Educating our way to Security

The Internet Security landscape is littered with the metaphorical bodies of those who routinely fall for the popular ruses perpetrated by malware authors, phishing scams and 419'ers. Much of the badware out there is reliant on convincing the target (or mark) to undertake some type of action, education is therefore a very important weapon in the fight against 'cybercrime'.

Introduction

In the early days of the internet, users exchanged files on Bulletin Boards and, inevitably, a few users started to write malware. Much of the early malware was not intended to do any harm, but simply to prove that something could be done. Most required the mark to open a file, and so effort had to be expended in order to make the file appear legitimate.

The early macro viruses often resided within a Word or Excel Document and would then exploit a weakness in Microsoft Outlook and e-mail itself to the users entire addressbook.

Much as those using the internet in the early days learnt the importance of not opening unexpected attachments, users today need to be fully educated as to the best way to minimise the likelihood of becoming a victim.

419 Scams

419 Scams are a form of Advance-Fee Fraud in which the target receives an e-mail offering them them a lot of money. In order to obtain this money, the mark is often asked to provide bank details, home address and even telephone number.

The text used in 419 emails varies considerably, but the basic theme is that someone somewhere needs a relatively small amount of money so that they can release a much larger amount. Marks who respond to 419 scams often find that their first 'contribution' is no longer enough, and will be convinced into sending more money.

Other marks do not experience this, and instead find that their bank accounts have been emptied by persons unknown. Any credit facilities in their name are also often heavily used.

But is it possible to educate users to recognise and avoid 419 scams? The signs suggest that this is already happening to some extent, the frequency of 419 scams does seem to be reducing somewhat.

It may be that more direct forms of Phishing are more effective, or that users are beginning to recognise the hallmarks of a 419 scam.

However, we should not be complacent. Badware and spam go through popularity trends just like any other product, and the popularity of the Internet almost guarantees an influx of inexperienced new marks for criminals to target.

It's generally quite easy to spot a 419 Scam, it'll adhere to most of the following

1. It was unsolicited and from someone you don't know
2. It offers you the chance to obtain something of great value
3. It requests either a 'small' amount or details about you
4. Often written in broken English
5. Often very emotive.

Those behind the scams will often invest quite some effort in confusing those marks who aren't entirely convinced. If the mark requests a photo of the author as 'proof' that they are who they claim, they will often be provided with one. If the criminal feels the need to add an additional feel of authenticity, the mark will often be asked to speak to the authors lawyer or accountant.

The techniques used to convince a mark are evolving regularly, and the act becomes all the more convincing once the mark has responded to that initial e-mail. It's therefore essential that we try to educate users in how to spot the hallmarks of a 419. Once they have responded to that initial contact, it'll be far harder for them to escape the conviction that they may just be about to become rich!

Phishing

Phishing is another confidence trick, it involves contacting a mark and asking them to provide sensitive details. First contact could be in the form of an e-mail claiming to be from the mark's bank (or more precisely, a bank in the hope that the mark uses it) or it could purport to be from less sensitive a service.

The e-mail will usually request that the mark re-enter their username and password, perhaps as the result of a security breach or some other external factor. The user is then presented with a link to a website masquerading as the bank/service mentioned in the e-mail.

Many users will then enter their username and password in the belief that they are on the correct website. These credentials are then firmly in the hands of the criminals behind the Phishing run, and may be misused for a wide variety of reasons.

Most phishing scams attempt to obtain Internet Banking credentials, but others have attempted to gain access to other services. Some may attempt to gain access to e-mail accounts for the purposes of sending spam, whilst others may covet Social Networking credentials for the same reason.

A recent study suggests that most victims of Phishing respond within an hour of receiving the e-mail. It's therefore very important that we teach users how to identify a potential phishing scam, as our more traditional defences are not usually live within the first hour of a new phishing run.

