

# 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/](http://www.virustotal.com/gui/)



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

<https://www.virustotal.com/subscription/event/klas19/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

The screenshot shows the VirusTotal Query Builder interface. At the top right are three buttons: a blue one with a grid icon, a grey one with a list icon, and a lightbulb icon. Below them are two rows of search fields. The first row contains 'File Type' with a dropdown arrow, 'Detections' with a dropdown arrow, and 'or more' with a dropdown arrow. The second row contains 'Min. File size' with a dropdown arrow, 'KB' with a dropdown arrow, 'Max. File size' with a dropdown arrow, and 'KB' with a dropdown arrow. Below these rows are two input fields: 'Antivirus label contains...' and 'Behavior report contains...'. To the right of the 'Behavior report contains...' field is another input field labeled 'File metadata contains...'. At the bottom right of the interface is a 'VirusTotal' logo.



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

---

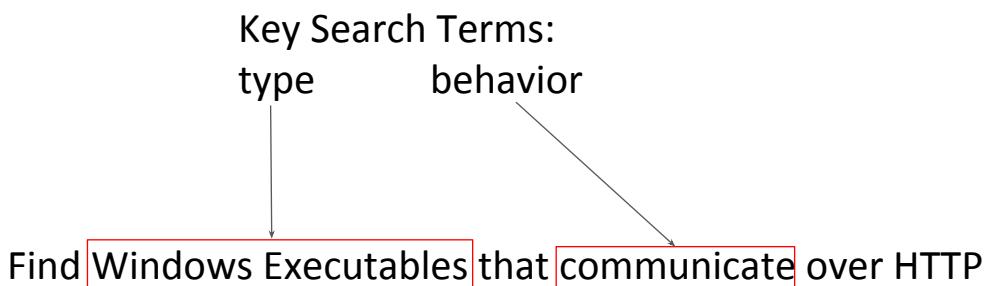
Find Windows Executables that communicate over HTTP



<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

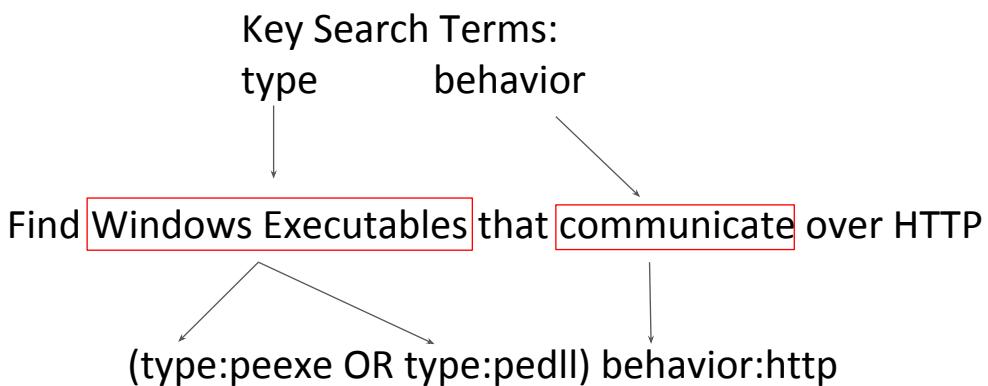
## Example 1



<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



 VirusTotal

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

[https://www.virustotal.com/gui/search/\(type%253Apeexe%2520OR%2520type%253Apedll\)%2520behavior%253Ahttp](https://www.virustotal.com/gui/search/(type%253Apeexe%2520OR%2520type%253Apedll)%2520behavior%253Ahttp)

- 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/\(NOT%2520type%253Apeexe%2520OR%2520NOT%2520type%253Apedll\)%2520\(itw%253Adropbox.com%2520or%2520itw%253Abbox.com\)%2520p%253A10%252B/files](https://www.virustotal.com/gui/search/(NOT%2520type%253Apeexe%2520OR%2520NOT%2520type%253Apedll)%2520(itw%253Adropbox.com%2520or%2520itw%253Abbox.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%253Artf%2520\(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve\)%2520NOT%2520tag%253Amacros/files](https://www.virustotal.com/gui/search/metadata%253A%2522Windows%2520User%2522%2520type%253Artf%2520(tag%253Acve%2520or%2520engines%253Aexploit%2520or%2520engines%253Acve)%2520NOT%2520tag%253Amacros/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%253Arus%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%253Arus%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%253Arus%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%253Arus%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 'Details' tab of a VirusTotal analysis page. At the top, a circular progress bar indicates 48 engines have detected the file. Below the bar, the file's SHA-256 hash is listed as f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf. The file is identified as a Win32 EXE and was submitted 1 month ago. The 'Community Score' is shown as 67.

The main content area is divided into several sections:

- DETECTION**: Shows 48 engines detected the file.
- DETAILS**: Contains basic properties:
  - MD5: f0b2e393c18182c7bd48ce1f6e6c6765
  - SHA-1: b6ea6907e036324b95995ef7d6a37ee05d37c5b
  - SHA-256: f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf
  - Authentihash: 3d8871749d75f76677de18bfef878b7aeaafab09460dadfeeed13cccb3183b968f
  - ImpHash: d0472d140aa0003beaf55821a63a5b03
  - SSDeep: 6144yhO/cBXBBA01rsU1XHBNvVgdiv94pSpuOEz7HLYE/k4VQ/SXkllm:y
  - File type: Win32 EXE
  - Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
  - File size: 552.38 KB (565637 bytes)
- RELATIONS**: Overlay and peexe.
- BEHAVIOR**: Not visible in the screenshot.
- CONTENT**: Not visible in the screenshot.
- SUBMISSIONS**: History section showing submission details:

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
- COMMUNITY**: Names section showing file names:

Names
f0b2e393c18182c7bd48ce1f6e6c6765.vir
Kidneys
Kidneys.exe

VirusTotal

<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

The screenshot shows the VirusTotal analysis interface for a file. The top bar indicates "48 engines detected this file". Below the bar, the file's SHA-256 hash is listed as f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf. The file size is 552.38 KB, and it was submitted 1 month ago at 2018-10-25 11:56:39 UTC. The file type is identified as "EXE" and "peexe".

The main interface has tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, CONTENT, SUBMISSIONS, and COMMUNITY. The DETAILS tab is selected, showing:

Basic Properties	Value
MD5	f0b2e393c18182c7bd48ce1f6e6c6765
SHA-1	b6ea6907e036324b95995e77da37ee05d37c5b
SHA-256	f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf
Authentihash	3d8871749d75f76677de18bfef878b7aeaafab09460dadfeeed13cccb3183b968f
Imphash	d0472d140aa0003beaf55821a63a5b03
SSDeep	6144yhO/cBXBBAQ1rsU1XHBCnVgdi94pSpuOEz7HLYE/k4VQ/SXkllm:y
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	552.38 KB (565637 bytes)

The Signature Info section lists the imphash value: d0472d140aa0003beaf55821a63a5b03.

The right side of the interface displays the History and Names sections. The History section shows the following timeline:

Event	Date
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

The Names section lists the file names: Kidneys and Kidneys.exe.

Σ VirusTotal

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 peexe overlay	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"/>	f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf Kidneys.exe peexe overlay	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 peexe overlay	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"/>	9e72e130898ab79c26c264775ec2ceccce514a823212f8131af9a44477c38091 Kidneys.exe peexe overlay	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"/>	aefe8c24adff73a20e4dff0260dc6ec33042b423fc921c350f355f61aaf70dce Kidneys.exe peexe overlay	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"/>	923fc901116decae68cfa461ab9c9064385fd2b9b206b3ba011e5008fe37b3 Kidneys.exe peexe overlay	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 peexe overlay	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"/>	c5eae65e0ce1325b79771f1a54bb2664e5e09139ced0ecd6e035cab1c7d09c45 Kidneys.exe peexe overlay	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%25227326001be3ced77b153640be93a8dff6%2522/files>

TLDR: You're actually matching the packer.

