THREAT FILES 2015

ITC
SECURE NETWORKING

EXECUTIVE SUMMARY

Firstly I would like to say thank you to all of our followers on social media and for their positive feedback around our weekly blog "Threat of the Week" (TOTW). Since its launch in 2013, circulation to CxO's, IT Executives & Security Professionals has grown by over 900%. Our aim is to be timely, informative and incisive but most importantly provide practical advice around threat detection and risk reduction for your business.

I'm delighted that the predictions we made in 2013 were accurate and I trust you will agree from this review that 2014 follows suit. Interestingly, whilst the numbers of attempts to compromise were down in 2014 there were actually more successful attacks than ever – this of course means Cyber Criminals are becoming more effective!

2015 will again push the envelope and widen the boundaries in the security market. This year we expect to see acceleration in attacks on corporations and individuals for monetary gain. While cyber criminals may have many different motives against business and governments - from theft of intellectual property to extortion to defamation to theft of other assets – we are observing an increasing trend in attacks against the C level and senior executives for the same motives at a personal level.

Clearly every CxO will be feeling the pressure and no one wants to be the next Sony whose breach has cost between £100m and £1bn, depending on who you believe. In 2015 we believe all Board Directors should make fighting Cybercrime a priority by ensuring that Information Security is central to the fabric and culture of their Business.

Please enjoy reading this review, which we are confident that alongside TOTW will help you protect your business and win a few battles in the long war against Cybercrime.

Tom Millar, Chief Executive Officer
ITC Secure Networking

CONTENTS

PREDICTIONS 2015

AFTER AN ALL TOO INTENSE 2014, WHAT DOES 2015 HAVE TO OFFER TO KEEP THE DILIGENT INFORMATION SECURITY COMMUNITY UP LATE?

HERE ARE SOME OF OUR THOUGHTS:

New improved Spear guns

2015 will be the year of really successful SpearPhishing attacks used to drop all manner of nasties. Zeus variants will continue to prosper, along with even more nasty ransomware, which will disrupt both the individual and the enterprise.

User education is a key factor in preventing infection and we will be offering user awareness programmes to our customers. We will also continue to tune the detection systems of our NetSure360° Managed Security platform. As well as continuing to add known Command and Control (C2) sites, we will be integrating functionality, such as the recently announced dynamic-dns functionality from Palo Alto, in order to detect rapid DNS changes typical of some malware.

Detection systems and rules for accepting inbound email will require tightening across the board.

Massive enterprise breaches

There will be an increase in these in 2015 for a number of reasons. The first is the obvious 'my dongle is bigger than your dongle' attitude of the young hacker hordes who are much more organised online than they are in their bedrooms.

The second, and to our minds a more worrying reason, is the availability of Malware as a service. Disgruntled ex-employees can buy, tailor, deploy and execute very targeted and efficient attacks without massive skills - think Sony Pictures. In order to combat these threats internal controls, both technical and physical, will need to be understood with disaster recovery/damage limitation procedures in place and tested as an integrated part of the business continuity process. We will be visiting all of our customers in Q1 to discuss this approach to regaining control.

Very organised crime

We have seen incredibly sophisticated and organised scams against all forms of online cash in 2014 and this will only increase in 2015. Not just content with stealing card and login details, organised gangs will collate, test and resell this data amongst themselves as well as to larger non cyber, terrifyingly organised entities. ITC will continue to support our clients, the police and associated agencies, whose efforts we salute, during 2015.

ThunderClouds

Cloud services will come under increased attack in 2015. Here at ITC we are very interested in the security implications of Software Defined Networking, particularly in speed of deployment, development and patching. We were surprised to see that VMWare are describing their SDN (NSX) engineering qualification as 'The next-gen CCIE', which is somewhat disrespectful of their former pals at Cisco who in our experience shouldn't be written off so casually.

Secret Sauce

We are due another Snowdenesque data leak. On Christmas Eve 2014 the NSA released 12 years of oversight reports identifying enormous numbers of security breaches by staff. Some deliberate, such as spying on spouses, or just accidental.

As well as the extremely shady timing of the release it appears to have exposed something of a hornet's nest of discontent amongst a significant number of agency types. Watch this space.

Unloved legacy servers

There will be more oldskool attacks on legacy (mostly Unix) code – like HeartBleed and Poodle. We can hear the legions of doom going through Unix source code from here! We will continue to update our customer base as soon as news of any successful activity breaks and we will be deploying risk qualification technology (where am I vulnerable?) together with attack identification and mitigation techniques on our NetSure360° Managed Security platform.

The internet of naughty things

As more and more household appliances become connected to the internet, the attack landscape is rolled out wider and thinner as if by a rolling pin. Although not currently the focus of Cyber Criminals, all attack vectors must be considered especially around wireless network breaches caused by the IoT. Watch this space for significant developments; if the lights have gone out, we may have been too late!

Software defined Networking

2015 will be the year that Software Defined Networking begins to take shape and be implemented by larger enterprises (probably true), CCIE's will be made redundant in favour of shiny new VMware NSX engineers and all networks will be designed, implemented and run by software. Of course they will.

PREDICTIONS 2014

2013 WAS A VERY INTERESTING YEAR IN INFORMATION SECURITY. WE ANTICIPATED THAT 2014 WOULD BE EVEN MORE EXCITING, NOT NECESSARILY A GOOD THING!

HERE WERE OUR PREDICTIONS FOR 2014:

☑ Malware

The volume of malware will continue to increase, targeted at multiple platforms (especially mobile – see right) potentially hidden in utilities and games on all platforms fixed and mobile. Mobile devices will be used as a platform to attack Enterprise especially Cloud data.

☑ CryptoLocker

Data encryption and destruction Malware like CryptoLocker will become more and more of a headache for Enterprise and individual users. Stay vigilant, keep backups, stay patched, keep A/V up to date and restrict local administrative rights.

☑ Windows XP shuffles off

The death of Windows XP presents an opportunity to restrict local administrative rights using Windows 7 or 8.1. Unfortunately the end of support for XP, coupled with Java version 6, will present rich pickings for the bad guys if they are not upgraded.

☑ Enterprise Private Clouds will grow quickly

The Enterprise is worried about Government snooping (and why wouldn't they be?) and most security analysts are predicting that attackers are becoming more interested in cloud data (see CryptoLocker). Cloud security will be an industry front line, not to mention a nauseating buzz phrase.

☑ Behavioural based anomaly detection

The grip of correlation based analysis (Arcsight,Q1Labs etc.) on Enterprise security management will be either threatened or enhanced (depending on your perspective) by the growth in anomaly based detection. Watch out for what Cisco plan for Sourcefire 3D in the coming year. We are very interested in Cisco's security technology integration with Sourcefire and the X series firewalls. Will Cisco MARS rise from the ashes as Cisco Jupiter, Saturn or possibly Uranus?

