Department of Information Systems

Arkansas. A State of Technology.

A QUICK OVERVIEW

ECESSA / TRACKING DOWN MALICIOUS TRAFFIC

Prepared By: Jake Engles

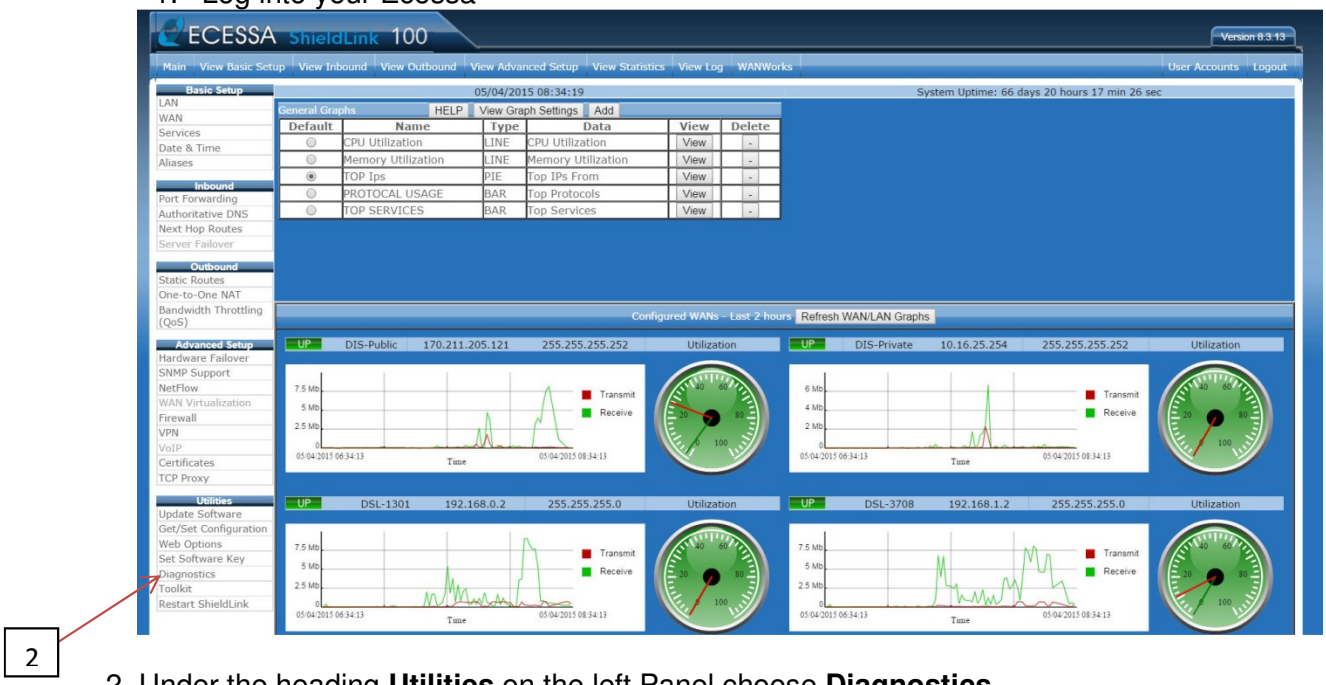
