

VirusTotal Enterprise

Evan Derheim

December 13, 2018

Agenda:

1. VirusTotal Introduction
2. How to use VT to find and track relevant malware
3. See It
4. Try It





What is VirusTotal?

- 70+ AntiVirus Engines
- Global malware intelligence services
 - 2 Billion+ malware samples
 - 1 Million+ files uploaded per day
 - 5 Million+ domains, URLs and IPs per day
- Free and advanced capabilities
 - Crowdsourced AntiVirus verdicts (free)
 - Threat hunting, IR, investigations, relationship analysis (advanced)
- Powerful intelligence tools: Intelligence, YARA, Hunting, Graph
- Part of Chronicle, Alphabet's cybersecurity company



VTINTELLIGENCE



VT HUNTING



VT GRAPH



VT API



What is VirusTotal Intelligence?



- VirusTotal Intelligence has been called the, “Google of malware”
- VTI extracts and indexes sandbox behavior, network information, office macros, PE imports/exports, authenticode signatures and a myriad of file other properties
- VTI provides the ability to search through VT’s dataset using:
- Access via web interface or APIs





Search for
relevant
malware

Search for trending malware based on:

- Malware family name
- CVE number
- Malware behavior (sandbox behavior)
- CCs it has communicated with
- Strings in the file
- Country
- File hash
- ...and 100+ more ways





 VT ENTERPRISE

DEMO
TIME



VT ENTERPRISE

Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community

FILE

URL

SEARCH



emotet

There are over [50 search modifiers](#) that you can use, get started with this [wargame](#) or watch a short [introduction](#)

Search for
malware
family





Find malware
family
samples

VTINTELLIGENCE ▼ emotet x

FILES 20+

<input type="checkbox"/>	2f17e7089c3d1dc0b9667f32093161771342193b6bd655b3388086593e731de3 ...93161771342193b6bd655b3388086593e731de3_2018-12-12_16:19:59.doc	24 / 60
	doc attachment macros obfuscated run-file	
<input type="checkbox"/>	292434550dccf3840465aa8da4253bb09f752f32328a4c2107a9c14746f782f3 INV 23748.doc	36 / 59
	doc attachment macros run-file	
<input type="checkbox"/>	5a5d6775a82ef31b587b369dbbdf8b82c2b6ad6652af0047ea28c4c1a62e47a8 Untitled-T7849.doc	37 / 58
	doc attachment macros run-file	
<input type="checkbox"/>	6891b71a9793ee457e64aede693de74bbb13dcdbc1a8a7a34cee40dec7a203ea 201812_58348165NI735489V.doc	40 / 60
	doc attachment macros run-file	
<input type="checkbox"/>	d3569e2066199f46928c41660b38c62656c54740b7e7c7f1e420191fce3958b5 ...b38c62656c54740b7e7c7f1e420191fce3958b5_2018-12-12_12:40:16.doc	28 / 59
	doc attachment macros obfuscated run-file	





Dig deep into every sample, discover CCs, second stage malware and more IOCs

41 / 60

41 engines detected this file

6755c2d4855a8b5ec2eb9dd9ab20edc55230c9cd12c372080bae52997899cf2e
2018_12_13_00_12_03.000897

254.5 KB Size | 2018-12-13 00:12:04 UTC | 5 hours ago

doc exe-pattern macros obfuscated run-file write-file

Community Score

DETECTION DETAILS **RELATIONS** BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 5

Graph Summary

Compressed Parents

Scanned	Detections	Type	Name
2018-01-09	2 / 59	7ZIP	1a2de5a07b23e700fc4a9f304b42b060

ITW Urls

Scanned	Detections	URL
2018-05-15	9 / 67	http://alferienwebagency.com/docs/Your-Gift-Card/
2018-11-20	4 / 66	http://alferienwebagency.com/docs/Your-Gift-Card/
2018-02-08	9 / 67	http://altingroup.net/Your-Holidays-Card/
2018-02-08	3 / 67	http://www.stadiaeng.com/Sales-Invoice/
2018-01-05	2 / 66	http://tntvietnam.vn/Your-eGift-Card/
2018-01-03	1 / 66	http://lewdownscalfolding.co.uk/INCORRECT-INVOICE/
2018-02-08	6 / 67	http://www.dicohotels.it/Outstanding-Invoices/

Contained In Graphs

Owner	Description
-------	-------------



Track new malware in real time



```
1 /*
2     Template YARA ruleset
3 */
4 import "cuckoo"
5 import "pe"
6
7 rule emotetAVsignature
8 {
9     condition:
10        // Any antivirus signature contains the given string
11        signatures contains "emotet"
12 }
13
14 rule emotetURLs
15 {
16     condition:
17        // Notify me when files reach out to these domains
18        cuckoo.network.http_request(/http:\\\\arkonziv\\.com\\.com/) or cuckoo.network.ht
19 }
```

- Receive an alert as soon as a new Emotet file is submitted to VirusTotal
- Customize your rules to find any kind of malware



Automate
using our API



Utilize our API for mass lookups and automation:

- Automate alerts
- Enrich data
- Integrate VT with your SIEM, SOAR, EDR or AV
- Download samples
- Find IOCs





Want to try VirusTotal Enterprise?

Gain free two week access here:

virustotal.com/subscription

Or

Schedule a threat hunting session info@virustotal.com

Q&A

Thank you!