Social networks will be used to socially engineer employees and compromise the enterprise. User training and awareness programmes will become an increasingly important piece of the defences.

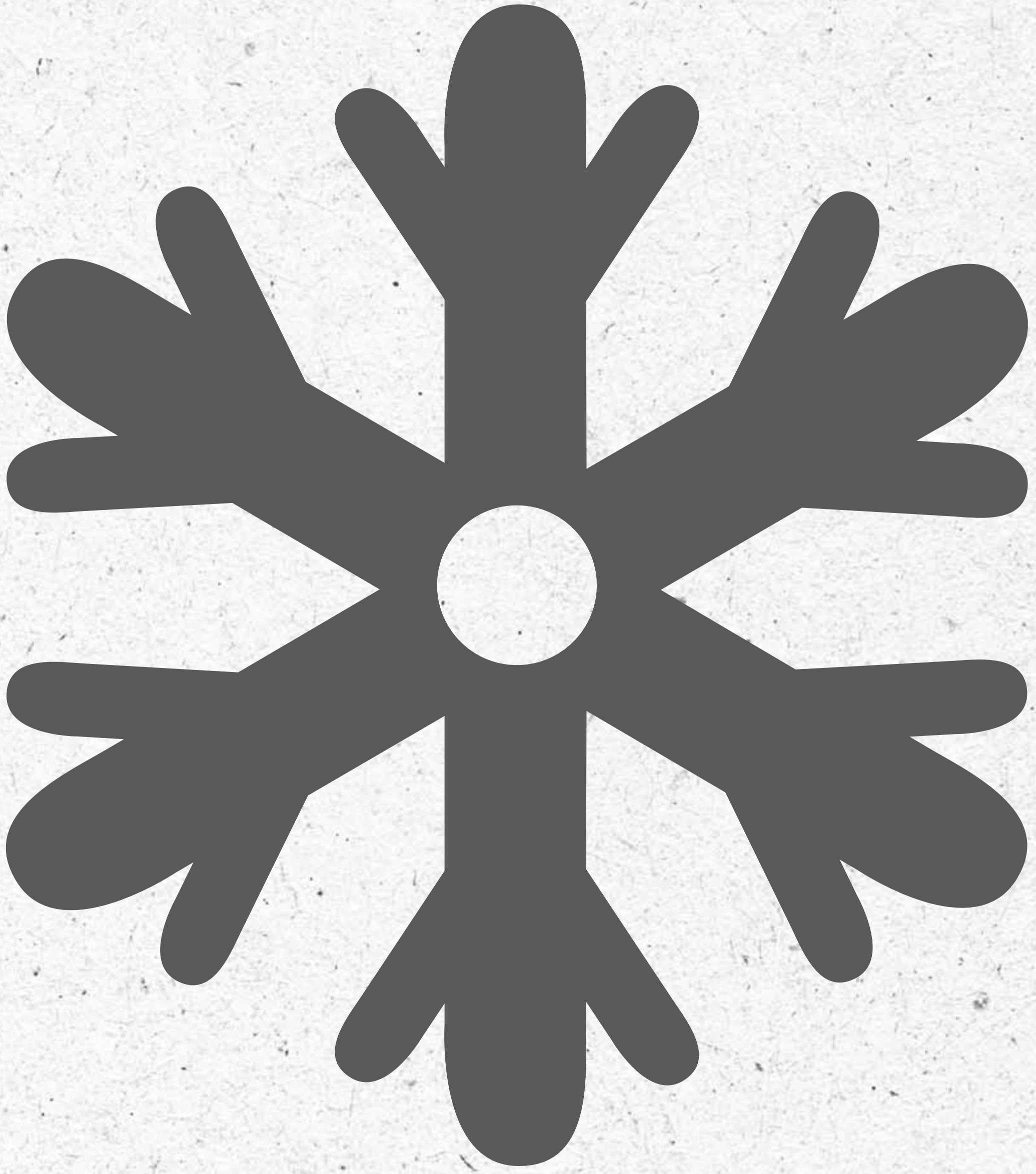
☑ Mobile security

Increasing levels of security for mobile devices will be provided by the device manufacturers (for example the Samsung Knox security suite). This technology from the boots up will provide essential device protection and will blur the boundaries between what is provided by the manufacturer and what is provided by Mobile Device Management vendors, although there is no suggestion that vendor tech will replace MDM. Securing the mobile device will be a big deal in 2014.

ITC will continue to develop our product and NetSure360° service portfolio in line with industry trends and customer requirements and will continue to debate current issues on this blog in 2014.

WHAT HAPPENED IN 2014

2014 will be remembered for the following: a massive growth in malware harvesting user credentials and financial details, ransomware software such as CryptoLocker causing massive issues, new exploits against old software both Unix and Microsoft based (ShellShock/HeartBleed/Poodle/SandWorm), and huge enterprise breaches such as Target and Sony Pictures.



WINTER

JANUARY - MARCH 2014

MAIN THREAT

RANSOMWARE- COMING TO A BUSINESS CRITICAL DIRECTORY NEAR YOU SOON. BE AFRAID!

THREAT #1

16 MILLION EMAIL ADDRESSES HAVE BEEN HARVESTED BY THE BAD BOYS, ARE YOU AMONGST THEM?

THREAT #2

CIOS TAKE NOTICE.
FAILURE WILL NO LONGER BE TOLERATED!

THREAT #3

STILL RUNNING XP?
DON'T BURY YOUR HEAD IN THE SAND

THREAT #4

ONE MONTH TO GO BEFORE XP PATCHES ARE DISCONTINUED. IT'S NOT LOOKING GOOD EITHER

2014 saw an enormous increase in successful Ransomware infections. Even though the most popular of these (CrytoLocker) was rendered ineffective through the capability to decrypt your stuff for free (thanks to research from FireEye and Foc-IT), there are many other variants and we predict more of the same for 2015 delivered using advanced SpearPhising techniques.

User education is the name of the game here.

MAIN THREAT

RANSOMWARE- COMING TO A BUSINESS CRITICAL DIRECTORY NEAR YOU SOON. BE AFRAID!

We predicted that 2014 would see an upsurge in Ransomware events.

Ransomware is software that typically encrypts your files and gives you three days to pay a ransom to allow you to decrypt the files. The main offender is still the now infamous Cryptolocker which uses a bug in a Windows API and very stealthily and nastily encrypts all images, spreadsheets and documents etc. to which the infected machine has access. That is to say all files located on both the local machine and all shared drives. NIGHTMARE!

In February 2014 it was announced that an American law firm (Goodson's in Charlotte, North Carolina) lost all of its legal documents to Cryptolocker after deciding to pay the ransom too late. Our best wishes are with their IT team for a speedy resolution.