Identification

A Phishing e-mail will

- Claim to be from a site/service/bank that you use (whether you do or not)
- Explain that you need to re-enter your credentials for some reason
- May threaten with account suspension if you do not comply
- Provide a link so you can log in
- May or may not contain broken English
- May or may not contain corporate logo's
- Probably won't contain your name

The biggest giveaway should always be the provision of a link. Most services now realise how dangerous this practice can be and will instead direct users to type the URL into their address bar. This makes it very difficult for phishers to hide the address of their phishing site without employing further tactics (such as DNS poisoning).

We touched upon the subject of traditional defences against phishing; there are some in place on some computers. It's therefore quite important that we look at the options available to ensure maximum coverage of these tools. However, they should only be employed as second line defence!

Blacklists

Many modern browsers incorporate a phishing blacklists. When the user visits a website, the browser will warn the user if the site is a known phishing site.

Although effective, the problem with blacklists is that someone has to maintain and update them. Phishing sites do not get reported until the phishing e-mails have been received, and so many users may already have entered their details.

One Time Passwords

One time authentication tokens are becoming popular, especially in the banking industry. It involves carrying a separate device that uses an algorithm to generate a password authenticating the user. This password is only valid once (and for a short time), so if it is entered into a phishing website is of little to no value to the phisher.

However, by entering any details into a phishing site, the user may have identified themselves as a viable mark for future attempts.

Although their popularity is increasing, One Time Tokens are far from widespread yet. Many users refuse to accept them as they view it as an over complication of the login process.

Spam Filters

Although not designed specifically to combat phishing, Spam filters are very adept at catching Phishing e-mails. They are not, and probably never will be, so effective that it's safe for users to trust any mail that gets through. Spam Filters can be very useful in helping reduce the influx of unsolicited mail, but users need to employ other defences as well.

Malware

Malware is any software which performs a malicious action without the users consent. Few users can be unaware of the potential dangers posed by viruses, worms and trojans, but many still do not understand the basic steps required to help partially mitigate this risk.

There's an unfortunate culture of belief that simply installing anti-virus software is sufficient to protect the user from infection. The reality is very, very different. With the rapid development of malware seen today, it often takes some time for anti-virus firms to develop and deploy detection signatures. This means that early victims of the malware will be infected despite having an up-to-date AV installation.

Even with user education, it's no longer possible to avoid 100% of infections;

Previously, malware often came from less reputable areas of the internet including pornographic sites. Even then, the user was often required to agree to the installation of software (advertising the malware as a video codec was a particularly successful tactic).

Today, malware has evolved and the user may be given no sign whatsoever that they are about to be infected. Malware authors have learned to exploit weaknesses in technologies such as Adobe's Flash and so are able to surreptitiously install their wares.

However, some authors still rely on the more traditional tactics, so user education may help to prevent at least a proportion of today's infections.

Let's take a look at some of the popular and avoidable methods of malware delivery;

By E-Mail

Malware is often sent as an attachment to an e-mail. The user will be prompted to open the attachment in some manner, the famous ILOVEYOU virus claimed that the attachment was a a love letter. The attachment had a filename of "*LOVE-LETTER-FOR-YOU.TXT.vbs*" but because of Microsoft's decision to hide filename extension details by default, appeared as "*LOVE-LETTER-FOR-YOU.TXT*".

Many users opened this attachment unaware that it was in fact a Visual Basic script, allowing the virus to execute. ILOVEYOU e-mailed itself to the user's address book as well as making changes to the host system.

Although the e-mail containing ILOVEYOU would have arrived from someone the mark knew, the unsolicited nature of the attachment should have been sufficient to deter most users from opening it. History, however, would suggest that this was not the case.

Video Codecs

Another popular method of malware delivery is through the use of Video Codecs. Users receive a message of some form (it could be an e-mail, a message on a social networking site, Instant Messaging or any other form) directing them to a site where they can watch something compelling. Many communications of this type claim to show a celebrity naked, having sex or in an embarrassing position (a recent example claimed to show TV Chatshow host Jeremy Kyle being punched).

When the user visits this site, they are told that they need to install a video codec in order to watch the video. A dialog will appear and the 'codec' will be installed. Some malware authors will then allow the site to play a video (even if unrelated to what the user was expecting), other won't. In either case the malware has been deployed onto the user's machine.