## Similar-To (vhash)

similar-to:f579682f1be62564aab114b2cb1dc06e7ced77406f61b1b8a11eb92f5ed88fdf

FILES 40+

File Hash	Type	Peexe	Overlay	Hash Count	File Size
719d15bc6874277ad6c62521064b9a8afeb7243aca864e9cb1c1d53c7f6ffed	PDFProfitLock.exe			13 / 68	518.08 KB
4c8af43ca299b2853928bd38f90fdc74291d2a3f8810a5b6574ef1cda71690e	PDFProfitLock.exe			12 / 65	530.49 KB
2aafdf61ac7974a25c52faa0c66c88b472fb74f96964495799fb6c9028692c974	Kidneys.exe			53 / 69	552.38 KB
b988c65c1f015491a0049c1e8e5becf303644efc83826133354d2735a0395721	Uninstaller.exe			25 / 65	540 KB
be69330bb44534fe4feb56f4d855971172ba8a8b5f9c98f9fea7e1417a0cf34	AREMAIN9.EXE			4 / 68	552 KB

VirusTotal

<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+

File Hash	Scan Status	Size	Date	Submissions	Submitters
13655185bac5e8ad856c3ld2ab93ba2af112a181f14ce66d22214b006b164ee8	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
de9d80a37b2179e0ef94055c5f588f56c16ed66568142b49e2aed36a6a65945	43 / 65	556 KB	2019-03-17 19:10:51 first seen 2019-03-20 12:00:10 last seen	2 submissions	2 submitters
a498aa74340381622ac341543e80de9f73beab9c7dd7cf68ea225ae6fffbfc	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
5155f749eb8977650b92393e84d368cc76dee1908514bc42d5a423afbc7ba260	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
e780fc9aa68787ad4d62e71c382f21b985a85112a2246b675fd92e3d5277f5de	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

VirusTotal

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

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbfe2a389bc3d54e37de8c7a8dc73a95a7f093b/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: 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/2db7425c7c9efffc87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

# Visual Similarity: PDF

The screenshot shows the VirusTotal interface for a search result titled "main\_icon\_dhash:2313230300020000". The results list several PDF files, each with a thumbnail, file name, detection count, size, and submission details. The files are:

File Hash	Detection Count / Total	Size	Last Seen	Submissions
944d60d78cea444fed42489abb7d2c6304296447c769e7cb583c369511d69cf5	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
26c093074ec4f0bf1ea5863c0e88cff700a445e81b249ea608f28c2d736c63d	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
45ce591e001e8de45e1fd19ec8a29fb63ca3d47ed63cda604d806aa96d29e	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
6219dc8787ddbf49b383e19d9da2b6758207e1d25dc32863722cd1dcbcd8ba6	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
e876d50e96bcf114f116102d2eb7c7ad4030e0fa7729388af8d697d2a2e6d2a	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

**VirusTotal**

<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/01c299e4895eb222d24ad9c6bbe2a389bc3d54e37de8c7a8dc73a95a7f093b/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/2db7425c7c9efffc87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45/detection>

# Visual Similarity: Office Documents

The screenshot shows the VirusTotal interface for visual similarity analysis. At the top, there is a placeholder icon labeled "main\_icon\_dhash:0103001101000301". Below it, a section titled "FILES 2" lists two files:

File Hash	Type	Detections	Size	First Seen	Last Seen
85f7ab110807cf0352ada5582611cc64af0e13ad8f32561d3e2c2763a70659c3	doc	33 / 56	46.02 KB	2019-03-12 14:10:29	first seen 2019-03-12 14:10:29 last seen
2db7425c7c9efff9c87fb45719ac4a9c7b24722f2cf19de1ba7f1b9d1f59de45	ADP-Document-3810922.doc	43 / 60	46 KB	2018-07-19 16:31:07	first seen 2018-07-30 04:48:49 last seen

Below the file list, there is a "VirusTotal" logo.

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

Trickbot EXE:

<https://www.virustotal.com/gui/file/01c299e4895eb222d24ad9c6bbe2a389bc3d54e37de8c7a8dc73a95a7f093b/detection>

Emotet PDF:

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

ADP Lure Doc:

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

# 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"

FILES 5

MD5 Hash	Detections	Size
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f	41 / 66	1.21 MB
tgyfutrc	pexe overlay	
c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	39 / 66	1.21 MB
tgyfutrc	pexe overlay revoked-cert signed	
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26	47 / 71	1.19 MB
zzbdrlimp	pexe overlay revoked-cert signed	
ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f	43 / 70	1.19 MB
imtvknqq	pexe overlay revoked-cert signed	
eda26a1cd80aac1c42cd8ba9af813d9c4bc81f6052080bc33435d1e076e75aa0	43 / 67	1.2 MB
yxugwjud	pexe 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%2522ALIS%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"

FILES 5	
<input type="checkbox"/> 88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f	45 / 71 1.21 MB
<input type="checkbox"/> tgtyutrc peexe overlay	
<input type="checkbox"/> c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	44 / 71 1.21 MB
<input type="checkbox"/> tgtyutrc peexe overlay revoked-cert signed	
<input type="checkbox"/> 7bcd69b3085126f7e97406889f78ab74e87230c11812b7940d723a80c08dd26	47 / 71 1.19 MB
<input type="checkbox"/> zzbdimp peexe overlay revoked-cert signed	
<input type="checkbox"/> ba15c27f2626514b063b65654e9d7c248dd651919fafb68cb4765d1e057193f	45 / 71 1.19 MB
<input type="checkbox"/> imtvlnqq peexe overlay revoked-cert signed	
<input type="checkbox"/> eda26a1cd80aac1c42cd9ba9af813d9c4bc81f6052080bc33435d1e076e75aa0	46 / 70 1.2 MB
<input type="checkbox"/> yxugwjud 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 which 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"

□ FILES 36

6cc84b3a58eea27e84f489b9bde5ac81fb0f0f5db6cd9327b26ffb776ad53288  
PO-2815.doc 25 / 59 147 KB  
□ doc copy-file create-file create-ole environ hide-app macros obfuscated

728bbbea8797c5e00a8737ebf6bebffffb3d84f9c86f144963a2940025329c28b  
complaint-143.doc 35 / 56 91.5 KB  
□ doc create-file create-ole environ macros run-dll run-file

59a24d9ac0ed2f2bea3883d7b943ab1229acf3f9f350f2dee6deb14c559920b  
document.doc 15 / 60 35.5 KB  
□ doc create-ole environ hide-app macros obfuscated open-file write-file



<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"

## FILES 5

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



<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+

b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4

mimilib.dll

pedll  64bits  assembly

30 / 63

120.5 KB

mimilib.dll

pedll

≈

37 / 69

104.5 KB

4a5ebda8ec96e7d3f1a976d748e7e42f95e46f9d46c360b886d13ee4212a6fa0

mimilib.dll

pedll

27 / 67

130 KB

 VirusTotal

<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:"SpLsaModeInitialize"

# Imports and Exports

```
exports:"InitializeChangeNotify" exports:"PasswordChangeNotify" exports:"SpLsaModeInitialize"
```

FILES 20+

<input type="checkbox"/> b04e58327191222e27405c2dc4871cb4c81e3ea732d70c67ad744088619c97e4				30 / 63	120.5 KB
<input type="checkbox"/> mimilib.dll				8 / 67	68.5 KB
<input type="checkbox"/> w1and1g.dll				37 / 69	104.5 KB
<input type="checkbox"/> f6413029e7a43d7eb5d44772efb413553e8896c2b287dd41de2fa380c58e611c				pedll	64bits assembly



<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:"SpLsaModeInitialize"

# 03

VTGrep

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

## VTGrep (aka Content Search)

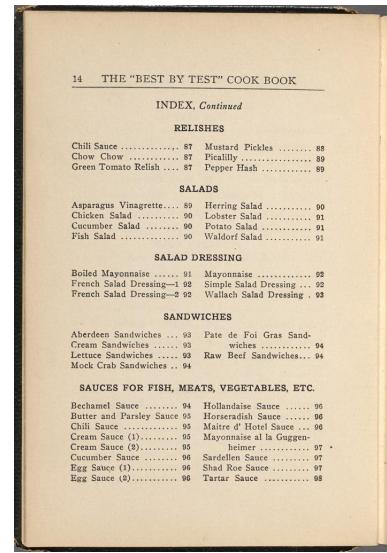
Use the “content:” search modifier to search for arbitrary hex or string patterns within files on VirusTotal



<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...