CryptoLocker and other (nasty, nasty) Ransomwares have two typical routes in (attack vectors if you want to sound like a pro). These are via email attachments or via Botnet infection.

User education is key to preventing email infection. It is imperative that you or your users take care with attachments coming from people not known or trusted.

The Botnet infection is much harder to detect though and requires the following as a bare minimum:

- Make sure you have a current backup of all your data
- Remove administrative privileges where they are not needed, including local admin
- Make sure your systems are patched
- Ensure your anti virus is up to date and ACTIVE
- Review access control to network shared data

The question that must be addressed is clearly 'to pay or not to pay'. The answer to us is obvious; don't pay if you don't have to. You won't have to if you have a plan and we can help you to build, implement and execute such a plan.

If you don't have to pay, Ransomware becomes Vapourware, and that is A Very Good Thing for all of us.

THREAT #1

16 MILLION EMAIL ADDRESSES HAVE ALREADY BEEN HARVESTED BY THE BAD BOYS, ARE YOURS AMONGST THEM?

Over the last years we at ITC, and all other security vendors for that matter, have been cautioning against the perils of nasty little malwares, often invisible to anti virus, enslaving machines for numerous nefarious purposes.

One of the primary functions of malware has been to lift usernames and passwords as they are used from the infected machine and then to upload them to Pirate HQ for on-sale, or direct use by the bad guys.

Showing considerable diligence, and unsurprisingly ruthless attention to detail, the German Office of Information Security (BSI) has announced that 16 million (!!!!) of these username and passwords have been lifted, and they have copied them and have a tool that enables users to check to see if their username is on the list

Although the page is in German, it is very easy to use – fill in your email address, tick the red box, and the system will come back and tell you if you are named and shamed.

The site is at: www.sicherheitstest.bsi.de

THREAT #2

CIOS TAKE NOTICE. FAILURE WILL NO LONGER BE TOLERATED!

As you will no doubt be aware, there have been numerous high profile incidents regarding the loss of data, specifically customer credit card details and other personal information, from vendors that include Adobe, Sony and the USA retailer Target, all of whom are alleged to have lost over 100 million records EACH (unbelievable isn't it).

The vectors for these attacks are many and varied involving code delivered inside the network, weak administrative controls and passwords, exploitable code in applications used within the business, weak patching on web servers and the usual suspects all of which we have covered in blogs in the past.

It was announced that as a consequence of the enormous breach, the CIO of Target moved on from the position and that the retailer would review its security policy from the ground up.

What all of these breaches show is that it matters not what the attack vector is; it is the DATA or the ASSET that is important.

Unless you identify what your critical assets are, it is impossible to manage the provision, operation and management of appropriate security controls for those assets.

THREAT #3

STILL RUNNING XP? DON'T BURY YOUR HEAD IN THE SAND

For years now we, in line with every other security company worth its salt, have been banging on about the end of support for Windows XP.

The day arrived. Windows XP is no longer being generally supported with security updates and bug fixes.

The obvious problem with this (the no security updates bit) is somewhat exacerbated by the following facts:

- Other versions of Windows contain almost identical core code, which will be continued to be patched
- Many government organisations such as the British and the Dutch have signed multi million pound/euro/bitcoin deals to receive bespoke support from Microsoft

This means that the bad guys may very well be able to reverse engineer patches to Windows 7 and 8, or indeed obtain data from the bespoke support packages should they ever leak from the corridors of power, however unlikely that may seem!

Windows XP is already being bullied, having an estimated 25% of all infections despite representing only one fifth of deployments. This is going to get worse. A lot worse, especially given the fact that in the hacking world, most of the bad boys and girls (in fact just naughty boys and girls) are just going for easy targets using recycled code.

Obviously we urge you to get rid of XP, but we understand if you haven't done this yet there may be some compelling reasons, such as SCADA systems (actually, a chill ran up this bloggers spine just writing that).

Here is what we recommend you do:

- Identify the location in the network of your XP machines at all times
- Monitor XP machine activity for Botnet, Worm and Malware behaviour
- Make a plan to get rid of XP!

THREAT #4

ONE MONTH TO GO BEFORE XP PATCHES ARE DISCONTINUED. IT'S NOT LOOKING GOOD EITHER

Next month will see Microsoft remove support from the venerable stalwart that is XP. That means that XP will no longer be patched, although its offspring will be, providing clues to potential weaknesses in the old girl's defenses to the bad guys.

How bad can this be we hear you cry, surely most issues with good old XP have been fixed by now? Unfortunately not.

Tuesday (11/03/14), Microsoft released a swathe of patches for Windows and Internet Explorer many of which have been seen 'in the wild' that enable hackers to run code on your machines without even asking.

Internet Explorer is looking like a fantastic attack vector for hackers and this week's patches fix no fewer than 18 exploitable issues that enable malicious code stored on web sites (probably also hacked – see last weeks TOTW) to control your machine. We believe that we have seen some malware with this exact vector very recently, be vigilant.

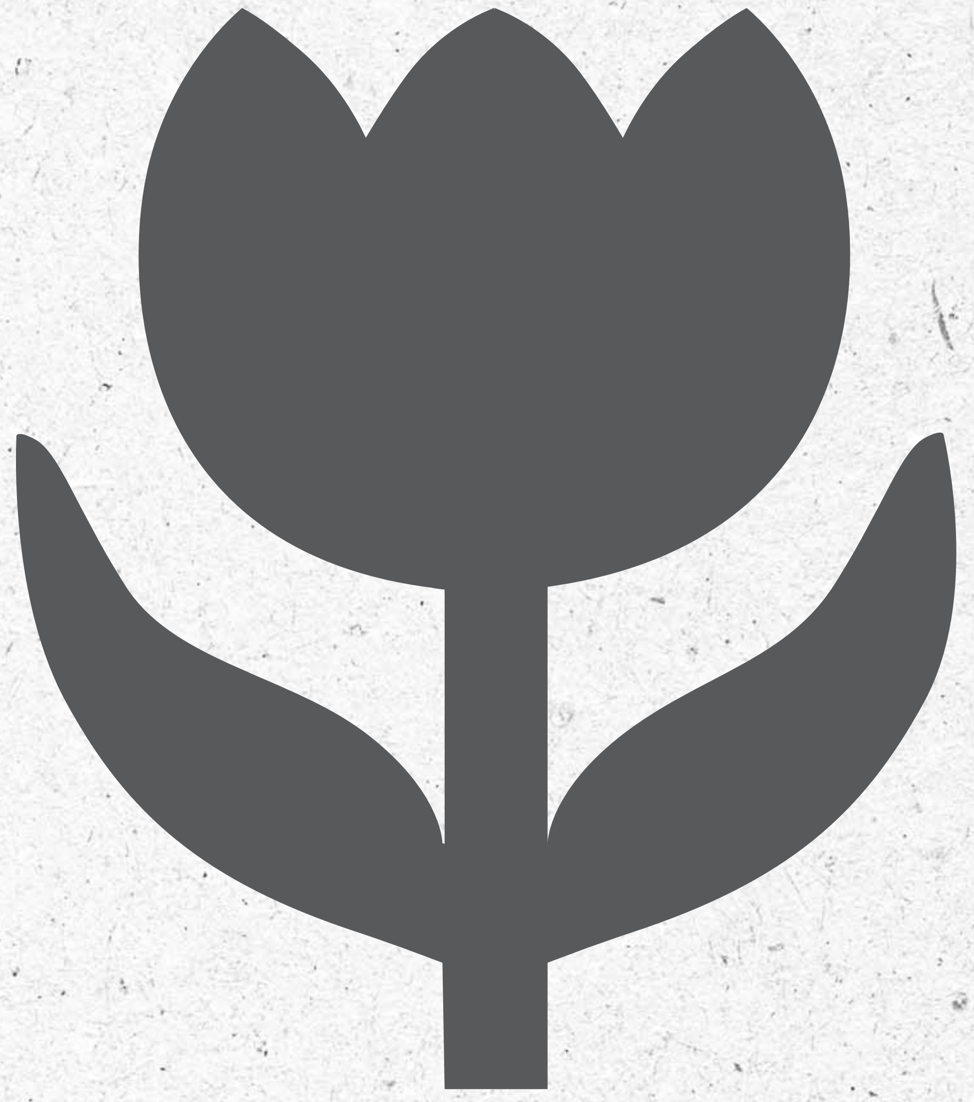
Obviously we recommend that you implement the MS patches as soon as you can, if not sooner. In fact you should probably be doing that now rather than reading this, if the truth be told.

