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 first in a series on informative documents

The Trojan Pandemic

Often when a serious Virus or Trojan infection sweeps across the globe many clients ask me, how could this have happened? We had the best Virus Protection in place; we scanned reasonably regularly for spyware. How does this type of thing get past all the firewalls and protection we have? And most importantly how can we stop this from happening again?

First of all, let me start by explaining what a Trojan is and does. A Trojan is not the same as a Virus or Worm. They are not usually destructive (in the sense of randomly deleting files). They typically do not spread on their own from one machine to another. A Trojan has one purpose. To allow your machine to be used by someone else, remotely. They open up back door access, either through your protection, or by bypassing it from the inside. Selectively disabling any security that may find or remove it. They actually want your computer to keep going, some even tune it up, to make it more useful to them.

In this recent wave, the Trojans, typically disable Windows and Antivirus updates, and then wait for a vulnerability to be found that allows access. Microsoft in an attempt to make its systems more secure started releasing Windows Updates and security patches over 10 years ago with the release of Windows XP. And they are still patching the holes in it today. But when they provide a patch, they also have to provide the details of what the patch fixes. This actually has the negative effect of telling the Botnet Herders or Trojan Masters (the bad guys) where the vulnerabilities are and how to use them.

And if you think XP is full of holes, Windows Vista, & Windows 7 haven't had 10 years of patches.

A Trojan typically has one of two goals. The Russian type (coming mainly from Eastern Europe and Russia) is looking to steal your money. The Chinese type (obviously coming from China or Asia) is trying to steal your secrets. Both have similar effects on your system. They infect your servers and terminals, open up back door accesses to your system exploiting any of the many security holes in Windows, and then wait.

The Russian type waits for you to access secured sites like Internet banking and then records your passwords. Then attempts to steal your money or use your credit cards. The Chinese type scans your hard drives for any research or technology that they can steal and use. Then both types use your computer to try and infect others.

Once the Trojan's payload is released, it takes control of the machine. **Everything that the machine does or doesn't do, is up to the Trojan**. This is why once infected your Virus protection and spyware scanners find it difficult to remove them. The Trojan is in control of the scan. A Trojan can recruit other remote computers and combine them in to a Botnet Herd, or Zombie Network. This group of computers combine in to one, super computer. Some herds have millions of computers. Last week the FBI captured and destroyed one herd with over 4 million computers across 200 countries.

Whole businesses have been setup in foreign countries, with the sole goal of stealing your money or secrets or both. If I steal $1 from a million people I not only get $1 million dollars, but I can also do this every week. Because each person only looses a small amount of money, **it often goes unnoticed**, and if discovered it may be too difficult to chase and recover, after all it's only $1. A great business plan. At the same time as stealing the owner's money, the herder uses malicious means to spread and gather more computers in to the herd, usually by Email from the infected computer. Having control of millions of computers gives them access to plenty of Email addresses to use to disseminate more malicious Emails, trying to catch more unsuspecting victims.

How do they do it?
About 3 years ago I attended a security seminar sponsored by Microsoft on this issue. They showed us how easy it was, and how the Trojans work. Microsoft had, at the time, recently released a scanning program that reported infection rates back to Microsoft. They were shocked to find that 86% of all computers scanned were infected. This was in late 2008, before Facebook or Youtube became really popular.

I was shown in a short demonstration how to use common code found on the web to inject an object with a Trojan. And how to start to accumulate other peoples computers in to a herd that I could control without their permission. I didn't believe how easy it was, I suspected that Microsoft were blowing it out of proportion so that they could come out and sell some new firewall product. But the sales pitch didn't come out (which is most unusual for Microsoft). Everyone asked the question "How do we Stop This?" The answer was, "We'll get back to you." 3 years later we are still waiting.

After the seminar I came back, still not believing it could be that easy. I decided to test this out for myself. I'm not a hacker by any standard, but I understood the basic principles. Within 15 minutes Matt & I were able to create and infect a number of computers. It scared me when, ***I suddenly realised that I had gained access to a Medical facility on the coast and could access private medical records***. It was that easy.

What you have to realise is the exponential growth of this type of infection. The 6 degrees of separation is true. If I send out only a small batch of Emails. And only **two** get read, within an hour I could have 10 computers under my control. Imagine if I sent out an email batch every hour for a week, that's 1,000's of computers under my control in the first week and millions 2-3 weeks later. That's if only 2 in 1000 emails gets opened.

Ok, you might say, "I won't open Emails from people I don't know". Problem, these emails are coming from people you do know. How many times have you received a duplicate email from the same person. I bet you assumed that they had hit the send button twice! Sure there are still plenty of those old scam emails still going around. Some have been circulating for over 10 years now.

But the worst threat now, is not only from an infected Email. Most Anti-Virus programs will protect you from those these days.

However, ask yourself this. Have you ever done any of the following?;

- Bid or even just looked at an item on Ebay or other auction site.
- Watched a Video on Youtube.
- Used Facebook at all.
- Read a joke Email from a friend.
- Downloaded Music from the Internet (without paying for it).
- Clicked a link in an Email sent from a friend, supplier or good customer.
- Viewed any image on Google Images.
- Or have any of your staff EVER done any of these on your business computer?

