ADCORP COMPUTERS
System Consultants
Small Business Specialists

Reception Address
108 Brisbane Street
Postal Address
P.O. Box 1885
TAMWORTH NSW 2340

Email: support@adcorpcomputers.com.au
Website: www.adcorpcomputers.com.au
ABN: 81 111 486 509
Telephone: 1300 736 343
Facsimile: 02 6761 6177

A White Paper on 'The Trojan Pandemic'
Written By Paul Adnett
Dated 12/12/2011
The third in a series on informative documents

Why is My Computer So Slow?

The Phantom Web Site

Many clients ask me this common question. Another statement I often hear when talking to clients about the risk of Trojan infection is, *"They can get in to my system, there's nothing to steal except the overdraft."*

So why is your computer so slow? The answer is, it's likely been compromised (a nice way to say hacked). And the hacker is using your computer to help infect or attack others. 60 minutes recently reported (20/11/11) that it is estimated that around 80% of business systems in the US have been hacked in the past 12 months. Some send out 1000's of emails with infected links or images to both their friends and strangers. And many use your computer to host a phantom web site. I must admit I was intrigued by the idea of phantom websites sitting on your computer without you knowing. So thought I would do some research to see how this is done.

It seems any web site, even high security web sites like banks and big corporate can easily be stolen. When you open your browser and type the www address of a web site. You are sending out a request to get everything at that address. And when I say get, I mean copy to your machine. A complete copy of even the most sensitive site is downloaded to your computer and stored in your temporary Internet folder. So what's to stop you uploading that to another place on the web? Nothing!

So I simply view a site, it downloads to my computer, and then I up load these files to someone else's. Then all I need to do is send people an Email with a link that says it's going to the original site but instead goes to my copy of the original. They click the link and get to a site that is identical to the original, in every detail.

Why not upload the infected file back to the original web site? Because, this needs a password, and the password to up load to let's say a bank's web host is, hopefully, going to be tough to crack. But I can create a fake Bank Web site that looks and feels and works exactly like the real one. Within seconds, without needing a password. Only now when clients login to my fake bank site I get a copy of their password.

So what's this got to do with your slow computer?
Well I have to put that fake bank site somewhere. Why not on your computer. Maybe the reason your computer is so slow, is that 1000 bank users are trying to use their Internet banking. Or should I say your Internet banking. I don't have to steal your money. I can use your computer to steal everyone else's.

The benefit of this business plan to the hacker is, its you that is breaking the law. You're the one the federal police will visit. And it doesn't use up that much of your Internet band width so the only tell tale sign is your computer seems slow.

And by the way, while the hacker is setting you up as a web host, he will also have scanned every file on your machine for your confidential banking details. He most likely will upload a key tracker as well which records your keystrokes when you visit your own bank. It's even possible that you will receive an Email with a link, that when you click on it, you will be sent to your own machine. **How ironic is that!**

Because the Trojan uses your computer to help attack and compromise others. The Hacker typically has many computers under his control. So, to prevent him from being tracked and caught. He may rotate the hosting to another computer tomorrow. Suddenly, your computer comes good and you put the slow day down to just a bad day. Only to find that next week your on the slow again. Pretty smart when you think of it.

This month the FBI shut down one of these hackers. Based in Eastern Europe. They had 4 million computers under their control and were reportedly obtaining $280,000 per day. By harvesting other peoples banking details and stealing a small amount of money from each.

This information is provided to help you understand what we in the IT industry have been saying for years. **Nothing is safe on the Internet.** Trust no one. And put in to practice all those security practices we've been telling you for years. You know what they are.

Of course, the bad guys won't rest on the laurels, after all, there's millions at stake. They will be working on the next great way to get your money. But hopefully you won't be paying for their extravagant lifestyles for now at least.

Of course, I am always happy to help clean out your Trojans and spend hours of chargeable time repairing the damage. So feel free to call at any time. But unfortunately I can not recover any lost funds from your bank accounts. I would however, prefer to spend my time more pro-actively, by preventing the issue if I can, or at least reducing the risk of infection.

Please contact me if you wish to implement the recommendations contained in this report in your system or have any questions about anything discussed in this document, I am always happy to discuss your situation in person.

Yours faithfully
ADCORP COMPUTERS

Paul M. Adnett
Senior Consultant
MICROSOFT CERTIFIED PROFESSIONAL

28 years in Tamworth and still providing service.