You should also get off XP before the end of April. We know it is hard but if you don't you will be a sitting duck and it matters not that Microsoft's reputation for security will be in tatters, that is to say more in tatters than it currently is. You will be taken down.

ITC recommends the use of Network Access Control technology from the lovely people at ForeScout. Fully integrated into our NetSure360° managed service, this technology allows you to control what can connect to your network and whereabouts in your network it resides.

We will be recommending that all of our customers with this solution deployed identify and report on Windows XP machines still connected to the network post April and if they can't be upgraded, shot or otherwise removed, that they are forced into a dark room with limited access to the rest of the network controlled by layer 2 Vlan and firewall rules.

We guarantee that within the next 12 months this blog will be covering a security breach based around an XP/IE exploit. Please don't let that be you.



SPRING

APRIL - JUNE 2014

MAIN THREAT
MY BLEEDING HEART

THREAT #1
EBAY GUM - STICKY TIMES AT THE WORLD'S BIGGEST TAT SHOP

THREAT #2
60% OF ITS STAFF DON'T REPORT A SECURITY RISK UNTIL IT'S TOO LATE

THREAT #3
WE HAVE A SHORT TIME TO BEAT A POWERFUL COMPUTER ATTACK

THREAT #4
GOT A MAC? PERHAPS YOU SHOULD THINK ABOUT AN UMBRELLA

MAIN THREAT

MY BLEEDING HEART

A bug was disclosed in specific releases of the OpenSSL cryptography library which meant that bad guys have been able, for some time (over 2 years), to silently extract data in memory from servers that run OpenSSL to encrypt data such as passwords, VPN tunnels etc. It appears that real life compromises may have been recorded in audit logs from as far back as November last year.

We've seen a massive surge in SSL based scanning activity – so it's safe to assume that if you run a website that's still vulnerable it will already be on a hacker's list somewhere.

Whilst a lot of attention has been paid to username and password details in the press, we don't really see this as the scariest part of this problem, unless you are personally unlucky (this is yet another reason to setup two factor authentication wherever you can). What is very worrying is that the private encryption keys of your devices will most certainly be held in memory and can most certainly be retrieved by a third party, without you knowing and with no logs whatsoever.

What this means is that even if you patch your vulnerable devices (more about this later), but have already been compromised (a fact you cannot possibly know), your keys will remain the same and it will still be possible for the attacker to decrypt your private traffic going forwards (unless you are running Perfect Forward Secrecy, and you would know if you were).

Appliances and systems such as load balancers, firewalls, web servers, database servers, routers, SSL VPN devices etc. all use the OpenSSL library and it is imperative that you identify if any of your internet facing equipment is vulnerable by checking with the vendor as soon as you can. You can follow this up with an analysis of internal systems with a view to patching but you must absolutely prioritise Internet facing kit.

As well as patching your systems you must re-certify all Internet facing systems as soon as you can, taking the opportunity to upgrade to 2048 bit certs if you have not already done so.

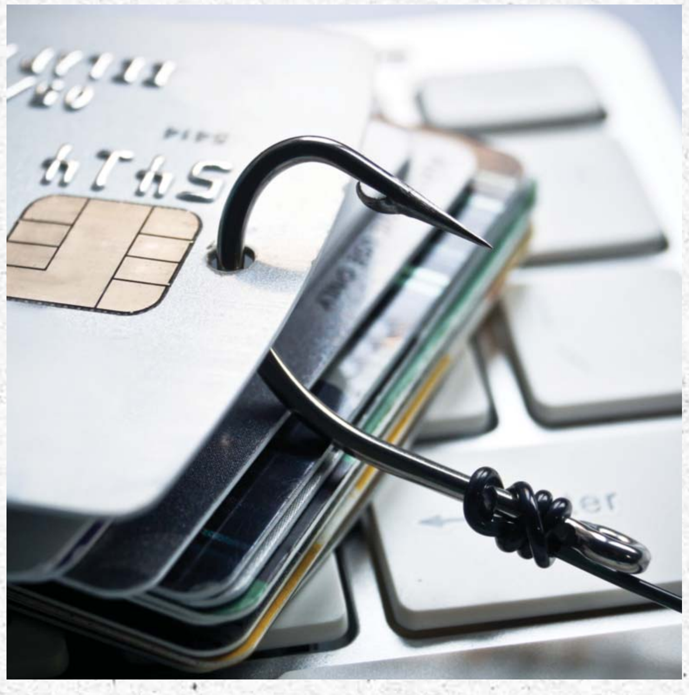
Furthermore if you have IPS devices then you should make sure they have signatures for the vulnerability enabled specifically for unpatched systems. Enabling these signatures globally will result in numerous false positives which may drop legitimate traffic. Cisco's signatures of this violation are delivered as disabled by default for this reason, so simply upgrading your signatures on Cisco kit will do nothing.

Something to think about with this revelation is that if an appropriately minded organisation, like, err, the NSA or GCHQ knew about this, then without doubt they would go on a private key exfiltration frenzy and have the capability to decrypt stored transmissions from, or between, your sites at will. It is probably best to assume that every secure communication that has been 'protected' by these vulnerable libraries may as well have been sent in the post, without an envelope. Really.