Because in all of these interactions, you are opening up and downloading something from someone else's computer. If they are one of the 86% of computers infected, then, **so now are you.**

60 Minutes on Sunday (20/11/11) announced that an estimated 80% of all businesses in the US had been hacked in the last 12 months. Here's a part of that interview transcript;

MICHAEL USHER: KT McFarland is a former Security Adviser to three US Presidents.
MICHAEL USHER: If you look up and down this street in Manhattan, Wall Street's just around the corner. All the major banks, the stockbroking houses – have they been hacked already?
KT: They have all been hacked. Eighty percent of all American companies have already been hacked. And yet, most American companies spend more on their coffee budget than they do on protecting their IT systems.
MICHAEL USHER: Isn't that ridiculous…

Even Facebook, Microsoft and Google themselves have all recently been hacked. How can this happen?

The weak link in the system is as always the human factor. As a test for a client in 2008, I sent an email to all his staff which said in the subject line "Warning this email contains a virus". And to his surprise a number of staff opened it. Curiosity kills.

Look at it this way. If I can upload a file to a site like Youtube, or Ebay, or Facebook which everyone can. And if I can inject a Trojan in a picture or video in less than 5 minutes. So can someone else. Put these two facts together and any picture, any video, any program or any Email could be infected or lead to infection. Then add the incentive of millions of dollars. What do you think will be the result.

Up until now most Virus protection has been focused on infected Emails. As this is the traditional method used to access many people in a very short space of time. But now rather than send out an infected Email. I just send out an Email with a link to an infected picture or video hosted on a well known web site. My Email is not infected and so your Virus Protection allows it through. And because this Email comes from someone you know who Emails you regularly you are likely to open it. And when you click on the link you are virtually opening up your browser and navigating to the site. How can your protection programs be expected to differentiate between this action and any other form of web browsing.

Unfortunately with the growth of social networking sites like Facebook and other popular sites like Youtube or Ebay, staff are accessing these sites without being tricked by a well worded

Email. They are browsing the content on these sites, and none of this content has been provided by the owners of the site, but rather by a 100,000 individual users. 86% of who are infected.

So what can you do to combat this threat in your business system?
The answer might upset some of your staff!
And Ebay, Facebook and Youtube.
There is no known Virus Protection, or Scanner currently available today that can provide real protection from this threat. Although all will claim to (to sell their product). The size of this issue has brought in to question the whole validity and usefulness of the Internet itself.

The only thing I can say is this. **None of my clients have been infected during the course of pursuing work tasks** or from a work related action. Considering Facebook, Youtube and Ebay are usually not used for work related purposes, and are the most common source of infection at the moment. I can only recommend that work computers be restricted to work. To reduce the risk of infection you need to actively work on reducing the surface area of attack. The surface area of your system is a term that relates to the number of exposed entry points in your system. These are directly in proportion to;

1. The number of Desktops in your system connected to the Internet.
2. The number of Emails you receive.
3. The number of Web sites you visit.

Reducing the Number of Desktops in Your System.
I'm not talking about reducing the number of Terminals, obviously you don't have terminals just lying around doing nothing. But you can actively reduce the number of Intelligent Terminals by replacing Desktops with Thin Clients. This also can save you up to $800 per year, per terminal. Not all business can utilise Thin Client technology but many can. Explore this option when replacing or upgrading your terminals.

Reducing the Number of Emails You Receive.
This involves ensuring your system automatically filters out as many junk Emails and spam Emails as possible. Unsubscribe from all those newsletters that you never read anyway. Delete catchall email accounts. Instruct staff on the correct use of Email and restrict it to business purposes only.

And Finally the No1 way to reduce the risk!

Reducing the Number of Web Sites Visited.

This is the No. 1, best way to reduce your risk. And is the cheapest to implement. But also the most controversial. It involves creating or revising your company policy on personal use of the Internet. And actively blocking popular un-necessary sites that are not related to work tasks. This also has an amazing ability of restoring the productivity of your staff.

Sites I would recommend you consider blocking at a minimum (unless they have some work purpose) are;

Facebook	MSN	Ebay	Youtube
Bebo	Flickr	Myspace	Twitter
Wikipedia	Skype		

All of these sites allow anyone to upload images or videos that can be easily infected.

Our statistics show that each Trojan infection cost a minimum of about $720 to clean in labour costs. And possibly much more if the client hasn't followed our previous security advice. And much, much more if data is lost, or the Trojan is successful.
Do not ignore this warning! Act Now.

Most ADSL modems have a built-in firewall. These are usually set to allow **all** outward bound traffic and block only inward bound (with exceptions for Email and Web Browsing). But most can restrict outward traffic too. Blocking sites can usually be done by simply adding the addresses of the sites to be blocked, to the firewalls outbound blocked list.
Simple, Effective and Cheap.

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.