YARA rules to learn and get practice sample –

1) Sample one

```
Rule BABADEDA_Crypter
{
        meta:
                description = “………”
                author = “……”
                reference = “ link…….”

        strings:
                $entry_shellcode = {hex values}
                $placeholder_1 = {hex values}
                $placeholder_2 = {hex values}

        condition:
                $entry_shellcode and all of ($placeholder_*)

}
```

Honeypots- https://github.com/paralax/awesome-honeypots

https://github.com/cowrie/cowrie

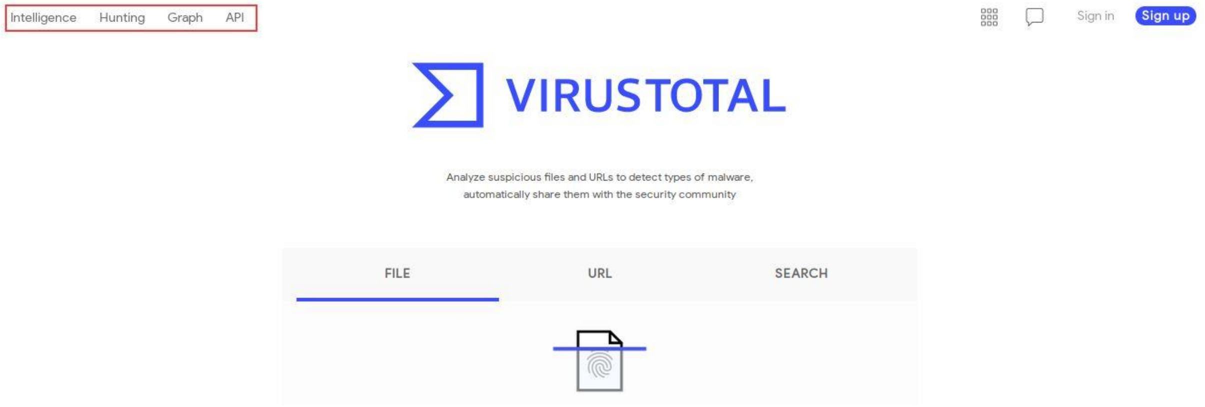
https://cowrie.readthedocs.io/en/latest/elk/README.html

Virus Total: for Threat Hunting using Yara Rules on VT Platform

Virus Total for Threat Hunting -

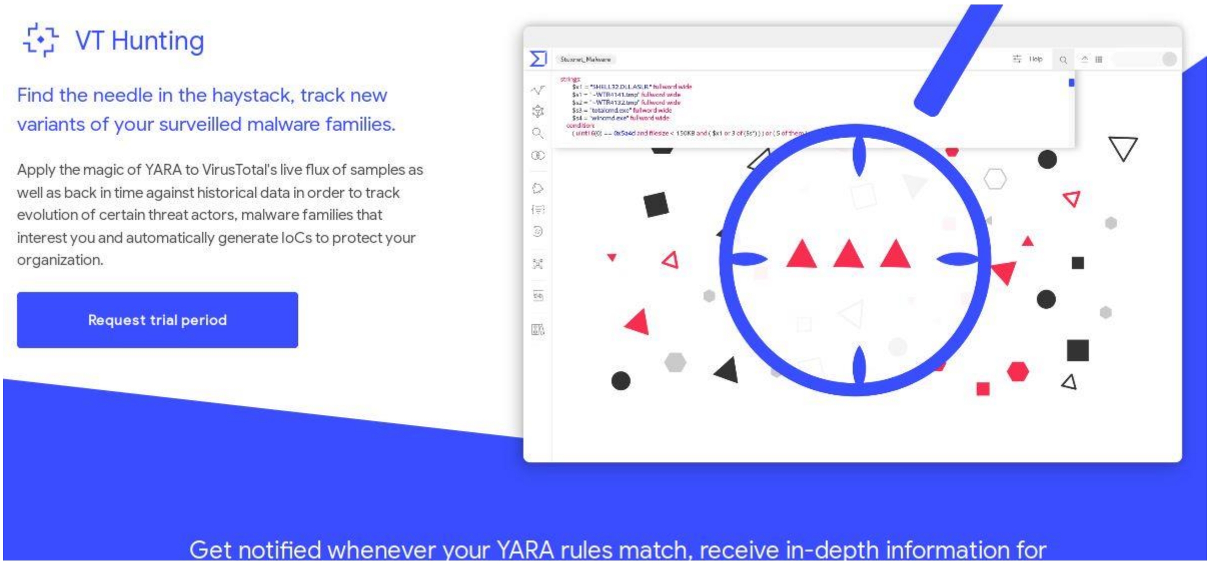
Dashboard of Virus Total- Highlighted frame provides access to do Threat Intelligence and Threat Hunt using Virus Total.

