Play **Threat or No Threat** at Infosec 2009!

Join Sophos and Utimaco on stand G50 to play a brilliant new version of the hit TV game show. **See page 6** » »

Hackers plant Shatner virus on satellite

Sophos reveals the truth!
Read all about it on page 2 » »

April 2009

the antidote

KEEPING THE SECURITY WORLD IN THE PICTURE

Conficker – a new name for an old problem

Has Conficker led to an internet meltdown? | **Page 5** » »

IT departments alarmed by risks of social networking

Graham Cluley

Once again, social networking websites are in the news...for all the wrong reasons.

System administrators are looking at these phenomenally popular sites with concerned eyes, not just because of productivity concerns, but also because of worries about malware authors, spammers and identity thieves exploiting the sites for their own financial benefit.

New research conducted by Sophos has revealed that 63% of system administrators worry that workers are sharing too much information on social networking websites.

Furthermore, a shocking two thirds of administrators polled believe that workers' activity on the sites could endanger security at their company.

So what are some of the dangers of social networking which go beyond productivity worries?

Spam and malware on social networks

Wherever potential victims gather, the spammers and malware authors are usually not too far behind. So it's not at all surprising that as the social networks have grown in popularity at an enormous rate, so reports of cybercrime being conducted through them have escalated.

> criminals are increasingly using social networking websites to steal identities, spread malware and send spam

A typical way in which attacks are spread is by hackers compromising the accounts of social networkers by stealing their usernames and passwords (perhaps by phishing or spyware) and then sending spam or malicious links to the victims' online friends and colleagues.

Web 2.0 sites such as Facebook, MySpace, LinkedIn and Twitter have all had their fair share of spam attacks and malicious content, designed to compromise PCs and steal identities just as readily as "traditional" attacks via email and compromised websites.

The problem is that users are much more trusting of content they believe to be from a friend or co-worker sent via a social networking website than perhaps they would a regular email.

Just like you need to properly secure your PC to prevent it becoming part of a botnet, so you also need to take proper care of your website usernames and passwords to prevent identity thieves and cybercriminals taking over your online accounts.

But it seems that we shouldn't be holding our breath hoping for Web 2.0 users to better defend themselves against internet threats, if their current online behaviour is

> social networks are typically poor at protecting users against these threats

anything to go by. Studies conducted by Sophos have uncovered that many users of social networking websites are regularly sharing far too much personal information online – data which could be helpful stepping stones for any identity thief hell bent on causing trouble and inflicting financial hardship on their intended victim.

Scams on social networks

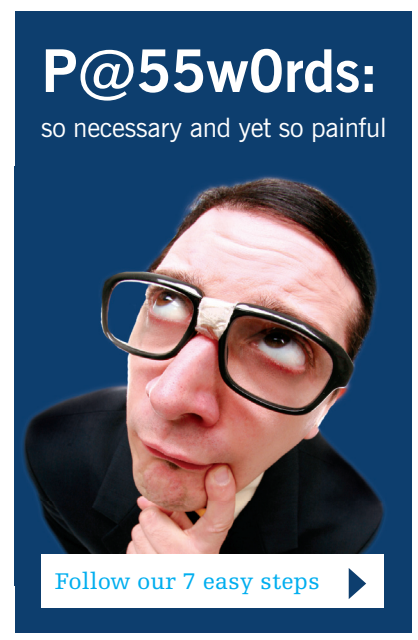
One increasingly common scam found on sites like Facebook occurs when you receive a message from a "friend" saying that they have lost their wallet and plane ticket home while holidaying abroad.

The fraudsters, who have obviously compromised your friend's account, try to engage you in conversation by sending emails and instant messages claiming that they have been mugged and desperately need you to wire some money to them. The conmen will even use information from your friend's profile to appear more plausible.

Even if it's a close friend, you're probably not keeping that close an eye on every movement they make – especially in the maelstrom of other status updates coming from your

Continued on page 2 » »

Inside



What Lies Beneath

Charles Southey

It is a sad but inevitable fact of life for every IT department that much of the real work that goes on there passes entirely unnoticed by the rest of the organisation, whilst every once in a while the most trivial of technical tasks earns praise and adulation beyond measure because it happens to have a visible effect out there in the real world.

Of course the latter is not really a problem: just because something is worth doing doesn't mean it should be hard to do and any form of recognition is welcome, even if it is like complimenting the builders of the great pyramids on their choice of typeface for the hieroglyphics on the doors.

But the converse isn't true either: just because something doesn't get noticed doesn't mean it isn't worth doing. There are hundreds of mundane daily IT tasks which even managers within the IT department are only vaguely aware of, but any one of which can be brought suddenly and sharply into focus across the organisation in minutes by simply *not* being done (or by being done wrongly).

Never is this more true than in the area of security. IT security companies like to think that security is high on the agenda of every CIO, and if pushed on the topic, CIOs will concede that it is important. But usually the topic of security is as welcome on a strategic IT meeting's agenda as a two hour health and safety briefing on the use of the whiteboard. The only time it becomes a hot topic is shortly after a major incident – but even then it soon fades away again once the initial excitement has passed.

Why is this? Can it be that IT managers just don't care about security? No, of course it isn't. Any CIO worth their salt is in that role because they have a passion for solving real-world business problems and boosting competitiveness and profitability through the effective use of technology – not because they want to be policemen. The business must be protected from criminals and idiots, but it is hugely irritating that resources have to be diverted from productive activities to do so.

Not only that, but this is a form of investment that has absolutely no upside but plenty of potential downside if it goes wrong. When something goes wrong it's very visible, very damaging and very unpleasant to be responsible for not stopping it. But when it all goes right – as it does 99.9% of the time – nothing. One cannot send out a daily bulletin jubilantly proclaiming "Hey! Nothing happened!" Disaster recovery measures are even less fulfilling: here you are spending time and money in the fervent hope that you're completely wasting your time and none of this will ever be needed.

