BitDefender unmasks online payment services spoof

Submitted by: MJO Associates
Monday, 8 June 2009

Stealth malware redirects browsers towards phony websites

BitDefender researchers have found that scammers posing as online payment services continue to be one of the top ten most spoofed identities in the world of spam and phishing, according to BitDefender's latest E-Threats Landscape Report.

The latest phishing campaign targets e-banking and e-payment users by deploying several malicious components. The initial approach is an unsolicited message advertising a product claiming to offer the ultimate 'open source Antivirus solution', and inviting readers to visit a web page where they can download the product.

However, upon clicking the link, the victim does not receive the promised security suite, but a fake executable – setup.exe – which is, in effect, a self-extracting archive. Its purpose is to replace the content of C:\WINDOWS\System32\drivers\etc and to alter the Web browser's behavior, by automatically loading maliciously crafted pages for phishing purposes of PayPal, Abbey and Halifax.

Each time the victim types the address belonging to one of these financial institutions, he or she will be redirected automatically towards the fake pages. Here, the log-in credentials (user name, password, security code) and other sensitive data (first and last name, complete home and e-mail address, credit card number, expiration date, Card Verification Code, and even PIN) are harvested by using PHP scripts. All other menu options available on each page redirect the user towards the appropriate sections of the genuine Web site.

According to BitDefender, the bogus Web pages load from domains registered in China and Korea.

"The current economic turmoil inevitably led to the proliferation of e-crime phenomena," said Vlad Vâlceanu, Head of BitDefender Antispam Research. "The latest trends BitDefender observed reveal several alarming aspects: first, since the beginning of this year, the scams and phishing schemes have followed an ascendant curve. Second, the complexity and aggressiveness of raids and attacks have dramatically increased. Finally, the number of victims followed the same growing pattern. Along with paying close attention to the e-mails they receive, it is important for computer users to have a reliable security solution installed onto their systems in order to prevent future attacks."

BitDefender's E-Threats Landscape Report provides an overview of the security threats landscape over the last six months and takes a look at what lies ahead in 2009.

To stay up-to-date on news from BitDefender and the latest e-threats, sign-up for BitDefender's RSS feeds

About BitDefender®

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified security software. Since its inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe - giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide. More information about BitDefender and its products are available at the company’s security solutions press room. Additionally, BitDefender’s www.malwarecity.com provides background and the latest updates on security threats helping users stay informed in the everyday battle against malware.

For more information see www.bitdefender.co.uk

# # #

Contact details:

Mike Ottewell
MJO PR for BitDefender UK
Tel: 01782 664 886
E-mail: mottewell@bitdefender.co.uk

Nick Billington
BitDefender Country Manager
(UK and Ireland)
Tel:08451305096
E-mail: nbillington@bitdefender.co.uk
Fax:- 0845 130 5069