Basic Information is identified using the **Virus Total Community Edition** but In-depth Analysis is provided when we are subscribed to **VT Enterprise Edition**



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

Clicking on Hunting Tab, we are landed to the below mentioned page. Same is for Intelligence Tab.



Find the needle in the haystack, track new variants of your surveilled malware families.

Apply the magic of YARA to VirusTotal's live flux of samples as well as back in time against historical data in order to track evolution of certain threat actors, malware families that interest you and automatically generate IoCs to protect your organization.

```
strings:
    $x1 = "SHELL32.DLL.ASLR." fullword wide
    $s1 = "~WTR4141.tmp" fullword wide
    $s2 = "~WTR4132.tmp" fullword wide
    $s3 = "totalcmd.exe" fullword wide
    $s4 = "wincmd.exe" fullword wide
  condition:
    ( uint16(0) == 0x5a4d and filesize < 150KB and ( $x1 or 3 of ($s*) ) ) or ( 5 of them )
```

Get notified whenever your YARA rules match, receive in-depth information for

Virus Total Does use Yara Rules for doing File Pattern Matching.

YARA Rule Sample – Structure of Yara Rules

Sample one

rule silent_banker : banker

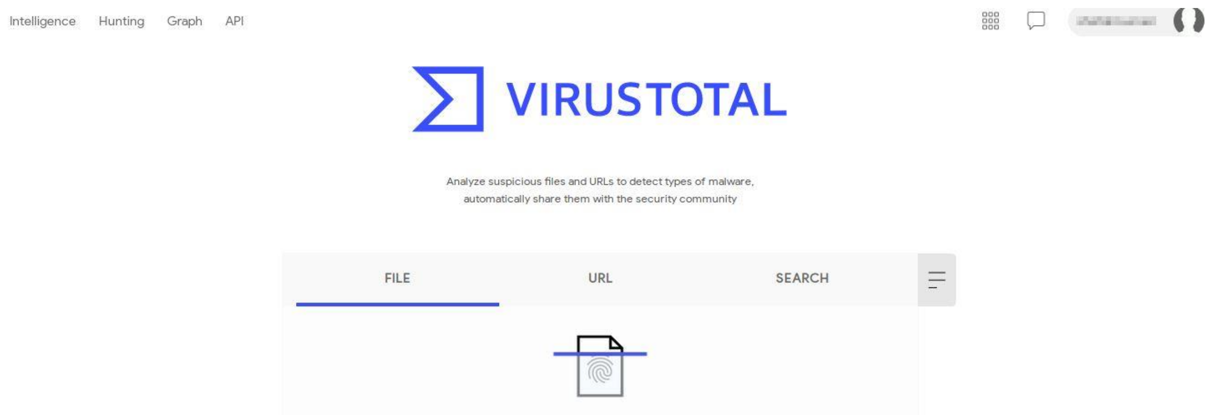
```
{
  meta:
    description = "This is just an example"
    threat_level = 3
    in_the_wild = true

  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
    $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

  condition:
    $a or $b or $c
}
```

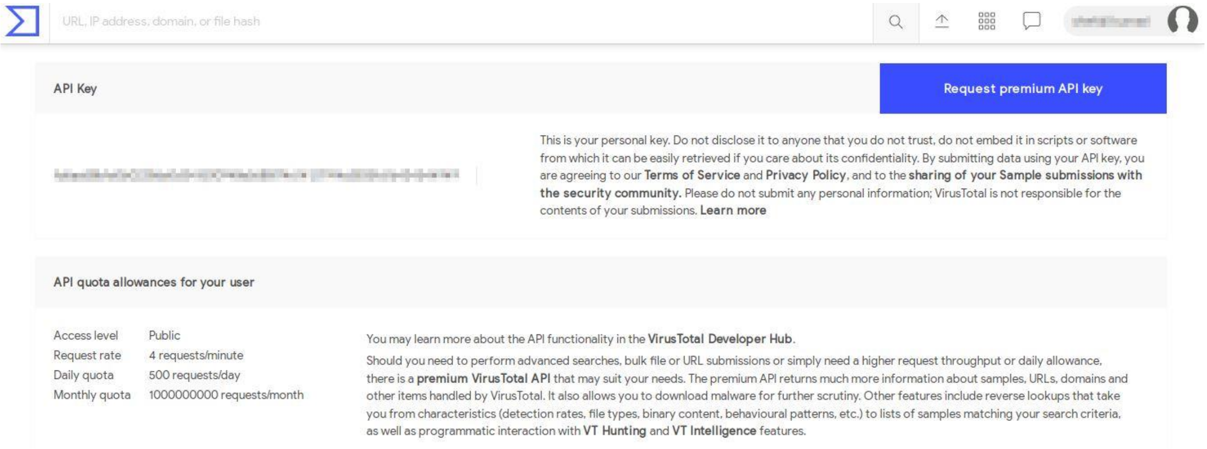
Link - http://virustotal.github.io/yara/

Create Your Account on Virus Total Community Edition by Signing Up. Loin using your created credentials for the same.



