Solving Ransomware pcap with Zeek – Sean Yarkoni

Solving the challenge Ransomware with Zeek on Ubuntu-20.04.2-live-server-amd64.

The challenge is:

There was a malware infection

1) What was the user looking for when he got infected?

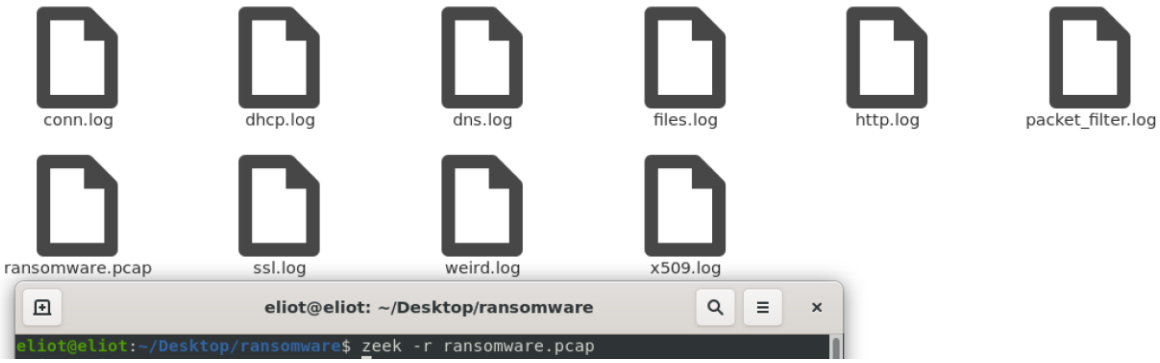
2) From where the ransomware was distributed?

3) What is the name of the ransomware?

Pcap file working with:

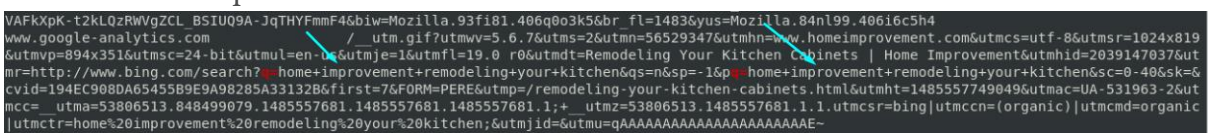
Solution:

In order for us to start we need Zeek to read the pcap file. For that will need to type: zeek -r ransomware.pcap -> This command will tell zeek to read the file and create different Log files that Zeek can create using the information that can be found in the PCAP.



Now we can start solving the challenge.

1) To find out what was the user looking for when he got infected, we can use the http.log file that Zeek created for us and use the column "host" to see where he visits and the column "uri" to see what he was searching for. We can do that with the command: cat http.log | /usr/local/zeek/bin/zeek-cut host , uri | grep q= (Note "q=" in the uri means query) and we can see in several places that the search was about "home improvement remodeling your kitchen" for example:



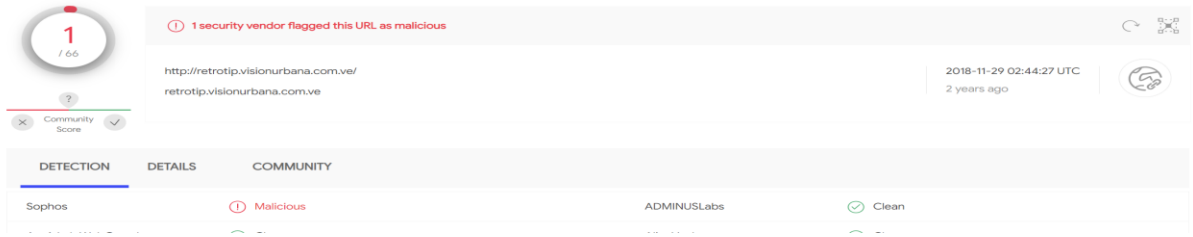
2) The origin of the file can be found using our knowledge and using outside tools like the website: https://www.virustotal.com/ to see where was the origin website of the ransomware, we need to collect every website that can be found in the pcap, because we analyzed the pcap file with Zeek we can use the http.log file and cut from it the host column by using the command:

cat http.log | /usr/local/zeek/bin/zeek-cut host | sort -u

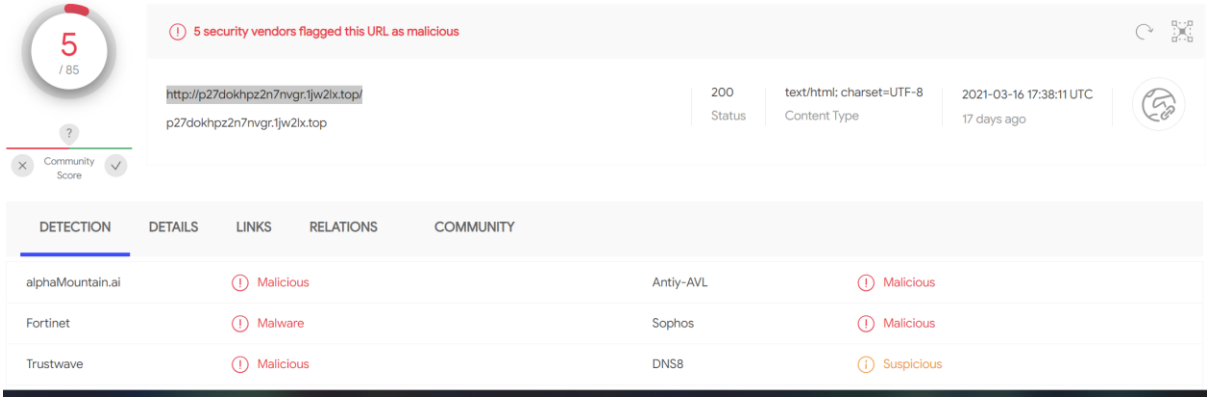
```
eliot@eliot:~/Desktop/ransomware$ cat http.log | /usr/local/zeek/bin/zeek-cut host | sort -u
-
1e46ba9c0151d4d34a7939daabd778ad.clo.footprintdns.com
2.bing.com
3a0849dbc3c36a673eb2ddd2fcf0494a.clo.footprintdns.com
40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com
6b8960d1b061131b015f93f32d0a56f4.clo.footprintdns.com
a4.bing.com
api.blockcypher.com
da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com
e623e8223493b6793a476840214720b1.clo.footprintdns.com
fpdownload2.macromedia.com
p27dokhpz2n7nvgr.1jw2lx.top
report.footprintdns.com
retrotip.visionurbana.com.ve
spotsbill.com
tse1.mm.bing.net
tyu.benme.com
www.bing.com
www.google-analytics.com
www.homeimprovement.com
www.msftncsi.com
```

Now with our knowledge we can see that most of the websites end with ".com" and one with "net" witch usually used but there are two websites the end differently and with nonfamiliar endings ".top" and ".ve" and those websites I will check with https://www.virustotal.com/ and see if there are malicious.

