Chapter 1 - Malware, viruses and other nasties

Malware

Malware is a trendy marketing name for the category of programs that invade your computer and do all sorts of things you haven't asked them to do – very similar in that respect to teenagers . Normal people probably call them a "bloody virus" – but a virus is a specific type of nastie, others are known as:

- Worms
- Spyware
- Trojans
- Bots.

The Virus

Everyone knows someone who has been the victim of a computer virus. Most stick in your memory because of the painful stories of losing wedding videos or because it thankfully saved you from sitting through hours of dreadful puppies/boyfriend/holiday snaps.

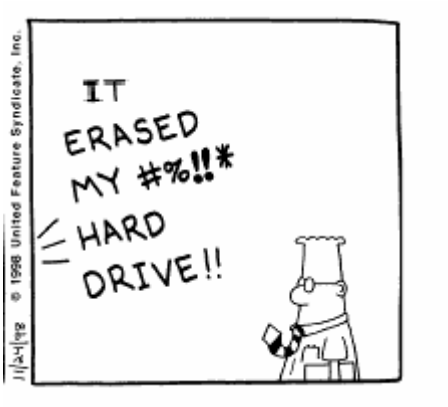
To a dictionary, the computer virus is an unwanted program that is unintentionally installed, or infects, a computer. To a computer user with only one or two computers in his care, a computer virus means nothing but trouble – But for someone responsible for dozens or hundreds, it is like being gripped by a demon from hell . For many years now, both the DTI (Department of Trade and Industry in the United kingdom) security surveys and the FBI security surveys have listed these pesky little programs as the number one horror for most computer managers both in the United Kingdom and in the USA. Mordac is about to feel the pain of his fellow IT managers, who claim that just an average virus outbreak can cost them around £10,000.

Dilbert Gives you the Business - page 76

History

The first computer viruses that emerged were actually quite funny- one was called ***the washing machine***. The program looked like the prompt on an early IBM PC running plain old DOS 3.0 with a flashing cursor. When the unsuspecting user typed a command a message was flashed on the screen "***Water detected in disk drive, spin cycle starting***". The playful program then made a noise remarkably similar to a noisy domestic washing machine – Usually to the delight of the victim, as the sound effect was much more realistic than most noises on TV or in the computer game of the day. The potential for harmful computer mischief had not been realised at this time, so the victim of this harmless prank could be enjoy it without losing sleep over potential permanent harm to his machine.

However by the 1990s computer viruses had become devastatingly destructive. And infection would often destroy your precious PC. These Spawns of Satan were sheer acts of vandalism and often served no conceivable purpose-- nothing more than digital vandalisms. – Always accompanied by cries of anguish.



Editors Note - Code red worm cost£££

Digital Darwinism

In nature the most successful parasitic organisms don't destroy the hosts they rely on. Instead they co-exist in a sort of symbiotically harmony, without causing any or at least not fatal harm. Just like well-known parasites such as the wart on the end of my nose, CatBert (or any other HR director) and the taxman. They drain some of the life out of you and live off you - but they don't kill you (sounds like hell – isn't that worse than death). And so the computer viruses have evolved. They suck the value from your computer but don't wreck it.

And that's how Virus technology has evolved. These days the vast majority of viruses are written or designed for criminal purposes. They are the pickpockets of the digital world and just as distasteful as the average child actor who plays the Artful Dodger. They wander through your PC and *have it away* with anything you leave unattended. Then they rush off to Fagan with all the goodies (thankfully there are no child actors and nobody sings "Gotta pick a pocket or two").

Dilbert gives you the business - Page 90

The new purpose of these nasty little programs, which will be elaborated in this and the following chapter, is:

- Generating spam
- Stealing credit card numbers and passwords
- Dialling premium rate numbers
- Displaying adverts
- Participating DDOS attacks.

Ultimately, although these activities appear fairly benign, they can lead to your identity being stolen and you bank accounts emptied – fairly serious I think!!

Worms

Q: "What's worse than finding a worm in an Apple?"
A: "Finding half a worm in an Apple you've taken a bite outa!!!"

Of course the real answer is finding a worm on computer!!!! Unless you are a computer expert, there is no difference between a worm and a virus. But Dilbert shows us the difference here.

