Malware

Malware is a term used to encompass a wide and growing variety of software threats to the security of computer systems. It consists of software designed to interrupt the normal operation of a computer for some malicious purpose. This may simply be to disrupt the normal operation of a system but more commonly and increasingly it is used to gain unauthorised access to resources and information.

Viruses, trojan horses, spyware and rootkits are all considered to be forms of malware. In many cases the boundaries between these different types of malicious software have become less clear and the term malware allows us to discuss these issues as a whole.

Malware is increasingly being used by organised crime. Malware can be used to steal banking and credit card details, as well as other personal data. This provides a low risk path for the theft of large volumes of money. Whereas older viruses disrupt computers and networks, modern malware presents more of a risk to an individual or organisation's privacy and information than it does to the continued operation of computer systems. Although recent malware can be quite subtle in it's action, slowing performance, a lack of resources and suspicious network traffic and unusual system behavior can all be symptomatic of an infection.

Whilst most malware is widely released by it's authors and spreads according to it's success, some organisations will find themselves the target of custom written malware designed to compromise the security of specific systems. This may form part of an Advanced Persistent Threat, and Stuxnet is probably the best example of this.

In terms of raw numbers the most common malware seen on Janet are those that have been particularly successful in attacking unmanaged desktop systems such as those belonging to students and faculty members. A lack of consistent and thorough patching and anti-virus software can leave them particularly vulnerable.

Malware accounts for the majority of security incidents reported to Janet CSIRT. The most common virus infections seen by CSIRT include Conficker [1], Sality, gbot, Morto, Torpig/Mebroot and Zeus [2]. When investigated many computers are found to be host to multiple other infections. Even older worms such as Blaster and SQL Slammer are still occasionally seen. The infections we see are usually limited to those we can detect at the IP level and those which are reported to us. Where prudent we will share information with the community on how to detect specific malware on the network.

Please report malware infections to Janet CSIRT even if you do not require our assistance. The trends that we can build from reporting this information to us are invaluable.

Links
[1] http://community.ja.net/library/janet-services-documentation/conficker-0

[2] http://community.ja.net/library/janet-services-documentation/zeuszbot