Second massive email virus attack in one month portends explosive growth in fraud, theft, spam and viruse

by Bend Weekly News Sources

Postini, the global leader in on-demand communications security, compliance and productivity solutions for email, instant messaging and the web, announced Monday that hackers and spammers are raising their onslaught in 2007 as witnessed by two massive, global email-borne virus attacks which took place from December 29 to December 31, 2006 and again from January 19 to January 21, 2007. Each of these attacks was so large that they drove up the level of viruses on the Internet up by a factor of 20 over usual activity.

Both attacks were designed to steal personal information and hijack the recipient's computer to add to ever growing "bot-nets" - massive networks of infected personal computers used to distribute spam and virus attacks. The size and sophistication of these back to back attacks implies that spam and virus levels on the Internet, which are already at all-time highs, will continue to rise as newly hijacked computers are brought into action and begin spewing even more spam and viruses.

This latest attack has become known as the Storm worm because the original email subject line was, "230 dead as storm batters Europe". At the time of the email, there in fact was actually a heavy winter storm occurring in Europe. This is the latest example of the attackers' sophistication and real- time capabilities, launching the attack and timing it to coincide with real news about the storm. The email that contained the virus frequently mutated to show dozens of different fake, sensational but believable headlines designed to tempt the reader into clicking on an attachment and thus infecting their computer. Other subjects included, "Russian missile shot down USA aircraft" and "Saddam Hussein alive!"

The infectious email had a file attachment that contained a trojan horse virus known as Downloader-BAI or AUTH-W32/Downloader. If a person clicks on the attachment, their computer will become infected with the virus which then attempts to send personal information (including email addresses, financial information and credit card information) from that computer back to the hackers who created the virus. They can then use this information for identity theft or sell it to others. The virus also provides a back-door for hackers to take control of the computer and add it to a bot-net to be used in future spam and virus attacks. This attack also illustrated the escalating vicious cycle of spam and viruses being fueled by and creating bot-nets. The virus was distributed by email, which was sent from bot-net zombies that had been infected by previous email-borne viruses and the intent of the virus was to infect even more computers and turn them into larger bot-net zombie network to use in future spam and virus attacks. The email subject, content and virus all mutated many times over the course of the outbreak in an attempt to evade detection. Anti-virus engine providers had to issue several signature updates throughout the outbreak.

As the virus attack began, Postini's PREEMPT email protection service immediately began blocking the worm. Over the three day period, Postini stopped more than 29 million infected messages from reaching the 36,000 businesses Postini provides email security services for. On January 20, 2007 alone, Postini blocked almost 17 million infected email messages, nearly 20 times the average daily virus volume in 2006.

The January 2007 Storm worm follows on the heels of another email-borne virus, the Happy New Year

worm, which attacked the Internet in late December 2006. The Happy New Year worm contained a subject line and an attachment exploiting the expectations of legitimate postcards and greetings from friends and families. The infected attachment contained numerous strains of malicious code (including Tibs, Nuwar, Banwarum, and Glowa) as well as two root kits designed to hide the presence of the malicious code from anti-virus scans. Ultimately, the goal of the Happy New Year worm was to create more zombie computers that could be added to bot-nets and used for additional spamming and other attacks.

Starting on December 28, 2006, Internet virus volumes began to dramatically increase and Postini PREEMPT email protection began blocking infected messages. At the peak of the outbreak on December 30, 2006, Postini blocked 19.5 million messages infected with the Happy New Year worm and its variants.

These two attacks were by far the largest to occur in the past 12 months. "The explosion of bot-nets, millions of infected computers controlled by malicious actors around the world, has changed the balance of power in the world communications security," said Daniel Druker, executive vice president of marketing at Postini. "As Valentines Day approaches, email users should continue to keep their guard up, as there are already new mutations of the Storm worm with love-related subject lines."

Second massive email virus attack in one month portends explosive growth in fraud, theft, spam and viruses by Bend Weekly News Sources