chronicle

VirusTotal Enterprise

Evan Derheim

December 13, 2018

VIRUSTOTAL

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

VTHUNTING

VTGRAPH

VTAPI

What is VirusTotal Intelligence?

VTINTELLIGENCE

- 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

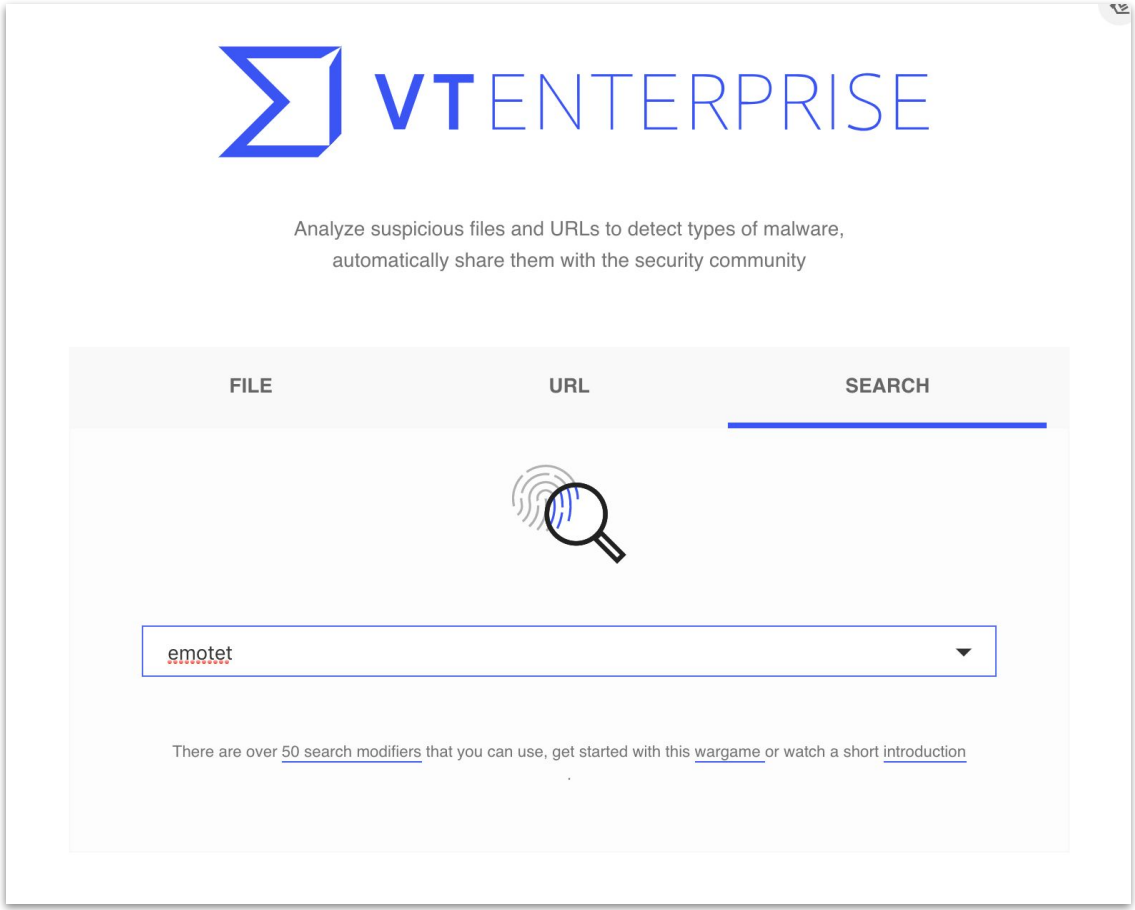
VTINTELLIGENCE

Search for trending malware based on:

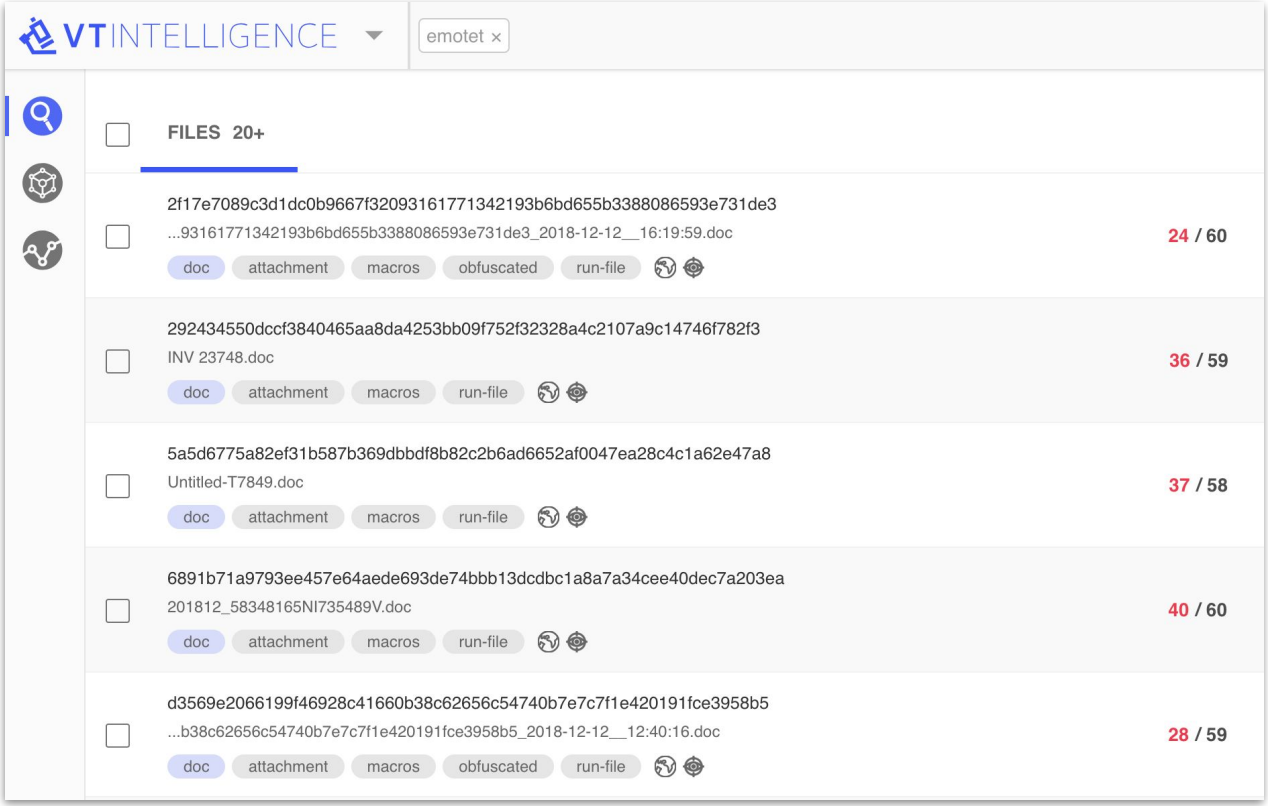
- Malware family name
- CVE number
- Malware behavior (sandbox behavior)
- CCs it has communicated with
- Strings in the file
- Country
- File hash
- ...and 100+ more ways


