Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Detecting Conficker on your network

From time to time Janet CSIRT may report activity to you that is related to the Conficker worm. Typically this is a record of traffic from an infected host, to a Conficker sinkhole server. These sinkhole servers pretend to be part of the worm's command and control infrastructure. The worm then attempts to load a web page on the sinkhole server, that were the server real, would contain instructions for the worm.

Our reports typically look like this

```
time,protocol,source,destination
2009-11-15T19:24:03,TCP,193.60.199.196:7377,83.68.16.6:80
2009-11-15T19:24:14,TCP,193.60.199.196:7315,74.208.64.145:80
2009-11-15T19:24:18,TCP,193.60.199.196:7408,205.188.161.4:80
2009-11-15T20:24:40,TCP,193.60.199.196:39963,199.2.137.252:80
```

This report details the time (UTC or GMT unless stated otherwise), protocol, source address and port, and destination address and port of connections related to Conficker infections.

The first step in tracing this activity to it's source is in identifying what device the source address, in this case 193.60.199.196, is assigned to. In some cases this will lead you to a specific computer and your search is over, but in many cases this address is assigned to a gateway device that performs Network Address Translation (NAT) such as a firewall, or a proxy server that filters web access from your site. In both cases inspection of the logs from the gateway device is necessary to identify the infected system.

For example, in the logs from a Cisco ASA firewall you could search for a log entry matching the traffic in the report:

```
Nov 15 19:24:14 192.168.0.1 %ASA-6-302013: Built outbound TCP
connection 21513792 for ext:74.208.64.145/80 (74.208.64.145/80) to
internal:192.168.0.5/7315 (193.60.199.196/7315)
```

Which shows that for this particular connection the ASA was translating from 192.168.0.5. The device that this IP address is assigned to is the source of the infection and needs to be investigated using your standard anti-virus tools. If your NAT device is not capable of producing such logs, we recommend that in order to comply with the Janet Security Policy, it is replaced with one that does. You should be able to follow a similar process with log files from your proxy device. It's recommended that your proxy server logs not only the URL requested, but the IP address the URL was fetched from. Domain names and DNS entries change rapidly and can be unreliable in an investigation.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/detecting-conficker-your-network