Attacks against legacy (mostly Unix) servers, including embedded machines and forgotten old web servers hit the news in 2014 and attacks will continue in 2015.

If only we all had the time to identify and migrate all this old stuff!

ITC's NetSure360° managed services platform has a number of techniques for identifying machines at risk and mitigating the threat against them whilst they wait in the patching queue.



THREAT #1

EBAY GUM - STICKY TIMES AT THE WORLD'S BIGGEST TAT SHOP

Everyone knows that eBay announced the loss of a gazillion customers' records including customers' name, encrypted password, email address, physical address, phone number and date of birth.

Not good.

This activity apparently took place between February and March last year and the suggestion from eBay was that the compromise was against a single database. In other words, your credit card data was not compromised, honest.

There were simply too many unanswered questions, ones that eBay really needs to get down to answering:

Why doesn't eBay encrypt all customer data, rather than just passwords? This is not computationally difficult and frankly is best practice. How do eBay know that no further data has been stolen? If this has been going on for a month, what is the real scale? Why didn't the exfiltration of masses of data trigger an alarm? What systems are in place to detect this?

These questions may have been answered in due course but the damage has been done. Change your eBay password, and all other online passwords that are the same, and be very vigilant.

THREAT #2

60% OF I.T. STAFF DON'T REPORT A SECURITY RISK UNTIL ITS TOO LATE

A recent report carried out by US cyber expert Dr Larry Ponemon found that some 60% of IT staff will only tell managers of a security risk that they have come across if they consider it to be 'serious' or 'urgent.' In most cases the criteria IT staff were using to judge whether or not a risk was serious was simply gut feeling and the report claimed that, for most IT workers, the concept of what constituted a serious security risk was rather different than the perspective taken by senior managers – which is very worrying indeed. In the report Ponemon highlighted that "The stakeholders with the highest responsibility seem to be the least informed," and that security threats were often being kept from bosses until they reached the point at which it was often too late for management to do anything about it.

THREAT #3

WE HAVE A SHORT TIME TO BEAT A POWERFUL COMPUTER ATTACK

In an unprecedented move, national law types across the planet simultaneously made a public announcement that we had just a few weeks to prepare for a massive infection event. The infections concerned were the Zeus/ Gameover Zeus malware, which harvests credit card, password and other input details from machines, and the nasty, nasty Cryptolocker (which we have banged on about in previous blogs). Cryptolocker encrypts your files and demands payment to decrypt them.

A super global arrest warrant was issued for the 2.0 Lex Luther himself, Evgeniy Mikhaylovich Bogachev in what will surely cause an escalation of hostilities, but will arresting one bad guy make any difference?

The long and short of this is that it is believed that a shedload of machines are infected with at least one of these pieces of malware or at least their daemon spawn, awaiting orders to pounce from their cat stroking command and control servers in the cloud. It is believed that a substantial number of these infected machines are running the no longer supported Widow Twankey XP.

THREAT #4

GOT A MAC? PERHAPS YOU SHOULD THINK ABOUT AN UMBRELLA

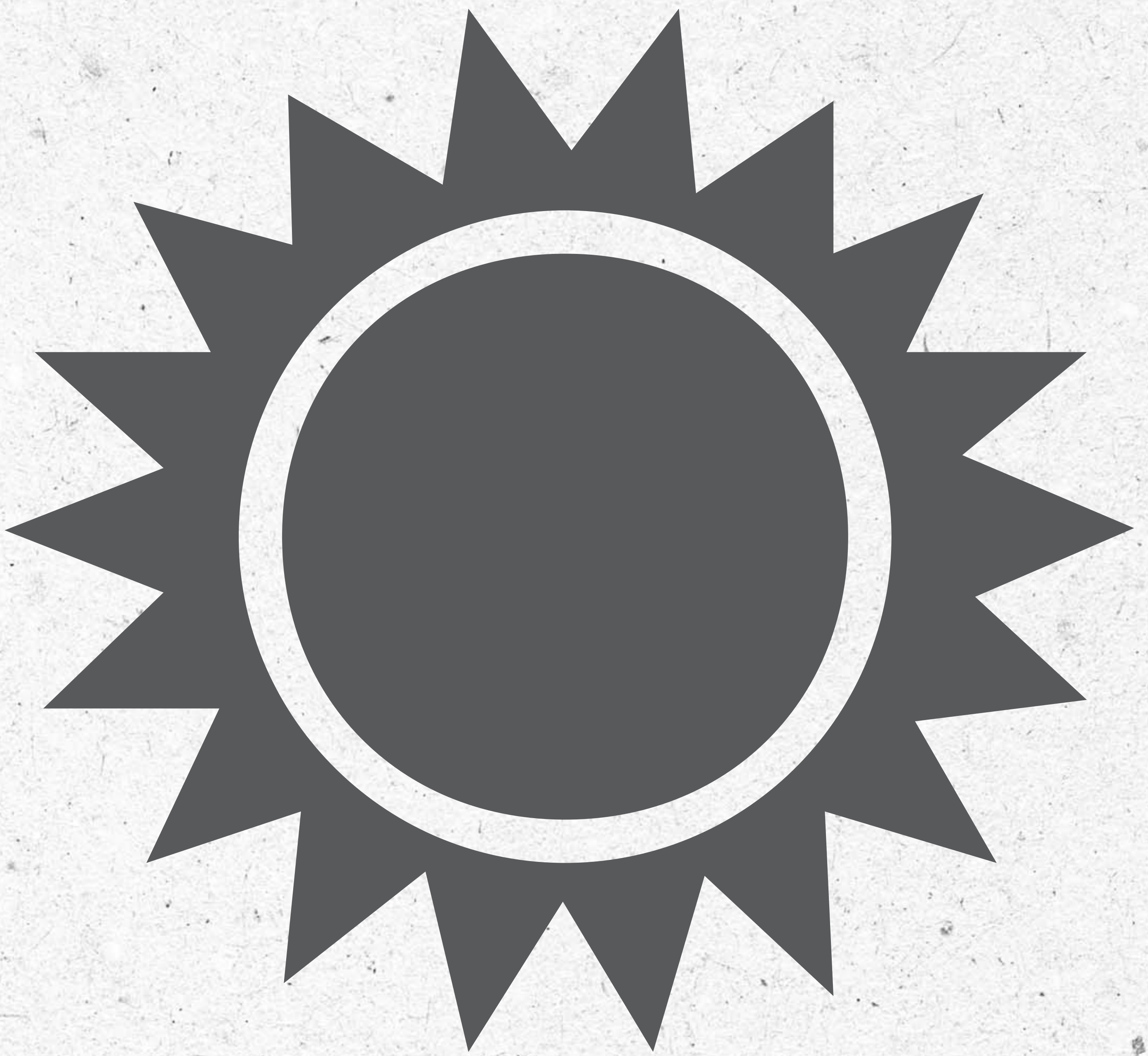
Apple released security updates for iOS7, IOS6 and OSX.

