CBL LOOKUP

IMPORTANT: Many CBL/XBL listings are caused by a vulnerability in Mikrotik routers. If you have a Mikrotik router, please check out the Mikrotik blog on this subject (https://blog.mikrotik.com/security/winbox-vulnerability.html) and follow the instructions before attempting to remove your CBL listing.

IP Address: 177.93.97.228

RESULTS OF LOOKUP

177.93.97.228 is listed

This IP address was detected and listed 2 times in the past 28 days, and 0 times in the past 24 hours. The most recent detection was at Mon Mar 4 21:55:00 2019 UTC +/- 5 minutes

This IP address is infected with, or is NATting for a machine infected with the Conficker malicious botnet.

More information about Conficker can be obtained from Wikipedia (http://en.wikipedia.org/wiki/Conficker)

Please follow these instructions.

Dshield (http://www.dshield.org/diary/Third+party+information+on+conficker/5860) 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 (http://www.sophos.com/en-us/support/knowledgebase/61259.aspx).

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

This was detected by a TCP connection from "177.93.97.228" on port "40170" going to IP address "38.229.146.66" (the sinkhole (sinkhole.html)) on port "80".

The botnet command and control domain for this connection was "n/a".

This detection corresponds to a connection at Mon Mar 4 21:58:48 2019 UTC (this timestamp is believed accurate to within one second).

Detection Information Summary	
Destination IP	38.229.146.66
Destination port	80
Source IP	177.93.97.228
Source port	40170
C&C name/domain	n/a
Protocol	TCP
Time	Mon Mar 4 21:58:48 2019 UTC

Behind a NAT, you should be able to find the infected machine by looking for attempted connections to IP address "38.229.146.66" or host name "n/a" on any port with a network sniffer such as Wireshark. Equivalently, you can examine your DNS server or proxy server logs to references to "38.229.146.66" or "n/a". See Advanced Techniques (advanced.html) for more detail on how to use Wireshark - ignore the references to port 25/SMTP traffic - the identifying activity is NOT on port 25.

Please note that some of the above quoted information may be empty ("") or "na" or "-". In those cases, the feed has declined or is unable to give us that information. Hopefully enough information will be present to allow you to pinpoint the connections. If not, the destination ports to check are usually port 80, 8080, 443 or high ports (around 16000) outbound from your network. Most of these infections make very large numbers of connections; they should stand out.

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 38.229.146.66 and keep watch for hits.

Recent versions of NMap (http://insecure.org/) 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 (http://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker/).

Enigma Software's scanner (http://www.enigmasoftware.com/a1/download/cfremover.exe) is apparently good at finding Conficker A.

University of Bonn (http://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker/) has a number of scan/removal tools.

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

1. 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.
2. 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 (http://www.mcafee.com/ca/threat-center/confickertest.aspx). In other words, try at least two.
3. 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?
4. 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.
5. 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.
6. 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.
7. Conficker also propagates by file and printer shares.

SELF REMOVAL:

Normally, you can remove the CBL listing yourself. If no removal link is given below, follow the instructions, and

come back and do the lookup again, and the removal link will appear.

I have verified that all of my computers and services accessible from the Internet through this IP address (computers, such as external router admin interfaces, web servers, Internet of Things devices such as DVRs, webcams and Baby Cameras) all have inwards Internet access turned off, OR, have had their passwords changed from the default factory setting.	REMOVE