Conficker

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.

Protecting yourself from Conficker

Protecting yourself from Conficker

The Conficker worm (also known as Downup, Downadup and Kido) is probably the most prevalent computer worm on Janet and the Internet at this time. It's success can be attributed to it's use of a number of different vectors it uses to infect machines:

- Exploiting a vulnerability in Microsoft Windows to gain remote access
- Guessing user's login passwords
- Using the auto-run functionality in Microsoft Windows to trick the user into executing it

The worm then disables anti-virus software on the infected system, and attempts to download further instructions from a large number of domains. It is not known what the intended payload is, as the operator of the botnet has not yet attempted to send it any commands. The identity of the person or group operating the Conficker worm is also a mystery.

The worm is currently inactive and current threat from infection is minimal, but we believe that the huge number of infected hosts poses a potentially critical thread, and immediate action is required. If infected systems are ever activated, perhaps sending spam or participating in a denial of service attack, the impact on your network could cause massive problems.

- Tracing Conficker Reports [2]
- Detecting Conficker Infections [3]

Five Steps to protecting yourself from Conficker

1. Install the update for Microsoft Security Bulletin MS08-067
2. Block Windows LAN service ports when unnecessary
3. Enforce a strong password policy
4. Disable auto-run
5. Install correctly configured anti-virus software

Microsoft Security Bulletin MS08-067

All systems must be protected against the vulnerability outlined in this Microsoft Security Bulletin [4]. This was the initial way the worm spread. Centrally managed systems should have had the relevant patches and updates applied through your usual patch management procedures. You should issue instructions for staff and students to update their personal systems.

The system also needs to be reachable on port 445/tcp to be infected by this route. This is

one of the ports used to support Windows LAN services such as NetBIOS [5]. The ports used by Windows LAN services must be blocked inbound and outbound at your network border. If you do need to access these ports over the Internet, exceptions can be made for particular hosts. You may also need to consider blocking these ports at at internal divisions on your own network. Does a public wifi network need to be able to use this ports? Also remember that many desktop firewalls block access to these ports, but still allow access from systems on the local network.

Do not rely on patching or firewalling to provide complete protection. Installation of the update can fail, and firewalls provide no protection against infected across a local network. Also, neither method provides protection against other means of infection, so it cannot be the only step you take.

Dictionary attack against user accounts

Windows allows remote machines to list valid user names, a useful feature in some environments. The worm finds user accounts, and then attempts a simple dictionary attack against the passwords for this account. If successful, the worm can install itself.

The attack uses a simple and very small dictionary of common passwords but is surprisingly successful. You must enforce a strong password policy for your Windows domains [6], even a simple one is better than nothing. You should issue instructions for staff and students to make sure they chose secure passwords for their personal systems.

Auto-run, and tricking users into running the worm

Once a system is infected, the worm copies itself onto any available USB drives. When the drive is placed in a clean and unprotected system, the system will attempt to auto-run the worm, infecting itself. The worm also uses some clever tricks to try and convince the user to run the worm themselves.

Protect yourself against this method of infection by disabling auto-run [7], and ensuring your anti-virus software performs on-access scanning of USB media. Make sure that you correctly understand the operation of your anti-virus software and that if on-access scanning of USB drives is enabled. Often anti-virus installed, but incorrectly configured. It is unlikely that scheduled scans will provide much protection.

Detecting Conficker on your network

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.

Links
[1] http://community.ja.net/library/janet-services-documentation/detecting-conficker-your-network
[2] http://community.ja.net/library/janet-services-documentation/tracing-conficker-activity
[3] http://community.ja.net/library/janet-services-documentation/detecting-conficker-infections
[4] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[5] http://community.ja.net/library/janet-services-documentation/blocking-lan-service-ports
[6] http://technet.microsoft.com/en-us/library/cc736605(WS.10).aspx
[7] http://www.us-cert.gov/cas/techalerts/TA09-020A.html