So what's to be done? Obviously it is possible to have some success at illustrating the value of this kind of work and investment using statistics, KPIs and benchmarks to show, for example, how you've managed to reduce the spend but stay protected or how many threats you are detecting and successfully avoiding. But there's only so much excitement this can generate and it takes yet more effort. The only way this stuff is ever going to be a source of competitive advantage is if your competitors get well and truly screwed by some security problem. But since all your competitors are almost certainly doing the same things you are, waiting for this is like praying for rain in the Sahara.

No, there is only one remedy for all this: the work simply has to be made to go away. Everyone is facing exactly the same threats, only the degree varies depending on how much of an interesting target you are and how your employees behave. There surely can be no justification for any company – no matter how big or wealthy – having to employ armies of IT administrators to customise and configure security solutions, or for that matter to carry out any other universal, mundane and low value-added task.

Much of the real work that goes on in every IT department passes entirely unnoticed

IT security should 'just work', which by the way, is exactly how the rest of the business sees most things relating to IT. We don't employ hordes of drivers and mechanics to deal with the problem of getting employees to and from work or handling the company fleet; we don't have power and lighting specialists on tap to ensure there is a comfortable working environment – all these things have become self-service commodities that everyone can use without specialist help being available on a continuous basis. And by the way, if that specialist help were around I'll bet those things would go wrong ten times as often.

Unfortunately we're still a long way away from the total commoditisation of information technology, but the green shoots are starting to appear. The emergence first of appliances and now of cloud computing suggests that at least the problem is being recognised: even if these are for the most part only solving what is actually the relatively easy problem of installing the software and still in many cases needing lots of customising and configuring to get them working.

The day will come. Those of us over a certain age can just about remember a time when you literally had to tune in your television stations using little wheels or dials which was a very time-consuming process. Nowadays you expect to buy it, take it home, plug it in, switch it on, and voilà. One day, in the not too distant future, there will be no IT departments at all – everything will just work and we can all focus on doing the creative stuff. But long before we get there – in fact with any luck just around the corner – will come the day when nobody in the company except the junior guy who plugged it in even knows the name of their IT security vendor. When that happens, that IT security vendor will truly have succeeded.

April Fool's!

On 1st April 2009, Sophos played its much anticipated annual joke, this time claiming that hackers had successfully infected an orbiting communications satellite with a virus known as W32/Shatner.

Under the control of sci-fi obsessed hackers, the Shatner virus was supposedly embedding subliminal images related to Star Trek into popular television programs such as "The Simpsons", "Friends" and "Doogie Howser MD" as they were beamed down to viewers on Earth.

A video documenting the incident is available to view at sophos.com

Risks of social networking

« « Continued from page 1

dozens if not hundreds of other contacts on the site.

This is just the latest skirmish in an ongoing battle taking place between cybercriminals and Facebook users. Incidents of unwanted adverts and malicious links being spammed to Facebook users from their friends' compromised accounts continue to grow.

> the fact is that you never know who you're talking to, until you really *talk* to them

Emails from social networking sites are much more likely to get into our email accounts in the first place, since they don't have the obvious tell-tale signs that botnet spam does (such as a known-bad sender IP address, or known-bad headers, or known-bad email construction) causing them to be filtered out.

The fact is that you never know who you're talking to, until you really *talk* to them.

We will no doubt see more electronic conmen using stolen Facebook identities to steal money directly from the innocent by posing as their online buddies, unless more people take greater care over securing their computers and personal data.

Special report

Facebook, trolls, and death threats

Graham Cluley
Senior Technology Consultant, Sophos

I wouldn't exactly describe myself as a naïve ingénue when it comes to the risks that people can face on websites like Facebook.

Indeed, in 2007 I and some colleagues showed just how easy it was to steal identities on social networking websites after we created a fake profile of a small plastic frog called Freddi Staur (an anagram of ID Fraudster) and invited strangers to become Freddi's friend. Scores of people accepted the invitation, many revealing their full names, addresses, dates of birth, phone numbers and even - in one example - their mother's maiden name in the process.

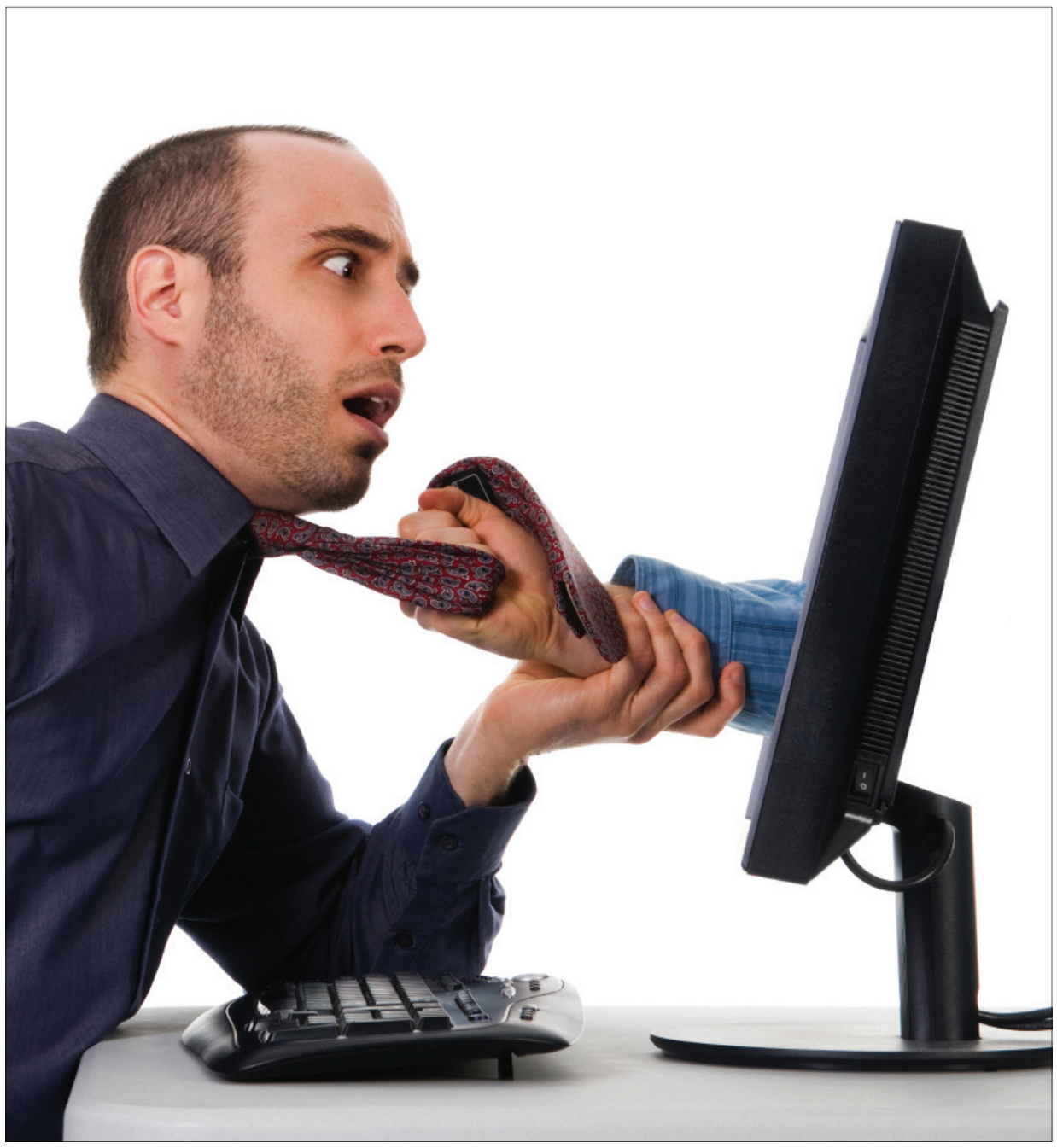
It was therefore a surprise to me last April when I discovered that someone had, without my knowledge, stolen my very own identity on Facebook - at least in one fashion.

