ua technology services

Keeping Safe on the Internet

Is it possible?

Cosma Papouis

Table of Contents

Introduction 2

Overview 2

But surely only PC's get attacked 2

Why and how do they attack? 3

What do the bad guys want? 3

Types of attack 3

How do they do it? 4

What can I do about it? 1

The 10 Internet Security Rules 1

SPAM 3

What Causes it? 3

What can the user do about it? 3

Conclusion 4

How do you stop spam and other attacks? 4

Introduction

Overview

The internet was conceived of as a method of sharing information between academics. Initially they were just happy that it worked and so security was never a consideration.

Over the years more and more of us have started to use the internet on a daily basis to conduct business. The bad guys have seen this and have moved in to do some business of their own.

This report looks at ways of minimising your risk. It is, by no means, comprehensive, and was written as the basis for a short talk given to the SEEN Networking group in Blackheath in November 2013.

But surely only PC's get attacked

It is often believed by Apple Mac users that they are not vulnerable to viruses and other attacks. This has never been completely true, but has appeared to be so as most attacks have been against PC's.

The reason for this is that due to a number of factors:

1. Malware writers tend to write attacks for the machine they have, which has tended to be a PC.
2. Microsoft has tended to be disliked and Apple users tend to be Apple fans.
3. Historically Microsoft operating systems (Win XP, Win 200) were easier to attack.
4. If you are going to write an attack you want to aim at the target with the largest chance of finding a vulnerable machine. PC's have been (and still are) the most used platform.
5. Microsoft tends to be used by far more companies.
6. Attackers aim for the lowest hanging fruit.

Nowadays things have changed:

1. Apple has increased its market share to approx. 20%, which makes it a much more interesting target.
2. Microsoft has improved its protection, making Windows 7 and Windows 8 harder to attack.
3. Most attacks are aimed at Adobe PDF's and Java exploits, which are available on most platforms (one attack can be effective on more machines).

While Apple Macs are still less likely to be attacked, they are not immune and Apple users can still suffer from SPAM and identity theft as they are not operating system specific attacks. This is borne out by the fact that companies (Apple included) are starting to offer various forms of Anti-Virus/Malware

Why and how do they attack?

What do the bad guys want?

Over the Years he game has changed

1. Initially it was fun. How much damage can I do?
2. Then they used to want to used your computer as part of a bot net
3. Then they wanted Creditcard and bank details

Now…

Extortion! – CryptoLocker is a new ransomware program that was released around the beginning of September 2013. This ransomware will encrypt all your documents and pictures plus some other files using a mixture of RSA & AES encryption. When it has finished encrypting your files, it will display a CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 in order to decrypt the files. This screen will also display a timer stating that you have 96 hours, or 4 days, to pay the ransom or it will delete your encryption key and you will not have any way to decrypt your files. This ransom must be paid using MoneyPak vouchers or Bitcoins. Once you send the payment and it is verified, the program will decrypt the files that it encrypted.

Law enforcement is taking the servers down. Alas that means that, if your key is on one of these servers, you have lost your data!

There are things you can do. But they are not guaranteed to work for very long (if at all). Download and run Cryptoprevent http://www.foolishit.com/download/cryptoprevent/

Types of attack

There are three basic types of attack

1. Random – Throw stuff out and see what comes back – emails, websites….
2. Phfishing – Semi random – Clients of xxxxx companys (Paypal etc)
3. Targeted – They want some specific info…

How do they do it?

They weaponise innocent things…

1. Emails (SPAM) that look like they are coming from a given website (Paypal, bank etc…)
2. Documents and pdfs – Use scripting vulnerabilities, often from a known contact
3. Documents and pdf's that are actually exe's – Baddoc.pdf.exe
4. CD's, Data keys left on the floor – You find it, think "Ooo! That is interesting", take it to work, put it in your pc and BANG!

They often need you to click on something to make it happen, but there have been cases of images that use vulnerabilities that infect when you look at a website.

The problem is that you may not know that you are infected. They could be watching for months.

What can I do about it?