VT ENTERPRISE
DEMO
TIME

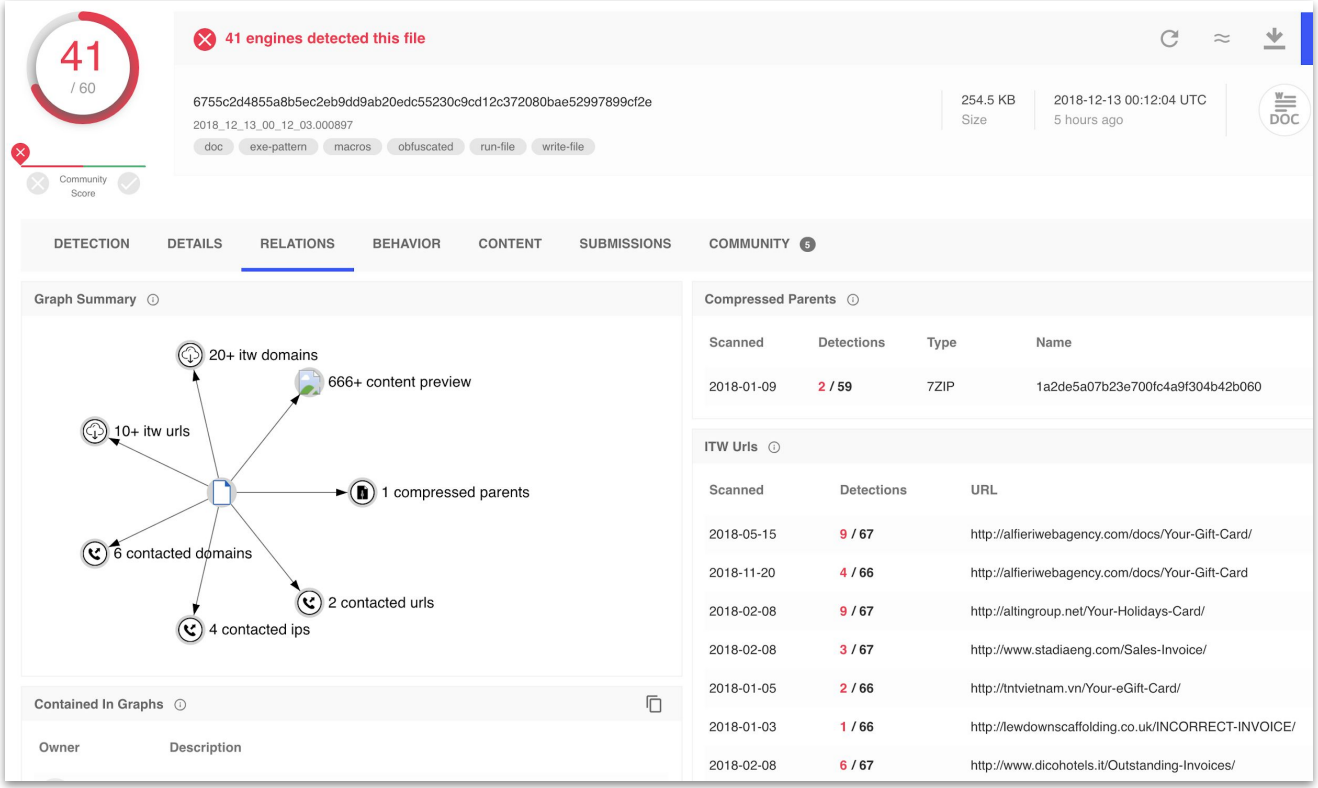
Search for malware family



Find malware family samples



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



Track new malware in real time

emotet

```
/*
    Template YARA ruleset
*/
import "cuckoo"
import "pe"

rule emotetAVsignature
{
  condition:
    // Any antivirus signature contains the given string
    signatures contains "emotet"
}

rule emotetURLs
{
  condition:
    // Notify me when files reach out to these domains
    cuckoo.network.http_request(/http:\/\/arkonziv\.com\.com/) or cuckoo.network.ht
}
```

- 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?

Q&A

Thank you!

Gain free two week access here:

virustotal.com/subscription

Or

Schedule a threat hunting session info@virustotal.com