

State of the Net: Security

In brief...

Over the last year we've heard a lot about identity theft as well as the usual suspects: Viruses, Trojans, keyloggers, spam, phishers and pharmers. 212,101 new malicious code threats were reported to Symantec in the first half of 2007, representing a 185 per cent increase over the second half of 2006. Vendors and analyst firms report that between 70 and 90 per cent of e-mail delivered to major corporations is spam, and my own server statistics show about 70 per cent.

However, the real story is not the numbers but the fact that Internet-related crime is firmly within the domain of professional criminals. While there are still casual 'hackers' out there, the relative ease of committing crime across the Internet, the vast number of potential victims worldwide and the minimal and often ineffective presence of law enforcement have combined to create an environment in which crime can flourish.

Intrusions into individual computer systems have certainly continued but, looking back over the past few years, the trend is very clear: Attacks are increasingly focused against Web-based applications, especially those processing credit card information. Automated intrusion tools also continue to prowl the Internet looking for vulnerable systems. For example, every day I see the same sequence of failed attempts to log into one of my servers using SSH. The only thing that changes is the source IP addresses, suggesting widespread use of the same scanning tool.

Phishing and fraud

Internet fraudsters continue to target specific countries, regions and events. They do so because people have become more aware of phishing and, presumably, response rates to widely-distributed generic phishing e-mails have dropped.

However, by spamming ISPs with customers in specific areas and referring to specific events, they are able to trick

users into providing information that can be leveraged for fraud.

To understand how easy these frauds are, imagine that you receive an e-mail on Friday afternoon offering tickets to Saturday's Sens game. The e-mail is well written, offers a plausible explanation as to why they are offering tickets at a discount rate, invokes an element of urgency (limited number of tickets, selling out fast, etc.) and includes a link to a Web site that looks completely legit. You select your ticket, fill out a form with your name, address, e-mail address, credit card number, expiry date, provide the extra digits on the back of your card (or front, if AMEX) and submit the form. Perhaps it tells you that you will receive e-mail with a link to electronic tickets or the site displays your 'ticket' on the screen. Or, maybe the site returns an error saying that it couldn't process your transaction and invites you to try another credit card.

Of course you won't get a ticket or, if you printed one, it's bogus. The criminal, on the other hand, is set to go shopping online with your credit card. In many cases, the goods will be shipped to unsuspecting third parties who themselves have been tricked into forwarding the goods. How?

Enter, the Internet dating scam.

Internet dating scams

Throughout history, criminals have sought ways to separate people from their money and relationship scams are nothing new. Plenty of people have found out too late that their boyfriend, girlfriend or fiancé wanted nothing more than their money. Unfortunately, the Internet and dating sites have taken these scams to a whole new level because geography is no longer a barrier.

With an Internet connection, a free e-mail account, inexpensive VoIP services, and a bit of creativity, you can look like you live almost anywhere. Add a blog or facebook page and, with a bit of work, you can flesh-out your fake online persona. There are numerous relationship

scams operating on the Internet and many fraud artists take advantage of online dating sites to make contact with their marks. Once the relationship is established, they contrive situations that require — you guessed it! — money.

Some of the best known scammers pose as Russian women seeking foreign men. Some may be in Russia but many are reportedly in Nigeria and other African countries. In these scams, the 'woman' approaches men on online dating sites, often telling them that it is her first time meeting men online. 'She' becomes interested and, weeks to months later, 'she' is asking for money to meet in person. Of course 'she' never shows up but other emergencies such as critically ill parents, accidents and thefts occur — all conveniently requiring money.

Other scams target women and, while some are solely financial in nature, others, like reshipping scams, seek to obtain the victim's involvement in other crimes. For example, a woman may get to know a supposedly Canadian or American man who purports to be working in a foreign country. Instead of money, the man eventually explains that many online vendors won't ship goods to the country he is working in because of fraud. She agrees to receive and forward packages for her new boyfriend — and is surprised when the police show up investigating the goods purchased using stolen credit card information. Similarly, victims may be asked to cash cheques or money orders to help out their new friend. While the cheques turn out to be bogus, the cash the victims send to their new friend isn't, leaving them holding the bag.

Domain tasting and kiting

As anyone who has mistyped a popular URL knows, there are many companies snapping up Internet domains simply to generate traffic to their servers in order to display ads. And, while it may be scummy to register common misspellings of popular domain names, at least they're paying for the domain. Recently the spotlight has come to rest on ►

Feature: *Internet Update I*

much less-ethical practices called ‘domain tasting’ and ‘domain kiting’.

