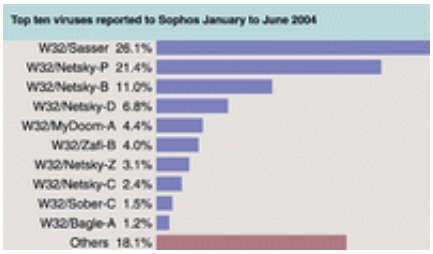
Virus Writing on the Increase

July 28 2004



Sasser Worm the Major Irritant of 2004, but Netsky Worms Dominate Reports *Sophos charts virus activity for first six months of 2004* A report published by Sophos, a world leader in protecting businesses against viruses and spam, **reveals that the number of new viruses being written is increasing**. In total, Sophos has detected and protected against 4,677 new viruses in the first six months of 2004, up 21% on the same period last year.

The Sasser worm accounted for more than a quarter of all viruses reported to Sophos so far this year, even though the worm only first appeared in May. Sasser claimed the top spot of the virus chart, in spite of the raging battle between the widespread Netsky and Bagle worms, which has wreaked havoc across the internet since mid-February. This war produced six of the most damaging viruses of the year so far, with Netsky-P proving to be the most prevalent. The good news for computer users was the May arrest of Sven Jaschan, the German teenager who

confessed to authoring both the Sasser and Netsky worms. For the first six months of 2004, the top ten viruses (as recorded by Sophos's global network of virus research labs) are as follows, with the most frequently occurring virus at number one: 1. W32/Sasser (Sasser worm) 26.1% 2. W32/Netsky-P (Netsky variant) 21.4% 3. W32/Netsky-B (Netsky variant) 11.0% 4. W32/Netsky-D (Netsky variant) 6.8% 5. W32/MyDoom-A (MyDoom worm) 4.4% 6. W32/Zafi-B (Zafi variant) 4.0% 7. W32/Netsky-Z (Netsky variant) 3.1% 8. W32/Netsky-C (Netsky variant) 2.4% 9. W32/Sober-C (Sober variant) 1.5% 10. W32/Bagle-A (Bagle worm) 1.2% Others 18.1% "Following in the footsteps of last year's hard-hitting Blaster worm, Sasser exploited a critical vulnerability in Microsoft's operating system in order to spread. This type of worm has proved to be extremely 'successful,' as Microsoft is finding it difficult to ensure computer users apply patches as soon as the flaws are discovered," said Chris Kraft, senior security analyst at Sophos, Inc. "Sasser may have taken the top spot, but six of the biggest viruses in the last six months were variants of Netsky and Bagle. These caused a continued nuisance for PC users all over the world, as the authors tried to publicly out do each other's viruses." "Reassuringly, virus writers haven't had it all their own way so far in 2004. Increased scrutiny from law enforcement agencies and Microsoft's bounty initiative to encourage people to snitch on virus writers, led to a very high profile arrest in Germany. Sven Jaschan, teenage author of the Sasser worm and member of Skynet, the gang responsible for distributing Netsky, confessed in May. The German virus-writing community has been relatively quite ever since," continued Kraft. MyDoom, the fifth most damaging virus so far this year, highlights the increasing trend of virus writers to attempt to create zombie armies of possessed PCs. This worm, which first appeared in January, opened a backdoor into infected PCs, allowing hackers to launch distributed denial of service attacks on the websites belonging to Microsoft and SCO. The sixth most prevalent virus so far this year, the Zafi-B worm, is a prime example of how virus writers can use their malicious code to distribute political messages. This

worm called for the Hungarian government to house the homeless and introduce the death penalty against criminals. It continues to be extremely successful in infecting computer users, spreading itself by email and peer-to-peer file sharing systems. **First mobile phone virus discovered:** The Cabir worm, first seen in June, was a proof of concept mobile phone virus. The worm that was written by the virus writing gang 29A, proved that it was possible for a virus to spread via Bluetooth to other compatible mobile phones in the vicinity. The worm posed no threat to mobile phone users as the virus was not released in the wild. **More arrests:** The first female to be charged with distributing a virus was arrested in February. Kim Vanvaeck, also known as 'Gigabyte', the suspected author of several viruses including Coconut-A, Sahay-A and Sharp-A, was arrested by Belgian authorities and charged with computer sabotage. If convicted, she faces up to three years in prison and fines of up to 100,000 Euros. In May, Wang Ping-an, a 30-year-old computer engineer was arrested in Taiwan for allegedly writing and distributing a Trojan horse that enabled hackers to steal sensitive information from the island's government computers.

"These arrests have sent a strong message to the virus community that authorities will not turn a blind eye to criminal computer activity. However, the real deterrent will be tough sentencing. It will be interesting to see what punishments will be dished out by the authorities against convicted virus writers and distributors," added Kraft.

Source: Sophos