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

# VTGrep: Example 1, ASCII Strings

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
STRINGS	HEX					

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



<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		
96e484009a93c796c2a405b5375b5b054abd3b5579d9f493d4f97a31aecf8b6b		
peexe	45 / 68	698 KB
testtab.png	46 / 66	390 KB
3e0b63b51df79e2f40b7a775d1d353d68594eef3617afd56804ac00775754d89		
peexe	54 / 69	394 KB



<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\anc  
horInstaller\_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

- 18d347001057c68cf2fad1d2f5af73e2dfa69aa46466fa43b40d7da360b79c01  
1fe7f68f073ebf9162f1a46a5d45d43c.virus  
pedil 41 / 69 140.5 KB
- a38567922a6424b4821569805aa74cd28e124985cf0d01838cc797568f6ba90c  
c2.dll 20 / 68 134.5 KB  
pedil
- 96e484009a93c796c2a405b5375b5b054abd3b5579df493d4f97a31aecf8b6b  
peexe 45 / 68 698 KB
- 191c372af20a9affa19acb522cb7af2e0b3cd0d38e4a88c1c2224a75ac35ded  
netmsgwy.dll 30 / 67 133 KB  
pedil
- 5739549850fe635fc0ac5de81ce1fd495669fcabc1b8ede35b82a22093c86399  
testtab.png 46 / 66 390 KB  
peexe

VirusTotal

<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 VTGrep interface with the following details:

- Navigation:** DETECTION, DETAILS, RELATIONS, **CONTENT**, SUBMISSIONS, COMMUNITY.
- String Types:** STRINGS, HEX.
- Search Results:** A large block of text from the OpenSSL FAQ is displayed, including:

```
You need to read the OpenSSL FAQ, http://www.openssl.org/support/faq.html
HKLW,"SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL","CheckedValue","0x00010001","%d"
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Software\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
setupapi.dll,InstallHinfSection DefaultInstall 128 %s
%s(%d): OpenSSL internal error, assertion failed: %
%-23s %s Kx=%-8s Au=%-4s Enc=%-9s Mac=%-4sts
%s",AfxGetHttpRequestMgr %s
```
- Filtering:** A dropdown menu shows "1" and "9" with an arrow pointing to it, and a star icon.
- Character Encoding:** ALL, ASCII, **WIDE**.
- Result Box:** A box highlights the string `" %s",AfxGetHttpRequestMgr %s` with a "WIDE" label.
- File Hash:** VirusTotal (Σ) is shown at the bottom right.

<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:%7B22002500730022002c0041006600780047006500740048007400700052006500710075006100730074004d0067007200200025007300%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

b2737192ea1c912daa3ca4c43224fb6afcc878c5e3303e86a459de06df7af33f	47 / 69	1.04 MB
HYPERTRM.dll		
pedll	🔗	
b3ed50daf7b7285122573eec71fdb744a796b6d55a861efd96bb5cd7520b32d	35 / 61	931.5 KB
virussign.com_4dfa27a5138b9b158ecf9bbc65906e0.vir		
pedll	🔗	
dc0e869bfbdbdeb1d4300e5ed57f347c53698107f30e4753ed4b1078ac1f99008	27 / 66	1.04 MB
b50e5fa05e9e995067226403d245afe		
pedll	🔗	
33b8bf2c05a88afaf175fe58c0e2f87158f211110a050f48620bba057a137c18	45 / 67	931.5 KB
97e4973c618813ba75014fe4d7f4dbcd379a9795		
pedll	🔗	



<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: "

<input type="checkbox"/>	FILES 9+			
<input type="checkbox"/>	f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96 iSatSrv.exe	<input checked="" type="checkbox"/> peexe <input type="checkbox"/> overlay <input type="checkbox"/> signed   	41 / 71	2.29 MB
<input type="checkbox"/>	acf46be54c303002d74df6c975083c706b3e1cb8a92e75516579cd0fe65ce918 iSatSrv.exe	<input checked="" type="checkbox"/> peexe <input type="checkbox"/> overlay <input type="checkbox"/> revoked-cert <input type="checkbox"/> signed   	30 / 65	192.06 KB
<input type="checkbox"/>	3bc3552b1701280d0fa1c534901c0b926fef61314a1e76eaa7f9623054225633 windmhip.exe	<input checked="" type="checkbox"/> peexe <input type="checkbox"/> overlay <input type="checkbox"/> revoked-cert <input type="checkbox"/> signed   	30 / 65	200.21 KB



<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 specific 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 klsihk.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

FILES 15

- feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713.sample  
...fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713.sample  
pedll 64bits assembly cve-2018-5002 exploit  
29 / 70 194.5 KB
- 3485c9b79dfd3e00aef9347326b9ccfee588018a608fb9ecd6597da552e3872f  
pedll 64bits assembly cve-2018-5002 exploit overlay  
44 / 69 194.5 KB
- 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



 VirusTotal

<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

The screenshot shows a list of files analyzed by VirusTotal. Each file entry includes a checkbox, the file name, its SHA-256 hash, the number of positive detections (red) and total scans (black), and its file size. Below each entry are several small blue circular icons representing different analysis details.

File Hash	File Name	Detections / Total Scans	Size
9dd4032902d83367286ebc453e440a423625a3cb7b3191a55811a2d51b222986	a27dbbfafaa2a384ba9cc3e0ceb0a86c6.e.virus	40 / 68	167.21 KB
f5c4782591675cd51ac3cdfd1bc719d576b7b98d529cf281b706d94fd1916c96	iSatSrv.exe	41 / 71	2.29 MB
acf46be54c303002d74df6c975083c706b3e1cb8a92e75516579cd0fe65ce918	iSatSrv.exe	30 / 65	192.06 KB
3bc3552b1701280d0fa1c534901c0b926fe61314a1e76eaa7f9623054225633	windmhlip.exe	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

content:{4d5a5000 [0-10000] 76 69 72 75 73}@0

FILES 20+

2576925e89c4fce16551a72cad0d54c880cc24a231b01504bd3ae85f54bf9cd8

Virus.Win32.Expiro.a

53ff4fa166854d5ad05c1271dfeff74cf56137d034

16eeea60a246493459a8d24bf55417460.virobj

8c2c15688fc3875b4419c9091204b89161d676c

Virus.Win32.Ultratt.8166.b

bce663271b2f08f72de77705022ad98664e5cd8

mz

928e5133ec0fdad4ddedf05322eb7ea5ca99d3a

Virus.Win32.HLLP.Taris.b

Match context

2010-06-16 19:48:16 first seen 17 submit note

ssic then ssic then ssic then miss note

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 00 01 00 .....  
00000040: BA 10 00 00 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 0D 0A 24 37 00 00 00 00 00 00 00 00 in32.\$7.....  
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 .....  
... ... ...  
00001C90: 00 50 FF 95 F3 1C 41 00 93 8D BD D5 19 41 00 8D .P....A.....A..  
00001CA0: B5 9F 19 41 00 57 53 FF 95 EF 1C 41 00 87 FE AB ..A..WS....A....  
00001CB0: 87 FE 32 CO AE 75 FD 80 3F 55 74 02 EB E7 C3 8D ..2..u..VU.....  
00001CC0: BD F0 18 41 00 EB 0B 00 00 00 32 CO AE 75 FD 80 ..A.....2..u..  
00001CD0: 3F FF 75 F1 C3 33 DB 57 53 FF 95 97 19 41 00 91 ?..u..3..WS....A..  
00001CE0: E3 OC 53 53 6A 12 51 FF 95 9B 19 41 00 B1 F9 C3 ..SSJ.Q....A....  
00001CF0: 41 56 50 20 4D 6F 6E 69 74 6F 72 00 41 6D 6F 6E AVP Monitor.Amon  
00001D00: 20 41 6E 74 69 76 69 72 75 73 20 4D 6F 6E 69 74 Antivirus Monit  
00001D10: 6F 72 00 41 56 47 20 43 6F 6F 74 72 6F 6C 20 43 or AVG Control C

VirusTotal

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

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

The screenshot shows the VTGrep interface with three main sections:

- Content Analysis:** Three boxes show extracted text:
  - content:"M4BUBc\_ / Asc"
  - content:"Dim AWYbM5aiAllCElynkc7xb4gRO"
  - content:"JACKY ROSEN"
- Compressed Parents:** A table showing statistics for compressed files.

Scanned	Detections	Type	Name
2019-04-01	28 / 59	ZIP	603f7b0eb76af3a55738036dacc8d417e9 1f69d3e231c51d0e91fd7befaacc0
- Macros And VBA Code Streams:** A section showing code snippets from ThisWorkbook.cls and OzqB.bas, with a preview of the code "Dim AWYbM5aiAllCElynkc7xb4gRO".
- VirusTotal Preview:** A preview window showing the extracted text "JACKY ROSEN" and the VirusTotal logo.

content:"M4BUBc\_ / Asc"

content:"Dim AWYbM5aiAllCElynkc7xb4gRO"

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

The screenshot shows the VirusTotal analysis interface for a file. At the top left is a circular progress bar with the number '39' and '/ 60'. To its right, a message says '39 engines detected this file'. Below this are file details: SHA256 hash (f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b), file name (SEP #979IGW.doc), size (83.88 KB), date (2018-11-23 00:26:16 UTC), and a '3 days ago' timestamp. A 'DOC' icon is also present. Below these details is a navigation bar with tabs: DETECTION, DETAILS, RELATIONS, BEHAVIOR, CONTENT, SUBMISSIONS, and COMMUNITY (with a '2' badge). The DETECTION tab is selected, showing a dropdown menu with the date '2018-11-23T00:26:16'. The main table lists 13 detection engines, each with a status icon, the malware name, and the detection engine's name. The table has a blue header row and white rows for the data.

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

VirusTotal

## T1/SOC/ANALYST POV

Or

EmotetDoc: f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

# A [Near] Daily Occurrence: Emotet Droppers

The screenshot shows the VirusTotal analysis interface for a file. The 'DETAILS' tab is selected. 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 names such as SEP #979IGW.doc, O2\_13\_11\_18.doc, PAY #397267OYCKGII.doc, and BIZ #460536H.doc. The 'Commonly Abused Properties' section indicates the file makes use of macros and may try to run other files. The 'Macros And VBA Code Streams' section contains a single entry: cHiZVOci.cls. The 'History' section shows creation time (2018-11-13 06:28:00), first submission (2018-11-13 06:54:16), last submission (2018-11-13 06:54:16), and last analysis (2018-11-23 00:26:16). The 'Names' section also highlights the file names listed above. The 'ExifTool File Metadata' section is present but empty.

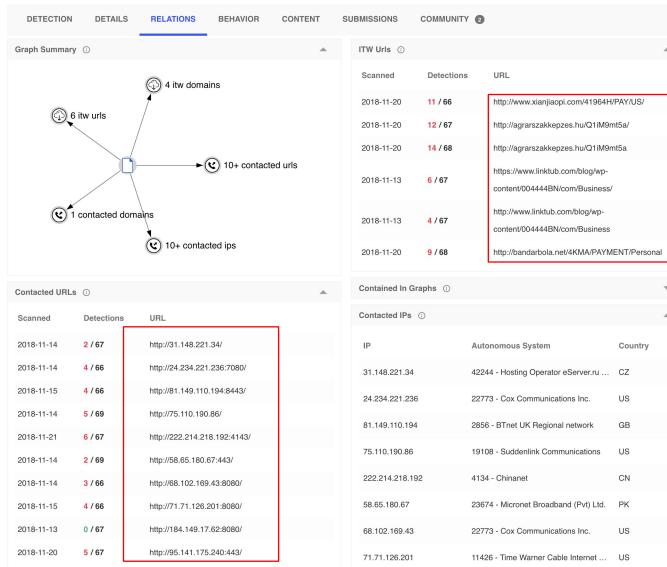
VirusTotal

## T1/SOC/ANALYST POV

Or

EmotetDoc: f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

# A [Near] Daily Occurrence: Emotet Droppers



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/BIZ/IhreSparkasse/
2018-11-20	10 / 67	http://www.xianjiaopi.com/6kYDYzhpWoYLQ67g/BIZ/IhreSparkasse
2018-11-20	11 / 66	http://www.xianjiaopi.com/41964H/PAY/US/
2018-11-20	12 / 67	http://www.xianjiaopi.com/733683H/BIZ/Commercial
2018-11-20	12 / 67	http://www.xianjiaopi.com/DTWn8HR6e
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	5bb9e4dc5f0c1b6269/d2f8dd4c05831891
2018-11-15	19 / 58	PDF	ddb93b71af85c90031eda95c00cc7
2018-11-06	4 / 58	PDF	FILE-1305716.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](https://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 ⓘ				Communicating Files ⓘ			
Scanned	Detections	Type	Name	Scanned	Detections	Type	Name
2018-11-24	<b>40 / 58</b>	MS Word Document	jnrUFoMW.doc.part	2018-11-20	<b>42 / 58</b>	MS Word Document	DOC_574023.doc
2018-11-23	<b>40 / 60</b>	MS Word Document	ACC2363.doc	2018-10-27	<b>41 / 59</b>	MS Word Document	Untitled-278017836827.doc
2018-11-25	<b>40 / 59</b>	MS Word Document	/data/cfs/malshare/9c8fc9d92225f9077f56 91e458c7d730	2018-10-19	<b>42 / 59</b>	MS Word Document	FORM-05649935773192.doc
2018-11-23	<b>38 / 60</b>	MS Word Document	Customer No 1247823.doc	2018-10-17	<b>43 / 60</b>	MS Word Document	zbetcheckin_tracker_092018
				2018-10-11	<b>41 / 58</b>	MS Word Document	Untitled-9877364339.doc

Σ [VirusTotal](#)

## Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators  
IR POV

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

FILES 5

File Name	Status	File Size
cc4b92e40ce2beab7cf1dbedf349f086d01facb7b31e94f43ac698e7e5367473	40 / 59	75.5 KB
DOC-62408603968.doc	doc macros run-file	
4088a57ed9bfac03cda27aa33200f516cf0600538dc8d01eb419d20a89ef1767	35 / 59	72.75 KB
Rechnung_2018_11_5633028508.doc	doc attachment macros run-file	
f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b	39 / 60	83.88 KB
SEP #979IGW.doc	doc macros run-file	
42e713e46dbc93170ae2513db3d5dd169552df74d9c042ef98564f666fe0e88d	39 / 60	82.5 KB
O2_12_11_18.doc	doc macros run-file	
64aa4b8f11436b02328018a92c0c78118d9465054e7f558b9be4db077cca5dc53	34 / 59	76.13 KB
2018_11Informationen_betreffend_Transaktion.doc	doc macros run-file	

VirusTotal

Central Pivot, First Document Observed:

f887e50af1c99ba73f280e28c7b0581b392782dba0bf2effc72d1719d039152b

Full context around campaigns and indicators

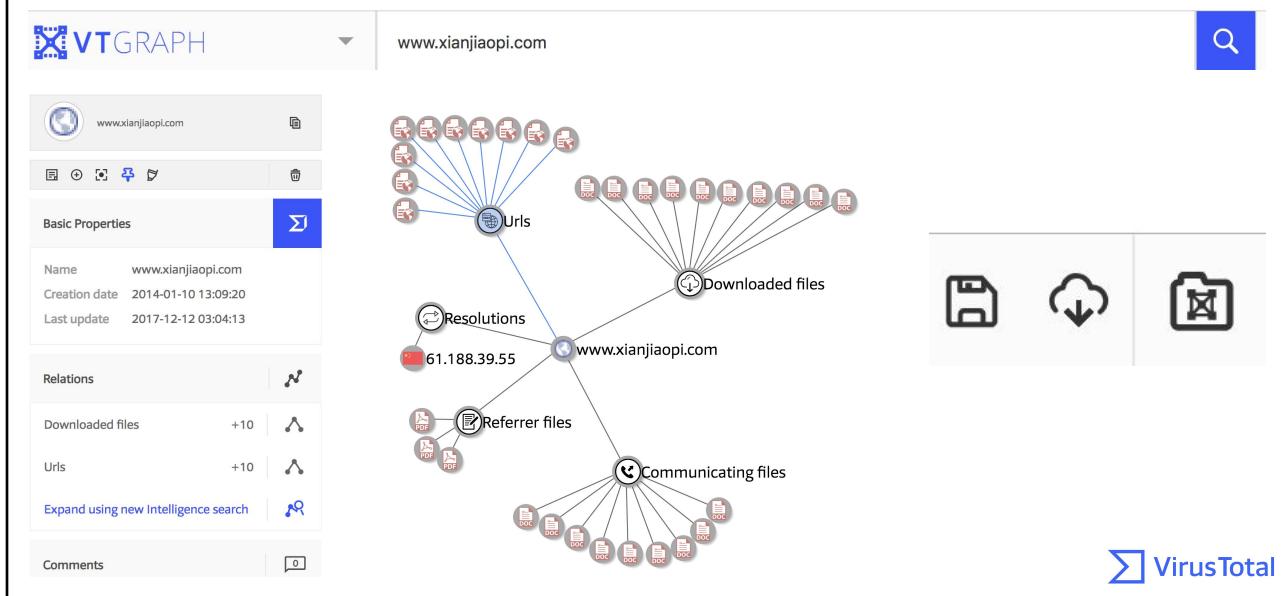
IR POV

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

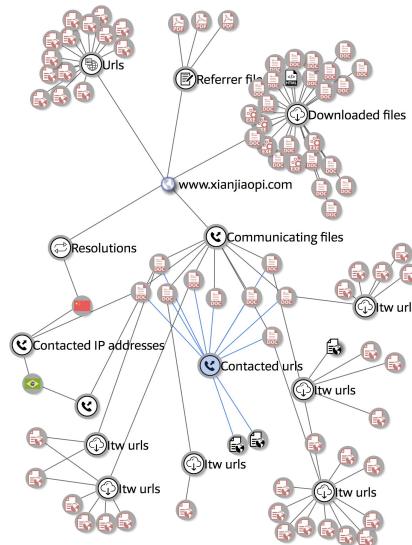
IR POV

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



 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](http://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=lug00AUDz7M>

- 
- 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/g1766a5d086d84a6d859f1c598620f704925844d218584cdb81e6c57363485283>

- 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-apt28-autoit.html>
  - <https://www.virustotal.com/graph/q7781518d548f4726aa4d70d9189b5a6d12d01c88fc494fc78d187056974da545>
- Messy/Large Campaigns - Emotet
  - 459397a134b2b4a201c2855bbb2ed4d1eeda9cc7637d7c65201e0a78217a8780  
C060ca7e926c137d2a9b90d0182b288b86117430f8a7614a1bff92b722ee1fa6
    - Source:  
[https://paste.cryptolaemus.com/emotet/2019/03/14/emotet-malware-loCs\\_03-14-19.html](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/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"  
        $b = {56 54 59}  
  
    condition:  
        $a or $b  
}
```

← INDICATOR  
S

← LOGIC



By default strings are considered ASCII

# Crafting a Custom YARA Rule

Malware family: **CobInt**

- 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 urimon.dll  int.dll  <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'> <requestedExecutionLevel level='asInvoker' uiAccess='false' /> <trustInfo xmlns='urn:schemas-microsoft-com:asm.v3'> xml version='1.0' encoding='UTF-8' standalone='yes' This program cannot be run in DOS mode.  ReflectiveLoader@@YGKPAZ@Z InitializeCriticalSection </requestedPrivileges> DeleteCriticalSection  Obtain userAgentString <requestedPrivileges> EnterCriticalSection LeaveCriticalSection InternetQueryOptionA	

Sample #2

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



Sample 1: 9540c062e1aefdb78e1f3f0b40c7f9d7f1a7c7fe90f2748e369a7d2e6fe4a6bb  
Sample 2: 2f7b5219193541ae993f5cf87a1f6c07705aaa907354a6292bc5c8d8585e8bd1

# Crafting a Custom YARA Rule (4)

Both Samples

## Imports

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

Basic Properties ⓘ	
MD5	616199072a11d95373b3c38626ad4c93
SHA-1	57201dd3a8b1585f5855e7d3927542c281b1494
Authentihash	46a3defc737d9160d0cf201aa0c02c2946c716415051798930424abc80d92fe0
ImpHash	9fd476779121c8ccabe0e029935bcfc
SSDeep	192:/puE9/Cgv6sln1TeqopZ7quwnd7eV8pP:RZHirpdqukB48pP
File type	Win32 DLL
Magic	PE32 executable for MS Windows (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()== "9fd476779121c8ccabe0e029935bcacb"
        )
        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 and unicode, after your closing quote.

# Retrohunt Results

100 %      Finished      blevene\_Chron-1538937604 1 month ago  
import "pe"  
import "pe" rule apt\_win\_cobint\_dll : Cobalt\_Group { meta: description = "Identify potential CobInt downloader DLL Trojan sa..."

```
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        $s2 = "Peflantivader" ascii
```

16 matches



## 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:

a76c79a4146cf5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3 (ursnif)  
=> rsrc image pivot => Yara Rule

# Retrohunt Results

## RETROHUNT NOTIFICATIONS

ff386b5a745139e444463d530b444b424f6013521344308b7870260f85a9dff29c e1cf39feafed3aa043465548a27a32fa.vir	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
pedll apt_win_cobint_dll				
977b0c1c833941a35fdc88d9f4972ced3e5957174a5e1958f5344b4ae4dc05a0 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
pedll overlay apt_win_cobint_dll				
a2d959c5f209c454409b8cd90922c937cde4750068e7ede4995bfadfd20e32418 payload.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
pedll overlay apt_win_cobint_dll				
44c14518d39aa2ff1fce1271e1425ad62c801186d9f5bd56e3e55cec50586087 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
1bd06d83b6ab57080e23c4d7d792a9445146d07bae00b02f8ee23a61c605967 rundll32.exe.bin	48 / 67	24 KB	2017-12-26 12:48:24 first seen 2017-12-26 12:48:24 last seen	2 submissions 1 submitters
pedll overlay apt_win_cobint_dll				
b2c6208b6636dea33243f0d19979013772add75e477d8fd00df07371d505354 invoice-xox.dll	44 / 66	10.5 KB	2018-09-19 15:44:40 first seen 2018-10-02 01:45:30 last seen	2 submissions 2 submitters
pedll apt_win_cobint_dll				
9540c06201aefcb78e13f0b40c7f9d7f1a7c7fe90f2748e369a7d2e6fe4a6bb 6b16c39baaa2a74ed053c84e01062fdc.vir	44 / 68	28 KB	2018-09-04 19:45:49 first seen 2018-10-03 23:01:45 last seen	2 submissions 2 submitters
pedll apt_win_cobint_dll				
0640eb2242aa77ecc5a95fe6ce7d0f5e7712586883786b50c33a1aea799a2af2 2710000.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
pedll apt_win_cobint_dll				



# Livehunt Results

## LIVEHUNT NOTIFICATIONS

cobalt\_group



44fb5685527f8faf9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d  
int.dll

47 / 66 11 KB

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

3 submissions  
2 submitters



44fb5685527f8faf9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d  
int.dll

47 / 66 11 KB

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

3 submissions  
2 submitters



44fb5685527f8faf9a721ff81ca4ce14e4e8da5f796c8568146d2e9145f1ff1d  
int.dll

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](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()== "9fd476779121c8ccabe0e029935bcacb"
        )
        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>

Rietspoof (bot):

8ea856534561e1fbe8c13c8901cdc9c8f7eb6139e76ef5eea8f9137c2295199

<https://www.virustotal.com/gui/file/8ea856534561e1fbe8c13c8901cdc9c8f7eb6139e76ef5eea8f9137c2295199/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_rietspoof_bot : commodity
{
    meta:
        description = "Identify Reitspoof Bot"
```

```
author = "blevene@chronicle.security"
date = "20-02-2019" //dd-mm-yyyy
reference =
"https://www.bleepingcomputer.com/news/security/multi-stage-r
ietspoof-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-ri  
etspoof-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 =>

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

## 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 =
    "a76c79a4146cf5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3"
    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) ==
    "059f9bf1cded9a989daeecde2df32db54318347d3975f343aaaf8d123d0ca517d")
}
```



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/a76c79a4146cf5cc1fb99ee7fce96da94d2dca00c029056bc1b7683058c02e3/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_exportsonly : 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 ("SpLsaModeInitialize")  
}
```

# 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_importsonly : 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/2d5f3edc4132f463cb6efe6379fda46e00fb725f51a9fb69d2b11161c43faa6%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/g4c327ce3e88e43f99191d7618b1b74e4eefee8ccd  
            2e44451ae8aa49ac1a36e47"
```

```
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>

3eb026d8b778716231a07b3dbbd99e2d3a635b1956de8a1e6efc659330e52de  
<https://www.virustotal.com/gui/file/3eb026d8b778716231a07b3dbbd99e2d3a635b1956de8a1e6efc659330e52de/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 =
"3eb026d8b778716231a07b3dbbd99e2d3a635b1956de8a1e6efc659330e52de"
    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>

37b04dcdfcaa885df0f392524db7ae7b73806ad8a8e76fb6a2df4db064e71  
<https://www.virustotal.com/gui/file/37b04dcdfcaa885df0f392524db7ae7b73806ad8a8e76fb6a2df4db064e71/detection>

---Will do in a notepad---

