MALWARE REMOVAL GUIDE

Malware Detection and Removal on Windows

There are a number of free tools that can help with this. None of them are perfect, and none of them will detect 100% of all known malware- so the important thing is to use all of them in the hope that the overlap of their detection is enough to remove the problem. However, it is still very possible that no tool will be able to detect and/or clean the malware. In this instance it is possible that an “expert” may be able to manually work out where the malware is hiding and how to remove it – however, the easiest solution is likely to be a rebuild.

Always Suggest Password Changing

Please note that it's worth suggesting password changing to the users regardless of what is found. If anything that might be a major security risk is found - in particular keystroke loggers, rootkits, remote admin kits, etc - the user, and any other user of the machine, **must** change their passwords for all services that they may have used on that system, and local passwords for all users – including Administrator – on the system itself. If they do online banking or credit/debit card purchases they should also inform their banks, and follow the exact procedures given by them – this is **vitally** important.

When to suspect malware

Definitely suspect malware if the user reports unexpected popups, browsers going to sites other than the ones they were actually trying to go to, and similar problems. Also suspect it if you spot software associated with peer-to-peer filesharing; traditionally such software tends to have malware included.

However, a good rule of thumb is "it's worth checking anyway, regardless of why the user is there" - the more serious forms of malware do not give any visible sign at all.

Detection and removal

The computer should **not** be put on the network until initial detection and removal has been done. This is because malware will usually attempt to spread via network connections. All of the tools below can be placed on a USB stick or CD. Current updates for the detection data can also be placed on the USB for most of the products below, and so they can be updated before scanning without putting the machine on the network.

The first thing to check is if the user has anti-virus software and if it is up to date. If not, then *McAfee VirusScan Enterprise* can be used (if the user is a staff or student of the University) - see http://www.ucs.ed.ac.uk/usd/cts/ol/issues/viruses/ - or a free antivirus like *AVG AntiVirus Free* (http://free.grisoft.com/) can be used. It is worth running a scan at this point.

Next, check for rootkits . Some antivirus/spyware software can detect rootkits natively but a standlone scan is worthwhile. At the time of writing F-Secure have a rootkit detector available for free download – *F-Secure Blacklight,*
see http://www.f-secure.com/blacklight/blacklight.html - which works very much like an antivirus scanner and is easy to use. It may vanish however, as it is now integrated into their commerical products.

SysInternals (now part of Microsoft) also have *RootkitRevealer* -

http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx - which displays files, processes and registry entries which exist in the raw data but are not visible to Windows. It is important to read the linked page carefully as some parts of the NTFS structure will always show up and are not indicative of a rootkit. If you wish to use this tool run it a few times on known clean machines just to see what to expect.

Note that until recently the presence of rootkit techniques was usually indicative of a complete compromise of the system. However rootkit techniques are now used by more and more of the lower level of malware (such as popup generators) in order to hide them from malware detection tools. This makes it far more complex to decide if a reinstall is the best way forward.

If a rootkit is found (and verified, particularly if using Rootkit Revealer - as mentioned it only shows signs that _may_ indicate a rootkit, and it takes some knowledge to determine if a rootkit is the cause) then an expert look at the system is likely needed, to determine if the rootkit is just hiding some files or is indicative of a fully compromised system. It may be safer to regard the system as being compromised and rebuild it – this will likely depend on how much work is required to backup the system and reinstall software.

Once rootkits have been eliminated as a potential problem it is time to scan for spyware and remove it if possible. Amongst the products available to do this are;

LavaSoft Ad-Aware SE Personal
http://www.lavasoftusa.com/products/ad-aware_se_personal.php
Remember to update (click on the globe) and then scan. Ad-Aware can be left installed for future use.

Spybot Search & Destroy
http://www.spybot.info/en/
Again, remember to update before scanning. Come with a memory resident part (TeaTimer) which monitors and prevents updates to critical registry entries. It works, but is not user friendly - best left disabled. SpyBot S&D can be left installed for future use.

AVG AntiSpyware Free
http://free.grisoft.com/
Free version has inbuilt 30-day trial of the full version which has a memory resident scanner; after 30 days this will cease working. Defender (see later) does not have this limitation, so after AVG has been used to scan it should be uninstalled so that it will not clash with Defender.

Microsoft Baseline Security Analyser
http://www.microsoft.com/mbsa/
This is not directly a malware tool, but it is useful. It checks whether all relevant Windows and Office updates have been applied, and does some basic checking on passwords, file shares and so on to see if the machine is insecurely configured. Note that you can either let MBSA pick up current data online, or download the Offline Scan File to a USB stick – the latter is recommended.

Windows Defender
http://www.microsoft.com/athome/security/spyware/software/default.mspx
This has a permanent memory resident scanner and so should help prevent repeat cases. Defender is likely the best choice to remain on the machine. Updates are downloaded via Windows Update – as such, the machine has to be on the network to be updated so always install this last, just before connecting to the network.

<u>Other Useful Tools and Techniques</u>

Safe Mode – many of the techniques used to hide malware depend on device drivers or programs run during the startup of Windows. By booting in Safe Mode many of them will not run and this

gives detection software a chance to see the malware. However, only do this **after** checking for rootkits, as the hiding software needs to be running so that the rootkit detectors can see that files are hidden.

SysInternals TCPView
http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx
A lot of malware uses network connections to spread, or to send or receive data. TCPView will show all processes that have network connections open, where to, and on what ports. With a bit of experience this can help determine what malware is running, and what it is doing.

SysInternals Autoruns
http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/Autoruns.mspx
This shows all the programs that are set to run at startup in one window and where in the system they are set to run from.

SysInternals ProcessExplorer
http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/ProcessExplorer.mspx
This is a powerful tool that allows you to determine what files processes hold open, what DLLs are loaded by what, and so on. It's complex but very powerful.

"Advanced Malware Cleaning" lecture by Mark Russinovich (SysInternals/Microsoft)
http://www.microsoft.com/emea/itsshowtime/sessionh.aspx?videoid=359
An hour-long lecture by Mark Russinovich talking about how to detect malware, even if it's not being picked up by anti-malware software, and how to remove it manually. Interesting and useful.

Conclusions

It is likely that some form of spyware will be detected on any machine; the vast majority will be tracking cookies, and those are minor risks to privacy; removing them is not essential. More serious are extra programs (such as add-on toolbars, "download enhancers", etc) that generate extra popups, change home pages, redirect URLs to competitor's sites, and so on. These should be removed. The user should be made aware that some software that they may have downloaded (for example, peer-to-peer filesharing software) may have installed the malware, and removing the malware may stop the software from functioning. It should be emphasised that any software that uses malware in such a fashion is perhaps not to be recommended.

Again, if a keystroke logger or similar is detected the user **must change all passwords and notify their banks, credit card agencies, PayPal, or whatever they may have used**. It should be emphasised that this is **not optional**, and it is very likely that the terms and conditions they have agreed to require this.