It transpired that any application that uses the Apple security library (like, err Safari and Mail) pre 10.9.2 (released on Tuesday 25 February 2014) is vulnerable to a man in the middle attack because of a coding error in the library.

What does this mean to you? It means that malicious types could intercept your traffic and snaffle your bank account details, your letters of undying love to Margaret Thatcher or your subscription details to Railway Magazine.

Seriously, this is bad news. To further compound this misery, it appears that Apple has pulled support for OSX Snow Leopard, only in use on 20 percent of Macintosh machines currently. There were no security updates for Snow Leopard in the last two rounds of patching.

What can you do about this? Obviously it is imperative that you patch personal machines and absolutely mandate that BYOD/CYOD and corporate Macs (if you have them) are patched. We recommend that you deploy Network Access Control systems to identify non-compliant machines connected to your infrastructure and enforce remediation or leave them out in the cold and damp until they are patched.



SUMMER

JULY - SEPTEMBER 2014

MAIN THREAT

THE SHELLSHOCK CONTINUES

THREAT #1

COULD THE LAST ONE TO BE HACKED PLEASE REMEMBER TO TURN THE LIGHTS OUT ON THEIR WAY OFFLINE

THREAT #2

SWEET 2FA! IF YOU'VE GOT IT, FLAUNT IT!

THREAT #3

EEEEK. 5 MILLION GMAIL CREDENTIALS PUBLISHED ONLINE - YOURS INCLUDED?

THREAT #4

OFF MY HEAD SON!

As with HeartBleed, attacks on old code are not going away any time soon.

It is important to understand how badly you are exposed using accurate mapping of your assets together with an up to date understanding of what you are vulnerable to. In fact these are two steps of our 'five steps to infrastructure security' programme.

MAIN THREAT

THE SHELLSHOCK CONTINUES

News indicated that Yahoo servers, along with Lycos and WinZip, were breached by a Romanian hacker group. Yahoo advised that no user information was exposed and they claimed that the servers were not affected by ShellShock. According to the comments by the Yahoo CISO, malicious code was executed on the servers by attackers looking for ShellShock vulnerable hosts. The attackers modified the ShellShock exploit and were running scripts that happened to match a vulnerability in some of the Yahoo Sports APIs. The main concern here is that ShellShock may only be the beginning, the door that was shut, Is now wide open.

The exploit for this vulnerability seems to be a good base for other exploits that in turn can cause major headaches to all IT Security professionals, especially those with old Unix implementations either as servers or embedded devices such as storage controllers.

Anyway enough of this ShellShock banter. Let's talk about one of our old favourites and purveyors of many a security vulnerability, step forward: Adobe.

Adobe announced (or admitted) that the Digital Editions version of its software communicates what you are reading back to Adobe HQ, unbelievably in unencrypted HTTP packets, in the name of piracy protection. Not only does this sort of privacy invasion suck, but you have to wonder what else Adobe has planned, not to mention what this 'functionality' could be talked into doing by the bad guys if the product was exploitable, which it is almost certain to be.

Enterprise managers using Adobe tools for secret business documents should look into this and have a strategy for locking them down.

THREAT #1

COULD THE LAST ONE TO BE HACKED PLEASE REMEMBER TO TURN THE LIGHTS OUT ON THEIR WAY OFFLINE?

In case you hadn't heard – the "Internet of Things" (IoT) is here to save us. Just stick sensors and IP addresses onto everything and all the world's problems will shortly thereafter be solved by a single cloudy Hadoop instance.

Take the humble light bulb as a perfect example. For the past hundred and thirty years or so the progress of the human race has been held back by our reliance on aptly named 'dumb' light bulbs – offering a single shade of white, only able to be controlled from a single button on the wall and, worst of all, lacking an API!

Compare this with a modern IoT connected light bulb – give a bulb an IP address and you can teach it to not just shine light, but also change colour, be controlled from a web browse etc. You might also open up a nice back door into your network too because the guy who designed that bulb was not interested in understanding how strong encryption should be implemented.

LIFX, one of a couple of companies who make net connected bulbs, released a security advisory that as a result of a botched encryption implementation .their bulbs were accidentally broadcasting your WiFi key to anyone nearby. An updated firmware was released that fixed the hole, but with a projected 212 billion 'IoT' devices coming online by 2020 there are clearly going to be a lot more vulnerabilities, the majority of which will likely go unnoticed and unpatched.

Knowing what should and shouldn't be on your network, and being able to accurately classify and assess the devices as and when they connect, has never been more important. If you don't get this under control now it's only going to get harder.

