Frequently asked for questions and definitions associated with computer and internet security

Malware definitions

Personal computers, Macs, smart phones and tablets, running various operating systems are all vulnerable to a variety of malicious software programmes often known as malware. This is the reason your computer should be protected with the latest software patches, operating system updates and have anti-virus software which is up-to-date and not time expired.

- Viruses
- Macro viruses embedded in software such as Microsoft Word and Excel
- Boot sector viruses
- Scripted viruses – including batch files, windows shell modifications, Java and others
- Keyloggers
- Malware that is designed to steel passwords
- Trojans
- Worms
- Backdoor Trojans
- Spyware and Adware

Computer **viruses** – are types of malicious programmes that can replicate themselves and spread from file to file, computer to computer, over networks, from USB drives and other flash drives such as the one you may have in your digital camera. The longer the virus remains the more damage it can do and it will continue to spread and infect anything connected to it. These types of viruses can infect your email programme and contacts list and send information to contacts in your list and send emails that replicate the virus and send it into the wild.

A **worm** is a malicious programme that replicates itself but does not infect other files. Once installed it finds ways of spreading to other computers. A worm exists as a separate entity while a virus adds code to an existing file.

A **Trojan** (as in Trojan Horse from Greek mythology), is a programme that pretends it's a legitimate piece of software – but when launched will perform a harmful action. They do not spread by themselves but are installed secretly and deliver a malicious payload without the users knowledge. Criminals use many forms of Trojan to perform specific functions such as; backdoor Trojans including Keyloggers, Trojan spies, password stealing Trojans and Trojan proxies – that convert your computer into a spam generating device.

A **key-logger** is a programme that is installed maliciously onto your computer and can record what key strokes you type and can obtain passwords and other confidential data. They can through the use of a backdoor Trojan send this information to a remote site. These may be contained within emails often purporting to be from banks.

What is spyware?

This is a piece of software designed to collect data and send it to a third party without your knowledge or permission, quite often it will incorporate a key-logger, harvest your email addresses and track your internet use. It can also use up processor power and slow your computer down. Sometime it is malicious other times it’s a piece of software incorporated into a legitimate program to gather information about how you use the product.

What is adware?

These programmes, which may be incorporated into software, be stand-alone or be part of ‘toolbars’, will launch adverts such as pop-up banners and redirect you to promotional websites. Often they are downloaded with free software – shareware and it may be installed on your computer without your knowledge. They can be associated with Trojans and browser hijackers. You are susceptible if you do not have the latest software updates and if your internet browser is out of date. Do not allow programmes to install their own custom tool bars – always use custom install if available rather than default install when installing software.

What is a rootkit?

These is malicious code that installs itself stealthily and cannot normally be seen. They are often used to hide Trojan activity. Most people log on to their computers using administrator rights which helps rootkits to install.

What is a ‘drive-by exploit’?

This is when you visit a website that has been infected by malicious code, you just need to visit the site and take no other action in order for your computer to become infected. Cyber-criminals inject their own malicious code into unsuspecting web sites because their servers are not protected sufficiently.

What is a botnet?

This is a network of computers controlled by cyber-criminals using Trojans to infect your computer to set up a network. This will slow your computer down and allow your computer to be used in a wider network. Check your router internet lights are not flashing when you are not using your network.

What is a DoS attack?

This is a denial-of-service attack. These will bring web sites down, hinder or stop their functioning because the server is bombarded with many requests in a short space of time. There are many ways of doing this, and also can be caused by a distributed denial-of-service attack which use multiple networked computers.

What is an exploit?

Defined as ‘using something to one’s own advantage’, is a piece of software code or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unexpected behaviour. Such behaviour often includes trying to take control of a computer system or allowing privileged escalation.

These are the answers to the most popular questions we get. It is just a start, please feel free to ask us any questions.

Camtek CSI operate mainly in London and the South East but also take enquiries and assignments from the UK nationwide and Europe.

Camtek CSI assist firms with business resilience issues relating to cyber-security, business continuity/disaster recovery and digital forensics. We carry out risk assessments on companies to identify any potential threats that they may have which may impact on them to successfully operate during a period of crisis, and develop a business continuity plan for them.

For more information please visit our website at www.camtekcsi.com
or email us at: enquiries@camtekcsi.com

V2 – Sept 2014