What drives the hacker of the new millennium?

Over the last 20 years, we have seen a huge, almost exponential, rise in the number of pieces of MalWare (viruses, trojan horses, worms etc) that are being released on the Internet.

It has gotten to the stage that in the last half of 2004, many of the anti-virus companies were recording up to 1,000 new viruses per month. This was in addition to hundreds of new Phishing emails appearing per month.

In the first half of this year, these figures have doubled. These are absolutely staggering statistics

What is driving this phenomenal growth? Is it that there are more spotty teenage geeks around today with less of a social life than years before?

It appears from research carried out by a number of the anti-virus firms over the last year that financial gain is at the root of this growth in MalWare. In 2003 and 2004, the stories that grabbed the headlines from a security perspective were of the viruses and worms that spread like wildfire through the Internet. These pandemics resulted in millions of computers being infected, and the losses through productivity and clean-up costs were astounding. These infections alone were often enough for the authors to earn bragging rights. That seemed to sate their desires for infamy at the time.

The headline viruses and trojan horses of this year have been far more worrying, even though they did not spread with the same voracity as their brethren from earlier years. What has made them particularly worrying is the shift in focus. They are more elaborate and stealthy. They are learning from the natural world around us about the survival, mutation and replication strategies that allow viruses and bacteria challenge the best of medical science.

This shift in focus has resulted in the financial gain of the author of the MalWare component. This reward system is resulting in more and more advanced technology being incorporated in the MalWare. For instance, many pieces of MalWare today will attempt to disable or cripple any security software on the PC such as firewalls, anti-virus software etc.

The income for the authors of these pieces of MalWare is generated from many areas. These include the SPAM originators that are looking for compromised machines on the Internet to purvey their unsolicited stream of ads for everything from Viagra to cheap loans and bodily enhancements.

Income has also been derived from criminal sources that have held online retail sites and online gambling sites to ransom. There was a large number of these incidents in 2004 and 2005. These ransoms were often paid to stop a Denial of Service (DOS) attack that was threatened or taking place. These DOS attacks were initiated using compromised PCs (“zombies”) on the Internet that had MalWare installed that allowed them to be controlled unbeknownst to the user and to direct traffic in a coordinated fashion against the victims site. This volume of traffic could be overwhelming and make it impossible for customers to transact with the site. Thus, the ransom was often paid. Research has indicated that a network of up to 10,000

zombies can earn the controller up to €500 per week on rental agreements! In the United States, 2 teenagers were arrested in 2004 for setting up a DOS attack on an online sports store, jerseyjoe.com. One of them had a competing business, and saw this as a way to cripple his competitors. He rented a “bot-net” of zombies to attack his competitor, and cost the jerseyjoe.com hundreds of thousands of dollars.

While we would like to think of this sort of activity as being murky and underworld, and limited to the “Sopranos” archetypes, the truth is far scarier. This is happening in large multi-nationals and State owned organisations in many areas of the world. In June 2005, 18 people (including many executives) were arrested in Israel as part of an FBI assisted investigation into corporate espionage. The State owned Israeli telecommunications company, Bezeq, was alleged to have been involved in retaining a programmer in England to develop a customised trojan horse that was to be sent to competitors. Once installed, it was to trawl the PCs and networks of the competitor for sensitive corporate information and upload it to an Internet based for Bezeg staff to download. This was a successful attack for the most part because most anti-virus software is based on signatures that have been distributed after a virus has been identified on the Internet. In this case, it was specifically targeted at a small number of companies, and thus the anti-virus companies never identified it as a risk, and no signatures issued. The originator of the email attached Trojan horse used social engineering techniques to get the unwitting recipients to execute the email.

There is a huge increase in the number of specifically crafted MalWare that is targeting a very small specific user community. These attempts are going to be successful as long as the specific code has not been identified by the anti-virus companies and signatures issued.

User awareness is key to this defending against this threat. Users should never access attachments on email received via the Internet. If they have asked someone to send them something specific, they should verify it has been sent to them before attempting to access it.

Some anti-virus companies are adapting to this threat and are trying to assist the beleaguered Information Security Teams in organisations that have to defend against these new threats. This area of development is in the activity-based identification of potentially malicious code rather than prevention based on distributed signatures alone.