

IT BackbonesTM

Security News



Give your mouse a heart!

search 

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

DNSChanger Redirects Users To Fake Bank Websites

Published 3rd July 2006

You want to pay up your credit card account immediately, as you just remembered that today is the due date. After getting on to your bank's website by carefully typing in the URL, you put in your account number and password, go to the credit card payment section and perform the transaction. Satisfied with completing a task in time, you move onto other chores, till you find out that the website you visited and punched in confidential financial information was in fact a fake one!

Security experts at MicroWorld Technologies inform that 'DNSChanger.eg' is a high risk potential Trojan that can redirect users to spoofed websites of leading banks, credit card firms and online shops.

DNSChanger.eg works by corrupting the process of translating a domain name to the actual website. When a user types in the web address 'jpmorgan.com', made up of text-strings, it needs to be translated to an IP address like '192.220.34.11', as the Internet understands only numerical info.

Now, the smart Trojan is designed to change the 'NameServer' Registry key value to a fraudulent IP address. So, even if the victim types in the right URL, he will be taken to a scam website that robs him of his identity and finances in broad day light.

"Newer Methods of 'Pharming' are getting truly sophisticated, threatening the very fundamentals on which the world does business online," observes Govind Rammurthy,

CEO, MicroWorld Technologies. “If Phishing requires you to be lured through emails that lead you to imposter websites, this one needs none of that sort. While the unsuspecting user continues an online transaction in good faith, he could be playing directly into the hands of a remote fraudster. It’s like creating a make-believe world to fine perfection and then looting everything that a victim has.”

In yet another mode of Pharming, attackers work by manipulating and corrupting a DNS Server itself. In here they poison the DNS cache, so that regular website requests are answered with fraudulent ones, affecting a large number of computers in a particular geographical area.

“While coordinated efforts are required among Banks, Other Financial Companies, ISPs, Security Firms and governmental authorities to curb these criminal networks, users can do their best by safeguarding their personal computers with up-to-date protection from Viruses and other intruders. As for enterprises, we know that more and more business critical operations are moving to the Internet and protecting office workstations has long become a basic necessity in Information Integrity and Security,” points out Govind Rammurthy.

MicroWorld produces the world’s most advanced AntiVirus and Content Security Solutions, growing at the fastest rate in the world today. ‘eScan’ from MicroWorld offers comprehensive Virus Protection and Content Security, working on its Unique MWL Technology. The other product from MicroWorld, ‘MailScan’, is a Mail Gateway solution that protects corporate mail systems by enforcing an integrated Security Policy across the enterprise.

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.