Dilbert gives you the business - Page 91

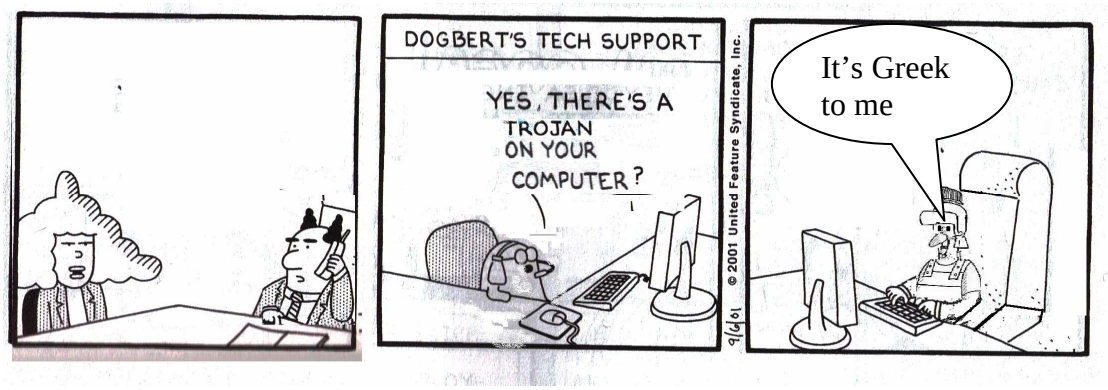
A worm, or to give it the full name a self-propagating worm, is the sort of virus that wriggles and worms its way from one computer to next, just like a wriggly worm in a sack o'spuds.

In 1988, One R Morris, Jr., being educated in Computer Science at Cornell, wrote the first self-replicating, self-propagating *worm.* And because he was a cautious fellow he decided to test it in a controlled environment ---- by injecting it into the whole Internet. And because he knew it would do no harm, he chose to release it from MIT, to disguise the fact that it was written by a Cornell student. It replicated and replicated more like a rabbit than a worm, leaving the fragile UNIX machines of the time in a "Panic" – tech speak for a smoking heap on the floor, or with a clogged cpu.

This effort shortened what could have been a magic career; Morris was convicted under the computer misuse act.

Trojan

A Trojan gets its name from the famous Greek mythological wooden horse – it presented itself as a gift, but was really an armoured troop carrier. It got passed defending guards by pretending to be something it wasn't.



It is just the same when a Trojan infects your computer – it is installed and masquerades as one of your favourite applications. They usually save off the original somewhere safe so that it can be envoke after the Trojan has done its evil work and allow you to get your usual functionality.

Trojan versions of "messengers" (IM or YM or other chat programs), browsers and Skype have all been found. When you run them, they steal passwords or load other nasties.

Sniffers and Keyboard loggers

Sniffers record traffic that goes past your computer on the network. If a sniffer can't eavesdrop on passing traffic, they may divert all traffic to go through your computer so that they can sneak a peak at the data and in doing so making everything slower than a warthog on a go slow. Either way they can inspect it for goodies like passwords, pin numbers or important documents.

Keyboard loggers can be hardware, in which case you may notice an extension plug on your keyboard lead. More commonly they are software, implanted by a Trojan. Both of them record what you type. As you can see from the news report below, they really do exist.

BBC NEWS

WATCH LIVE BBC News 24

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science/Nature
Technology
Entertainment
Also in the news
Video and Audio
Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports
RELATED BBC SITES
SPORT
WEATHER
CBBC NEWSROUND
ON THIS DAY
EDITORS' BLOG

Last Updated: Thursday, 17 March, 2005, 13:39 GMT

E-mail this to a friend Printable version

UK police foil massive bank theft

Police in London say they have foiled one of the biggest attempted bank thefts in Britain.

Yeron Bolondi was arrested for money laundering and deception

The plan was to steal £220m ($423m) from the London offices of the Japanese bank Sumitomo Mitsui.

Computer experts are believed to have tried to transfer the money electronically after hacking into the bank's systems.

A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit.

Unit members worked closely with Israeli police.