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

VT API key-



API Key

Request premium API key

[redacted]

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our **Terms of Service** and **Privacy Policy**, and to the **sharing of your Sample submissions with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submissions. **Learn more**

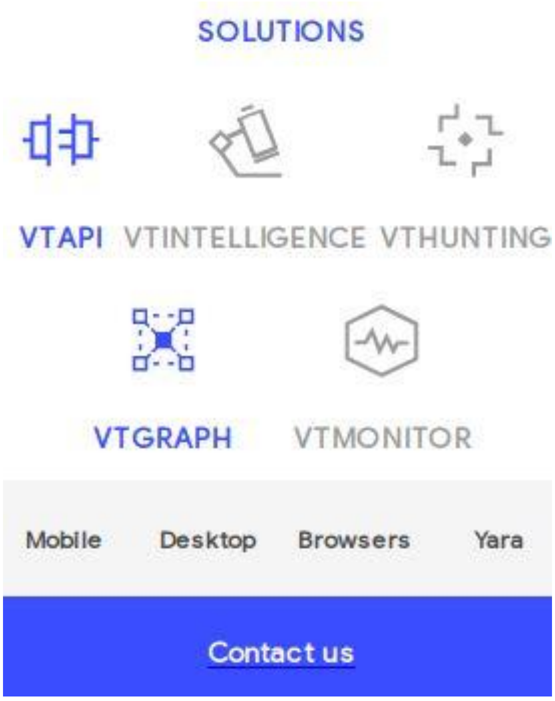
API quota allowances for your user

Access level	Public
Request rate	4 requests/minute
Daily quota	500 requests/day
Monthly quota	1000000000 requests/month

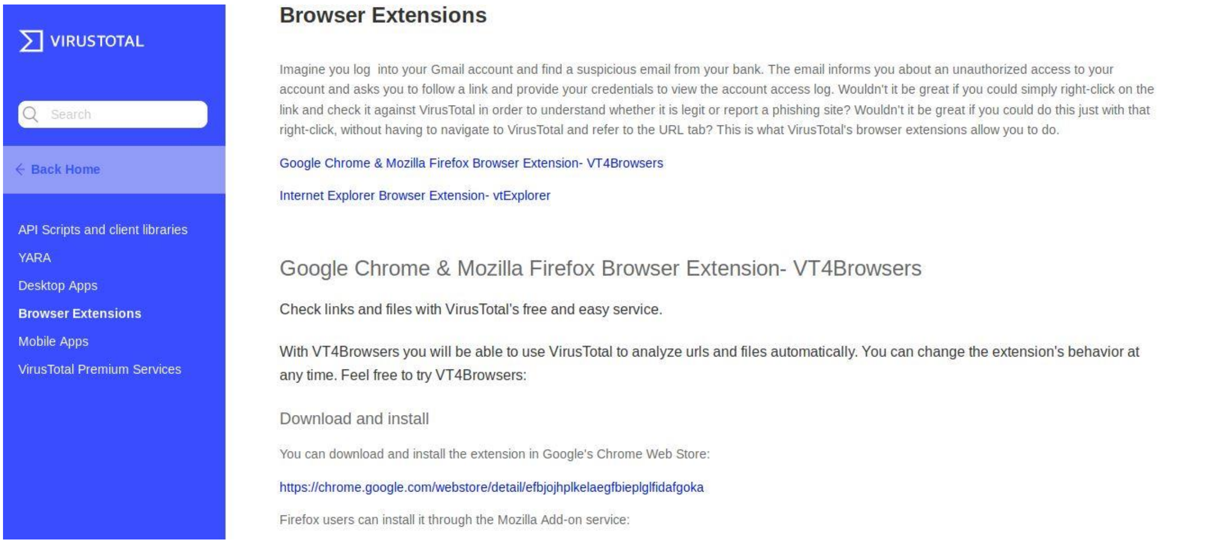
You may learn more about the API functionality in the **VirusTotal Developer Hub**.

