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>

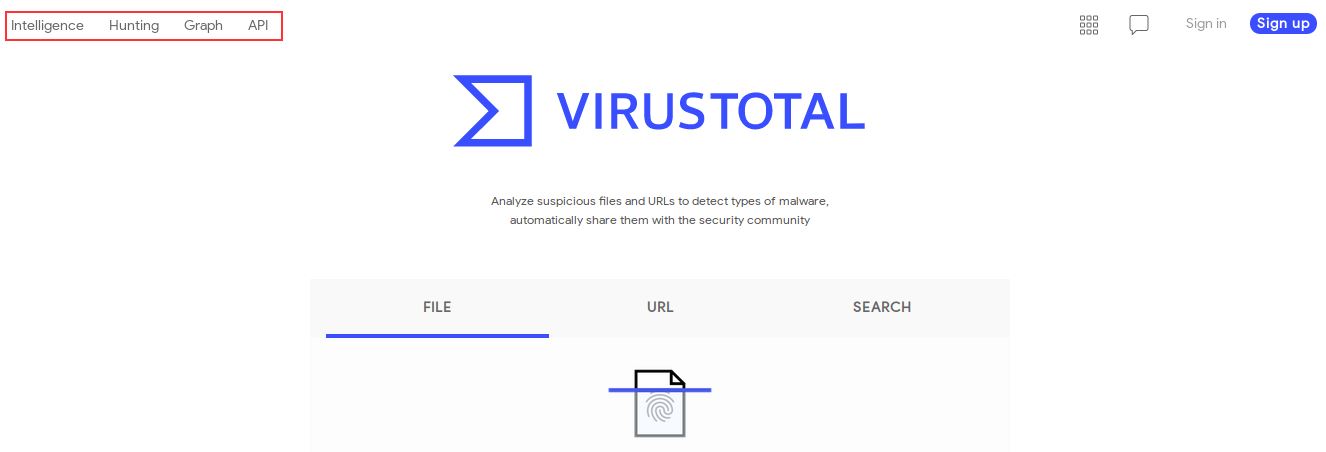
<https://cowrie.readthedocs.io/en/latest/elk/README.html>

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

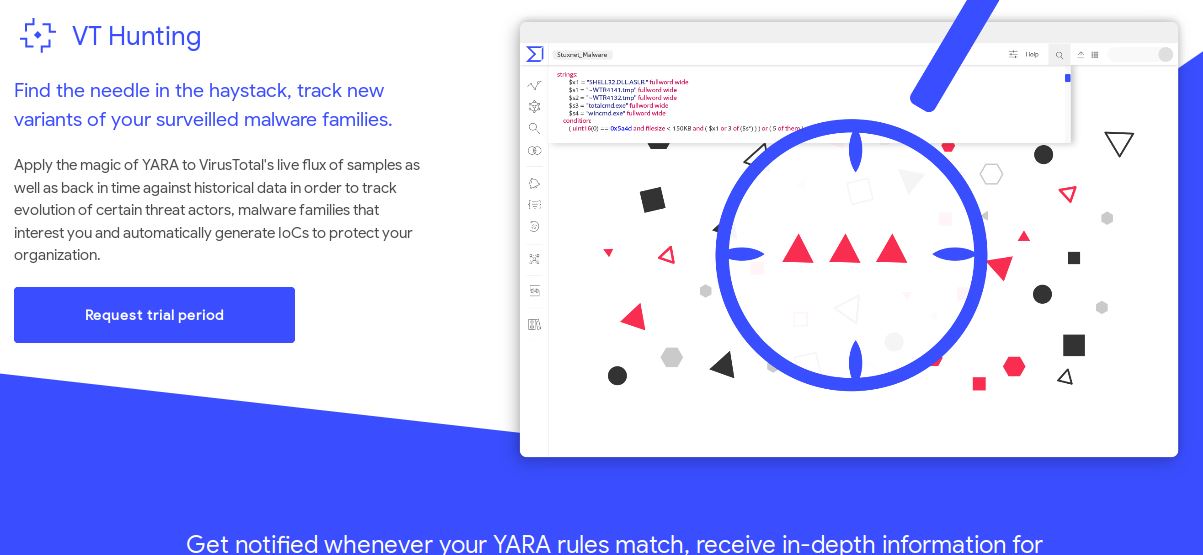
**Virus Total for Threat Hunting -**

**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**



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



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"

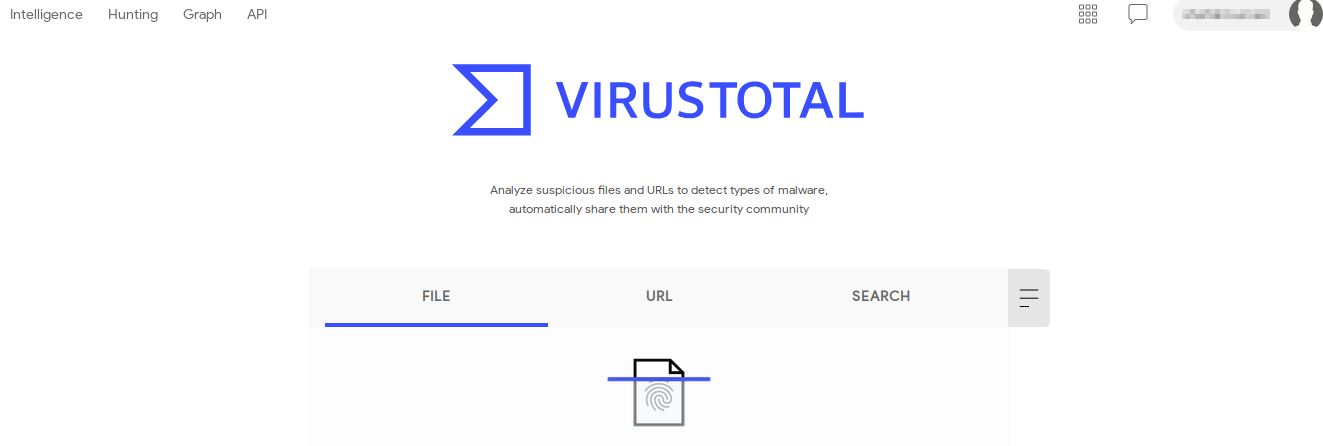
condition:

$a or $b or $c

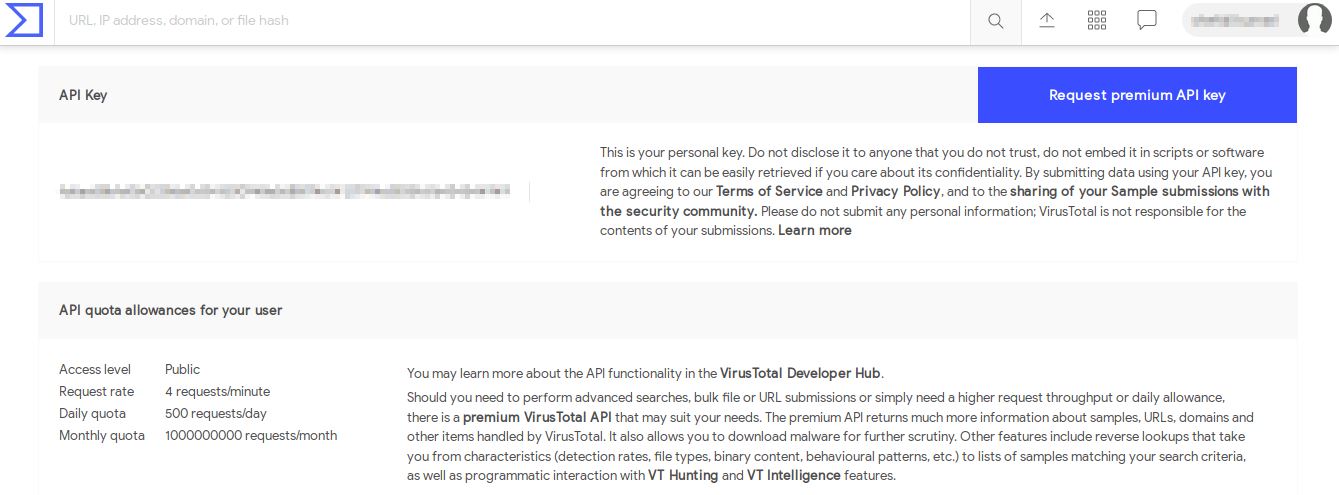
}

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.



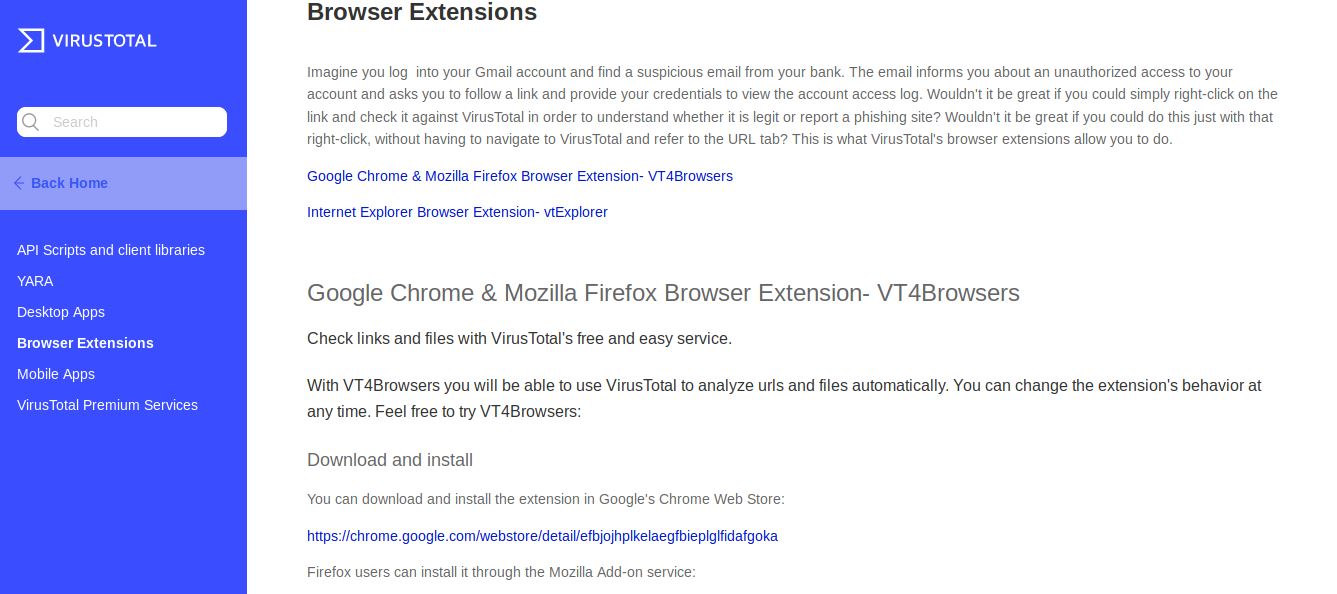
VT API key-



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>



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>