Wikipedia defines domain tasting as, “...the practice of a domain name registrant using the five-day ‘grace period’ at the beginning of the registration of an ICANN-regulated second level domain to test the marketability of the domain. During this period, when a registration must be fully refunded by the domain registry, a cost-benefit analysis is conducted by the registrant on the viability of deriving income from advertisements being placed on the domain’s Web site.”

To add some perspective, according to Bob Parsons, the CEO and founder of GoDaddy, in February, 2007, 55.1 million domain names were registered and, of those, 51.5 million were cancelled and refunded. Then there’s the practice of kiting, which refers to deleting and immediately reregistering the domain to continue using it for free.

Some of these practices have been going on for years and registering countless domains for free and placing ads, such as from Google AdSense, on them has apparently generated significant revenue for these companies. But, in January 2008, domain tasting gained new attention when Network Solutions, one of the world’s largest Internet domain registrars, was accused of the practice, with a twist.

To test out the allegations, I went to the Network Solutions site and searched ‘monitormagazine2008.com’. Their site informed me that the domain was available for registration. I stopped there, not even ‘adding it to my order’. About a minute later, I ran a ‘whois’ on the domain, and — surprise! — Network Solutions had registered the domain almost immediately after I simply searched it. The whois information read, “This Domain is Available — Register it Now!”, along with Network Solution’s URL. And, when I typed: `monitormagazine2008.com/` into my Web browser, I found myself at a Network Solutions Web page that read, “This Site Is Under Construction and

Coming Soon,” and indicated that, “This Domain Is Registered with Network Solutions.”

If I decided I didn’t like Network Solution’s terms or prices and wanted to register the domain with another registrar, I would be told that the domain isn’t available. Presumably if there is no interest within the five day grace period Network Solutions will cancel the registration to avoid paying for it but, since they automatically create DNS records to point it to an ‘under construction’ Web page, it is also possible that they keep statistics on how many hits the domain gets.

On their Web page that addresses the issue, Network Solutions writes, “In response to customer concerns about domain names being registered by someone else just after they have conducted a domain name search, Network Solutions is implementing a new security measure to protect our customers.” I can’t imagine how someone could find out that I was searching a domain at Network Solutions and register it, unless there is a serious security problem at Network Solutions or there was spyware installed on my PC. But I can imagine why Network Solutions might want to register the domain quickly so that I have to buy it from them or wait five days and risk somebody else snapping it up.

Consumers under attack

If you go online to shop or obtain information, you may not know it but you are under attack.

For years we’ve heard that you can’t trust everything you read and, when it comes to the Internet, it’s more like ‘you shouldn’t believe *most* of what you read’. For example, many people use Wikipedia, which does have a lot of good information and links to useful references. But, when Virgil Griffith released *WikiScanner*, a program that analyses changes made to Wikipedia and correlates them to source IP addresses, it became clear that many organizations were removing unfavourable informa-

tion about themselves. (It also revealed that their employees are dumb enough to do this from IP addresses attributable to their organization.)

News and product reviews have become worse. I find product reviews helpful, especially when choosing between several products that more-or-less do the same thing. Unfortunately, there is clear evidence that many reviews and testimonials are completely bogus. For example, I recently cut and pasted part of one review into Google and found the exact same positive product review on more than a dozen online stores. While it might make sense that someone who bought a product and liked it would post a review on the site they purchased the product from and maybe even one or two other favourite sites, it’s obviously a sales tactic — and a lazy one at that.

To confirm my suspicions, I googled and found Web sites advertising for article, review and testimonial writers. For example, one read, “I need four positive testimonials written for my membership Web site. Write two to five paragraphs, each giving positive feedback about your experience with our site — to be posted in testimonials section of Web site. Each testimonial should be unique from the other. Please keep in mind you will not be given access to the membership. Looking forward to your rave review!”

Others included requests for photographs, including those of the author and his or her children — in this case, for a site offering supposed fertility information.

What I also found alarming was the number of ads for people to write medical information. Next time you’re looking for medical information online, carefully consider what Web site you are on. The article you are reading *may* be written by a physician — or someone who was paid \$5. to write it. ■

Eric Jacksch is an Ottawa-based information security consultant, writer and photographer. He can be reached via: E-mail: ejacksch@monitor.ca

Feature: *Internet Update II* by Eric Jacksch

State of the Net: What's new?

The future is now!

Every year brings new services and applications to the Internet and 2007 was no exception.

Facebook has become unimaginably huge, instant messaging has continued to explode and it's almost impossible to surf the Web without coming across a video served up from YouTube.

But what's next?

Hottest new product of the year?

Sling Media, founded in 2004, released its third-generation product in September of last year and, from all accounts, it's going to be huge.

