Summer of Viruses.

This has been one of the worst 6-month periods in the history of the Internet with regard to the number and type of viruses that have been infecting machines across the world.

It really started in March and April when the authors of the NetSky and Bagle started a tit-for-tat slagging match in each new variant released. Within the code of each virus, the authors were making defamatory remarks about each other.

We have also seen the more recent variants of the Bagle virus (variant AD) sending copies of the source code of the virus around with itself. This was a worrying development, as it now meant that thousands of people would have the capability of developing a new variant of the virus, with relative ease. This has also made it more difficult for law enforcement agencies to secure convictions, as there is now a copy of the source code for the virus on millions of machines. This means that existence of the source code could not be used alone to secure a conviction.

The trends in the viruses that have been released in the last 12 months include:

- Rapid spread
- Multiple infection methods
- Increasing complexity
- Self-defence mechanisms
- Financial gain for author

Rapid Spread

The speed with which viruses are spreading throughout the world today is frightening. A couple of years ago, it would have taken days for a virus or worm to spread across the globe. Now we are seeing new worms being described as Warhol worms. This title is taken from Andy Warhol predicting that everyone will have 15 minutes of fame, and that is the speed with which one of these worms can spread across the globe. This puts huge pressure on the anti-virus companies to identify a new virus, 24 hours a day-everyday, and publish new signatures. Then, users must download and apply these new signatures to protect themselves. Thus, the time exposed to danger has increased significantly for Internet users before they are protected when a Warhol worm/virus appears.

Multiple Infection Methods

Part of the reason that the worms and viruses mentioned above spread so quickly is that they are using more than one attack vector. Some of the new viruses such as Rbot-GR virus use a combination of methods. These include:

- Microsoft SQL Server vulnerabilities
- Microsoft Operating System vulnerabilities
- Back doors left by other worms and viruses
- Network shares

As can be seen, this is quite complex, and not something lashed together in a few minutes by a bored teenager.

We are also seeing more extensive use of Social Engineering techniques to encourage users to open attachments of emails, or visit web sites that can download malicious code to their machines. More and more people are being taken in by these techniques, particularly as they can appear to come from someone that is known to the recipient as a result of the virus/worm forging the From email address.

Increasing complexity

These new viruses are using Blended Threats to disperse themselves in the wild. More and more of the techniques that are being used are drawing on the actions of viruses in the biological world. They are looking to infect more hosts in a very short period of time, but not actually "kill" the host they are one, just use it to infect others. They can often sit on a host that is infected for some period as a "carrier" waiting for a particular time/message to wake up activate its payload. The fact that many of the authors are now distributing their source code with the virus means that new virus writers have a wealth of proven sample code to take modules from and craft new viruses. One of the latest viruses, Rbot-GR (known as the Peeping Tom virus!), will turn on the WebCam attached to an infected PC without the user knowing, and send a live video stream to the hacker of anything that is happening within view of the WebCam. This has to be one of the ultimate invasions of privacy. This is also a very prolific virus, and spreading rapidly.

Self-Defence Mechanisms

Many of the newer viruses have techniques built-in that are intended to make the anti-virus companies life more difficult. For example, some viruses have an exclude list of email addresses for all the anti-virus companies to delay the discovery of a virus by these companies for as long as possible.

They also have a list of all the processes that are running on a PC when any of the major anti-virus and personal firewall products are installed. If the virus gets on the PC before a signature for that virus has been downloaded, the virus can cripple that anti-virus software so it remains on the infected PC even after the signature has been updated. The firewalls on a PC are also disabled or crippled to ensure that the virus can replicate or allow external connections to a back-door installed on the PC.

Financial gain for author.

This is a more disturbing trend in the virus proliferation in the recent past. To date, virus infection has been annoying, sometimes destructive and a real pain in the backside for systems administrators to remove. Financial impact was measured in downtime and resource utilisation.

Now, there are a more sinister set of financial threats facing the Internet connected population.