Should you need to perform advanced searches, bulk file or URL submissions or simply need a higher request throughput or daily allowance, there is a **premium VirusTotal API** that may suit your needs. The premium API returns much more information about samples, URLs, domains and other items handled by VirusTotal. It also allows you to download malware for further scrutiny. Other features include reverse lookups that take you from characteristics (detection rates, file types, binary content, behavioural patterns, etc.) to lists of samples matching your search criteria, as well as programmatic interaction with **VT Hunting** and **VT Intelligence** features.

VT Community only provides you VT API and VT graph, but VT Intelligence and VT Hunting comes with VT Enterprise Edition.



VT is also available as Browser Extension- https://support.virustotal.com/hc/en-us/articles/115002700745-Browser-Extensions



Browser Extensions

Imagine you log into your Gmail account and find a suspicious email from your bank. The email informs you about an unauthorized access to your account and asks you to follow a link and provide your credentials to view the account access log. Wouldn't it be great if you could simply right-click on the link and check it against VirusTotal in order to understand whether it is legit or report a phishing site? Wouldn't it be great if you could do this just with that right-click, without having to navigate to VirusTotal and refer to the URL tab? This is what VirusTotal's browser extensions allow you to do.

Google Chrome & Mozilla Firefox Browser Extension- VT4Browsers

Internet Explorer Browser Extension- vtExplorer

Google Chrome & Mozilla Firefox Browser Extension- VT4Browsers

Check links and files with VirusTotal's free and easy service.

With VT4Browsers you will be able to use VirusTotal to analyze urls and files automatically. You can change the extension's behavior at any time. Feel free to try VT4Browsers:

Download and install

You can download and install the extension in Google's Chrome Web Store:

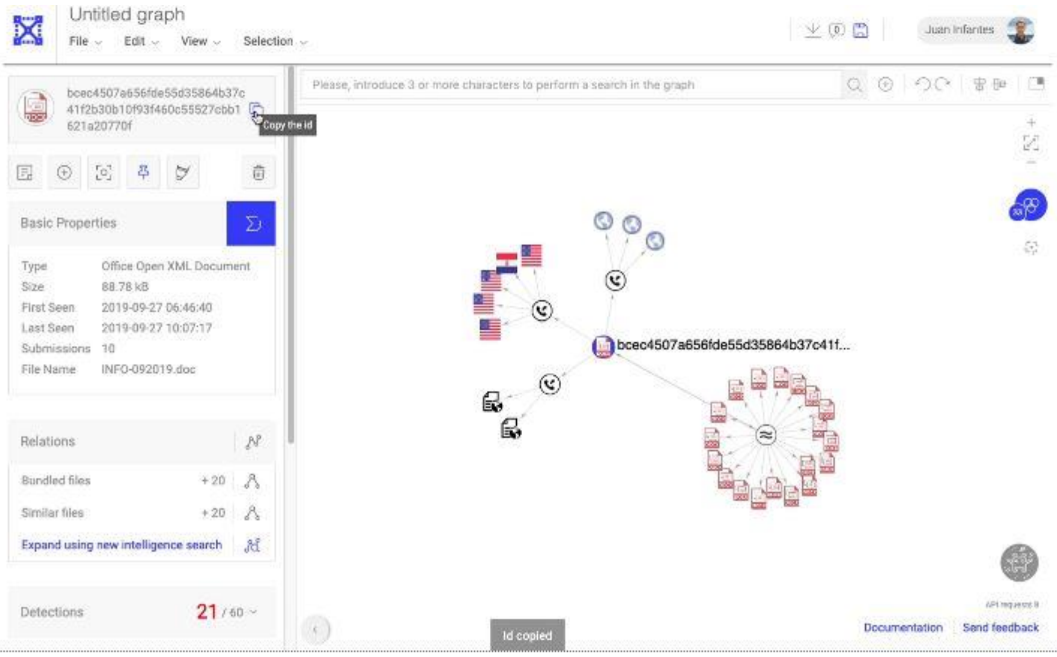
https://chrome.google.com/webstore/detail/efbjojhplkelaegfbieplglfidafgoka

Firefox users can install it through the Mozilla Add-on service:

Virus Total is also available for Desktop and Mobile.

Try Using VT Graph for sample analysis. Try understanding all walkthroughs provided in VTGraph.

https://www.virustotal.com/graph/new



bcec4507a656fde55d35864b37c41f2b30b10f93f460c55527cbb1621a20770f

Type	Office Open XML Document
Size	88.78 kB
First Seen	2019-09-27 06:46:40
Last Seen	2019-09-27 10:07:17
Submissions	10
File Name	INFO-092019.doc