```
rule apt_win_RisingSun : Lazarus
{
    meta:
        description = "Identify RisingSun Implant which McAfee Alleges 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 =

```

"37b04dcdfcaaa885df0f392524db7ae7b73806ad8a8e76fb6a2df4db064e71"

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 :maldoc { meta: description = "Potential Emotet maldoc 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: 69f44ca082ed90c97d9c4ebaee589d7e41c69b02e582cc69886ebf..." }	5 matches	
100 %	Finished	blevene_Chron-1553117311	1 day ago	rule astra_docs { meta: description="ver1 of astra_docs" author="JDP" strings: \$header = {(d0cf11e0a1b1ae1)} \$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	?	C	W	□	▼
<input type="checkbox"/>	6ec9d3a2302a7cd6b170b155a9a2f0eed3c264e25a2c829a5d87df2e44ee9dc	<b>45 / 65</b>	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"/>	log file.exe	<b>peexe assembly overlay apt_win_nedrat gazahackerteam</b>					
<input type="checkbox"/>	7b081379d83e7bcfac3619f4b274f5d5e073b81618803f8fed0127bb8f6918	<b>12 / 64</b>	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"/>	OFXVKAAL.EXE	<b>peexe av_emotet av_trojan_win_emotet emotet</b>					
<input type="checkbox"/>	ba8aca44fb35315e502e66ae0e7be7aff535af42934024bd61391db8977f2ba	<b>14 / 67</b>	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"/>	DISM.EXE	<b>peexe overlay av_emotet av_trojan_win_emotet emotet</b>					
<input type="checkbox"/>	aca9e4365fbfe563fc21779c81d54ec6037be9c8a2202b3bef0428c388389da6	<b>38 / 66</b>	6.31 MB	2019-03-22 16:11:10 date matched 2019-03-22 16:03:47 first seen	1 submissions 1 submitters		
<input type="checkbox"/>	etohaknairnik.exe	<b>peexe av_emotet av_trojan_win_emotet emotet</b>					

 VirusTotal

<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>



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

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

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

## 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-imacpro ~/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-imacpro ~/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

```
x blevene@blevene-imacpro ➔ vt search "metadata:VPS2day size:75KB+ size:100KB-" -I -n 25  
b331ae16014d6219f1e2e3a2e2d568e7836bfb0e6b40ec081a3c71edd508a37  
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a  
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765  
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa  
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb  
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096  
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810  
2589053adc1f830c667dfd5ac4fad0c8161b8a48ae2c30200fc5e3b8bb7957  
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9  
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229  
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789  
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77  
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab  
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37  
f46ab59d7c9aaee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8  
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb  
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a  
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb  
2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616  
dc0b933d259b5e5d361da3ae3cff5bba53e8895db485dc9a3f4a4b42c3  
16590482d1729a5353599009a917e36cab70e497fbfc4a7e808c0ba6cbedc65  
874adf9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778  
e2544724e868485ed7d4de0b95fd240d7221d2b2fc3b7834b7bd287f303dfb2  
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6  
3d3f497a038e03061a11ee8ce239700d928c40d25b764934003690d6748db0bee
```



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

```
x blevene@blevene-imacpro ~ vt search "metadata:VPS2day size:75KB+  
size:100KB-" -I -n 25  
b331ae16014d6219f1e2e3a2e2d568e7836bfb0e6b40ec081a3c71edd508a37  
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a  
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765  
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa  
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb  
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096  
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810  
2589053adc1f830c667dfd5ac4fad0c8161b8a48ae2c30200fc5e3b8bb7957  
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9  
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbca9cc92229  
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789  
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77  
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab  
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bca9a8e6474983b37  
f46ab59d7c9aaee2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8  
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb  
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a  
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb
```

2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616  
dc0b933d259b5ec516e5d361da3ae3cff5bbba53e8895db485dc9a3f4a4b42c3  
16590482d1729a5353599009da917e36cab70e497fbcf4a7e808c0ba6cbecd65  
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778  
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2  
9b713329c00f2a98883ea68144c621490804f1bd09aef8fc1ef242229db914b6  
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee

MORE WITH:

```
vt search 'metadata:VPS2day size:75KB+ size:100KB-' --identifiers-only=true  
--limit=25  
--cursor=NMVJrqPKAQDQfT7jSr1KeBeKydxSVWQmAzaDAYONliFGM48Fpojy71m03vls  
zn-_bIXffP3-KhEal9_f35_P56-tmtcFDShu_0qH7jseq--N_q56lLdt9c77NP9e8nhOy3-n67  
wM80-uY6ppwTbV70fZE071ujFG2qa-LCzo_vD927tEqsQk5tP0u_Yotp1cQWaxlXNYFHa  
gShZUPw9B0nhyd_MyCkuWveSgPbfSqspxSjKCMdPaEGS5VkoZWVukdwfaOPox0HuqG  
MreCKeIHfJLa5JxW5H2ZpmX4yfAXBLHAn11zwrDg9QibBHh2adccCKgFh14RcFSbC_XP  
1nAygxZOElRylkvzbt1OpEQGjtjyOndCcYY8jg7K-dFOLxDZNnlkj5zyog6TzYLJ-78O7eWtxl  
ttTFBZj-6A2NuXj0TICARP1HM6AXLO8qy7usBTpeGupeLs3Fre76h_ALFyk2UeCrC5LNdL  
GjatmMOV9yPVC2wF11Wkq2Xe0hRMoMe1SeUilK835phuoh1b54lutu7cXxvoag9FW0  
g9pdNvTNfJK7XgjimQ84r6SrjklxwaR6paB9PIT7PgWbSQjrKF_GN7GJHemTuH_zZ5XSJX  
OUjjnQF4TiZ5LXNqGZUuWufokJwkZ4aAd31XLDRawzIx_F0H-jRoSivWbNzDJmgzbWDJ  
Kwz-5D2U7qgzmcdmD6vSj9Wx4gL52IALzxPvWvS3TbP2XK6uF1wuzZH7S-UgQNz0qHr  
4bC5jhY5b-MNVIMDHRzO2UuicOj0IRVFBR9mNifBMGKiz3gx8fDERVN8cM5kqfPbtrh  
XMzE-dzrlVZITJHAHTPtVfksmoVGnfGjwoxcTwcxB3g0RMASONuS3bS-Oc-R4TRMXPxM  
OXzZSPwAH1xV2wnrqLBIGO-In5SEYTT6nk06-EVcGx5CrOqEWvbzzQ1u0oW_z4rc3h88  
T3gi3ygh1AWA7h9-QAgwT25iO5Ufq-15yOyp52uhnz3iZaqhvUXVuEDCB9uLqS7QZQOx  
NyTK30vx8Yj1PZ02VelUI0WArzGncmzPb0oyOq5_P-13_h4UV00oZqG-clFqRumRNpczn  
byJW2ShUwHYtuDCkpwjsER4VIFR1SbNmJJIM5CvA3AOK1bVwEFSWhNyqN4uy6p33V  
B5c_Cu8AQmqo4Zjm7NCbK9h-BbCOiN3ZxVbIqP3A1s__7PSpKAm9Z8xj9djulsRvEv-uzb  
Lshi_M-IOvJf9Jlnr8lviPxNiiSvAvGntIVXoR_A_IGWL-lcjWiYI2joW_yD5jX_-teXVRRLjr5-k_  
_7x_8DAAD_
```

# APIv3 - Search and Download VTI