DIS APSCN/LAN Support

Traffic Dump – Using Ports and Addresses to find malicious traffic

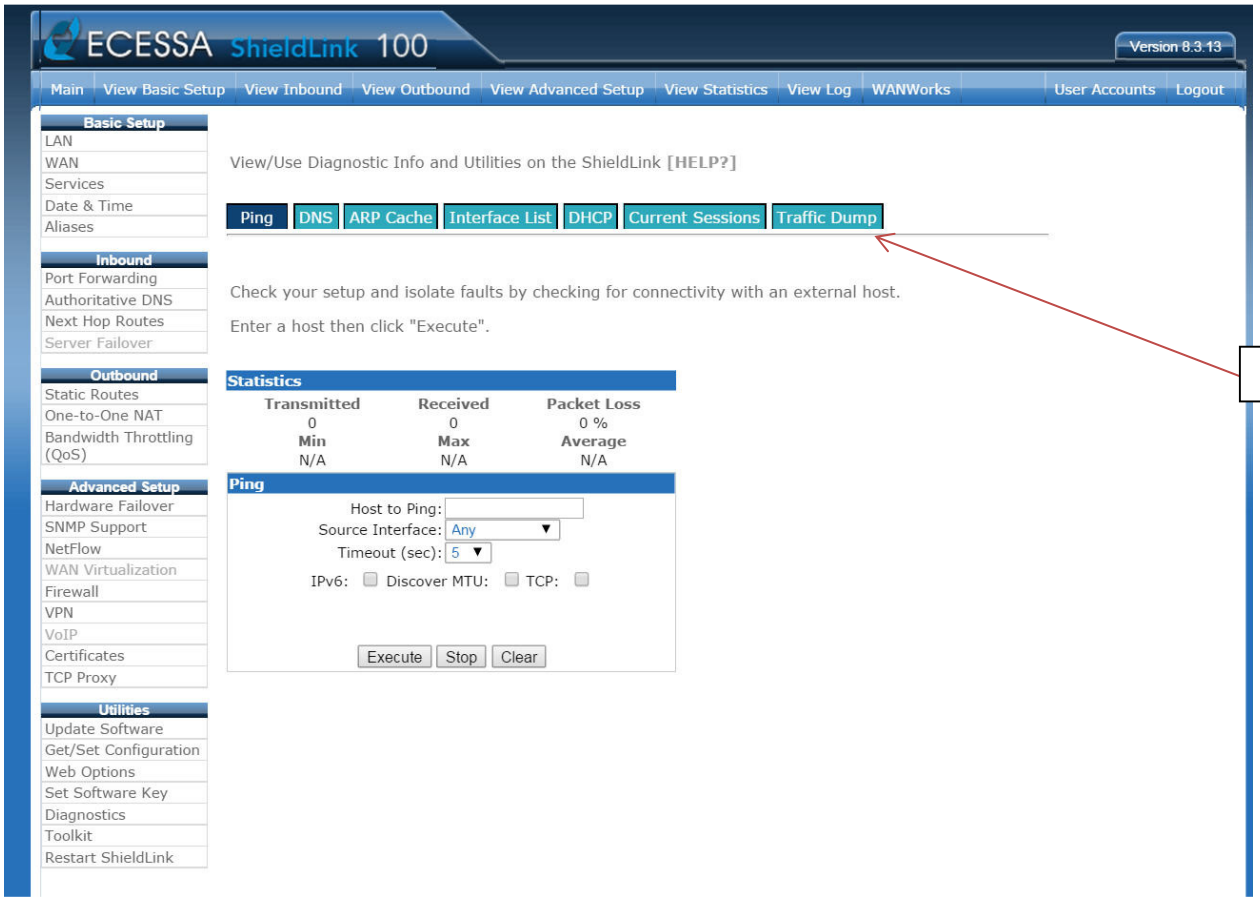
Finding Traffic on your Network: **USING PORTS**

