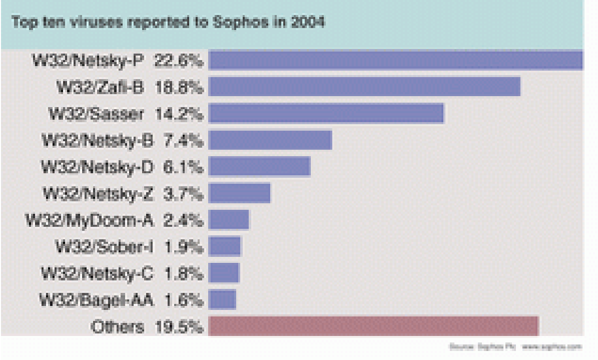
New Spam Tactics and Top Ten Viruses for 2004

December 9 2004



New Viruses Increased By Over 50% Over 2003; North America Accounts for Nearly 48% of All Spam

Sophos, a global leader in anti-virus, anti-spam and policy-based network security, reports today that the top threats affecting users in 2004 were on average more inventive, with nastier repercussions. From the virus front, Netsky-P worm, which was first seen in March, has accounted for almost a quarter of all virus incidents reported, making it the hardest hitting virus of 2004. Meanwhile, North America, particularly the United States, continued to contribute the most to worldwide spam, with nearly 48% of all spam being sent from North American computers during 2004.

"Unfortunately, in 2004, we saw increased collaboration among cybercriminals through organized crime rings and collusion between virus writers and spammers," said Gregg Mastoras, senior security analyst at Sophos Inc. "In 2004, we also saw financial motivation become the driving force behind spam and viruses. In response, legislators and the software community both increased attention on the problem. As the criminals use their ingenuity to get past our safeguards, we as a community must use ours to improve technology, increase user awareness and reduce the profitability of their ventures."

Sophos's worldwide network of virus and spam labs have identified a number of new trends in 2004.

The Virus Landscape

-- Sophos researchers have identified 10,724 new viruses so far in 2004, a 51.8% increase in the number of new viruses, bringing the total viruses in existence to 97,535.
Of these, Netsky variants accounted for 41.6% of all viruses reported to Sophos, capturing an unprecedented five of the top ten slots on this year's Top Ten round-up. The top ten viruses of the year are as follows:

Name Percentage First seen

1. W32/Netsky-P 22.6% MARCH 2004
2. W32/Zafi-B 18.8% JUNE 2004
3. W32/Sasser 14.2% MAY 2004
4. W32/Netsky-B 7.4% FEBRUARY 2004
5. W32/Netsky-D 6.1% MARCH 2004
6. W32/Netsky-Z 3.7% APRIL 2004
7. W32/MyDoom-A 2.4% JANUARY 2004
8. W32/Sober-I 1.9% NOVEMBER 2004
9. W32/Netsky-C 1.8% MAY 2004

10. W32/Bagle-AA	1.6%	APRIL 2004
Others	19.5%	

-- German teenager Sven Jaschan, who wrote both the Netsky and Sasser worms, is responsible for more than 55% of all virus reports in 2004. Jaschan was apprehended and confessed to his involvement in May 2004, but his worms continue to spread. In November 2004, eight months since its original discovery in March, Jaschan's Netsky-P worm was still the world's most widely reported virus.

-- Mobile viruses continue to pose minimal threat to the enterprise, despite an increase in "proof-of-concept" experiments.

2004 Spam World

-- The United States continues to lead the world in spam, accounting for more than two of every five spam emails.
Despite CAN-SPAM legislation and the Operation Web Snare crackdown in August, where the Department of Justice arrested over 150 people in connection with online computer crimes, US computers originated over 42% of all spam, more than three times the amount from the second largest spamming country, South Korea. The top ten spamming countries are as follows:

Country	Percentage
1. United States	42.1%
2. South Korea	13.4%
3. China (& Hong Kong)	8.4%
4. Canada	5.7%
5. Brazil	3.3%
6. Japan	2.6%

7. France 1.4%
8. Spain 1.2%
9. United Kingdom 1.1%
10. Germany 1.0%

Others 19.7%

-- Spammers on average change their domain every two days now, as compared to every week three months ago.
In 2004, spammers became more inventive using new obfuscation techniques, rotating domain names and hiding their domain owner information. In the past 12 months, the speed at which they use new techniques has gone from weeks and days to hours and minutes - soon it will be seconds. This accelerated spam activity now requires constant spam operations with analysis and research at every hour of the day.

-- A number of new spam campaigns made their debut in 2004, widening the content beyond the typical prescription drug and mortgage application emails.
According to the Anti-Phishing Working Group, in October alone, phishing campaigns hijacked more than 44 brands worldwide. New 2004 spam campaigns included:

-- Work from home/prepare to succeed
-- Training courses and well-paid jobs in financial sectors
-- Rolex and other counterfeit products
-- Religious spam that urges users to convert

Changing Universe: Combined Threats

* Cybercriminals are involving innocent users in a wider variety of scams

Unprotected users are at risk at unknowingly abetting crimes through remote control and use of their computers. Over 40% of spam comes from PCs that have been hijacked by viruses. Some worms have used armies of zombie computers to launch distributed denial of service attacks against websites such as SCO, Microsoft, Kazaa, 10 Downing Street, the Pakistani government, RIAA, online betting websites, anti-virus and anti-spam companies. In addition, phishers are recruiting mules in complex money-laundering schemes through legitimate seeming requests.

-- A new generation of phishing was identified, which used Trojans to steal personal information from users visiting legitimate sites.
From phishing emails that warn consumers of phishing to money laundering rings, phishing scams have become both more elaborate and more graphically realistic in 2004. Most worrisome, however, are a new generation of phishing attacks that wait for users to visit real banking websites before surreptitiously monitoring and secretly recording the login process through Trojan horses.

-- Despite an increase in law enforcement, the volume of threats, such as viruses and spam, continues to rise.
2004 heralded a significant increase in arrests in both the virus and spam communities. Well-publicized arrests include Jaschan and the US Department of Justice's "Operation Web Snare" in August, where more than 150 people were either arrested or convicted in connection with online computer crimes.

Unfortunately, this is but a small fraction of the perpetrators in existence, and some criminals, such as Jaschun and 29A virus-writing gang member Marek Strihavka, are being rewarded by security companies who employ them after their arrests.

Worryingly, Sophos also reports a continuing need for a formal framework allowing disgruntled computer users to report virus infections or spam easily. Despite legislation, no government has the resources or the infrastructure to effectively and efficiently process public complaints and warnings.

"In looking back at 2004, users and security professionals might become overwhelmed with the sheer volume and insidiousness of this year's threat analysis," warned Mastoras. "But we all need to remember: with proactive protection through user education, anti-spam and anti-virus technologies, as well as constant vigilance, we can mitigate the impact of these threats. In 2005, organizations will not only need to strengthen their corporate policies to achieve this proactive protection, but also to take advantage of technology to ensure the enforcement of such policies."

Continued Mastoras, "In 2005, we're going to see more mass-mailing worms like Netsky and Bagle. Spammers will keep on spamming. All of these criminals will continue to collude and create inventive attacks. But by working together, the security industry, the government, the business world and the public at large can all find ways to make these attacks less profitable and less impactful, thus lessening the draw for these criminals."

Citation: New Spam Tactics and Top Ten Viruses for 2004 (2004, December 9) retrieved 17 April 2024 from https://phys.org/news/2004-12-spam-tactics-ten-viruses.html