



Home


[About us](#) | [Mobile/PDA](#) | [News Alerts](#) | [Disclaimer](#) | [Contact](#)

## Major Retailers Experience 161% Increase in Attempted Hacker Attacks, According to SecureWorks

Posted : Thu, 04 Dec 2008 18:24:16 GMT

Author : SecureWorks

Category : [Press Release](#)

News Alerts by Email [click here](#) )

[Create your own RSS](#)

News | [Home](#)

### [1 Hour Ready PCI 6.6](#)

Easy solution with dotDefender PCI 6.6 Compliance - 30 Days Trial

[www.applicure.com/PCI\\_Compliance](#)

### [All 3 Credit Scores Free](#)

Get Your Free 3-in-1 Credit Report And All 3 Credit Scores Instantly!

[www.CreditReporting.com](#)

### [Fraud & Risk Consulting](#)

Customized fraud solutions designed specifically to reduce your losses.

[www.analyticsinmotion.net](#)

### Online Shoppers and Retailers Advised to Take Protective Steps this Holiday Season and Beyond

ATLANTA, Dec. 4 /PRNewswire/ -- SecureWorks(R), a leading Security as a Service provider, reports they have seen a 161% increase in the number of attempted hacker attacks they are blocking for their retail clients. Attempted attacks increased from an average of 56,000 per client per month in the first six months of the year to 133,000 per client per month for the last five months. The attack statistics represent the attack activity for 36 major retail corporations located across the country.

SecureWorks' security researchers attribute the overall increase to a rise in attempted authentication attacks, SQL Injection attacks and network scans.

"We saw a large increase in hackers looking for open ports, as well as those trying to identify the applications and other services our retail clients were running," said Wayne Haber, director of architecture for SecureWorks. "An increase in network scans is often a red flag because many times it is followed by attacks specifically targeted at the organization's services," said Haber. "Attempted network scans against our retail clients increased 61% in 2008 going from an average of 56,000 per client per month in the first six months of the year to 90,000 per client per month in the last five months of the year," continued Haber. The number of attempted authentication attacks -- attacks used to compromise user names and passwords -- increased steadily throughout the year, jumping from an average of 6,000 per client per month in the first six months of the year to an average of 34,000 per client per month in the last five months. The numbers continued to increase through the most recent month, November, where authentication attacks spiked to 137,000 per client per month. "It is not surprising that the attempts to steal customer credentials greatly increased just before the holiday shopping season. The November authentication attacks also followed a significant increase in network scanning in October where we blocked 202,000 network scans per client," said Haber.

"One of the methods used to bypass authentication are brute force attacks -- where hackers systematically try large numbers of username and/password combinations in order to gain access to the retail organizations," said Don Jackson, director of Threat Intelligence for SecureWorks. "Hackers know that if they can successfully steal customer usernames and passwords, they can get access to retail accounts to make fraudulent online purchases and redirect those purchases to mailing addresses of their choice," continued Jackson.

Attempted SQL injection attacks, a technique that exploits security vulnerabilities in Web applications by inserting malicious SQL code in Web requests, increased significantly in May for our retailers, going from an average of 20 per client per month to 237 per client per month. It then hit a peak in July with 17,000 attempted SQL Injection attacks per retail client and since November has dropped off to normal levels, averaging 18 per client per month.

"The abnormally high attack levels in July, August and September are a result of the rash of SQL Injection attacks we saw this year from a Chinese SQL injection tool and the Asprox trojan," said Jackson. <http://www.secureworks.com/research/threats/danmecasprox/>

"In July, August and September, hackers used the Chinese SQL Injection tool and the Asprox trojan to launch thousands of SQL Injection attacks so as to build up their botnets," said Jackson. "With these attacks, they sought out websites that utilized active server pages linked to a Microsoft SQL Server backend and unfortunately a lot of retailers use this platform, thus

Ads by Google

### [ID Theft Recovery](#)

Get your identity back now Stop being a victim

[www.RepairMyCreditNow.com](#)

### [Credit Repair Services](#)

Credit Repair Resource Increase your credit score

[www.creditfixservices.com](#)

### [Get ID Watchdog®](#)

Find, Stop, Fix It. Guaranteed To Protect Your Personal Info. Try Now

[www.IDWatchdog.com/Free\\_Trial](#)

### [Identity Theft Manchester](#)

Be Sure You Have Access to Legal Aid if You Fall Victim to ID Theft.

[www.PrepaidLegal.com](#)

### [\\$0 - Free Credit Report](#)

View your 2009 Credit Report today! And get All 3 Scores as of 1/6/09

[FreeCreditReportingInSeconds.co](#)

Choose Theme



Search



Web [www.earthtimes.org](#)

You can



Current News

News Category

[Business](#)  
[Entertainment](#)  
[Environment](#)  
[General](#)  
[Health](#)  
[Sports](#)  
[Technology](#)  
[World](#)

Add to Google Toolbar

[Breaking News](#)  
[Press Releases](#)

they became a big target. Of course, this boded well for the hackers because if they could infect high trafficked sites then their chances of infecting large numbers of computers and turning them into bots would be much greater. The bots were then used to send phishing e-mails and launch additional SQL Injection attacks. For retailers, the danger of a SQL Injection attack is that if it is successful then the hacker can potentially gain administrator access to the affected server, thus opening up the entire customer database to the hacker, complete with the customers' account information which could include credit card data, bank account information, name, address, etc. Even worse, under some circumstances, once the hacker has successfully infiltrated the database server they can use it as a jumping off point to access the rest of the company's network," continued Jackson.

"With the holiday season upon us and shoppers flocking to the Internet to make gift purchases from the convenience of their computers, retail organizations and online shoppers should be aware of the threats and should employ protective measures," said Haber.

#### Security Tips for Online Retailers

Retail organizations should make sure their Web presence is secured against cyber attacks by employing a defense in depth strategy including:

-- Keeping all servers and workstations fully patched to protect against attacks targeted at the latest security vulnerabilities, especially Web application attacks such as SQL injection and cross site scripting.

-- Employing a default deny policy on firewalls at their network perimeters. This policy involves blocking all network traffic except traffic that is explicitly allowed.

-- Employing effective security practices on services requiring authentication, including password aging, password complexity, authentication delay and automatic lockout on repeated failed login attempts.

-- Employing intrusion prevention at the network perimeter to block attacks on key services accessible from the Internet including Web servers and mail servers, while allowing legitimate traffic to pass.

-- Monitoring servers and security devices 24x7x365 for security issues and requiring preventative actions to be taken on security threats in real time.

-- Regularly testing the organization's security posture via vulnerability scans and penetration tests.

Online consumers also need to take precautions, not only during the holiday season but whenever they are making online purchases. "E-commerce always increases around this time of the year, and with an increase in e-commerce comes an increase in criminal activity," said Jackson.

#### Security Tips for Online Consumers

Jackson recommends the following shopping tips for online consumers:

1. Be wary of holiday gift cards and holiday coupon offers sent via e-mail -- these often have malicious links within the offer which lead to downloads of info-stealing trojans or the hackers try to scam you out of your bank account information.

2. When visiting your favorite online retailer to purchase gifts, be sure to type the actual Web site address of the retailer into your browser. Do not follow links provided by e-mail offers or pop up ads. Many times these are fraudulent sites made to look like the legitimate retail sites.

3. When making online purchases, always use a credit card that limits your fraud liability. Avoid using debit cards to do online purchases when possible so as to limit your personal exposure to any possible fraudulent transactions.

4. When making online purchases, always look at your Web browser for the https (as opposed to http) protocol that precedes a Web address. The "s" let's you know that the Web site is providing a layer of security for transmitting your personal information over the Internet.

5. Be wary of unsolicited e-mails, even from senders that you know, that include links or attachments. Before clicking on links or attachments, ALWAYS verify that the correspondent sent you the e-mail and enclosed link or attachment.

6. Be wary of e-mails notifying you that your banking certificate or token is out of date and to download a new certificate or token. Before taking any action, verify with your financial institution by calling them on a number that is not provided in the email.

7. Online computer users should avoid using weak or default passwords for any online site.

"We traditionally think of financial institutions as being the primary target of hacker attacks, but the fact is cyber-criminals are targeting other industries, like the billion-dollar retail industry, in order to get their hands on valuable personal data so they can reap the rewards from selling or using the data to commit fraud," Haber said.

#### About SecureWorks:

With over 2,000 clients, SecureWorks is one of the market's leading Security as a Service providers. Organizations are protected from external and internal cyber-threats through SecureWorks' On-Demand Security Information and Event Management (SIEM) platform, the SecureWorks Counter Threat Unit (SM) and three fully synchronous Security Operations Centers (SOCs) staffed with SANS GIAC certified analysts working 24x7 to safeguard client systems. SecureWorks has won SC Magazine's "Best Managed Security Service" award for 2006, 2007 & 2008 and has been named to the Inc. 500, Inc. 5000 and Deloitte lists of fastest-growing companies.

[www.secureworks.com](http://www.secureworks.com) .

SOURCE SecureWorks



Copyright © 2008 PR Newswire. All rights reserved.

[More...](#)



BradsMoney.com



## I Make \$5,000 a Month From Home

"It really wasn't that hard. Free government programs got me started!"

**READ MY STORY**

Feedback - Ads by Google

**Article : Major Retailers Experience 161% Increase in Attempted Hacker Attacks, According to SecureWorks**

[Print this article](#)

[Share this article](#)

**Stay Updated**

[News gadget on your Google homepage](#)

[Subscribe to a news feed in Google Reader](#)

**Share on**

<a href="#">Del.icio.us</a> 	<a href="#">Digg</a> 	<a href="#">Facebook</a> 	<a href="#">Fark</a> 	<a href="#">Google</a> 	<a href="#">reddit</a> 	<a href="#">Slashdot</a> 	<a href="#">StumbleUpon</a> 
--	---	---	---	---	---	---	--

**Have your Say**

Name

Email

Subject

Your Comment

**Enter Verification code**  
837344

[About us](#) | [News Archives](#) | [Browse old Archive](#) | [Feedback](#) | [Disclaimer](#) | [Mobile/PDA](#) | [News Alerts](#)

The views expressed in the articles are not necessarily those of earthtimes.org and we accept no responsibility for the views or opinions expressed in the articles either direct or indirect.

© 2009 www.earthtimes.org, The Earth Times, All Rights Reserved | [Privacy Policy](#)