'The main trend I have observed this year has been the spread of malware activity across several forms of technology and applications.'

Eddy Willems, EICAR

A YEAR OF THREATS ACROSS SEVERAL TECHNOLOGIES

While waiting in the departure hall of a Russian airport on my return from an IT conference I reflected on the year that has nearly passed and noted that it has been interesting in every security aspect.

The main trend I have observed this year has been the spread of malware activity across several forms of technology and applications. It appears that the parties that are orchestrating security attacks are gaining an increasing foothold to build a stronger, more sustainable commercial economy based on carefully crafted security attacks.

Social engineering reached a high level of sophistication this year via the 'Zhelatin-Stormworm' gang, named after the trojan it circulated. This gang was responsible for what started out as the 'Storm worm'.

First spotted in the early part of the year, the spread of the Storm worm started via emails purporting to provide information on some severe storms that had struck parts of Europe at the end of January. Users who fell for the trick were directed to a website containing malicious code aimed at turning *Windows* PCs into spam bots. Over time, emails containing links to the Storm worm took on many different forms, with subjects ranging from supposed missile strikes to reports of genocide and other socially engineered trapdoors. The worm even got into users' blog accounts and created new blog entries with links to the trojan itself. Several million computers were infected worldwide as part of this massive botnet until it was broken down into smaller parts. And still the story continues.

Spammers took a step ahead in their ongoing battle against anti-spam measures by using images to defeat hash filtering and string matching. They also used malware-infected computers (e.g. the Storm worm botnet) to launch spam emails to defeat network/sender reputation filtering. *Excel*, RTF, PDF, RAR and even MP3 spam are just some of the other next-generation techniques spammers have used this year to avoid detection.

The banking industry continued to be a key target for phishing scams and highly sophisticated targeted attacks. As trojans became more technically complex, the malware writers implemented new techniques in their attacks, including filters that keep a closer track of users' online banking activity. Such tracking methods make it easier and more effective for fraudsters to collect account details using a variety of methods. I have seen very advanced dedicated phishing and spyware attacks against several large banks, but also some against smaller regional banks, which demonstrates the keen interest of organized criminals in this approach.

Cybercrime and real-life political unrest came together as a form of 'cyber war' causing general unrest in Estonia earlier in the year. Disputes over the relocation of a Russian Red Army monument not only led to arrests in the real world, but several Estonian government and other public sector and media websites were heavily targeted via Distributed Denial of Service (DDoS) attacks by an extremely active network of hackers. Several key sites were rendered unreachable.

The mobile malware industry has also been very active this year. 'Personalized' SMS spam, financial lottery scams, and several new items of spyware were reported for mobile devices.

It is concerning to see complex mobile trojans and spyware being developed by growing commercial entities, with the aim of making solid profits to support further development of the malicious economy. However, the increase in the volume of malware for mobile devices seems to be slowing (though it could be the calm before a storm). The rise of adware also seems

to have stagnated – of course this does not necessarily indicate that these threats will stop.

The *Mac* seems to be becoming increasingly appealing for malware writers, with several trojans appearing this year, such as DNSChanger which hijacks DNS settings and then redirects the user to malicious websites.

So what is the next step for viruses and information threats? Despite the emergence of new operating systems such as *Windows Vista*, new mobile content and devices like the *iPhone*, cyber criminals are still using tried and tested ways of attacking Internet users.

Furthermore, we have seen a significant return of DDoS attacks and attacks that use browser vulnerabilities to penetrate the system. The most significant thing that distinguishes the present situation from that of several years ago is the fact that email is not being used as the primary vehicle for spreading malware. Instead, instant messaging services and web exploits are two of today's key means of distribution.

Anti-virus and security vendors have improved their technologies considerably and introduced several new ones. Presently, end points or PCs are protected much more effectively than they were several years ago. The average length of time that most new malicious programs survive in the wild has been cut to a number of hours.

Company data is worth a lot of money on the dark side of the web and criminals will go to significant lengths to harvest it. But let's predict what will happen next. Malicious users will attempt to reach beyond the current security solutions – a task that is a shift from 'getting around' anti-virus programs or security devices and implies more action in fields that have not yet been mastered by normal security and anti-virus protection, or areas in which protection is not an option for any number of reasons. This is more than likely where the new front will be in the information war.

We will face more botnet problems, threats to Web 2.0 sites, *Windows Vista* malware, malware targeting online games, along with attacks on IM software and more problematic rootkits. I think that hackers will also turn their attention to virtualization software because companies are increasingly looking into virtualization for their defence.

I was so deep in thought at the airport that I nearly missed my chance to have one last chat with Irishka, a student from Rostov University whom I had met on my trip and who had helped me a lot in communicating with the locals. It occurred to me that we should all make the effort to invest more time in real life than in our virtual one before it's too late. Maybe it's time that malware writers considered this as well.

Prevalence Table – October 2007

Virus	Type	Incidents	Reports
W32/Netsky	Worm	1,985,492	34.61%
W32/Mytob	Worm	1,358,652	23.68%
W32/Bagle	Worm	699,466	12.19%
W32/MyWife	Worm	347,694	6.06%
W32/Virut	File	272,344	4.75%
W32/Zafi	File	151,562	2.64%
W32/Mydoom	Worm	143,486	2.50%
W32/Bagz	Worm	106,980	1.86%
W32/Stration	Worm	78,441	1.37%
W32/VB	Worm	74,208	1.29%
W32/Grum	Worm	59,226	1.03%
W32/Sality	File	55,037	0.96%
W32/Rontokbro	File	41,565	0.72%
W32/Autorun	Worm	31,506	0.55%
W32/IRCbot	Worm	29,357	0.51%
W32/Parite	File	28,197	0.49%
W32/Klez	File	27,433	0.48%
W32/Rjump	Worm	26,636	0.46%
W32/Sdbot	File	22,453	0.39%
W32/Bugbear	Worm	17,579	0.31%
VBS/Small	Worm	17,465	0.30%
W32/Rbot	Worm	14,060	0.25%
W32/Fujacks	File	13,162	0.23%
W32/Sohanad	Worm	10,565	0.18%
W32/Jeefo	File	10,008	0.17%
W32/Looked	File	8,666	0.15%
VBS/Butsur	Script	7,977	0.14%
W32/Tenga	File	7,116	0.12%
W32/Perlovga	Worm	6,133	0.11%
W32/Feebs	Worm	5,820	0.10%
W32/Mabutu	Worm	5,667	0.10%
W32/Fleming	Worm	5,519	0.10%
Others[1]		67,260	1.17%
Total		5,736,732	100%

[1]The Prevalence Table includes a total of 67,260 reports across 140 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.