A) http://retrotip.visionurbana.com.ve/



B) http://p27dokhpz2n7nvgr.1jw2lx.top/

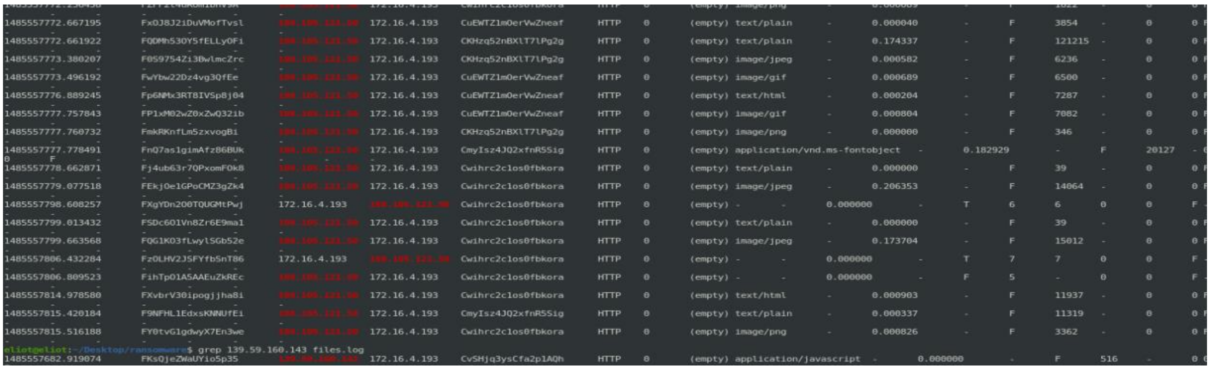


Bout websites seem to be malicious but the http://p27dokhpz2n7nvgr.1jw2lx.top/ have a higher chance to be the sores of the infection.

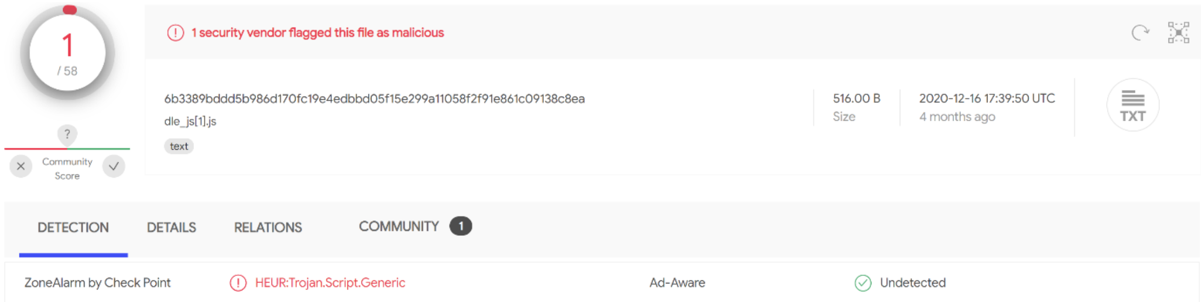
After we have confirmation that these two websites might be the distribution point, we can go to the file.log and search the IP address of bout of the websites and see if there is anything that might be the software to do so we will type:

grep 198.105.121.50 files.log (- p27dokhpz2n7nvgr.1jw2lx.top)

grep 139.59.160.143 files.log (- retrotip.visionurbana.com.ve)



From the result we can see that most of the files from .top don't seems to be malicious but the file from .ve can be, in order to get the file we can use an external tool (Wireshark/NetworkMiner etc…) and upload it to https://www.virustotal.com/ and see if the file is malicious.



As we can see the ransomware was downloaded from 139.59.160.143, in order to see how the user got to that website we can go to the PCAP file and grep anything that is related to that IP address and find the referrer to that website, type: grep 139.59.160.143 *.log and we can see that the referrer was http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html

3) The name of the ransomware can be seen in challenge 2 wan we upload the file to https://www.virustotal.com/ and when we type: grep 139.59.160.143 *.log and the name is dle_js.js which is a JavaScript file

How Zeek help us in the Ransomware case?

1) We toke the ransomware.pcap file and run it throw Zeek to get a sorted Log files of the traffic captured in the PCAP file by category.

2) We looked at all the files and figure what they contain before getting in to work.

Conn.log is a file containing TCP/UDP/ICMP connections

Dhcp.log is a file containing dynamic host configuration protocol leases.

Dns.log is a file containing domain name system activity.

Files.log is a file containing file analysis results.

Http.log is a file containing hypertext transfer protocol requests and replies.

Packet_filter.log is a file containing list of packet filters that were applied.

Ssl.log is a file containing SSL/TLS handshake info.

Weird.log is a file containing session initiation protocol.

x509.log is a file containing X.509 certificate info.

3) We used a tool called Zeek-cut to work only with the relevant columns and information we needed to solve our challenge using the log file that Zeek generated for us. The command Zeek-cut shown itself very useful in this challenge when we (the user) know what we want or need from every log file we used.