These include:

- Ransom
- Theft of banking and other credentials
- Theft of software license codes
- Increased online bills

Ransom

There have been many instances over the last 12 months of online organisations ranging from retailers and gambling sites to pornographic sites that have been threatened with a Denial of Service attack. This is where thousands of machines on the Internet simultaneously send traffic to the target web site, overwhelming it. This can result in users not being able to access it, and with very low levels of loyalty on the Internet, they will go to a competitor. These machines that attack the site are known as "Zombies" and are machines that are infected with a virus, often without the owner's knowledge, and remote-controlled by the hacker for the Denial of Service attack. This attack is stopped when the ransom has been paid. There have been many organisations in the US and the UK attacked in this manner, including www.paddypower.com. The source of these attacks is believed to be Eastern European and Russian criminal gangs. Blocks of these Zombie PCs are traded

among hackers for real financial considerations. These blocks have been estimated to include anything from 1,000 to 100,000 Zombie PCs, and are also known as “Bots”, from the word robot.

Theft of banking and other credentials
Some of the viruses circulating today include keystroke loggers and code that scours a hard disk looking for information that may be considered useful.
A keystroke logger is a piece of software on a PC that is invisible to the user, but records a copy of all keystrokes entered. The software is intelligent and can determine what looks like a credit card number, billing details, expiry dates etc. This information is then saved, and sent to the author of the virus. The same process is used to record the UserID and passwords used for accessing online systems such as bank accounts and share dealing systems. With this information, the virus author could then logon as the real user and fraudulently enter transactions. This could involve stealing sums of money from the accounts of the user.

Increased online bills
In this situation, there are a couple of scenarios. One is where the user is connecting via a dial-up connection. When the user is infected, the dial-up settings are changed, and International premium rate numbers are dialled instead of the local number generating call revenue for the author of the malicious code. The other is where no changes are made to the dial-up settings, or where there is a broadband connection, and the virus/worm are using the bandwidth of the user for replication. Dial-up users will get huge phone bills as the connection to the Internet never drops and broadband users will start to get bills for data transfer above their thresholds. This is very frustrating for the user, as the bills must be paid, and the dispute settled later.

There have been many instances of all of the above incidents in an Irish context over the last 12 months. Protecting oneself against these new threats is an increasingly expensive task, from both a time and financial perspective.

The risk is increasing on a daily basis, and is recognised across the industry. Microsoft is responding to many of these issues with the release of its much-vaulted Windows XP Service Pack 2. While the initiative is to be welcomed, many organisations are adopting a wait and see approach. This is due to a number of issues already identified with the Service Pack, some of which Microsoft have already fixed through a Hot-Fix.

However, if we are vigilant about a few key steps, we can take reasonable steps to protect of computers.

As has been written about in this column before, the three most important things to protect yourself online are:

1. Install anti-virus software from one of the market leaders and keep the signatures up to date. The recognised market leaders include:
    a. Symantec
    b. McAfee
    c. Sophos
    d. Trend
    e. Kaspersky Labs
2. Install a personal firewall. Again there a number of recognised products in this area:
    a. ZoneAlarm
    b. Tiny Personal Firewall

    c. Symantec
    d. McAfee
3. Apply vendor supplied patches from companies such as Microsoft. These companies are moving to regular, monthly releases of patches. Vendors are also attempting to make this easier to apply through features such as Windows Update.

It is imperative that once you have installed anti-virus software and personal firewalls, that they are maintained. Users should get into the discipline of checking each of the three areas mentioned above for updates every time the user connects to the Internet. It should become as routine a task as putting on a seatbelt in the car.

A further note of caution should be sounded around the opening of emails with attachments, even if they are from recognised email addresses. Many of the email attachment type viruses will forge the To and From addresses based on email addresses harvested from the infected PC. This means that a recipient will often recognise the From address, and therefore trust the email. One of the recent variants actually modified the From address surname to be the same as a that of the To address, hoping to deceive the recipient into believing the email is from a family member!

Looking forward, we have seen a number of virus writers releasing “proof of concept” virus code for new platforms. These have included the Symbian mobile phone operating system, and the un-released 64-Bit Windows operating system. It shows that the virus writers are right up there with new technology, and will not be giving the user community or anti-virus companies any respite in the near future.