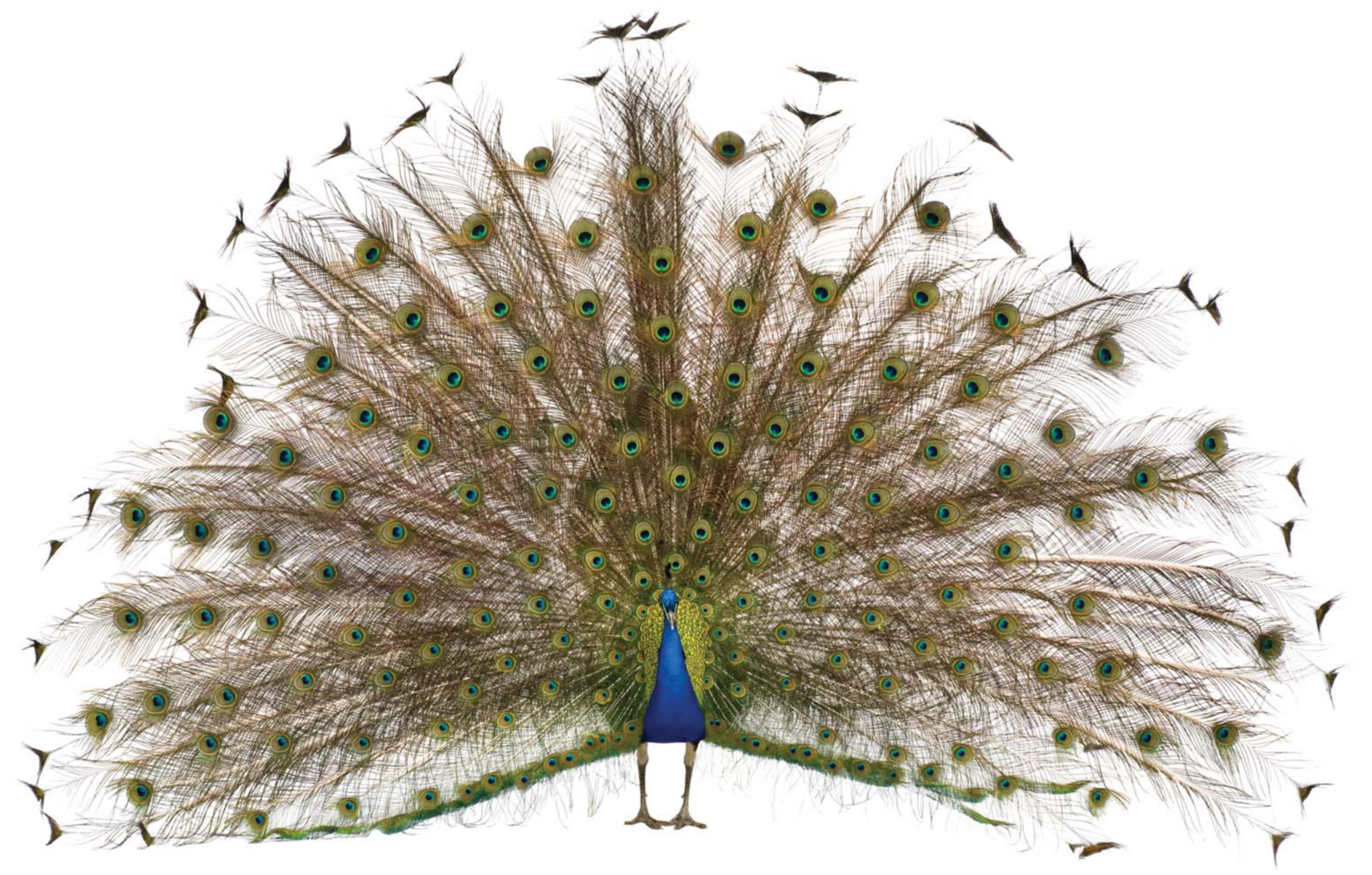
THREAT #2

SWEET 2FA! IF YOU'VE GOT IT, FLAUNT IT!

The publication of private, personal but more importantly (apparently) NAKED celebrity pictures stolen from accounts in Apple's Cloud brought a couple of core security principles into sharp focus.

The first is that, somewhat surprisingly, even massive outfits like Apple seem to allow their API's to bypass some of the basic security controls in place for a normal user authentication. In this case an API was used to brute force the accounts of celebrities without causing the accounts to be locked out after 3 failed attempts. Authentication is authentication no matter if you are a user, an API or even a bot.

The second is that Username and Password as credentials are not enough in this brute force, password stealing (Zeus and variants) botnet world. It is becoming an imperative that online providers mandate the use of two factor authentication for logins from unknown or new devices. We would go so far to say, if it doesn't have 2FA, don't use it.



THREAT #3

EEEK. 5 MILLION GMAIL CREDENTIALS PUBLISHED ONLINE - YOURS INCLUDED?

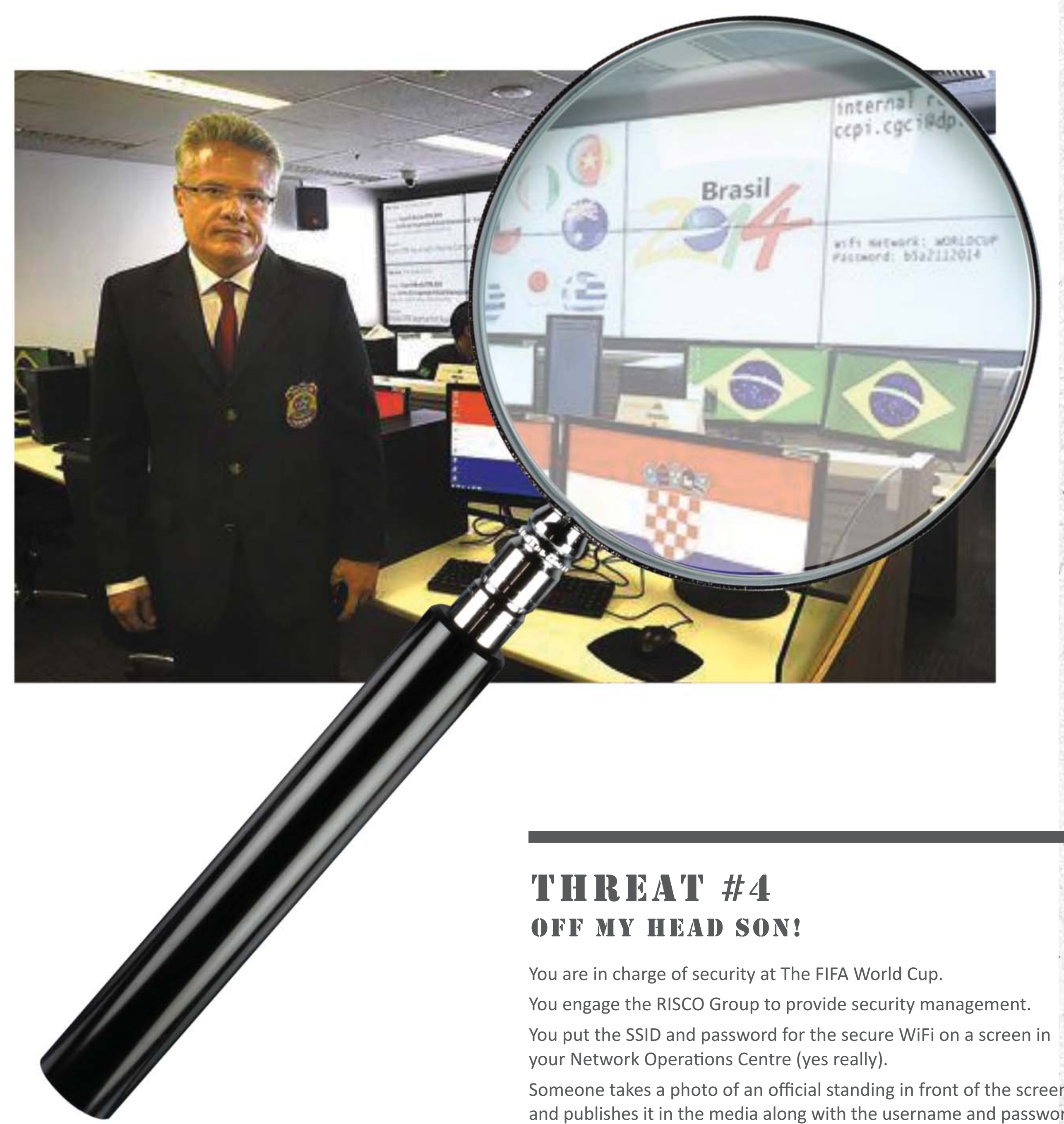
Reports started appearing about 5 million Gmail account details being published in Spring 2014. Presumably a subset of the 1.2 billion user details currently in the hands of our Russian friends harvested over the last few years via phishing and malware scams and now correlated, sorted and productised. Your identity for sale, by Boris Goddamski.