Main Screen with Speedometer View

1. Log into your Ecessa

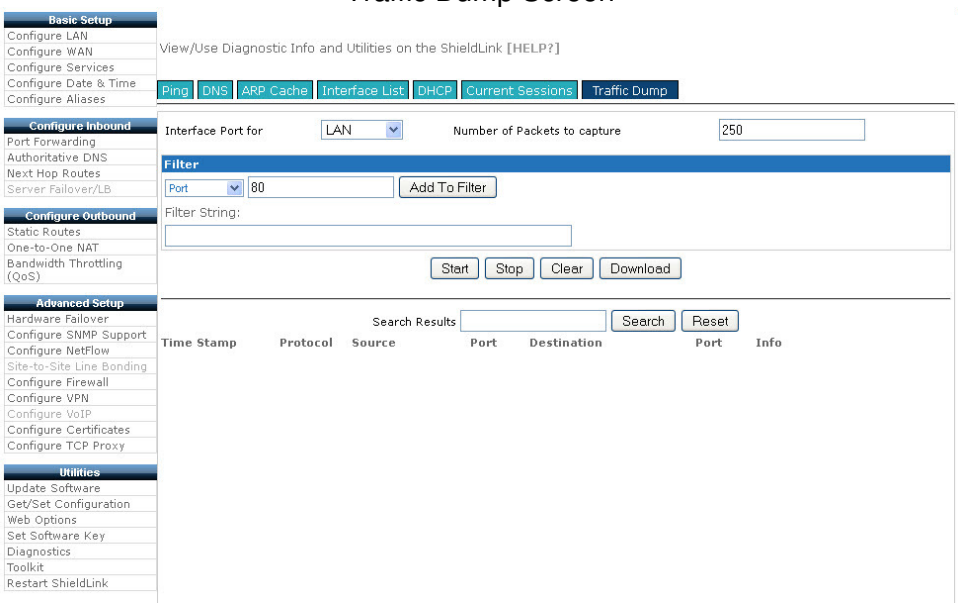


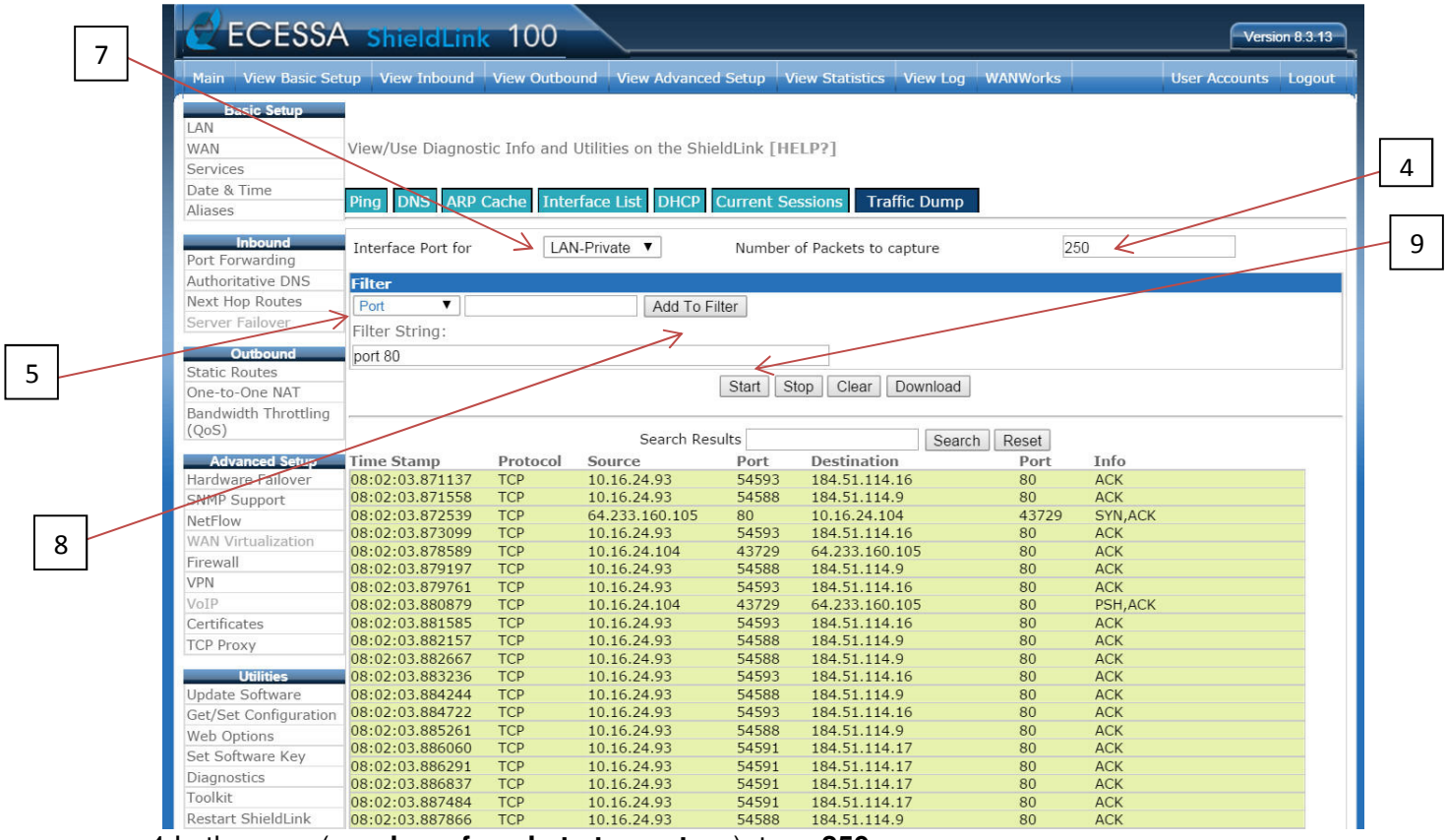
2. Under the heading **Utilities** on the left Panel choose **Diagnostics**