The 10 Internet Security Rules

1. **Keep computer viruses and spyware out** – There are hundreds of new computer viruses created every month. Some are relatively harmless, but most are designed to delete files, compromise your confidential information, or damage your operating system. Both PCs and Macs are vulnerable, and the latest generation of viruses can even spread without human intervention. The best way to stop them is installing antivirus software and update it regularly. Same applies to spyware.
2. **Block hackers and intruders with a firewall** – There are hackers lurking in every corner of the web. Some are teenagers with minor technical skill, some are pranksters, and some are just vandals. But they all have a lot of help; there are at least 30,000 web sites dedicated to helping hackers. Hackers can delete personal information, and even use your personal computer to send SPAM. A firewall separates your computer from the Internet and decides what gets in or out. Firewalls are the most effective defence against other intruders.
3. **Be careful when opening email and attachments** – Most of us get dozens, if not hundreds, of unsolicited emails. Some, even the ones from friends or co-workers, can carry a virus, worm, or Trojan horse that can wreck a computer. The rule of thumb is: If you get an email from someone you don't recognize, or if the subject line or the purpose seems questionable -- don't open it. Instead, delete the email and any attachments.
4. **Be selective about what you download and from which sites** – Part of the fun of surfing the Internet is downloading games, applications, and other kinds of software, but they're often the source of viruses and other malware. Be selective about what you download.
5. **Choose a password that's better than "password", it has to be complex** – Passwords are one of your first lines of defence. Make it difficult for hackers to guess. An ideal password is a combination of letters and numbers and contains a minimum of eight characters. You should avoid easily guessed combinations like addresses and birth dates. And it's a good idea to change your passwords periodically.
6. **Don't let your web browser remember your personal information, turn such options off and use a tool such as Lastpass**– Your web browser may offer to remember frequently used passwords and credit card numbers. Although it may make online shopping or banking a little easier, you should decline the offer. Having the potentially costly data stored on your computer means it could be accessible to hackers.

7. **Protect your kids online, watch them and what they do on the Internet** – On the Internet, your children may be exposed to objectionable material. Or they may be tricked by others into directly giving personal information. You can monitor your kids' online activities by putting the computer in a family room instead of the bedroom. Install security software that blocks access to objectionable material and potentially dangerous services. (K9).
8. **Keep your private life private, you don't know people out there – Nothing says you have to use your real DOB or Mothers maiden name** – Even though you may develop friendships online with people, be aware that the people you're communicating with might not be who you think they are. Never give out personal information (such as phone numbers or where your kids go to school) via online forums like instant messages, email, and web forms.
9. **Backup your computer, regularly, both data and OS configuration- Thanks to Cryprolocker it is doubly important that this is kept off site, not mapped as a drive and has versioning** – One way you can keep your valuable information safe is to keep a backup of it. These days, high-capacity disk drives and CDs can quickly copy your valuable files onto a removable disk or CD-ROM that you can store in a different location. 3-2-1
10. **Update your security software regularly, upgrade to new versions** – OK, you've installed some security software. But hackers are a productive group, constantly creating and spreading new viruses. In order to stop the latest attacks you'll need to schedule regular updates for your computer's security, preferably daily.

SPAM

What Causes it?

Spam can be caused by a number of different things.

1, The user may have given his/her email address to a website (possibly a legitimate site) that has then either used it or has sold it to a spammer (or it may have escaped).

2, The user has received a piece of SPAM and clicked on the "take me of this list" link. Typically this just confirms that the address they used is valid (never click on ANY link in SPAM)

3, Much SPAM is sent out in a scatter gun approach. Let's assume they have your domain name (xxxxxxxxx.com). The spammers will start at a@xxxxxxxxx.com then b@xxxxxxxxx.com then c@xxxxxxxxx.com.... etc. They are slightly more intelligent than that in that they use "dictionary's" (i.e. they will use names, common words etc. rather than a, b, c as in my example, but the principal is the same). The Email address' you use (first names) are all available in standard dictionary's.

4, Someone else has given his/her address to a "dodgy" website.

What can the user do about it?

In reality not a lot.

1, When the emails come in s/he can mark them as SPAM in the mail client. This would be most effective if s/he logged in to through webmail and did it there as this would block spam at the server.

2, You as a company could pay for a service such as Mimecast or Postini that do much better virus scanning than standard, built in, software does. This would also provide you with a searchable mail archive.

3, You as a company could change your email policy so that you use a more complicated name format E.G. .@xxxxxxxxx.com or some variant. You could, of course, use a random email name such as jdnjsbdj@xxxxxxxxx.com, but even that will not stop spam and rapidly becomes a management nightmare.

Conclusion

How do you stop spam and other attacks?

As I said above, you can't. But there are things you can do to minimise your exposure.

1. NEVER click on links in email. If you need to use a link manually type the address in to your browser. Ensure it really is http://www.paypal.com NOT http://www.paypa1.com
2. NEVER open attachments you were not expecting, even if they are from known sources (confirm with the sender that they really sent it)
3. Never click on the "Please Remove me" links. This just confirms your email address
4. Look out for the Green “Extended validation” banner in the address bar. Https://, padlock
5. Turn on the Junk mail filter in your email client and mark items as spam. (this takes time to have an effect, but does slow things down eventually)
6. Use a mail filter such as "MailWasher"
7. Pay for a professional Spam cleaning service. These are very good, but do require users to log in occasionally to confirm if there have been any false positives.
8. Never give your email address to websites (or anyone for that matter) unless you are sure they are legitimate. I maintain "sacrificial" email addresses for places where I am not totally confident of the status, but need to give an email address to access a service. This is an OK service http://10minutemail.com/10MinuteMail/index.html
9. If you are attacked… Just wait. It will subside eventually as long as you do nothing to confirm that you have received it.
10. In extreme cases change your email address.

I hope this helps.

SPAM is a global issue and no one has a solution (I wish I did, because I would be sending this email from my yacht in Caribbean :))