What happened was this. Some pumpkin-brain on Facebook thought it would be a good idea to create some controversial groups on the social-networking website and feed the flames by posting inflammatory language. So far, so normal. But what this chap also did was decide to steal an online photograph of me and use it as his profile picture.

Inevitably, someone on Facebook recognised my picture, put two and two together, made five, and announced that I must be the person posting the nonsense onto the website. Furthermore, encouragements were posted to bombard both my own work email address and other email addresses at Sophos with 'information about what Cluley has been up to'.

All this was occurring as I was having a rather splendid holiday - with very poor internet connectivity - in Siem Reap, Cambodia.

Things got progressively nastier, as photos of me and my wife were posted to Facebook (complete with rather unflattering comments about the bushiness of my eyebrows and speculation as to where I buy my shirts). One guy, who claimed to be with the armed services, said that he had found out where my wife lived (probably not that tricky as my surname is somewhat unusual) and was considering shooting her. Another emailed me saying he intended to burn down my house.



As my wife and I were adventuring Indiana Jones-style amongst the temples of Angkor Wat at the time you can understand why we might have felt a little alarmed as to what we would find upon our return to the UK. The poor internet connectivity also made it tricky to contact the outside world, but I did file reports to Facebook asking them to delete the offending material.

Facebook's response was, I'm sad to say, mixed. Maybe I've upset them in the past with my Frog-related antics, but I would have expected them to have taken stronger action when presented with evidence of death threats on their network. Instead, Facebook advised me to contact the police and only eventually removed the photographs when I logged them as a breach of Sophos's copyright.

Not only were hotheaded internet users making death threats against me and my wife because they believed I was responsible for the troll-like postings on Facebook, there was also at least one group on Facebook which was created claiming I was a paedophile, and saying that web users could visit my site at grahamisakiddyfiddler.c**t.uk. Another group listed me as one of the 'Top 20 c**ts on Facebook.'

> "hotheaded internet users were making death threats against me and my wife"

I'm used to being disliked for expressing my opinions on computer security – I've even had virus writers lampoon me in their malware before – but to be on the receiving end of death threats against my wife and accusations of being a child abuser takes things to a whole new level of seriousness.

It was only when a journalist published a story about my experience that Facebook finally removed all the slurs against me and my family and closed down the discussion groups that were, frankly, out of control.

To my mind, Facebook should have acted faster in my case. But I was fortunate enough to have connections in the media to make my position clear. Imagine if I had been a more vulnerable member of society, or had not been alerted to what was being said about me?

And what is Facebook doing to stop this kind of abuse happening in the first place? A quick search on their website finds literally thousands of groups with extremely inflammatory titles and highly vulgar language.

Readers with long memories may remember in 2000 that The News of the World newspaper published a 'name-and-shame' list of alleged paedophiles, which resulted in a paediatrician having her house vandalised, and innocent families asking to be rehoused as mobs descended onto the streets. It seems to me that as more people get on the internet and believe everything that they read, that the chances of mobs attacking innocent people rises all the time.

The News of the World was far from the most highbrow newspaper in the UK in the first place, but its decision to publish the names of alleged sex offenders brought it into even more disrepute.

When is a file not a file?

Paul Ducklin

Sometimes it is easy to examine a file and to tell what it is. Program files, at least on Windows, start with the two bytes 'MZ', after Mark Zbikowski, the Microsoft coder who invented the original EXE file format for DOS. Image files in the GIF format, often seen on web pages, begin with 'GIF89a'. Many files carry a tell-tale format marker in their header bytes.

Such markers are quaintly known as *magic numbers*.

Other file formats have no official magic, but are still recognisable. Programs written in Python, for instance, are just plain text files. But the idioms of the Python language usually make such programs stand out - the first word in a Python file is often 'import', denoting the libraries the program uses; lines which don't start with spaces often start with the word 'def', since that is how Python functions are defined, and so on.

But what of encrypted files? How can you tell if a file is encrypted? Technically – assuming that the file is not re-encoded in some structured way after encryption – you can't. At least, you can't if the encryption is any good.