Software Downloads

Malware is also commonly spread by purporting to be other software. It may claim to be a 'hacked' version of proprietary software, a free game or indeed anything else. Malware of this type is commonly found on 'warez' sites and peer-to-peer networks such as Limewire and Bittorrent.

The user downloads the software and runs it and their system becomes infected. This infection may go undetected, especially if the software they were expecting also runs. This tactic is becoming increasingly common given the inflation associated with software prices, both Microsoft Windows and Microsoft Office are common targets of this tactic.

Enterprising malware authors have also targeted much more niche software in the past. Security Administrator Tool for Administering Networks (SATAN) was redistributed for quite some time with malware hidden within.

Avoiding Malware

As we've already discussed, it's no longer possible to avoid 100% of malware through user behaviour alone. The days of malware being a sign of visits to the 'dodgy' areas of the net are long gone, users can be infected by hacked mainstream sites as well as through their own naivety.

However, user education can help to reduce the attack surface, so let's take a look at some of the tips that we should be passing to users. Unlike 419 Scams and Phishing, there's no one sign common to all malware; as in Darwin's evolution, for malware diversity is key to survival.

To avoid malware users need to;

- Ask whether they were expecting an attachment
- Disable Filename extension hiding, and learn the different extensions
- Ask whether it's worth the risk to watch one video
- Ask whether their downloaded software seem legit (is it too good to be true?)
- Only download software from trusted sources
- Maintain an up-to-date AV Installation
- Not allow Administrator rights to those who don't need it
- If possible, run their browser in a sandbox

Sadly, some of these tips probably fall outside of the current skillset of the average user. Although, as an industry, we've been trying to educate the users for years, we've failed to understand an important point: *Preaching about security isn't enough, we need to teach those users the skills required to follow our advice.*

It's very easy for those in the Industry to wonder why these users don't simply google "how to sandbox browser X". The problem is, these users wouldn't even contemplate doing so, because it sounds geeky and is likely to be too complicated. We need to begin designing solutions aimed at helping these users to instigate some of the solutions that we suggest.

Scareware

Scareware is a relatively recent development, it works by playing on peoples fear of the other types of malware. The scareware can be installed on the users system in a variety of ways, but the most common is to perform a free 'anti-virus' scan of the users system;

The scareware performs a fake scan before announcing that the users system is infected. The user is then prompted to clear the infections by downloading the scareware purporting to be an anti-virus suite.

Once installed, the scareware will often prevent the user from running any other application by claiming that it is infected. The user will regularly be confronted with dialogs (often with broken english) claiming that the system is infected and that their credit card details are being stolen.

In order to fix these 'infections', the user is directed to run the scareware. Except that to do so, they must first upgrade from the 'free' version. The user is directed to a website to make payment, after which the scareware may or may not uninstall.

It's quite difficult to provide guidance to users without doing a great disservice to the numerous genuine free AV scanners, however;

- Is it a brand you recognise?
- Was the scan unsolicited?

If the answer to the latter is no, it's probably safe to assume that the software is scareware. As an important note, the most noxious of scareware I've come across so far is "*Security Tool*"

Conclusion

The IT Security Landscape is constantly changing, and users often find it very difficult to keep pace. As an industry, we need to lend these users the support required to help them understand their part. It's very easy to dismiss these user's as 'stupid', but the reality is that their mistakes impact upon us all. By allowing these users to fall prey to malware authors, we simply generate more trade for these 'cybercriminals' and guarantee that crime on the Internet retains a valuable incentive.

In order to stem the tide, we need to begin properly educating users on how to avoid the most common pitfalls. Such a move may also help to improve security on corporate networks as the users become more aware of what they should and should not be doing.

The difficulty is, as always, how to begin. We cannot force users to undertake security training, but we can encourage them to do so. Users don't need to understand the complexities of modern operating systems in order to be taught the basics of security, and it's up to us as an industry to offer users that opportunity.

As the security landscape changes, so must the education that we give. The Status Quo, however, seems untenable; how long until AV companies are simply unable to cope with the huge influx of malware? As the potential for profit increases, so will the number of malware authors.