Conficker

Janet CSIRT routinely processes netflow data to detect signs of Conficker infections on Janet.

- Protecting yourself from Conficker [1]
- Detecting Conficker on your network [1]

The Conficker worm attempts to contact a number of different domains every day. Due to the efforts of the Conficker Working Group these domains have been redirected to a number of known honeypots known as sinkholes. The operators of these sinkholes then generate reports which are forwarded to Janet CSIRT. Due to the large volume of data that the Conficker Working Group has to process globally, Janet CSIRT detects this traffic to the sinkholes in netflow, before we receive external reports from the sinkhole operators.

Traffic to these sinkholes (and in our reports) is not necessarily indicative of a Conficker infection. Over time the addresses and use of the sinkholes can change. Organisations *must* always seek confirmation of the data in our reports, matching it with local network logs and anti-malware tools before any action is undertaken.

Our Workflow:

- Once the level of Conficker traffic reaches a given threshold in a particular time period, our system generates a report and automatically starts an incident. Large volumes of traffic cause the report to be truncated for convenience.
- The incident will automatically forward the report to your organization. Upon receiving any reply, the incident will be closed unless the reply specifically and clearly asks for assistance or clarification.
- If no reply is received then after a period a reminder will be sent, containing any further reports of traffic we have generated.
- If no reply is received after this reminder then a final reminder is sent and the incident is closed, marking it as having not been responded to. From time to time Janet CSIRT reviews these incidents.

If you have any questions, comments or suggestions for improvements to this work flow then please feel free to get in touch.

Notes:

Please do not block the destination sinkhole addresses unless you are confident that you can detect and respond to this traffic. Blocking the sinkhole addresses does not alter the operation of the worm, and prevents Janet CSIRT from providing this service to you.
If you are interested in deploying your own systems for detecting this traffic then please get in touch. Janet CSIRT can provide you with code, information and advice.

Links

[1] http://community.ja.net/library/janet-services-documentation/detecting-conficker-your-network