3. Select the tab **Traffic Dump** / on far right hand side of the available tabs.

Traffic Dump Screen





4.In the area (**number of packets to capture**) type **250**

5. Under **Filter** choose (**Port**) or (**Port Range**) in the drop down menu.

6. A single Port or a Port range can be entered here. If you are just looking for traffic on a specific port, enter the port number or numbers you are trying to track. This can be a port or a range of ports. Example Port Range: 4152-4177 or Port number: 25

7. Back at the top **(interface port**) use **Lan Private** – or the name of your **inside LAN interface.** These can be named differently on some Ecessas. You want to look for traffic on the inside of the network.

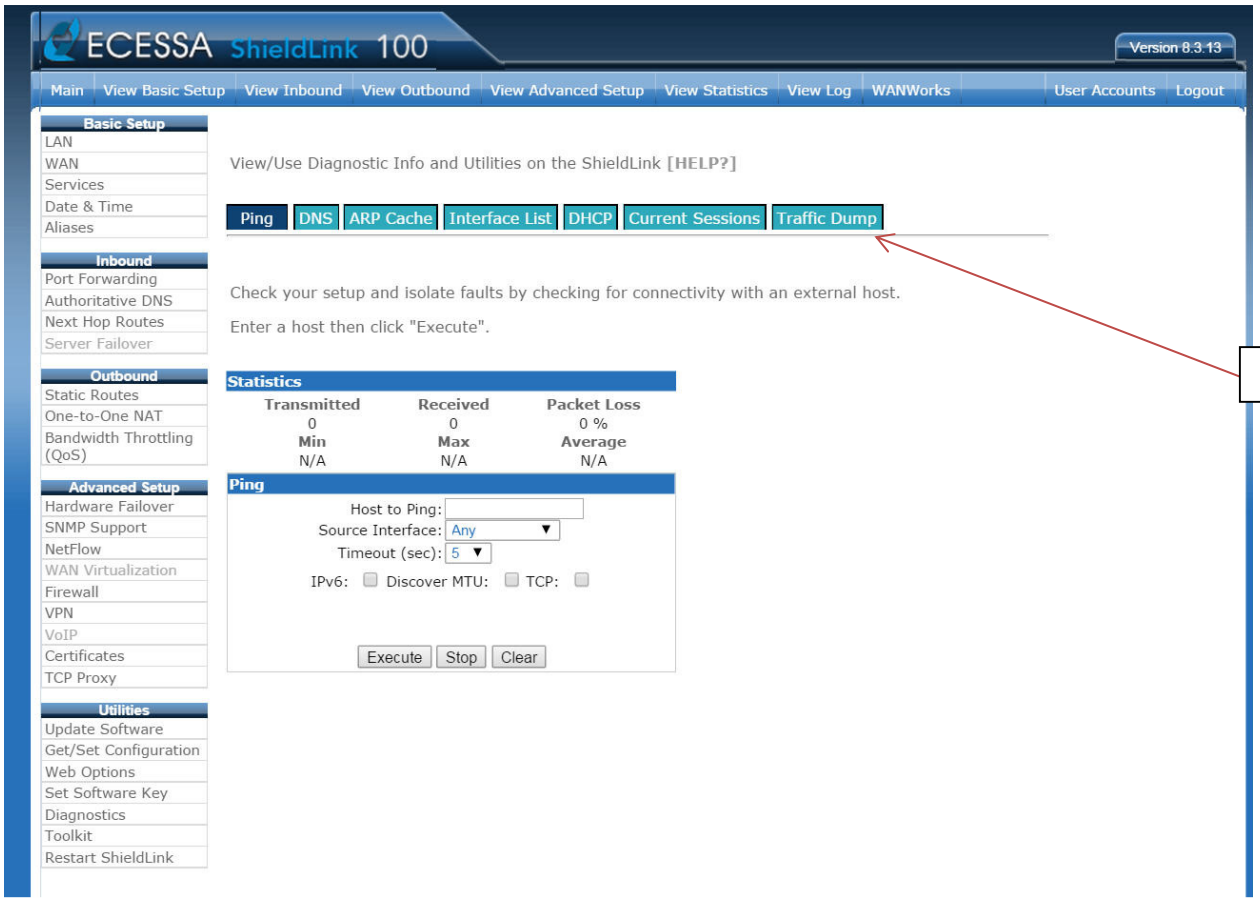
8. Click **Add to Filter**.