Strongly-encrypted data is indistinguishable from a stream of strictly random bytes, since to be strongly encrypted, the data must contain no discernable patterns which might be used to infer its original form.

> "strongly-encrypted data is indistinguishable from a stream of strictly random bytes"

Written English, for example, contains the letters ETAOIN very much more frequently – and predictably so – than VKXJQZ. Similarly, in English, Q is very much more often followed by U than by any other letter.

When encrypting data, it is vital that this, or any other sort of frequency skew, is removed. This leaves you with a file in which every possible byte value is equally likely at each byte offset in the file, and in which any byte is equally likely to be followed by any other. To an external observer, such a data stream appears random, even though you can easily reconstruct the original file using the decryption key.

The difference between random and *really* random can be subtle, and the difference may go unnoticed for years. The stream cipher RC4, for example, produces output which is nearly, but not quite, random. One particular flaw in RC4 means that the second byte of any RC4 cipher stream has the value zero twice as often as it should – a cryptographic chink which led to the cracking of WEP, once considered suitable for WiFi security.

> "how can you tell, after encrypting a file, whether it really is encrypted? How can you be sure your encryption software is working correctly?"

This begs the question: how can you tell, after encrypting a file, whether it really is encrypted? How can you be sure your encryption software is working correctly?

And the answer is: you can't. (You may be able to prove that it *isn't* working properly. But absence of proof isn't proof of absence.) You really do need to trust your vendor!

The danger of data loss

2009 is turning out to be another bumper year for stories about embarrassing data leaks hitting the headlines. Hardly a week has gone without stories of websites being hacked, customer databases being accessed, or USB drives and laptops containing confidential information being lost.

More and more organisations are recognising the necessity of encrypting sensitive data, investigating weaknesses on their websites, and controlling the use of USB drives in the fight to prevent sensitive data leaking out of their hands and into the hands of hackers, competitors and the media.

And, of course, data leaks may not only be embarrassing for your company's image – but can also put the finances of your customers and staff at risk.

Take, for instance, US healthcare provider Kaiser Permanente. They warned workers about the risk of identity theft, following the discovery of staff records in the hands of a third party who was subsequently arrested earlier this year. A computer file in the possession of the arrested man was found to include the names, addresses, phone numbers, Social Security numbers, and dates of birth of 29,500 Kaiser Permanente members of staff.

But it's not just about losing laptops, not encrypting sensitive staff records, and mislaying flash drives.

What do the blueprints for President Obama's helicopter, nuclear power plant secrets and confidential patient records all have in common? Well, none of them are supposed to be in the public domain – but all of them have leaked onto the internet thanks to careless use of peer-to-peer file-sharing programs.

Often seen on the White House lawn, Marine One is the official helicopter of the President of the United States. It's one of the most highly secured aircrafts in the world, always flying alongside a group of identical helicopters which act as decoys in case of an attack.

You wouldn't, therefore, expect engineering and communications details about Marine One to be found on an IP address located in Baghdad.

The discovery sent shockwaves through the teams who work hard to protect Barack Obama, and should remind everyone of the importance of securing sensitive information properly.

> “sent shockwaves through the teams that protect Obama”

P2P software, commonly used to share movies and music files (often risking copyright infringement), is increasingly also the vector by which confidential information has been broadcast to the world.

Peer-to-peer file sharing applications are extremely popular ways for people to pirate music and movies, and in almost all cases are not suitable for work use. Many have default configurations that will scan your entire hard drive for media files and share them automatically, resulting in accidental leakage incidents like this and others which have hit the headlines.

Disk and file encryption, data loss protection and general anti-malware technologies are other tools at your organisation's disposal to make sure your firm doesn't end up making the headlines in tomorrow morning's newspapers.

Safeguarding against data loss

If company laptops or other mobile devices can't be found, it doesn't always mean that they've been stolen. Companies often lose track of these IT assets because there's no clear record of them. Encryption and inventory management can help to safeguard against the loss of confidential data.

When large companies and organisations run inventory checks of their electronic devices, managers often end up scratching their heads. How can it be that suddenly only 90 company laptops can be located instead of the original 100? Theft or absent-minded employees are just two of a number of possible explanations. Over time, companies can lose track of mobile devices in the everyday 'chaos' of the enterprise. If a device changes department, location, or user – and this might happen several times in the span of just a few months – it is often subsequently listed as "missing." The danger is that confidential data on those devices can get into unauthorised hands and be sold to third parties or exploited for someone's own ends.

Protect your data as a security precaution

Losing data is every company's worst nightmare. To prevent it from happening, devices at risk and confidential documents should be protected from the offset. Professional encryption solutions protect data with a security shield to stop people from accessing data that they're not supposed to. Inventory management solutions can help keep track of everything, and introducing company-wide security policies make employees aware of possible security threats. Taking these measures will not only protect confidential data, but also prevent numerous devices disappearing.

Encryption means no more worries about mislaid data

The larger the company, the more difficult it is to track the whereabouts of mobile devices. Occasionally, it is only a case of laptops or USB sticks moving to a different floor in the same building, but when entire departments move, it can mean a new site or even a different country.

Inventory management solutions can help trace where devices are and which devices are no longer in use. Although the hard drives on retired equipment can be overwritten several times to protect confidential documents, or the special deletion software now available to prevent data from being reconstructed can be run on the devices, neither of these approaches can guarantee 100 percent security. However, if the devices had already been equipped with encryption protection, the disposal wouldn't require any extra effort or expenditure.

Disposal costs would be reduced, as would the worry that data could inadvertently end up in the public domain if there should be a lapse in security at the disposal company. Professional security software for mobile devices also ensures that a hard drive that has been removed from one computer cannot be read in another.

Conficker – a new name for an old problem

Mark Harris

Viruses and malware don't make the headlines very often these days. Melissa, Loveletter and Sasser all hit the headlines in their day for a variety of reasons. But nowadays the constant stream of Trojans, password stealers, backdoors and so on, rarely gets more than a passing mention. Computer security is assumed to be in the front of people's minds. Not opening attachments, not clicking on links in emails, applying patches when they are published and having up-to-date anti-virus software installed were all seen as common sense and something that every administrator would be following. Or at least you would think.

