c47f87677c2807
0252e1e82ce3992e48b6dabc90f33188183ac5029b8d5049f47d087bdfb5bcab
6fb4b6a4e5367ce4bff82fdadb3b3ef64a393b9ee86e677ebaec658606310bd0
ef363c3be4fe16411dcfb52599c9242ef0377daa8742c1e672ace0055f3c88d8
15049d944375f2022a5b3f31dcd0ea9c02f517a6153d9cfc4d8c841d7efe2248
fd35b23d2c02bdd57245acf109fb6961bfaa205a91083983b80898ff2ab5c14d
3736b350803dbac08691679556a35216c318ddd5e10722c5279118d812e721c0
e66a2a247964480415d75b1f524f13f14081c737cdfdca39559a706bd808e8b7
8e13b9d80a746203d2a0e768491c62ee550402e17274e022453adcc7ef1ffbde
9c644b4cab4c4ccc485c2656c291a1089fffe9e0bc6f07d2c17db2bf578095d
ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8
253c4cbf357de49e240ba1695570e20667586dbdeccd820a2d94e773e85b1889
d0a48a5b3faf5e9a531b8fcf2c0be676b20975dfceec624109fec560c4a240aa
21c4e6dfb9017b6de79676649b69de5962883eba8315c0ceef6523bb16d11e72
```

e985706257e2c9f781723aee5007ccc3bfd16671302e0a53cda1164023cab94e
4f582ecdd2c8d27e78e774e928a81e9e2f825a90bf2a47659da69810487cb9ee
98d56ba99a8ac192c0cdfed04d989dd60c16e2a8213fc9958be2a6de55696694
e1f459ebd4092ab0b452f3ad6de821d216bd5dc284c497c8c598d01e5543de3f
b2c46f10674f5896b5286607eedf7926dc041e9d12b714df5e9c47cf68ac53d5
cd80b1f027bd4b60b9ff07f66de99d8fcd94dd8efa831bf6671d12c1a2f64c8d
c819375b811d44d9b4df8a60abb1d172e5bbe6ca9aaab69d32e1fddd731cc956
d8235ef57a807f41a4fe10638556b0b190c288ec7dbdb3caa7051daed36d4c89
117a74639b66dc02c05bb001fd56fe7ac9bee3e455da4f610512ae2da266863a
af69fa9caa8854bc3925dad5d3b44e5703a229327239c904aa7ecf5b41ec00e4
c5d5e51532eed12cb9d86dfe9db390bc1d11b5b6f0d87e554b66f925bec5aa56
cb0f11d274f1afa6b165f083e4bfc16bc180b1973c19af2cf682907e43fd1dc9
ebfa7d124cea4879272fbd573905f8ab2c26ca8726456b6729934cdd137e5413
560698ec061d49e68641ddc7540b41dbb51e92ec95d313227ed3c60c62f4753d
49c183642a00ef798fbc3863dc81152088edc1ad564dd48f500991dcbe3531b
832ea36a11d13e0ce5f6fcd527627c777428f2d44efd0b4ad54ca8fa5a6cd035
3036fae7550f78c47af3d8d9e9f241cb0a84da9c48c71d9ed849830c1fa53311
ecdbfa957b07ed7f07b614e2e3a2a75925ef05540bdee6e03827516b4ae09611
a880bc28ca5d5ce380e8a577cc238e0d917515ebcc07b352bb43db54d858b2dd
bb90f394332450601dbb10c539d68cb8ad9d03ddc25efc41b81e4e8bafd90aee
ffc7533231c9c6cb6f8ce6b3b0d9a9d1b66046650bf67c36d3d38111f84b61c8
5deb49db0a16cd1588a0b3d8ceea97d9d6cf73ca83814a32c540947359994b4a
39ade6f3e847ba1c2918920743e85fbc71642a2eac731a3ab1387cb8e491b038
39ade6f3e847ba1c2918920743e85fbc71642a2eac731a3ab1387cb8e491b038
b3fd922d6e9b405ec4415aac4927e53f173d2b8c91f105f516d1f147f42412e6
4f5cc216cb3f6a77c14ecf803095ca44003dcb1ce54944209c859ace9e02e535
31d1194936842cfca74d2526cbc75f0801ce54eeab9a85bb107fd3d5b627d055
9054f32c2bb375fea99bced0b9ea0654d724b6b53a48ca03c3f8d1b379160fcd
893fef03eb3ab0afb9193858f7fa7a34c847d5b18ef2ca89ba97f57515d9894f
c0e6ecc25387d5d537bf24110acd31232028d1c2bff7e3cdef67c28218f3da6b
7e2dc01cd6f14c57d95fe9421f5120b2bbe858028a3330fb1f3f3c1909bbc45d
f64f5f11a5c0d2a6983607b4b8789b6be3ab0dd1ba7114e876fcb5ab2c8d8585

APIv3 - Hunting Notifications

```
blevene@blevene-imagpro ~$ vt hunting notifications list --cursor=JM3PTsIwHADgu4_RxJvSysQFEmLmKGQCMxDDYDEh3dbRn-va2T9b1PjuHrh9t-8XbUA1aIaEc52dYTwMw6gH463TjslRqVvMOsB9gL3lxuJC8p4rfo6F0QoLrxyoy1lpBzWUzIFW9tlweZWAzs5rkPzDEzJ-Kr2x2szj5nFNd5rmqyXJ98lrOV1uP05WU5j-nn4osf0vmrLd3VMSRHSRbFKbREcmhKiDRVpUmUTwrKJem-nhGV5dxovCcumfpXEUZIG67DbbRYvlylJ6G2wuNYSWnDzB4Lu0FtdW-7QjPzd_AcAAP__
```

```
- hunting_notification <5223863694327808>:  
  body: ""  
  date: 1554217750 # 2019-04-02 11:09:10 -0400 EDT  
  file: "1a7a99b970fdbe2c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
  subject: "AV_trojan_win_Emotet: Emotet"  
  tags:  
    - "emotet"  
    - "av_trojan_win_emotet"  
    - "1a7a99b970fdbe2c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
    - "av_emotet"
```



Full Console Output

```
blevene@blevene-imagpro ~$ vt hunting notifications list  
--cursor=JM3PTsIwHADgu4_RxJvSysQFEmLmKGQCMxDDYDEh3dbRn-va2T9b1PjuHrh9t-8XbUA1aIaEc52dYTwMw6gH463TjslRqVvMOsB9gL3lxuJC8p4rfo6F0QoLrxyoy1lpBzWUzIFW9tlweZWAzs5rkPzDEzJ-Kr2x2szj5nFNd5rmqyXJ98lrOV1uP05WU5j-nn4osf0vmrLd3VMSRHSRbFKbREcmhKiDRVpUmUTwrKJem-nhGV5dxovCcumfpXEUZIG67DbbRYvlylJ6G2wuNYSWnDzB4Lu0FtdW-7QjPzd_AcAAP__
```

```
- hunting_notification <5223863694327808>:  
  body: ""  
  date: 1554217750 # 2019-04-02 11:09:10 -0400 EDT  
  file: "1a7a99b970fdbe2c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
  subject: "AV_trojan_win_Emotet: Emotet"  
  tags:  
    - "emotet"  
    - "av_trojan_win_emotet"  
    - "1a7a99b970fdbe2c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
    - "av_emotet"
```

APIv3 - ASCII Cinema

<https://asciinema.org/a/179696>



<https://asciinema.org/a/179696>

Thank you.

info@virstotal.com
virstotal.com/learn