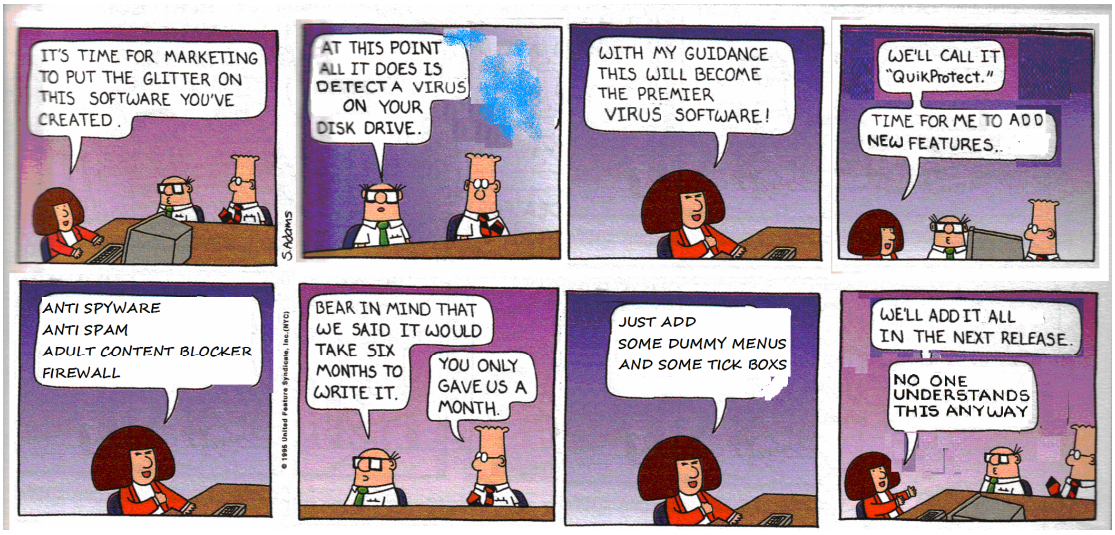
The investigation was started last October after it was discovered that computer hackers had gained access to Sumitomo Mitsui bank's computer system in London.

They managed to infiltrate the system with keylogging software that would have enabled them to track every button pressed on computer keyboards.

HOW DO YOU AVOID GETTING INFECTED

Dilbert has kindly provided some useful tips to avoid infection.

- Install good virus protection software - These days there really is no excuse to have a valuable Win-tel computer and not have anti virus software. Windows has become more secure over the years and Vista has nice security features (i.e. Firewall and anti-spam with more in I.E) but extra protection is required



Even the marketing department, knows enough to explain to Dilbert what is needed and they have got it about right. It should have

- ⇒ Automatic signature update
- ⇒ Memory resident so it is active all the time
- ⇒ Email Scanner
- ⇒ Anti-SPAM
- ⇒ Ant-spyware
- ⇒ Firewall

Cost can not be an excuse anymore – good software is available free of charge. Good examples are:

1. AVG from GRISOFT
2. AKA form ajaja

- Always scan all disks and USB drives before you use them
- Always save programs sent to you to disk and scan it with your virus scanner before run it.
- Never run or install software sent to you from someone you don't know or that appears apropos of nothing.
- **Avoid Limewire**, Bearshare, and **Kazaa** or other P2P clients can be used to download and share MP3 audio files, movies, videos - Some of these are illegally copied, some with malware

What DO YOU do if you Get a virus

The easiest thing to do is look around for a 14year old boy, or any other teenager for two reasons. Firstly, if you do let a teenager use your computer regularly, it is probably him that gave you the infection in the first place. Secondly, they simply get more practice on computers.

If youthful help is not available - DON'T PANIC!!! All is not lost but do not just ignore the problem. .

If you are in a company with an IT department,

- Notify them and follow their advice.
- If they aren't in follow their procedures
- If they don't have any, disconnect your computer from the network.

If you are at home,

- Remove any media from the floppy, CD or DVD drive
- Remove any USB drives
- Shutdown any applications that the system does not absolutely need to function. Consider not saving any documents if you haven't changed much – it could allow it to survive the experience.
- Write down or print off as much information as possible about the virus – this will include popup messages or warnings, or if it arrived by email, look for specific messages in the subject line or body. Save it just in case.
- Run your virus software - **scan the whole system**
- When a virus is found then try the following options – any of them should leave your system usable.
  1. attempt to Repair the virus
  2. attempt to Quaranteen the virus
  3. attempt to Delete the virus

- If no virus is found download the lastest set of signatures. Then **scan the whole system** again.
- If the virus is still not detected, use an online detection agents. These run from the web browser and do not require any installation. These will have the advantage of being bang up-to-date and being from a different signature set. Two good ones are available from either
  1. http://www.kaspersky.com/
  2. http://housecall.trendmicro.com/uk/
- Again, If the virus is still not detected, try using **a bootable scanning disc or a system rescue disk**. These are CDS or USB sticks that contain a basic start-up environment and a scanner. Sometimes a virus hides in a paging dataset on the computer and therefore avoids detection. Follow the instructions that came with it.

If none of these reveals a definite virus alert, you almost certainly have another system problem. However, to be sure to do the following:-

- On another computer, using the information you saved earlier try hard to find out as much as possible – do a search on the internet with your favourite search engine (i.e. Google).
- Lastly, email your virus software vendor for help

Enjoy your computer!!!!

---------- end of chapter ----------