In the past weeks, malware has been front page news again and this time it's Conficker. Attention-grabbing headlines about computers going into meltdown on April 1st have swamped the media. So what is it about this threat that is so different? The short answer is nothing! The first version came out several months after Microsoft issued an emergency 'out of band' patch for the vulnerability. The importance of this patch was widely reported.

Conficker initially infects via unpatched machines, then spreads via USB keys and file shares with no (or weak) passwords. It also tries to call home to websites to get functional updates – again, nothing unusual about that. The only slight difference is the algorithm it uses to select websites. It doesn't actually do anything else.

Many vendors had proactive 'zero day' protection against the exploit, and detection for both the first version and subsequent versions of Conficker were published very quickly. So why are individuals and organisations continuing to get infected?

If a network is patched, has up-to-date security software, and a good password policy, it is considered to be protected. So the obvious conclusion is that a lot of organisations aren't following these simple guidelines – recent Sophos research showed that the security software of six out of 10 endpoints tested was out of date.

Conficker will probably disappear with a whimper, but it's a perfect example of why endpoint security still has to be top of the priority list for every administrator. Ensuring important patches are applied, anti-virus is up to date, controlling the use of USB keys and monitoring and managing compliance of security policies will help to prevent Conficker and the other tens of thousands of pieces of malware seen every day, from making those newspaper headlines a reality.

Tips for choosing an effective encryption solution

The most effective encryption software for mobile devices uses secure algorithms, such as the well-established AES algorithm. This algorithm also allows for installation at a later stage and can be used on several different operating systems. Additional criteria when selecting encryption software include low maintenance requirements, transparent and automatic operation, a high degree of stability, and a short test phase. The more thought a company puts into its security policy at the purchasing stage, the better and faster it will then be able to meet this list of requirements.

> the more thought a company puts into its security policy at the purchasing stage, the better and faster it will then be able to meet this list of requirements

Efficient software for administering data security must provide simple mechanisms for the central configuration of all relevant security rules. Structuring the rules in a comprehensible manner will result in fewer potential sources of error and a need for less training and planning. Furthermore, professional security solutions provide protection that is more extensive and of a higher quality than an operating system's own tools. The advantages are that security policies can be enforced across platforms, the entire hard drive can be encrypted, removable media can be backed up, and heterogeneous PC environments can be supported – surely an asset to any company looking to keep their reputation as well as confidential data protected.

Top five tips for securing data at Infosec

1. Train your staff
Many employees still continue to underestimate the risks that unprotected data on laptops and mobile storage media pose on business trips or at trade shows. Companies should point out potential risks to their staff prior to the event. This also means clear rules of conduct concerning the use of mobile devices.

2. Set up secure passwords
Passwords are the first walls of defence, consisting of a combination of numerals, letters, and special characters. Passwords should be checked and rechecked one final time before the event.

3. Smartcards plus password
Smartcards (or tokens) form a second wall of defence serving as increased security. They contain information that allows access to a laptop only in combination with the user's password. Fingerprint readers are another option - users must identify themselves with their fingerprint when booting up or logging in.

4. Password-protected screensavers
During long technical discussions at the booth, screensavers are activated when the computer has not been in use for a while. A new password request should be required in these cases.

5. Encrypt all important data
Automatic data encryption for information stored on your laptop's hard disk or external storage media is a must. Your data is safe even in the event of theft at a trade show.

Passwords: so necessary and yet so painful

Carole Theriault

There has been increased focus on computer users employing poor passwords to safeguard their many computer accounts – be they eBay, Facebook or an online bank. This is becoming a serious problem as hackers are increasingly taking advantage of our poor password etiquette and employing attacks to sniff them out, in order to get them unauthorised access to steal money, information or identities.

Password theft is a bit like a burglar attempting to break into a house by karate chopping the front door rather than finding an alternative route in. If the main door is flimsy and cheap the most unfit bruiser is likely to succeed. A steel reinforced solid oak door, meanwhile, presents the Bruce Lee of burglars with a virtually insurmountable challenge. So, as there is no additional cost to having hard-to-guess passwords, why are so many of us hiding our most private information behind our pet, computer or child's name?

Now, it's possible that many computer users don't fully understand the importance of their passwords. The password is quite simply the head honcho of security in your computer's armoury. Typing in the password is the same as flashing a VIP badge at some exclusive event and watching the guards usher you in with no questions asked.

The other problem is one of scale. If we had only one password to remember, perhaps we would take the job of creating it much more seriously. But many of us have dozens and dozens of the things – about a third of the websites I visit require some sort of username and password. Many users arrive rather quickly to the conclusion of making passwords easy to remember and use the same password for all their online accounts.

On the face of it, this approach is rather rational. You don't want to forget your passwords so you make them easy by keeping them short, simple and meaningful. The unfortunate side effect is that it also makes the job of illegally hacking into an account much easier. Hackers often employ dictionary attacks – they use a program to match the passwords to words in the dictionary. They also share lists of key combinations, often used by poor password users, such as 'QWERTY' or '12345'.

The advice from experts is use easy-to-remember, but difficult-to-guess passwords. Combine letters with numbers and punctuation. Make them long – the more characters, the harder they are to guess. Don't follow any keyboard sequence. Don't write it down anywhere. Mix up capital with lowercase letters. And make them unique for each and every account – after all, you don't want the bad guys to finally guess one and get in to all your accounts.

And, no, the irony here is not lost on me. This is painful. It does not fit in with computers making our lives easier. But tools such as password management programs do exist to try and mitigate this problem. Designed to store all your difficult-to-remember passwords behind an encrypted database, these tools only need you to remember the one master password. Some people, though, are uncomfortable with using a third-party application, but it sure beats having a three-letter password that rhymes with 'bat' to safeguard your accounts. After all, it doesn't take a genius to see that attempting to get your money back from your bank or online store because someone stole your password doesn't sit high up on the 'things-to-do-before-you-die' list.