9. Start your Search… Remember you are looking for the (10.X.X.X) / Private machines that are giving off the traffic as listed in #5 and #6.

Finding Traffic on your Network: **USING ADDRESSES**
Main Screen with Speedometer View

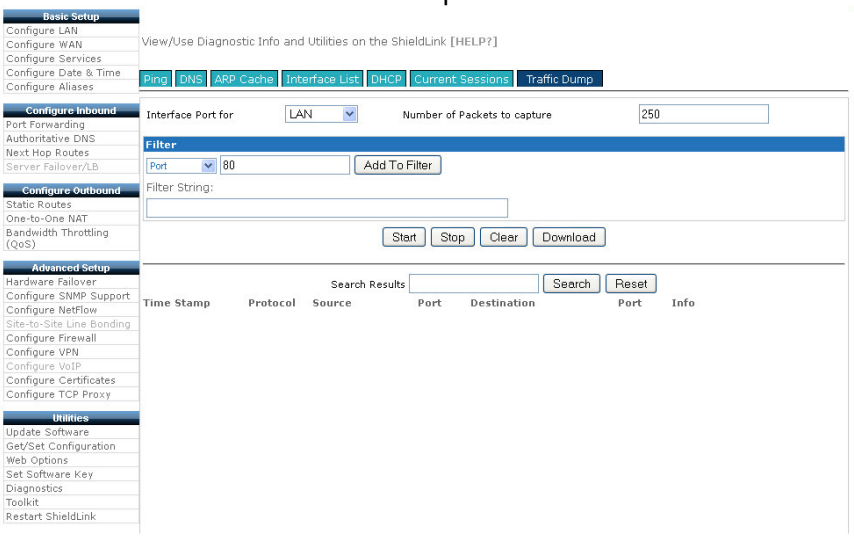
1.Log into your Ecessa

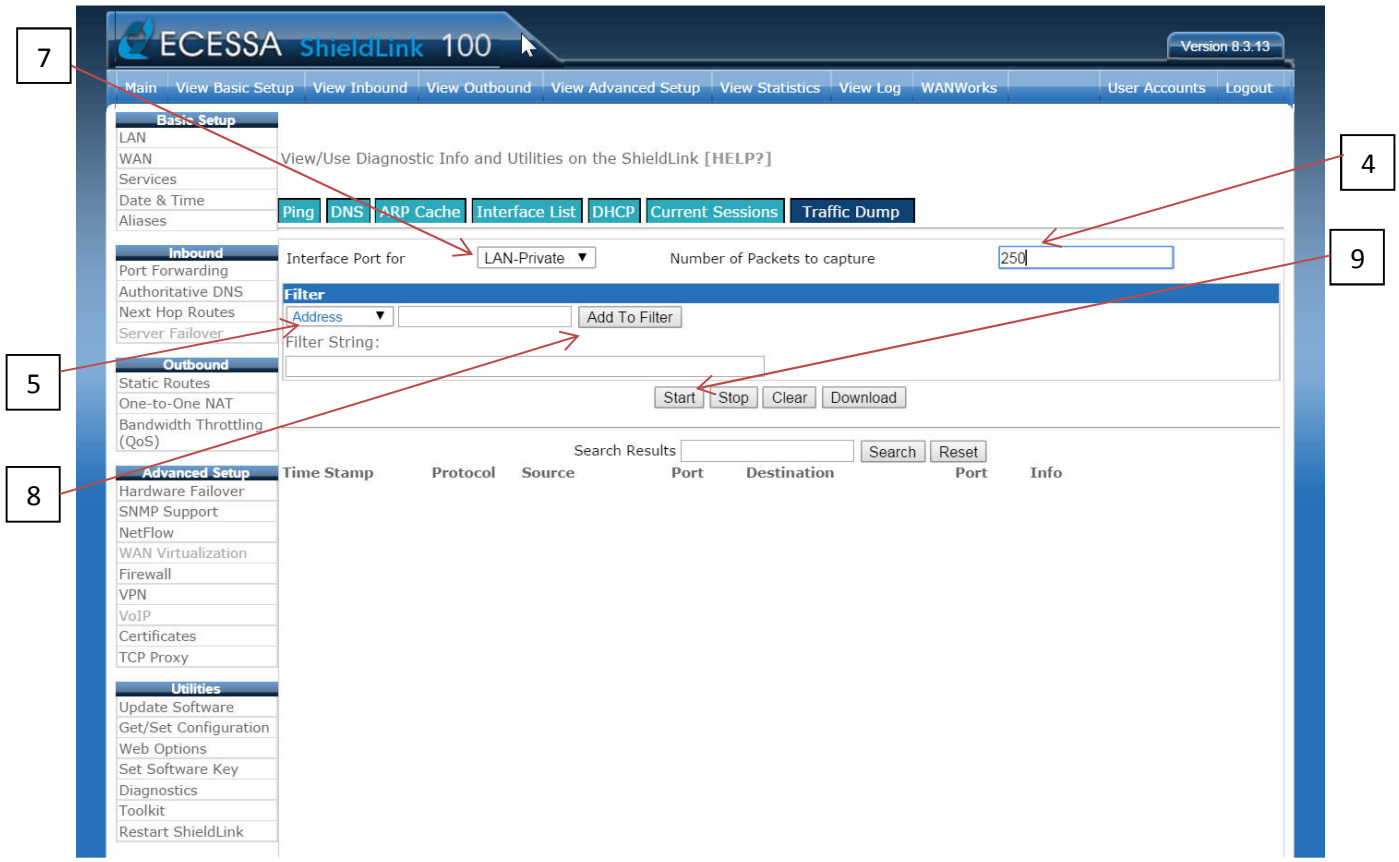
2. Under the heading **Utilities** on the left Panel choose **Diagnostics**



