



Kaspersky Lab White Paper

The Malware Business

From computer vandalism to crimeware

Until quite recently, viruses and other malicious programs tended to be isolated acts of computer vandalism, anti-social self-expression using hi-tech means. Most viruses confined themselves to infecting other disks or programs. And 'damage' was largely defined in terms of loss of data as a virus erased or [less often] corrupted data stored on affected disks.

Over the course of the last few years this has changed. Today we're faced with 'crimeware', malicious code created for the purpose of making money illegally. The criminal underground has clearly realized the potential for making money from malicious code in a 'wired' world and much of today's threats are written 'to order'.

We've seen a clear shift in tactics from the writers of malicious code. The relative decline in the number of *global* epidemics signals a move away from the use of mass attacks on victims worldwide. From their peak in 2003, the number of *global* epidemics has fallen steadily. During 2005, only two threats resulted in *global* epidemics: Mytob and Sober.y. And Mytob can only be included with reservations: although it was global in its reach, its effects were felt largely by large corporations, not small businesses or home users. Of course, this isn't to say that there aren't any epidemics: it's just that they aren't *global*. Rather, attacks are becoming more targeted.

This is partly because law enforcement agencies across the world have developed far more expertise than ever before in tracking down the perpetrators of e-crime. It's also partly because anti-virus researchers have now had many years practice in dealing with large-scale epidemics. Fast response to new threats, in the form of virus definitions, is just the visible tip of the iceberg here. Anti-virus research teams worldwide have developed 'early warning antennae' giving them early visibility into malicious activity on the Internet. And when an attack occurs, the servers used to gather confidential data harvested from victim machines can be tracked and closed down, mitigating the effects of an attack.

There is a third reason, however, that is intrinsic to the motives of the criminal underground. Since much crimeware is designed to steal confidential data from victim machines, later used to make money illegally, it follows that the harvested data has to be processed and used. Where millions of victim machines are involved, not only does this make detection more likely, it's also a huge logistical operation. So for this reason too, it makes more sense for malicious code authors to focus their attacks.

Typically, this means targeting machines one thousand at a time in small-scale, low-key 'hit and run' operations. Or it may mean tailoring a piece of code for an attack on a single victim, or a small number of victims.

Such attacks are often carried out using Trojans. In the last few years, we have seen a massive rise in Trojans numbers: they have now become the weapon of choice for authors of malicious code. Of course, Trojans come in many different flavours, each purpose-built to carry out a specific function on the victim machine. They include, backdoor Trojans, password stealing Trojans, Trojan-Droppers, Trojan-Downloaders and Trojan-Proxies.

They can be used to harvest confidential information [username, password, PIN, etc.], for computer fraud. Or they can be 'conscripted' into a 'zombie army' to launch a DDoS [Distributed-Denial-of-Service] attack on a victim organization. This could be to extort money: a 'demonstration' DDoS attack offers the victim a 'taster' of what will happen if they don't pay up. Alternatively, victim machines can become proxies for the distribution of spam e-mail. Often, victim machines are combined into networks, using IRC channels or web sites where the author has placed additional functionality. The more complex Trojans combine infected machines into a single P2P [peer-to-peer] network. These so-called 'bot' networks offer an effective way of controlling victim machines.



The trend away from global epidemics and towards low-key, localized attacks has gone hand in hand with a further significant change: a relative decline in the use of mass-mailing to distribute malicious code. Until recently, most epidemics involved worms that hijacked the mail system to distribute themselves proactively, harvesting additional contacts from infected machines as they spread. This was the method used by worms like LoveLetter, Klez,

Tanatos [Bugbear], Sobig, Mimail, Sober and Mydoom to cause global outbreaks. Now, increasing numbers of malicious programs are being deliberately spammed to victim machines. This allows the author(s) to control the distribution of their code, rather than let it spread at will.

For the same reason, the malware 'bundle' dropped onto victim machines now often includes a Trojan Downloader. As the name suggests, these Trojans are designed to download malicious code from specified web sites. They are used not only to control the spread of malicious code, but also to automatically update it across the Internet. They are also used increasingly to install non-viral adware or 'pornware' programs without the knowledge or consent of the user.

The change in motivation that has driven the switch in strategy has also led to an increase in the number of rootkits. The term 'rootkit' originated in the Unix world and it became used to describe to a collection of programs employed by a hacker to evade detection while trying to gain unauthorized access to a computer. Today, the term is also applied to the techniques used by authors of Windows®-based Trojans to conceal their actions. During the last 12 months, increasing numbers of Trojans and 'spyware' programs have incorporated rootkit capabilities.

In a world where malicious code is often written to leak confidential data silently to a third party, rootkits are used as a stealth technique, to hide Trojan activity on a victim machine. This is done either by replacing legitimate system files or libraries, or by installing a kernel module on the system. The aim is to intercept system information and so prevent the user from seeing what's really going on. What's 'going on' may vary, of course. Rootkits are not only used to increase the life expectancy of out-and-out malicious code such as viruses, worms and Trojans. They are being used increasingly by adware programs, quasi-legal applications used to advertise goods or services, to prevent their removal from the system on which they're installed.

Not all malicious attacks take the form of a virus, worm or Trojan. There has been a huge rise in the number of phishing scams during the last 12 months. 'Phishing' is a form of cyber crime based on social engineering techniques [a fancy name for using non-technical methods to trick users into breaching normal security guidelines]. The name is a conscious misspelling of the word 'fishing' and phishing scams involve stealing confidential data from a user's computer and subsequently using the data to steal the user's money.

So what does the future hold? There's little chance that crimeware will go away any time soon. As long as the 'low-key, hit-and-run' methods outlined above prove successful for the writers of malicious code and those who employ them to make money illegally, they will continue to be developed. Some will break new ground, of course, finding new and better ways to achieve the same goal. In particular, crimeware authors are likely to target the growing numbers of wireless devices that are increasingly used by enterprises and users alike.

About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers.