



Web Retailing: Virtual Reality
infectionvectors.com
August 2005

Overview

The Internet boom and bust has left web commerce market looking just like the brick and mortar world, dominated by large companies that have been around for a long time and struggling to beat criminals. Two recent reports point to interesting trends online: that well-established companies continue to rule the web retailing world, and the threats against them are growing.

Match Dot Com

Years ago, there were ads in most IT industry magazines extolling the power of the web for doing business. Those that mastered the ecommerce waters, as the tag lines went, would destroy everything we knew about how to do business. The “brick and mortar” shops were in trouble, or so the Internet evangelists thought. As we now know, good business skills are basically the same across any medium, and the web has proven to be just another mechanism (like telephone, catalog, and showroom sales) for moving products. With that come the same basic problems of “real” stores. The virtual world has also proven to be the same magnet for crime that the physical world is, except that with the automated power of the modern web server, that crime can be committed much quicker.

As to the businesses flourishing on the web, Internet Retailer Magazine recently released its ranking of the top 400 web-retailing sites. The top 10 list should look familiar to North American readers:¹

1. Amazon
2. Dell
3. Office Depot
4. Staples
5. HP Direct
6. Sears, Roebuck, & Co.
7. SonyStyle
8. CDW Corp.
9. Newegg.com
10. Best Buy

These retailers all understand the devastating effects of a single breach in security, both in terms of customer confidence and the real money they would lose in the wake of an

event.² The costs of securing an infrastructure are often quite high, and difficult to justify for many CIOs. The precise calculations for deriving the amount that is being spent and how much needs to be spent are likely to be very different from one retailer to the next. Unfortunately for these retailers, the Internet community as a whole could be swayed against spending money on the web by attacks on smaller businesses. If the overall feeling turns against Internet shopping because of the security risks, then no amount of spending will save the online markets. This may be the best solution for some retailers, who are only in the web sales game because their competitors are selling there.

The idea that the Internet will collapse as a medium for legitimate sales has been mentioned before. Dr. Hannu Kari has said for years that 2006 will be the beginning of the end for the web, when it will begin to fold under its own weight of security issues such as malware.³

If such a prediction scares a retailer, how can they proceed?⁴ Changing the “security ethos” of the world is not an easy task. That is especially daunting when one considers that the bulk of the problem lies with the consumer themselves in terms of phishing attacks, spyware, web browser exploits, etc. Many consumers have learned to look for the “padlock” for secure sites, but few consider that there are not many cases (in fact, there hasn’t been any) of credit card data being lifted from the wire and then used in a crime. Data is stolen from hosts, whether they are large databases or single home PCs. Online retailers/credit card companies will need to furnish the same types of authentication mechanisms that banks are moving to already.

Openings

The risks associated with online business of all kinds are mounting. A report from SANS Institute in July of 2005 shows a significant increase in security holes in the second quarter of the year, in a very diverse set of products.⁵

What is the tie-in to online retailing? The broad set of vulnerabilities represents a sizeable leap over the same time period last year (22%). Furthermore, the group includes threats to customer data on many fronts. This is not unique to this vulnerability update, but it gives a good opportunity to see how many places personal data is in jeopardy at any given time:

Storage	Customer Account Data	CA BrightStor ARCServe Backup Veritas Backup
Browsers	Customer Personal Info/ Spyware Issues	Firefox/Internet Explorer
Firewalls	Access Control	Zone Alarm
Clients	Specific Accounts	iTunes RealPlayer

More information on each of these can be found at the SANS Institute site found in the references section below.⁶

Closing the Loop

As has been mentioned in previous infectionvectors.com reports, whether the Internet is a profitable venture for big business is a question that can only be answered by each respective company. Beyond their individual investment in security and efforts to keep their customers with “warm fuzzy feelings” about security in general, publicly participating in groups like the Anti-Phishing Work Group and others will be necessary. Public perception regarding the security of their personal data is much more important to web commerce than the status of a single patch or configuration change request.

There are more reports regarding ecommerce and web security available at infectionvectors.com. See <http://www.infectionvectors.com/> for more details.

References

1. "Internet Retailer's Top 400"
Mark Brohan, Internet Retailer, June 2005.
<http://www.internetretailer.com/article.asp?id=15099>
For the interested, Walmart finished at #12. And although that is a tremendous figure for web-based business, it represented about 1% of their total sales for last year.
2. "Lock It Up"
Lauri Giesen, Internet Retailer, September 2004.
<http://www.internetretailer.com/article.asp?id=12770>
3. "Internet about to collapse, says Finnish scientist"
Ken "Caesar" Fisher, ARS Technica, 18 October 2004.
<http://arstechnica.com/news.ars/post/20041018-4318.html>
4. Additional information about the state of the Internet from a business leaders perspective can be found in:
"How To Save The Internet"
Scott Berinato, CIO Magazine, 15 March 2005.
<http://www.cio.com/archive/031505/security.html>
5. An article concerning the release of the popular SANS Top 20 update:
"Internet security threat rising"
James Brown, Computing, 26 July 2005.
<http://www.vnunet.com/computing/news/2140344/sans-warns-increased-threat>
6. And the report itself:
SANS Institute Top 20 – July 2005
<http://www.sans.org/top20/q2-2005update/>
And the press release for this quarter:
http://www.sans.org/press/q2-2005update_release.php