We need to apply the risk-reward strategy. The difficulty of the password should be proportionate to the value of the information it is safeguarding. I would spend a lot more time coming up with a virtually impossible password for my online banking accounts, but would worry less about the password for the chess forum I belong to. I would care very much if my earnings got into the wrong hands, and would care a lot less about people seeing the history of my chess moves. However, as the value of the pound continues to plummet, I might be wise to change views on this.

The secret of a good password

- Don't use dictionary words
- Combine letters with numbers and punctuation
- Make them longer than 8 characters
- Don't follow any keyboard sequence
- Don't write a password down
- Mix up capital with lowercase letters
- Have unique passwords for every account

> "use easy-to-remember, but difficult-to-guess passwords"

Play Threat or No Threat!

Learn about circumventing data loss and cyber attacks, watch malware and hacking demos, and play Threat or No Threat with Sophos and Utimaco at stand G50

Our full presentation schedule

Tuesday 28 April	
10:30	Social networks: The new frontier for malware, spam and ID theft
11:15	The foibles of securing virtualised systems
12:00	Why bother encrypting your data? *Live password hack demo*
14:00	Who said JavaScript was easy? *Live web-based malware demo*
15:00	Why bother encrypting your data? *Live password hack demo*
15:45	Threat or No Threat

Wednesday 29 April	
10:30	Social networks: The new frontier for malware, spam and ID theft
11:15	Typhoid Mary: SophosLabs' research of Linux threats
12:00	The foibles of securing virtualised systems
14:00	Who said JavaScript was easy? *Live web-based malware demo*
15:00	Why bother encrypting your data? *Live password hack demo*
15:45	Threat or No Threat

Thursday 30 April	
10:30	Social networks: The new frontier for malware, spam and ID theft
11:15	Why bother encrypting your data? *Live password hack demo*
12:00	The foibles of securing virtualised systems
14:00	Who said JavaScript was easy? *Live web-based malware demo*
15:00	The foibles of securing virtualised systems

Security in 2009: the story so far

Graham Cluley

Security moves quickly, with new threats and trends being reported on a seemingly never-ending basis. But what have been the main information security stories that have been shaping the year to date, and what quirky tales might you have missed?

Conficker

No prizes for guessing this one. Conficker has been the biggest malware story of the year – if not the last few years. Spreading via a mixture of poorly chosen passwords, auto-running USB flash drives and a Microsoft security hole, this worm managed to dig its teeth deep into many businesses and proved difficult to prize away.

Much media attention was focused on 1st April, when Conficker changed its instruction-hunting algorithm – but the worm will continue to be as big a threat as it ever has if computer systems are not properly defended.

The British Botnet Corporation

The BBC found themselves in the middle of a huge controversy after its Click television programme bought access to a botnet of thousands of computers worldwide, and used it to send spam messages.

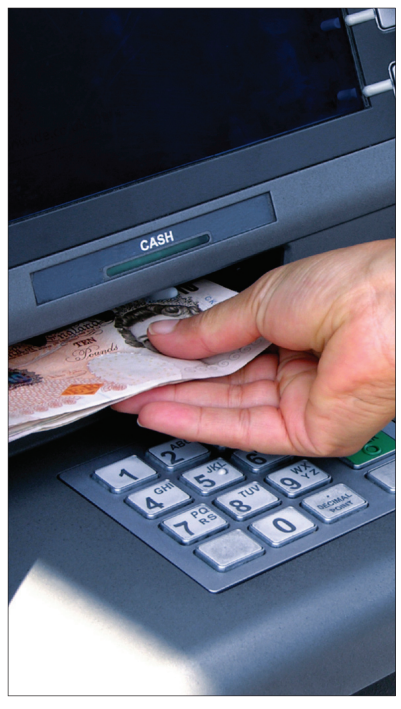
Most anti-virus companies, although supporting the aim of raising awareness of botnets, disapproved of the BBC's methods saying that they had breached the Computer Misuse Act and could just as easily have emulated the experiment in safe laboratory conditions.

Mac OS X malware

Although Trojan horses and viruses are much less common on the Apple platform than on Windows, it doesn't mean they don't exist at all. During 2009 Sophos has encountered more instances of Mac OS X malware being planted on websites, with the intention of making money out of unsuspecting web surfers.

Worryingly, it has become apparent that criminal gangs involved in highly-profitable Windows malware are amongst those now developing attacks against Apple's operating system.

With anti-virus usage on Apple Macs much less common than on Windows, security experts are concerned that hackers may find easy pickings on the platform.



Malware in ATMs

The credit crunch may have made many lose a little faith in the financial markets in recent months, and that was reflected last month when Sophos discoved a Trojan horse that could infect – and steal money from – cash machines.

The Skimer Trojan horse steals account and PIN details from bank customers who insert their card into affected cash machines. Fortunately, installation of the Trojan horse requires physical access to the internals of the device, and the only report of security breaches came from Russia.

Diebold, the makers of the affected ATMs, issued an update to its cash machine software, and recommended that it be installed on all of its ATMs globally.

Smartphone security

Yogi Parmar

The popularity of mobile phones has exploded over the last 15 years – everyone from your granny to your five year old nephew has one. And now, the must-have gadget of the nineties has morphed into a device that offers much more than the ability to text.

Smartphones offer additional functionality and are akin to a PC – you can surf the web, email and download applications. But as these handheld devices seep into business operations, employers need to consider the associated security implications.

The main concern for businesses is the disclosure – accidental or deliberate – of confidential data stored on smartphones. The loss of a phone is likely to be the most common scenario, so businesses need to treat these devices in the same way as any other PC – sensitive information must be encrypted and only relevant business information or applications should be allowed on these devices in order to keep a handle on the issue.

Mobile spam is a growing problem. Earlier this month, SophosLabs received reports of a new campaign that alerted users via SMS that their bank details had been posted on the internet, including a link to a website. Anyone who used a computer to visit the website would be infected with a Trojan designed to give hackers access to their PC.

