# **Title:** A report on Malware traffic analysis using Security onion

**Introduction of Security onion:**

It's an ubuntu-based Linux Distribution for intrusion detection, network security monitoring and log management. Security onion contains tools which collects, detects and analyzes data such as Snort, Suricata, Snorby, Bro(Re-branded name : Zeek), Sguil, Squert, ELSA, NetworkMiner, PADS and many more.

**NSM Principles:**

In order to get security one must do Collection, detection and analyzation of data.

**Sguil:**

1. Provide username and password to login
2. Select monitoring interface-enp0s3
3. Click Start SGUIL
4. The sguil dashboard will appear where there's two events(real-time and escalated):

Upper-Part:

Real-Time contains: (ST(status of internet), CNT, Sensor, Alert ID(Every ID is provided by Snort IDS), Date/Time, Stc IP, Sport, Dst IP, DPort, Pr(Protocol number), Event Message)

Lower-Part:

Main tabs – IP Resolution, Agent Status, Snort Statistics, System Msgs, User Msgs

**Malware analysis steps, commands and observations:**

1. Open the terminal
2. Type sudo soup(security onion update), enter user password + enter.
3. Type sudo rule-update(for snort rules)
4. Visit malware-traffic-analysis.net
5. Download and unzip the zip file
6. Locate the unzipped folder with ls -l
7. Type sudo tcreplay -I enp0s3 -M 10 name of pcap
8. The alert message will show on sguil dashboard
9. All the event messages starts with ET which is emerging threats
10. Select the first message and check the show rule box, to know about packet data check show packet data
11. To locate a particular snort rule sudo find / -name snort.conf
12. Will find and display the snort rules
13. Execute less copied one of the snort rules
14. Hit right click on the alert id and select transcript where the transcript will appear
15. In the destination the referrer and the host URL is strange
16. As the squil detected and showed message that flash version is outdated
17. When we check the vulnerable flash version in google we will find that in exploit database there are some certain flash player versions which can be underflowed with integer and can be remotely inject code in the browser
18. To extract a selective flash file we will use networkminer
19. Select and click Calculate MD5/SHA1/SHA256 hash
20. Copy the MD5 hash
21. Visit to virustotal.com/gui/
22. Click search and paste the copied md5 hash
23. Right click on the next event and select view corelated event
24. Click on one of the corelated event. There we will see the flow is established from source ip and there's pcre pattern as well as signature id
25. Right click on one corelated event and click Bro to view transcript.
26. As per observation we can understand it was trying to get something from the displayed code and the connection was established and in reply the destination returned content-type: text/html but the destination shows MZ
27. To check whether it's an html or not we need to drag and drop the file in the

terminal
28. The terminal shows that it pretends to be an html file but it's actually a PE32 file. So it was disguised.
29. Again checking the MD5 file in virustotal.
30. When rest of the bro was opened they were not malicious only the first one was malicious
31. As the next event is orange colored so that makes it a medium type of alert and the three of the events have the same source ip which means they're connected to each other
32. Last one of these three is a trojan which's host claim to send html content where flow was established from server and the contant is PE which is pact executable and the class type is trojan-activity
33. The next alert shows possible ip check ip-addr.es. This ip-addr.es is its content type.
34. After checking it in virustotal 4 engine detects ip-addr.es as malicious and informed that it's a bot networks, advanced malware command and control
35. In communicating file it shows that this exe file is communicating with a specific URL
36. On this last event the traffic private ip to destination ip and it is communicating with two different set of ip
37. The it tried to reach out to 204.152.254.221 but it failed and couldn't find it.
38. After skipping a lot of the ip in the serial(for not finding anything in the transcript) we found communication in 72.34.49.86. Here we can see some data which is receiving raw file.

39. After skipping another two we found a file which pretends to be an html file but the file utility claims it's a png image data

**Overview:**

The user visited a compromised site which was outdated and vulnerable flash version which allows remote code execution The client downloaded a malicious executable file which encrypted all the files of the user which is known as CryptoWall 3.0. As it involves money it's a ransomware. The user was asked to visit an onion site. Then the user installed the Tor browser and visited.