```
x blevene@blevene-imacpro ~ /Malware_Stuff vt search "metadata:VPS2day size:75KB+ size:100KB-" -n 25 -d  
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb [ok]  
b331ae16014d6219f1e2e3a2e2d568e7836bfb0e6b40ec081a3c71edd508a37 [ok]  
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a [ok]  
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa [ok]  
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765 [ok]  
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9 [ok]  
2589053adc1f830c667df5ac4fadf0c8161b8a48ae2c30200fc5e3b8bb7957 [ok]  
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096 [ok]  
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbc9cc92229 [ok]  
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810 [ok]  
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789 [ok]  
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77 [ok]  
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab [ok]  
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bc9a8e6474983b37 [ok]  
f46ab59d7c9aae2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8 [ok]  
6354d6716654177ebf8f705971eee33e37280734eb2f3f3d0a9cdbab95ab22bb [ok]  
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb [ok]  
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a [ok]  
2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616 [ok]  
dc0b933d259b5ec516e5d361da3ae3cff5bb53e8895db485dc9a3f4a4b42c3 [ok]  
16590482d1729a53599009da917e36cab70e497fbcf4a7e808c0ba6cbedc65 [ok]  
8744df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778 [ok]  
e2544724e868485ed7d4de0b95fd240d7221d2b2fc7b834b7bd287f303dfb2 [ok]  
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee [ok]  
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6 [ok]
```



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

```
x blevene@blevene-imacpro ~ /Malware_Stuff vt search "metadata:VPS2day  
size:75KB+ size:100KB-" -n 25 -d  
20150fb9e6d1245c1c4be577dfaee198a474ab39595cd191963bea6da6645ceb [ok]  
b331ae16014d6219f1e2e3a2e2d568e7836bfb0e6b40ec081a3c71edd508a37 [ok]  
3b8f3ddf364e1ae822b4cf53052eb1a2ed8eca3c18b3ee36a2e0da94fc20023a [ok]  
7430193891a295771ef76047dde5a7965adb23f86dac0631f102111e4d8587aa [ok]  
7564707affb852b6dd91ba86876965a6f9c78ed910b95a157c022c1402cb4765 [ok]  
9f1c60dfe106ec7cbad8a68319b60af6dc727a4e4d429baf1f64b4d417f715d9 [ok]  
2589053adc1f830c667df5ac4fadf0c8161b8a48ae2c30200fc5e3b8bb7957 [ok]  
d3f153e3ee3cc3d14212e14a37644c47e9f2d26c97861d504fea71940c706096 [ok]  
93fa8abcfaf60fd33ebdc7ec31cce252605a225e1f5302ba8c19dbc9cc92229 [ok]  
b0f42cae8f2493068f26d1f49f946e620058106166be21bd63baefcb180f7810 [ok]  
62247624c068970cd4cff25cb07e8c94cdac59bd44de799f3db1664ce0913789 [ok]  
f57fe36d26c052360dad052b486ce8a93a0f518aa1eb32bbc8ea526752f41d77 [ok]  
f2e55acc8c59b0ae0d9af5d6fdc4cde720ab44f56e0918603b81520b3709b2ab [ok]  
8445b6e4cc719abdd73d428e7f67aec6d3654b84d15f404bc9a8e6474983b37 [ok]  
f46ab59d7c9aae2d76f156fdec348affcc8d16dbf47f8aa85a8d2e31168a89b8 [ok]  
6354d6716654177ebf8f705971eee33e37280734eb2f3d0a9cdbab95ab22bb [ok]  
984362a42eb6c372f22a0c90cece3df3ab71169eaa7853d23c4b228e5d8caacb [ok]  
4134c7efd5bd2f8894e8311031959ffa637e324e127366dfa133f538096f215a [ok]
```

2c5da5f76808b9fc6f4b7a1105d2f69816fa264f7d713c36d0600569b3c21616 [ok]  
dc0b933d259b5ec516e5d361da3ae3cff5bbba53e8895db485dc9a3f4a4b42c3 [ok]  
16590482d1729a5353599009da917e36cab70e497fbef4a7e808c0ba6cbedc65 [ok]  
87a4df9398fb294d19edd844ce9b5e5753a988cf0c2174e18ce7767b10b3c778 [ok]  
e2544724e868485ed7d4de0b95fdd240d7221d2b2fc3b7834b7bd287f303dfb2 [ok]  
3d3f497a038e3061a11ee8ce239700d928c40d25b764934003690d6748db0bee [ok]  
9b713329c00f2a98883ea68144c621490804f1bd09aec8fc1ef242229db914b6 [ok]

## APIv3 - VTGrep

```
blevene@blevene-imacpro ~ vt search "content:FirstStageDropper.dll OR content:SecondStageDropper.dll" -I  
feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713  
3485c9b79dfd3e00aef9347326b9ccfee588018a608f89ecd6597da552e3872f  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
43f7ae58e8e5471917178430f3425061d333b736974f4b2784ca543e3093204b  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
2d7cb5ff4a449fa284721f83e352098c2fdea125f756322c90a40ad3ebc5e40d  
a63437a044d3ad01c52b0b18016bfdb8af2338067a4216be2dcaa04ec8ecee97  
bf38bea3f89a697b0be13413b0fb1db2154b3dc79fffbbee238014e4adeb0b880
```



Where -I is identifiers only (hashes)

```
blevene@blevene-imacpro ~ vt search "content:FirstStageDropper.dll OR  
content:SecondStageDropper.dll" -I  
feaa627fa65c452b75522ea3633e51f1842fc7577a523d43c5ea529c8aa08713  
3485c9b79dfd3e00aef9347326b9ccfee588018a608f89ecd6597da552e3872f  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
a09273b4cc08c39afe0c964f14cef98e532ae530eb60b93aec669731c185ea23  
43f7ae58e8e5471917178430f3425061d333b736974f4b2784ca543e3093204b  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
a260d222dfc94b91a09485647c21acfa4a26469528ec4b1b49469db3b283eb9a  
2d7cb5ff4a449fa284721f83e352098c2fdea125f756322c90a40ad3ebc5e40d  
a63437a044d3ad01c52b0b18016bfdb8af2338067a4216be2dcaa04ec8ecee97  
bf38bea3f89a697b0be13413b0fb1db2154b3dc79fffbbee238014e4adeb0b880
```

# APIv3 - Upload A Rule

```
blevene@blevene-imacpro ~ ➔ 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 = "ca30c42334fc693320772b4ce1df26fe5fd0110bc454ec6338d79dfffa4ae8"
        hash02 = "1b213a457a9d1949febb5aca7402ee6a200cb871c6c03e22e8f862007404ec5"
      strings:
        //not actually contained in import table
        $s1 = "acledit.dll"
        /ekjynhaedfreratafrhnakmkioplpliynhaioplhaterafderayunn
        $u1 = {656b6a796e6861646566726465726174616672686e616d6b696f706c706c69796e6861696f706c68617465726166646572746179756e6
d}
      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 == ".rel0k")
        )
        and 1 of them
    }
  blevene@blevene-imacpro ~ ➔ vt hunting rulesets enable 5529739319771136
```



## Full Console Output

```
blevene@blevene-imacpro ~ 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 =

```

```
"ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8"  
    hash02 =  
"1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5"  
  
strings:  
    //not actually contained in import table  
    $s1 = "acledit.dll"  
  
    //ekjynhadefrderatafrhnamkioplpliynhaioplhaterafdtaynum  
    $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-imacpro ~ vt hunting rulesets enable 5529739319771136

# APIv3 - Start a Retrohunt

```
x blevene@blevene-imacpro ~ vt retrohunt start ~/Documents/YaraRules/trojan_win_psixbot.yar
blevene@blevene-imacpro ~ 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 = "ca30c42334fc6c093320772b4ce1df26f5f1d0110bc454ecc38d4f9dffea4ec8"
        hash02 = "1b2138457a9d1949fe5aca7402ee6a200cb871cc6c03e22e80f862007404ec5"
    }
    strings:
    //not actually contained in import table
    $S1 = "aledit.dll"
    //ekjynahedfrderatafrhnakiolpliylnahaterafdtayum
    $U1 = {(566b6a796e686164656726465726174616672686e616d6b696f706c69796e6861696f706c68617465726166646572746179756e6}
  }

  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 == ".rel0k")
    )
    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-imacpro ~ vt retrohunt start
~/Documents/YaraRules/trojan_win_psixbot.yar
blevene_Chron-1554220302
blevene@blevene-imacpro ~ 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 =