3.Select the tab **Traffic Dump** / on far right hand side of the available tabs.

Traffic Dump Screen





4.In the area (**number of packets to capture**) type **250**
5. Under **Filter** choose (**Address**) in the drop down menu
6. **Address** or a number of **Addresses** can be entered here. If you are just looking for traffic on a specific Address, enter the Address number. If you are looking for multiple Addresses enter them into the **Filter String** using the “and” / “or” statements Example Address: 8.8.8.8 Example of using the “or” command in your search - host 8.8.8.8 or host 8.8.4.4
7. Back at the top **(interface port**) use **Lan Private** – or the name of your **inside LAN interface.** These can be named differently on some Ecessas. You want to look for traffic on the inside of the network.
8. Click **Add to Filter**, unless you have typed your search string manually in the **Filter String** box.
9. Start your Search… Remember you are looking for the (10.X.X.X) / Private machines that are giving off the traffic as listed in #5 and #6.

Traffic Dump as opposed to Current Session

The reasoning behind the preference for “traffic dump” as opposed to “current sessions” is the information that is provided. You see the three way handshake – syn, ack and syn-ack.
You also have the options to use the “and” command /statement or the “or” command / statement.
The “or” command can be entered into the Ecessas Traffic Dump Search String.
This command causes the Ecessa to look for any number of addresses or ports all in a single query.
When searching certain bots that are known to communicate with a number of IPs,
the “or” command allows for you to look for a private address on your network that could be trying to contact any number of IP addresses. Conficker is a perfect example. It communicates to several known sinkholes (IPs that a bot notifies of its existence).
An example of an “or” command entered into the filter string of an Ecessas Traffic Dump when searching for Conficker sinkholes: host 149.93.23.110 or host 38.102.150.27 or host 216.66.15.109 or host 38.229.131.151 or host 38.229.162.131 or host 38.229.167.179 or host 54.83.43.69 or host 216.66.15.114 or host 38.229.145.209 or host 38.229.168.228 or host 38.229.139.16 or host 38.229.156.133 or host 38.229.142.121 or host 38.229.181.163 or host 38.102.150.57

The “and” statement can be used as well. This causes the Ecessa to look for a match of addresses or ports put into the search string of Ecessas Traffic Dump and will only show the traffic that is going to the specified IPs or the specified ports in tandem.
Example: “Mars” statement that states certain given addresses or are complaining about unwanted traffic. You would then use the “and” statement with the given Ips in the search string of Ecessas Traffic Dump: host 8.8.8.8 and host 8.8.4.4

These two commands / statements can be very helpful for specific types of Botnets, Malware, and Virus traffic.
If you know the exact IP address that is being attacked and or used in the virus ticket and is of a singular value, “current sessions” is a great tool for that particular kind of situation.

