Dealing with worms or viruses

This advice is principally to help a Janet organization respond properly to reports from Janet CSIRT that a worm or virus is present in their network.

The intrusion of worm and virus software to one or more of your computers is the most common class of network abuse. In some cases it does little obvious, direct or immediate harm to your network; but it does need dealing with systematically and promptly:

- You do not know what damage you are exposed to by loss of data, unauthorised access to information or denial of service;
- Most worm and virus software attempts to install itself on a great number of other computers which may be outside your network, and you will not wish to be responsible for damage there;
- These attempts to propagate usually involve address scanning, which is itself an abuse and brings your network and the whole of Janet into disrepute;
- Worm and virus software, particularly that which may persist on an infected computer as a zombie or bot under the control of someone else, can carry out further abuse on a large scale such as bulk e-mailing or a Denial of Service attack, for which again you will not want to be responsible;
- The performance and other behaviour of your network may become unpredictable or different from what you expect and need.

Immediate action

If you are reacting to a report from Janet CSIRT, please acknowledge our e-mail as soon as possible.

Find the computer responsible

If Janet CSIRT sends you a report of activity such as address scanning which probably indicates a worm or virus, our report will include the source IP address in your network and the times when scanning started and stopped. Usually there will be at least a few lines of flow records which give a time precise to within a second and accurate and an IP address (not yours) which your computer sent a packet to at that time.

If the address in your network is used by an individual computer, that is the one to deal with first; it is possible that there was another computer emitting its abuse through this one, but that will only become clear later.

Most networks have a NAT gateway, a proxy or a firewall which is the externally visible source of some or all traffic from your network. To identify the internal address from which the abuse actually comes you will need local knowledge from resources such as:

- Logs of NAT activity;

- Records of login activity by users;
- Records of Web or other access through a proxy;
- Packet sniffing with a hardware device or software.

It is highly desirable that you have enough logging in place, and enough familiarity with it, to be able to identify potential abuse after the event.
If instead you need to monitor packets in real time with a dedicated sniffer device or with software such as *Ethereal* or *tcpdump* running on a standard desktop or laptop computer, there are a few precautions to bear in mind.

- It may not be easy to find a point in your network at which you can attach the sniffer. Ordinary switch ports will not give access to packets on other ports. You may be able to configure a ?spanning port?, or you may be able to temporarily insert an Ethernet hub in some shared link or links and monitor traffic from one of its ports.
- Any ordinary computer you use for monitoring will be exposed to at least as many threats as the other computers in your network, and if ever it is compromised with a worm or virus it may be connected at points in the network where it is more easily able then most to infect others.
  It is best to use a freshly installed computer with fully up-to-date patches for the operating system, all applications and anti-virus products. After use, treat the computer as suspect until it is thoroughly checked or rebuilt.
- It is likely that you can get the information you need from your router or hardware firewall, either by increasing logging levels or by temporarily configuring to block the packets concerned and examining the resulting errors.

- *tcpdump* is a standard package which should be available with any Linux-like operating system, although it may not be installed by default.
- Wireshark is available for both Linux-like and Windows systems: http://www.wireshark.org/ [1]

Remove it from the network

Most commonly you will unplug the Ethernet cable. Whether you power down the computer is then up to you. For a wireless connection you will need to disable the link, this is usually accomplished easily within the network user interface. Other possibilities include removing a USB wireless dongle or disabling one or more access points.

If the computer responsible is an important server, it may be very inconvenient to remove it from the network or turn it off. You might be able to make it safe enough to continue working for a short time, during which you must monitor its behaviour; but an objective risk analysis will rarely conclude that that is a good idea.

Repair

1. Find the unwanted software.
2. Remove unwanted software.
3. Update the operating system.
4. Update your anti-virus and similar defensive software.
5. Check for secure configuration and operation.

Note that you will want to connect the computer to a network to update and check it, but that it

is in the same insecure state in which it became infected originally, so the procedure is dangerous.

- You may have some offline method for installing a known good copy of the operating system and application software and configuration; perhaps a CD or a set of CDs.
- You can provide a small network specifically for this purpose. It should be separate from your networks in production use and not directly accessible from Janet or the Internet, and it should have no machines on it except the one you are repairing. It may be practicable to attach a small NAT device to your network (such as a ?DSL router? marketed for domestic use) and use the NAT segment it provides.
- You should allow your anti-virus and other similar software to scan the machine before it is reconnected, and you may be able to use a very small and restricted network as described above to scan the repaired machine for any unexpected listening ports.

Prevention

Normal good housekeeping is essential, including regular updates to operating system, applications and anti-virus software.

Ideally you will monitor the behaviour of your network (to detect any scanning or other unwanted activity) and you should consider blocking certain kinds of traffic at your router or firewall:

- Blocking LAN service ports [2]

Links
[1] http://www.wireshark.org/
[2] http://community.ja.net/library/janet-services-documentation/blocking-lan-service-ports