> the main concern for businesses is the disclosure – accidental or deliberate – of confidential data stored on smartphones

As 'M-commerce' grows in popularity, the financial element that this introduces is likely to fuel the problems of mobile spam and malware. Given the uptake and ease-of-use of devices such as the iPhone, they could become a target. Attacks are likely to be made by hackers to gain access to confidential information, and as such, security should be taken seriously.

Smartphone best practice

1. Ensure the data is encrypted. Some devices will inevitably be lost, that's just a fact of life. With the correct encryption procedures in place, lost or stolen devices will be useless to fraudsters.

2. From an enterprise point of view, make sure all email goes through any existing content filtering systems that are in place. It is far easier to manage email security at the gateway, and this also reduces the burden of device management.

3. Run mobile malware detection. Although rare, examples of malware for mobile devices have been seen. As mobile internet use continues to grow in popularity, we're likely to see more people pay for goods online via their phone - at this stage the devices will become a far more financially viable target for cybercriminals.

News roundup

Strengthening data security

The recently announced partnership between Gartner leaders Sophos and Utimaco brings together two industry leaders, combining encryption, endpoint protection, and network access control expertise.

Bringing two core security measures together will enable organisations to manage today's complex threats and comply with the increasing number of security regulations simply and effectively.

Their combined expertise and integration plans will provide protection, support and return-on-investment through one expert company.

Sophos Partner Program

Launched on 20th April 2009, Sophos's new programme offers new and existing channel resellers a generous margin structure, enhanced support and training, as well as new deal registration and margin protection initiatives.

This value-based programme offers a comprehensive portfolio of tools and resources designed to help channel partners to grow their business.

If you're an IT reseller and interested in partnering with Sophos, contact **uk_partners@sophos.com** or call **01235 544100** to have a chat with a member of the channel team.

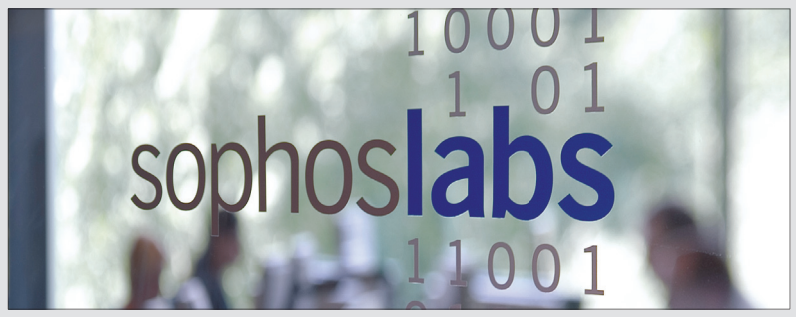
Microsoft UK Challenge

The annual Microsoft Challenge will take place in June 2009 in Wales.

The event generates funds for the NSPPC and raised £550,000 last year – organisers are hoping to break the record this year.

In 2008 Sophos entered a polished team of athletes and secured a respectable 53rd place – this year, team captain Richard Whittle is taking no prisoners. "We have an exceptionally fast team – watch out for the trail of smoke behind us as we aim for podium position!" Anyone wishing to contribute to this fantastic fundraising event by sponsoring the Sophos team should contact **pressinfo@sophos.com**

Learning in the Lab



As part of its ongoing commitment to educate computer users on the threat of malware and spam, SophosLabs is opening its doors to education organisations in a bid to teach young people about protecting themselves and their computers whilst surfing the net.

Previous education days hosted at Sophos's headquarters in Oxfordshire have been a success and teachers are encouraged to get in touch with Sophos to arrange similar events for their students. For more information, please contact **pressinfo@sophos.com**

And finally...

Graham Cluley takes a look at the quirkier side of the IT security world.

It's war out there, with computer security experts embroiled in an ongoing, escalating battle against an increasingly sophisticated army of cybercriminals. But sometimes you have to laugh at the strange stories that get reported.

A hacked road sign in Texas

Here are three tales of the absurd that I have uncovered recently, and that acted as a pleasant distraction from the run-of-the-mill security stories.

1. In Texas there is a hacking epidemic taking place. No, not against Windows computers - but against electronic road signs.

Someone is breaking into the software running construction roadsigns at the sides of the highway and displaying bizarre messages such as "OMG THE BRITISH R COMING. THEY R WATCHING YOU" and "CAUTION! ZOMBIES AHEAD!".

Joking aside, hacks like this are illegal, and you can imagine how messing around with road signs could actually lead to a dangerous accident. No doubt the authorities are looking closely at the nearby University of Texas to see if the pranksters might have planned their hack from there.

At first I thought it would be great if hackers took a "year off" attacking computers and concentrated their efforts on road signs instead - but imagine how many marriages would be ruined as stressed husbands-and-wives tried to navigate around Swindon?

2. Late last year, a Japanese woman who was addicted to the online game "MapleStory" was arrested after breaking into her virtual husband's account and killing his avatar.

The woman was alleged to have committed the virtual murder after her fellow player and online lover "divorced" her in the game without warning.

So, if you have ever wondered why the cops aren't fingerprinting your car after it gets broken into, you'll be reassured to know they're all creating bare-chested 6'4" demi-gods to slip in unnoticed amongst the citizens of Second Life.

3. We all know that password security is a serious business. You should always use a non-dictionary word that is hard to guess.

