"The volume of malicious code seems to be growing quicker than ever."

Péter Ször
Symantec Security Response

EPOCalypse NOW!

The general public may be wondering whether *Microsoft*'s repeated rewards for the heads of virus writers have had any effect on the global virus-writing landscape in 2004. Others are probably waiting to experience sweet revenge.

Given that friends will not always act like friends – especially when it comes to the temptation of a reward in exchange for information – some might expect virus writing to have been discouraged by the existence of such a bounty. On the other hand, conspiracy theorist might imagine that virus-writing groups encourage worm-writing contests just to collect the rewards – or even attempt to raise the rewards in order to demonstrate that they are the real bad guys, just like in the old Wild West.

So what has happened to the virus-writing landscape in 2004? Well, the number of Win32 virus threats this year grew by a whopping 300% over the same period last year, resulting in almost 4,500 variants this year so far. That said, there were a total of 5,500 Win32 creations in 2003. I am not going to get into the 'good old days' talk, but in 2001 (the year of CodeRed and Nimda) there were 741 new Win32 variants during the entire year. In contrast, there were over 700 new Win32 variants during just the first two weeks of June 2004. Thus, the volume of malicious code seems to be growing quicker than ever, and virus writers do not appear to be afraid of creating more. The question is: would the situation be even worse without *Microsoft*'s reward announcements?

Where does the quick growth come from, you might ask. The answer is in the Gaobot, Randex and Spybot families that have all reached beyond the triple 'A' variations – there are over 1,200 variants in each family.

Recently, the media reported that 'the author' of Gaobot, as well as someone 'associated' with Randex, had been arrested as a result of successful police raids. However, even weeks after these reports the number of new variants belonging to these families showed no decline. In fact, Gaobot is wildly distributed in open source format, resulting in a situation that is worse than the effects of virus construction kits. Indeed, Gaobot variants have more than a dozen exploits, stealth and some primitive polymorphism as well, not to mention that they are packed sometimes even five times if not more. Clearly, Gaobot variations have been developed by a number of people. In addition, the distributed source code suggested that newer editions of Gaobot were offered for sale via *PayPal* payments.

In fact, Gaobot variants introduced the exploitation of the LSASS vulnerability before Sasser appeared. Once Sasser came out using the same exploitation, Gaobot introduced a vampire attack against Sasser by hijacking its propagation routine, forcing it to propagate the Gaobot code. Next, Dabber variants exploited the vulnerability in the 'FTP server' code of Sasser. The worm war is far from over.

So what is the situation in the virus labs? Some of us think it is too difficult to get through a paradigm shift to handle Win32 from now on. Others attempt to measure up to the challenge, but the expectations are so high that they quickly decide to get involved in something different instead.

And what if there were MSIL EPO and metamorphics, 64-bit *Windows* viruses on IA64 or even mobile phone worms that spread via Bluetooth? Where would you hide? And what if this were all for real?

Working in the anti-virus industry has always required dedication, and this is what we all need even more now. Be dedicated to prevent the EPOCalypse!

[See p.4 for Péter Ször and Peter Ferrie's analysis of W64/Rugrat, the first known virus for the 64-bit Windows operating system on the Intel Itanium platform. Next month's Virus Bulletin will contain the Peters' analysis of Cabir, the first virus capable of spreading via mobile phone - Ed]