I must admit that I wasn't paying much attention to Sling until a buddy who winters in Florida told me about a cool phenomenon at his local Fox TV station. Unfortunately, it wasn't one of the few hundred channels I get via satellite, so I couldn't just tune in.

Then he mentioned the Slingbox he picked up off Woot, gave me the string and password I needed to access it and, to make a long story short, I was soon sitting at home in Ottawa watching off-air TV from Florida.

There are several Slingbox models. Some have tuners, some can control a cable box or satellite receiver and one that does it all. But the basic concept is the same for all: Access to audio and video via the Internet (or your local network).

The product seems to compensate automatically for varying bandwidth and



Slingbox Solo: *Includes composite video, s-video and HD inputs as well as stereo audio. Setup is a breeze. ... 'I was expecting a reasonable but less-than-TV quality. However, ... the quality was excellent.'*

it includes the use of a free location service that allows users with dynamic IP addresses to automatically find and locate their Slingbox while on the road.

Unlike other products I've seen, Slingbox does not require a local computer — it connects directly to your router/switch via Ethernet and can, therefore, be accessed both remotely and from your local network.

Windows and Mac clients are available and, while I'm not sure I'd want to try it without an unlimited data plan, a PDA/cell phone version is available, as well.

The test-drive

I contacted Sling Media and they were kind enough to loan me a Slingbox Solo to test out. The Solo includes composite video, s-video and HD inputs as well as stereo audio. Setup was a breeze. I literally had it up and running in less than five minutes, connected to and controlling a satellite receiver.

Having tried it first across the Internet, I was expecting a reasonable but less-than-TV quality. However, the product clearly detected that it was running across a local network, boosted the data rate to just over 3,000 Kbps (as opposed to the

207272

LAPTOPS

GREATEST SELECTION

SALES and REPAIRS

from \$99

all UPDATED INVENTORY at
www.OttawaLaptops.com
613-829-8087, 2527 Baseline



350 to 800 Kbps I was used to viewing across the Internet) and the quality was excellent.

In addition to being able to watch my satellite TV from anywhere with a high-speed connection (and I'm looking forward to trying that out next time I'm stuck in a hotel), the resizable client is perfect for watching the news in a corner of your monitor. It also handled being dragged between monitors on a dual-monitor PC gracefully, which is more than can be said for many other video applications.

The history

But what started this in the first place?

Like many media sites, Fox 13 Tampa Bay (WTVT) has a live Web-cam in the studio.

It also added a 'Live Studio Cam Chat' on the page that allows users to chat with each other. What's unique is that the anchors log in from notebooks on the anchor desk during the newscast.

So... Here I was, watching TV off-air via the Internet and chatting with anchors John Wilson and Kelly Ring during the evening news. Of course, they would stop reading and typing when it was their turn to look into the camera and, if you were just watching them on TV, you'd never know.

Chris Boex, Senior Web Producer at Fox 13 Tampa Bay explained that they started the Web-cam as part of a transparency initiative. They intended the chat to be for viewers but Wilson decided to log in during the newscast and it simply grew from there. As a result, they have a small core group of regulars during the evening news, with visitors dropping in from literally all over.

My bet is that this is just the tip of the iceberg and I'll be keeping an eye on Fox 13 Tampa Bay to see what Chris comes up with next. ■

Eric Jacksch is an Ottawa-based information security consultant, writer and photographer. He can be reached via: E-mail: ejacksch@monitor.ca

INTERNET SERVICES

**Annual and
Monthly
Unlimited
Plans**

**Free Email
Free Web Space
Free Virus Filter
Free Spam Filter
24 Hour Sales &
Technical Support**

One Time \$10.00 Account Activation Fee applies to all accounts.
Last Month on Deposit applies to monthly services.

DOMAIN NAMES

- **\$15.00 per year .ca Domain Name Registration**
- **\$100.00 per year Domain Name Hosting includes Web, DNS, Mail**
(One Time \$50.00 Activation Fee)
- **Unlimited Virtual Email accounts with Hosting**
- **Mondenet Technical Services Inc. is a CIRA Certified Registrar**
- **\$85.00 / month Server Co-Location**
(One Time \$200.00 Activation Fee)

TELEPHONE SERVICES

**\$25.00* per month Residential Telephone Services
in Quebec and Ontario. Features available.**

We do inside telephone wiring and jacks.

Monthly rate applies in *most* areas. Please check with our Sales Manager for pricing in your area and help with other phone questions.
911 is standard with our phone service.

**Come visit us at our new location
2285 St. Laurent Blvd., Suite D5**

www.mondenet.ca bob@pobox.mondenet.ca

526-0155