```

```
"ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8"  
    hash02 =  
"1b213a457a9d1949feb5aaca7402ee6a200cb871c6c03e22e86f862007404ec5"  
  
strings:  
    //not actually contained in import table  
    $s1 = "acledit.dll"  
  
    //ekjynhadefrderatafrhnamkioplpliynhaioplhaterafdtaynum  
    $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  
0252e1e82ce3992e48b6dabc90f33188183ac5029b8d5049f47d087bfd5bcab  
6fb4b6a4e5367ce4bff82fdadb3b3ef64a393b9ee86e677ebaec658606310bd0  
ef363c3be4fe16411dcfb52599c9242ef0377daa8742c1e672ace0055f3c88d8  
15049d944375f2022a5b3f31dc0ea9c02f517a6153d9cfc4d8c841d7efe2248  
fd35b23d2c02bdd57245acf109fb6961bfaa205a91083983b80898ff2ab5c14d  
3736b350803dbac08691679556a35216c318ddd5e10722c5279118d812e721c0  
e66a2a247964480415d75b1f524f13f14081c737cdfdca39559a706bd808e8b7  
8e13b9d80a746203d2a0e768491c62ee550402e17274e022453adcc7ef1ffbde  
9c644b4cabcc14cccc485c2656c291a1089ffffe9e0bc6f07d2c17db2bf578095d  
ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8  
253c4cbf357de49e240ba1695570e20667586dbdecccd820a2d94e773e85b1889  
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  
0252e1e82ce3992e48b6dabc90f33188183ac5029b8d5049f47d087bfd5bcab  
6fb4b6a4e5367ce4bff82fdadb3b3ef64a393b9ee86e677ebaec658606310bd0  
ef363c3be4fe16411dcfb52599c9242ef0377daa8742c1e672ace0055f3c88d8  
15049d944375f2022a5b3f31dc0ea9c02f517a6153d9cfc4d8c841d7efe2248  
fd35b23d2c02bdd57245acf109fb6961bfaa205a91083983b80898ff2ab5c14d  
3736b350803dbac08691679556a35216c318ddd5e10722c5279118d812e721c0  
e66a2a247964480415d75b1f524f13f14081c737cdfdca39559a706bd808e8b7  
8e13b9d80a746203d2a0e768491c62ee550402e17274e022453adcc7ef1ffbde  
9c644b4cabcc14cccc485c2656c291a1089ffffe9e0bc6f07d2c17db2bf578095d  
ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8  
253c4cbf357de49e240ba1695570e20667586dbdecccd820a2d94e773e85b1889  
d0a48a5b3faf5e9a531b8fcf2c0be676b20975dfceec624109fec560c4a240aa  
21c4e6dfb9017b6de79676649b69de5962883eba8315c0ceef6523bb16d11e72
```

e985706257e2c9f781723aee5007ccc3bfd16671302e0a53cda1164023cab94e  
4f582ecdd2c8d27e78e774e928a81e9e2f825a90bf2a47659da69810487cb9ee  
98d56ba99a8ac192c0cdfed04d989dd60c16e2a8213fc9958be2a6de55696694  
e1f459ebd4092ab0b452f3ad6de821d216bd5dc284c497c8c598d01e5543de3f  
b2c46f10674f5896b5286607eedf7926dc041e9d12b714df5e9c47cf68ac53d5  
cd80b1f027bd4b60b9ff07f66de99d8fcfd94dd8efa831bf6671d12c1a2f64c8d  
c819375b811d44d9b4df8a60abb1d172e5bbe6ca9aaab69d32e1fddd731cc956  
d8235ef57a807f41a4fe10638556b0b190c288ec7dbdb3caa7051daed36d4c89  
117a74639b66dc02c05bb001fd56fe7ac9bee3e455da4f610512ae2da266863a  
af69fa9caa8854bc3925dad5d3b44e5703a229327239c904aa7ecf5b41ec00e4  
c5d5e51532eed12cb9d86dfe9db390bc1d11b5b6f0d87e554b66f925bec5aa56  
cb0f11d274f1afa6b165f083e4bfc16bc180b1973c19af2cf682907e43fd1dc9  
ebfa7d124cea4879272fbd573905f8ab2c26ca8726456b6729934cdd137e5413  
560698ec061d49e68641ddc7540b41dbb51e92ec95d313227ed3c60c62f4753d  
49c183642a00ef798febc3863dc81152088edc1ad564dd48f500991dcbe3531b  
832ea36a11d13e0ce5f6fc527627c777428f2d44efd0b4ad54ca8fa5a6cd035  
3036fae7550f78c47af3d8d9e9f241cb0a84da9c48c71d9ed849830c1fa53311  
ecdbfa957b07ed7f07b614e2e3a2a75925ef05540bdee6e03827516b4ae09611  
a880bc28ca5d5ce380e8a577cc238e0d917515ebcc07b352bb43db54d858b2dd  
bb90f394332450601dbb10c539d68cb8ad9d03ddc25efc41b81e4e8baf90aee  
ffc7533231c9c6cb6f8ce6b3b0d9a9d1b66046650bf67c36d3d38111f84b61c8  
5deb49db0a16cd1588a0b3d8ceea97d9d6cf73ca83814a32c540947359994b4a  
39ade6f3e847ba1c2918920743e85fbc71642a2eac731a3ab1387cb8e491b038  
39ade6f3e847ba1c2918920743e85fbc71642a2eac731a3ab1387cb8e491b038  
b3fd922d6e9b405ec4415aac4927e53f173d2b8c91f105f516d1f147f42412e6  
4f5cc216cb3f6a77c14ecf803095ca44003dcb1ce54944209c859ace9e02e535  
31d1194936842cfca74d2526cbc75f0801ce54eeab9a85bb107fd3d5b627d055  
9054f32c2bb375fea99bced0b9ea0654d724b6b53a48ca03c3f8d1b379160fcf  
893fef03eb3ab0afb9193858f7fa7a34c847d5b18ef2ca89ba97f57515d9894f  
c0e6ecc25387d5d537bf24110acd31232028d1c2bff7e3cdef67c28218f3da6b  
7e2dc01cd6f14c57d95fe9421f5120b2bbe858028a3330fb1f3f3c1909bbc45d  
f64f5f11a5c0d2a6983607b4b8789b6be3ab0dd1ba7114e876fc5ab2c8d8585

# APIv3 - Hunting Notifications

```
blevene@blevene-imacpro ~ ➤ vt hunting notifications list --cursor=JM3PTsIwHADgu4_RxJvSysQFEmLmKGQCMxDDYDEh3dbRn-va2T9b1PjuHrh9t-8XbUA1aIaEc52dYT...lweZWAzs5rkPzDEzJ-Kr2x2szj5nFnD5rmqyXJ98lrv0V1uP05WU5j-nn4osf0v...ld3VMSRHsRbFKbREcmhKiDRVpUmUTwrKJem-nhGV5dxovCcumfpXEUZiG67DbbRYvlyiJ6G2wuNYSWnDzB4Lu0FtdW-7QjPzd_AcAAP_
```

```
- hunting_notification <5223863694327808>:  
  body: ""  
  date: 1554217750 # 2019-04-02 11:09:10 -0400 EDT  
  file: "1a7a99b970fdb...c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
  subject: "AV_trojan_win_Emotet: Emotet"  
  tags:  
    - "emotet"  
    - "av_trojan_win_emotet"  
    - "1a7a99b970fdb...c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
    - "av_emotet"
```



## Full Console Output

```
blevene@blevene-imacpro ~ ➤ vt hunting notifications list  
--cursor=JM3PTsIwHADgu4_RxJvSysQFEmLmKGQCMxDDYDEh3dbRn-va2T9b1PjuHrh  
9t-8XbUA1alaEc52dYT...lweZWAzs5rkPzDEzJ-Kr2x2szj5nFnD5rmqyXJ98lrv0V1uP05WU5j-nn4osf0v  
mrld3VMSRHsRbFKbREcmhKiDRVpUmUTwrKJem-nhGV5dxovCcumfpXEUZiG67DbbRY  
vlyiJ6G2wuNYSWnDzB4Lu0FtdW-7QjPzd_AcAAP_
```

```
- hunting_notification <5223863694327808>:  
  body: ""  
  date: 1554217750 # 2019-04-02 11:09:10 -0400 EDT  
  file: "1a7a99b970fdb...c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
  subject: "AV_trojan_win_Emotet: Emotet"  
  tags:  
    - "emotet"  
    - "av_trojan_win_emotet"  
    - "1a7a99b970fdb...c8321398be15c30a0367fc66d7d36c72f7e3e3cca332c556f"  
    - "av_emotet"
```

## APIv3 - ASCII Cinema

---

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



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

---

# Thank you.

[info@virustotal.com](mailto:info@virustotal.com)  
[virustotal.com/learn](http://virustotal.com/learn)