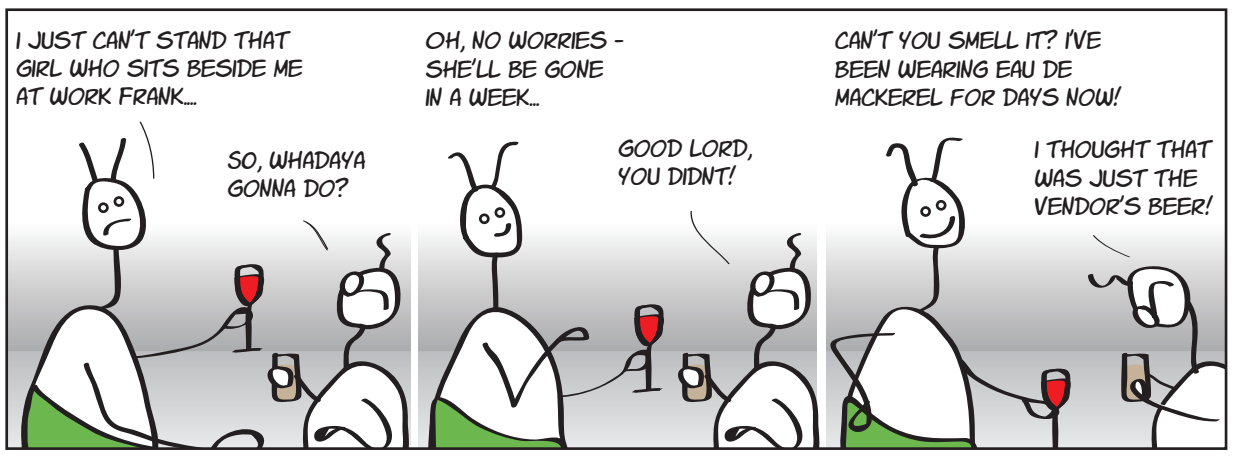
Steve Jetley, a customer at the Shrewsbury branch of Lloyds TSB was disappointed last year, however, when he tried to change his password to "Lloyds is pants" after a dispute. The bank responded by changing it – without his permission – to "no, it's not". This amused Steve at first, until he was told he couldn't change it back to "Lloyds is pants" or his suggested alternatives of "Lloyds is rubbish" and "Barclays is better".

He eventually tried "Censorship" only to be told it was too long to be a password, and should be no more than six letters long.

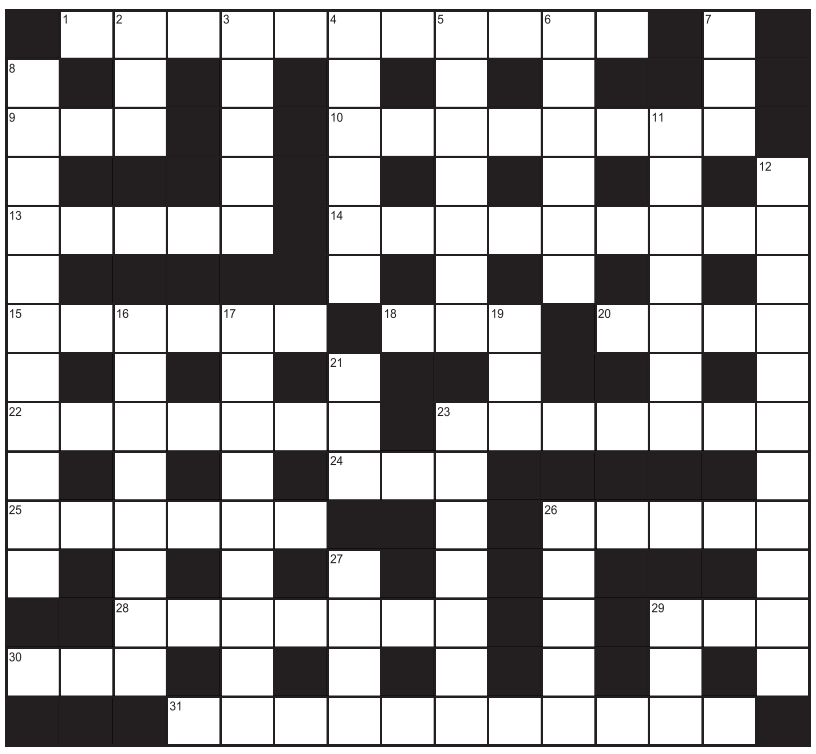
And they call this security? Thank heavens for people with a sense of humour like Steve Jetley who expose this kind of idiocy.

Office politics

Carole Theriault



Encrypted Crossword



Across

1. Near-terminal symptoms started after first message found in briefcase – such files in the mail should be handled with care (11)
9. Start controlling information found in lamb roast (1,1,1)
10. Codes for recognising people in hats, conclusion of talk put forward (8)
13. Scamming software makes unlikely claim first taken from shoe (5)
14. With me around, German motor comes after environment-friendly online business (9)
15. Compression/encryption tool to stow the Queen? (6)
18. Message daemon gets back into fat man (1,1,1)
20. "Mebroot" rootkit hides vehicle certificate, showing river in Spain (4)
22. Two terms of cricket produce common form of 5 (7)
23. Workstation table surface? (7)
24. Hex editor contains program extension (3)
25. Parasite from 2001 is large ruminant with energy force (6)
26. Selects, we hear, the Spanish spot on screen (5)
28. Guy gets mixed up with fool, search for space being professed purpose of agency intrusion (7)
29. Even upstart can find name record indicator (1,1,1)
30. Charge into memory (3)
31. Attempt to follow man is vital place to store configuration data (8,3)

Down

2. Pile of stones on hilltop form anonymising system (3)
3. 11. Mud-plastered tumbler is most popular tool for handling documents (5,7)
4. Security subverter becomes Vanity Fair writer after falling in Tay (6)
5. Attack taking advantage of flaw gets one involved in former scheme (7)
6. Targeted attacks can overcome most anti-virus, if started where Bing Crosby did (6)
7. Underwater vessel comes up to find data transfer system (3)
8. Clever Penny sharpens hand-held tools with many uses (5,6)
11. See 3d
12. Code analysis tools remodel pics in disarray (11)
16. Tartan total for simple integrity measure (8)
17. Wear away outside of first-rate green-skinned monster to find fault identifier (5,4)
19. Excellent archive format (3)
21. Half of 10? (3)
23. Unscramble German burial place (7)
26. Go-between provides speed or privacy as pyro gets confused around ten (5)
27. Norse god replaces thousand with first formers, producing poor-quality sound or loop device (4)
29. Distant boots provided by pixies, oddly (1,1,1)

Stumped or looking to check your answers? Email pressinfo@sophos.com to receive the finished crossword!