The CBL – A Network Administrators Best Friend when looking for up to date information on your malicious traffic

The CBl: http://cbl.abuseat.org/lookup.cgi Can be your best friend when trying to track down specific kinds of viruses. The CBL reports to Spamhaus who then, in return, reports to MARS.

CBL can give you a more up to date and accurate information on your Virus, Botnet, and or Malware. The information given is precise to within one second. When searching for certain kinds of bots this up to date information is pivotal because destination ports for certain bots, often referred to as “Sink Holes” can change with every time the infected machine / machines gives off the unwanted traffic. The CBL also will give you the date and time of the last detection of the malicious traffic for your particular IP. Checking the CBL with the IP address you have received a “mars” alert on periodically will let you know if you have found all infected machines or if the traffic is still being detected.
The CBL also will tell you if it is a spam sending Trojan or what kind of bot you are dealing with. This information allows for you to check for unwanted (for example spamming – port 25) traffic.

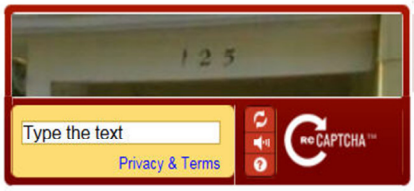
SAMPLE BELOW:

CBL EXAMPLE INFORMATION:

CBL Lookup Utility

It is with great regret that we have implemented a Captcha on this page. After 11 years the number of automated/abusive queries have grown so high it's now necessary. Only manual use of this lookup page is permitted. All automated/scripted queries are prohibited, and may result in listing of the source IP address.

IP address: [redacted]



LOOKUP

IP Address [redacted] **is listed** in the CBL. It appears to be infected with a spam sending trojan, proxy or some other form of botnet.

It was last detected at 2015-04-29 19:00 GMT (+/- 30 minutes), approximately 7 days, 21 hours ago.

This IP is infected (or NATting for a computer that is infected) with the **Conficker** botnet.

More information about Conficker can be obtained from Wikipedia

s **not** use port 25.

Please **follow** these instructions.

Dshield has a diary item containing many third party resources, especially removal tools such as Norton Power Eraser, Stinger, MSRT etc.

One of the most critical items is to make sure that all of your computers have the MS08-067 patch installed. But even with the patch installed, machines can get reinfected.

There are several ways to identify Conficker infections remotely. For a fairly complete approach, see Sophos.

If you have full firewall logs turned on at the time of detection, this may be sufficient to find the infection on a NAT:

Your IP was observed making connections to TCP/IP IP address 216.66.15.109 (a conficker sinkhole) with a destination port 80, source port (for this detection) of 1701 at exactly 2015-04-29 18:52:14 (UTC). All of our detection systems use NTP for time synchronization, so the timestamp should be accurate within one second.

If you don't have full firewall logging, perhaps you can set up a firewall block/log of all access (any port) to IP address 216.66.15.109 and keep watch for hits.

WARNING: DO NOT simply block access to 216.66.15.109 and expect to not get listed again. There are many conficker sinkholes - some move around and even we don't know where they all are. Blocking access to just one sinkhole does not mean that you have blocked all sinkholes, so relistings are possible. You have to monitor your firewall logs, identify the infected machine, and repair them if you wish to remain delisted.

Recent versions of NMap can detect Conficker, but it's not 100% reliable at finding every infection. Nmap is available for Linux, xxxBSD, Windows and Mac. Nessus can also find Conficker infections remotely. Several other scanners are available here.

Enigma Software's scanner is apparently good at finding Conficker A.

University of Bonn has a number of scan/removal tools.

