

Tuesday, May 27, 2008

## Are you being watched at work?

Excellent [PC Mag article](#) on Employee Monitoring. Personally I've worked to monitor employee's email, web and Instant messaging as part of my Forensic and Investigations work while working at several of my jobs, so this is a very real concern. See an Excerpt below:

[...]

It's possible that someone has been reading your e-mails, listening to your phone calls, and tracking your Internet use. No, it's not a foreign spy. It's not even your exâ€”it's your employer. And she doesn't even need to tell you she's doing it.

Employers can legally monitor their workers however they want. They can log and review all computer activity as long as they own the machines. The most popular method of keeping tabs on employees is to track Internet use: A whopping 66 percent of companies monitor employee Internet activity, according to a survey released in February by the American Management Association and the ePolicy Institute. What are they looking for? Frequent visits to sexually explicit sites, game sites, and social-networking sites like [Facebook](#) on company time. Almost a third of those who said they monitor their employees have fired someone for inappropriate Web surfing.

[...]

Posted by Lawrence Pingree in Security at 10:45

Sunday, May 25, 2008

## Automated Forex Trading

Off topic, if any of you are interested in automated investments with as little as \$1000 and profit potential of 7% per month you should check out <http://trademaster.zulutrade.com> it offers automated signal services that are free to the trader. All you do is fund your account, pick a trade signal provider from their performance page and sit back and watch the trades execute. (Of course past performance is not indicative of future performance based on market conditions). If you want to learn more about the Forex and Trading, I suggest clicking on the "School" section at <http://www.babypips.com>

e

Posted by Lawrence Pingree in Security at 11:16

Friday, May 16. 2008

## **Paypal XSS, ethics and the law**

Today a man by the name of Harry Sintonen announced that the paypal payment processing site was exploitable by an XSS attack. In the back of my mind I was thinking how fitting his last name was "Sin"tonen. Apparently he demonstrated this to a journalist and during the "online interview" executed an XSS attack that exploited the vulnerability on the paypal website and used an alert pop-up to show the issue. The article is [here](#)

Now, I understand that its important that these types of companies (such as paypal) need to be looking for this type of bug and I'm certain that Paypal has an army of security personnel that are slated to ensure this sort of thing does not happen. What I'd like to take issue with is the fact that the public has no business executing attacks against websites on the internet and the fact that they are doing so is not only unethical but criminal. Its great that people know how to execute attacks, XSS and SQL injections are not that tough, especially given that paros proxy, web scarab and tamperdata for firefox etc allow you to easily push these to websites using your desktop. But just cause you CAN do something doesn't mean that you should and I feel publicizing this sort of this is just downright irresponsible and if its not illegal in finland, it darned well should be!

Posted by Lawrence Pingree in Security at 15:05

Thursday, May 15, 2008

### **Interesting Security Poll of users on the street**

One thing that all of us forget is some of the basics in security. The following article is a survey RSA had performed in 2007 which asked security related questions about user activities. I found the numbers somewhat amusing and validated my own thinking in terms of where efforts needed to be focused. I thought it was interesting that Government employee's seem to be more on top of security (at least physical) than the corporate world.

Read the article [here](#)

Posted by Lawrence Pingree in Security at 09:54

Tuesday, May 13. 2008

## Intrusion Tolerance replacing intrusion detection?

Is "Intrusion Tolerance" replacing "Intrusion Detection and Prevention"? I doubt it.

Reading an [article on DarkReading](#) today about a new project started by "Aron Sood" that he's dubbed "Intrusion Tolerance". Basically the approach is simple, his idea was to take a "clean" copy of a web, dns or other server and rotate it into 1st position on the DMZ on a regular interval roughly 1 minute. He commented that this would lower the window of opportunity for a system to become breached and limit the data loss exposure.

In my humble opinion, Intrusion Detection and Prevention is not going away any time soon and here's why:

1. Web Servers don't normally store sensitive data these days (Application Databases do).
2. This does nothing to prevent zero day application exploit via the exposed web server.
3. To infect a system only takes moments and therefore any exposure for even more than 1 second can lead to a breach. Case in point - Place an unpatched Windows XP system on the internet for about 10 minutes and whammo, you'll have several worms infecting your machine in that timeframe.

Summary:

Although this technology helps aid us security folks in our endeavour, its by no means a panacea. Honestly, this is only one small component that can be added to your overall security strategy and call it a day. Don't drop your Firewall, Intrusion Detection and Prevention and other compliance technologies on account of someone saying they will "limit" your data loss. I'll be keeping an eye on this technology as it has some promise if combined with the right complementary technologies. We'll see.

Read the Article [here](#)

Read about SCIT - Self Cleansing Intrusion Tolerance [here](#)

Posted by Lawrence Pingree in Security at 12:13

Thursday, May 8. 2008

## Identity theft and Renault website

Posted by Lawrence Pingree in Security at 11:30

Friday, May 2. 2008

**Social Security and Personal information on Riverside Court**

Posted by Lawrence Pingree in Security at 13:29