



PersonalBackup^{X4}


[Articles](#)
[News](#)
[Reviews](#)
[Releases](#)
[Downloads](#)
[Contact Us](#)
[White Papers](#)

Sponsors:

Prevent data theft & viruses through network connected USB sticks, PDAs & media players. [Control user access to endpoint connections](#) with GFI EndPointSecurity - Free trial!

Check your website security with a FREE [website security audit](#) by Acunetix. Audit your web applications for [SQL injection](#), [cross site scripting](#) & more with [Acunetix Web Vulnerability Scanner](#)

Phishing Touched An All-Time High In March

Friday, 28 April 2006 11:15 EST

MicroWorld Technologies has been reporting a lofty rise in magnitude and strategy of phishing attacks worldwide in the last two months. Now, an analysis by 'Anti-Phishing Working Group' reveals that phishing attacks reached an all time high in the month of March with more than 18,000 new unique phishing attempts along with 10,000 phishing websites being added on the Internet. The total number attacks will run into millions, as each of these attempts targeted thousands of computer users.

As reported earlier by MicroWorld, this sudden escalation is partly due to the Tax filing season in United States. According to the APWG report, Financial Services amounted to 90% of the total phishing attempts, giving a clear indication on where lies the interest of phishers. ISPs and Retail chains stood at second and third places respectively. Of countries hosting phishing sites, US topped the list with 35%, China with 12% and Korea in the third place with 9% share.

Phishing is the method of Online Identity theft using Smart Social Engineering or malwares like Trojans and Keyloggers, or sometimes combining both these techniques together.

In the former method, phishers send spoof emails pretending to come from legitimate banks and business houses that carry a link to click on. The link opens up a fake website which looks extremely similar to the official website of the mocked firm. In here, you are asked fill in a form with your personal and financial information, which later gets sent to the phisher.

In the latter operation, computers are infected with Trojans, Keyloggers or Rootkits to capture classified information while the user visits authentic banking or other financial websites. This stolen data will be mailed to a remote hacker through IRC channels or mails. Recently, MicroWorld Technologies had detected a new breed of URL Redirecting Trojans which can reroute users to fake, fraudulent websites even when they type in the correct web address in the browser.

"If you want to counter phishing, you need to tackle spamming first," says Govind Rammurthy, CEO, MicroWorld. "Because majority of phishing scams spreads via targeted spamming. We at MicroWorld leverage the most advanced spam checking technology using RBL/DUL methods and a series of futuristic Content Filters. To counter phishing specifically, we've got highly sophisticated algorithms to identify such mails alongside a consistently updated list of phishing websites."

With increased user awareness on traditional phishing, online fraudsters are moving more and more towards Keyloggers, IRC backdoors, and 'URL Redirecting Trojans' to steal financial data. While they are getting better at their cunningness and technology, any online transaction without foolproof security is an invitation to trouble, at the least.

News

[Lawmakers Crack Down on Wi-Fi Crime](#)

Apr 28, 2006, 15:17 EST

[Server-side Sessions Are A Hack](#)

Apr 28, 2006, 15:13 EST

[Nyxem Virus Spreads Once Again](#)

Apr 28, 2006, 11:27 EST

[InfoSecurity Europe - A Haven For Dangerous Viruses](#)

Apr 28, 2006, 11:26 EST

[Phishing Touched An All-Time](#)

[High In March](#)

Apr 28, 2006, 11:15 EST

[A comparison of US and](#)

[European Privacy Practices](#)

Apr 28, 2006, 08:41 EST

[If you're paranoid, Skype might be your best bet](#)

Apr 28, 2006, 08:37 EST