If you're unable to find the infection, consider:

- If you used a network scanner, make sure that the network specification you used to check your network was right, and you understand how to interpret a conficker detection.
- Some network conficker scanners only detect some varieties of conficker. For example, nmap misses some. If you can't find it with nmap, try other scanners like McAfee's. In other words, try at least two.
- Are you sure you have found _all_ computers in your network? Sometimes there are machines quietly sitting in back rooms somewhere that got forgotten about. It would be a good idea to run

```
nmap -sP <ALL of your network specifications>
```

which should list all your computers, printers and other network devices. Did you see all the computers you expected to see?
- The infected computer may be turned off at the time you ran the scan or not on the network. Double-check everything was turned on during the scan.
- If you have wireless, make sure it's secured with WPA or WPA2, and that "strangers" can't connect. WEP security is **NOT** good enough.
- Many versions of Conficker propagate via infected thumbdrives/USB keys. When an infected machine is found, ALL such devices associated with the machine should be considered suspect, and either destroyed or completely reformatted.
- Conficker also propagates by file and printer shares.

If you simply remove the listing without ensuring that the infection is removed (or the NAT secured), it will probably relist again.

How to resolve future problems and prevent relisting

Norton Power Eraser is a free tool and doesn't require installation. It just needs to be downloaded and run. One of our team has tested the tool with Zeus, Ice-X, Citadel, ZeroAccess and Cutwail. It was able to detect and clean up the system in each case. It probably works with many other infections.

Is this IP address a NAT gateway/firewall/router? In other words, is this IP address shared with other computers? See NAT for further information about NATs and how to secure them.

If this IP address is shared with other computers, only the administrator of this IP address can prevent this happening again by following the instructions in NAT to secure the NAT against future infections. In this way, no matter how badly infected the network behind the NAT is, the network can't spam the Internet. The administrator can also refer to Advanced BOT detection for hints and tips on how to find the infected computer behind a NAT.

What affect is this listing having on you?

The CBL is intended to be used only on inbound email from the Internet.

If you are being blocked from IRC, Chat, web sites, web email interfaces (eg: you're using Internet Explorer or Firefox to send email) or anything other than basic email with a mail reader like Exchange, Thunderbird etc, the provider of this service is using the CBL against our recommendations. Contact the provider and refer them to http://cbl.abuseat.org/tandc.html and refer them to item 2 and 7.

If you are an end user: If you get an immediate popup indicating your email was blocked when you attempt to send email, this means one of two things:

- You aren't using your provider's preferred configuration for sending email. This is most frequent with roaming users (eg: you're using an Internet Cafe, and are using your home provider to send email). A provider will normally give you instructions on how your mail reader should authenticate to their mail servers, perhaps on a different port (usually 587). Make sure that you comply with the provider's instructions on mail reader configuration where it refers to "SMTP relay server", "SMTP authentication" etc.
- If you are complying with your provider's instructions, your provider is violating the CBL Terms and Conditions and blocking their own users. Contact your provider and refer them to http://cbl.abuseat.org/tandc.html and refer them to item 6 and 7.

If you get the blocking email message by return email (instead of by immediate popup), your provider is listed in the CBL, not you. Contact your provider and tell them that their IP address is listed by the CBL.

Note that the CBL is not responsible for how providers misuse the CBL. This is their problem, not ours.

If your IP address changes periodically (such as with reconnecting to your provider, connecting through an Internet Cafe etc), this is usually a dynamic (DHCP) IP address, meaning that it's most likely not you that is infected. As above, make sure that your mail reader is configured correctly as per your provider. In this case, delisting the IP address will probably not do anything useful.

If this listing is of an unshared IP address, and the affected access is email, then, the computer corresponding to this IP address at time of detection (see above) is infected with a spambot, or, if it's a mail server, in some rare cases this can be a severe misconfiguration or bug.

The first step is to run at least one (preferably more) reputable anti-spam/spyware tools on your computer. If you're lucky, one of them will find and remove the infection.

If you are unable to find it using anti-virus tools, you may want to take a close look at the discussions of netstat or tcpview in the "Per-machine methods" section of Finding BOTs in a LAN.

If the above does not help, you may have to resort to taking your computer to a computer dealer/service company and have them clean it.

If all else fails, you may need to have your machine's software re-installed from scratch.

WARNING: If you continually delist [redacted] without fixing the problem, the CBL will eventually stop allowing the delisting of [redacted].

If you have resolved the problem shown above and delisted the IP yourself, there is no need to contact us.

Click on this link to delist [redacted].

<< Back to CBL homepage