Although some of the data appears to be old, some is current and we recommend that you change your Google password and please TURN ON TWO FACTOR AUTHENTICATION.

Two factor authentication is more readily available than you might think, Facebook, Twitter, Dropbox all have it as well as most cloud and dev services like Github. Make the effort, turn it on. Today.

At ITC we have a number of clever tricks up our sleeves, including the ability to have a look on the dark side TOR (the Mordor of The Internet) to see what people are saying about your people or your organisation.

Apologies for banging on about two factor authentication but it really is the best way to keep yourself safe in the cloudski, just do it.



THREAT #4

OFF MY HEAD SON!

You are in charge of security at The FIFA World Cup.

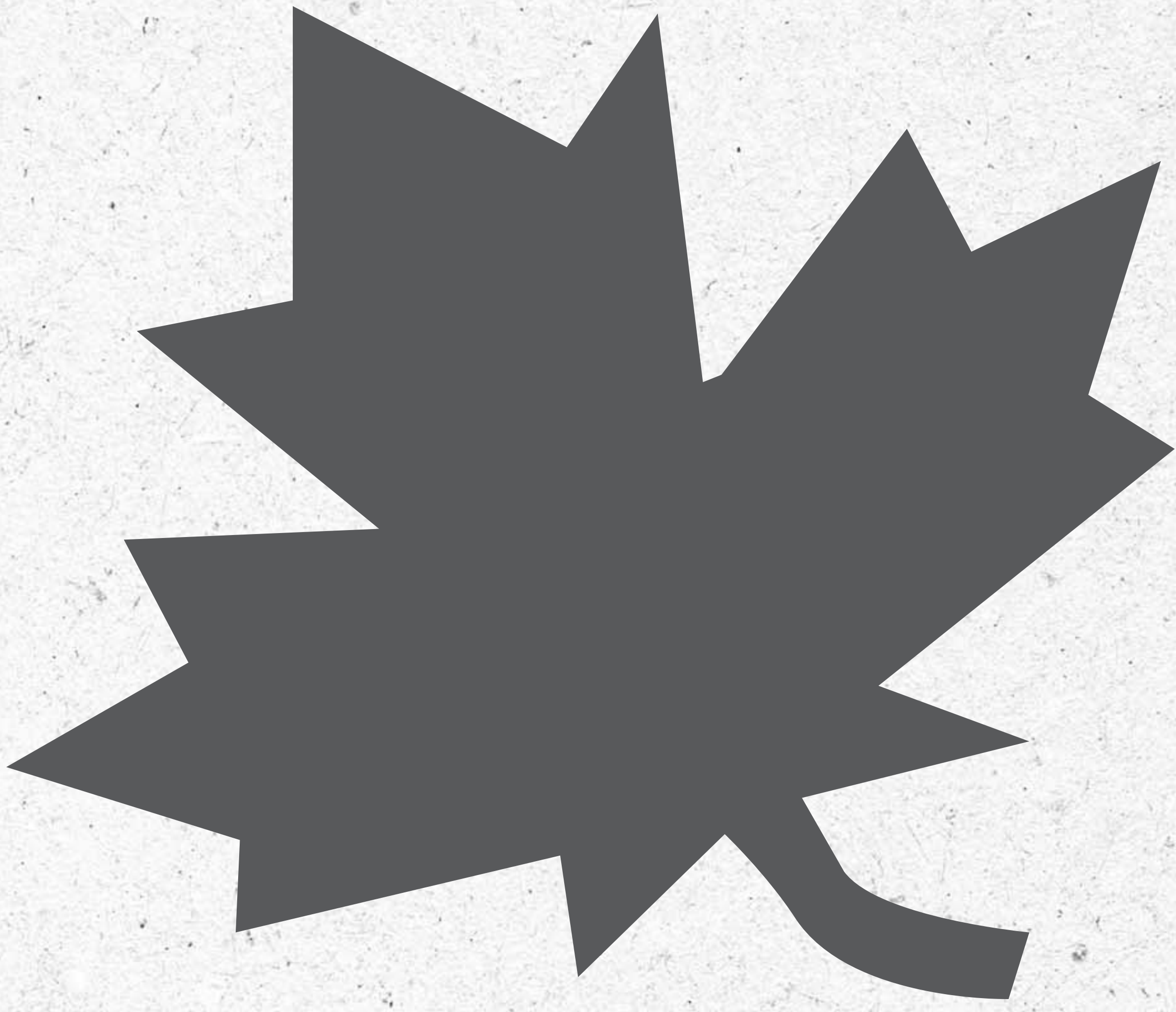
You engage the RISCO Group to provide security management.

You put the SSID and password for the secure WiFi on a screen in your Network Operations Centre (yes really).

Someone takes a photo of an official standing in front of the screens and publishes it in the media along with the username and password:

SSID: WORLDCUP
Password: b5a2112014 (brazil2014 get it)

Which just goes to show, you can have all the systems in the world, but you can be let down badly by simple controls – no photography in the security centre, let alone having it up there for all to see on a big screen. Honestly.



AUTUMN

OCTOBER - DECEMBER 2014

MAIN THREAT

MICROSOFT, BIGGER AND BETTER THAN SHELLSHOCK AND HEARTBLEED, CRITICAL CALL TO ACTION

THREAT #1

SANDWORM VS POODLE

THREAT #2

HOW MUCH IS THAT DOGGY IN THE WINDOW, THE ONE WITH THE WAGGLY TLS?

THREAT #3

OLÉ! FINALLY, AN INTERESTING POWERPOINT PRESENTATION

THREAT #4

END OF SCHOOL REPORT FOR ITC THREAT OF THE WEEK

MAIN THREAT

MICROSOFT, BIGGER AND BETTER THAN SHELLSHOCK AND HEARTBLEED. CRITICAL CALL TO ACTION

Like death and taxes, bugs in Microsoft software are a grim inevitability. Exacerbated by end of support software (watch out for Server 2003 in July 2015) and with armies of script-kiddies ready to pounce, these pose a real headache for long suffering sysadmins and security teams.

It looks like Google are starting to add fuel to the fire with their recent disclosure of a privilege escalation issue, which they reported to Microsoft 90 days previously and did not wait for a patch to come out. With friends like these...

Effective patching including emergency patching, alongside vulnerability management and accurate asset data are essential tools which need to be fed and watered appropriately to stay on top of this potential nightmare scenario.

If we were to tell you that any one of your domain users could become Admins without the Admin password, you probably wouldn't believe us. But it appears to be true. Microsoft released a critical update to fix a bug in the Kerberos processing of nearly all Windows releases, a bug which enables an attacker with domain credentials to become an Admin, or in fact assume the identity of ANY other user without a password.

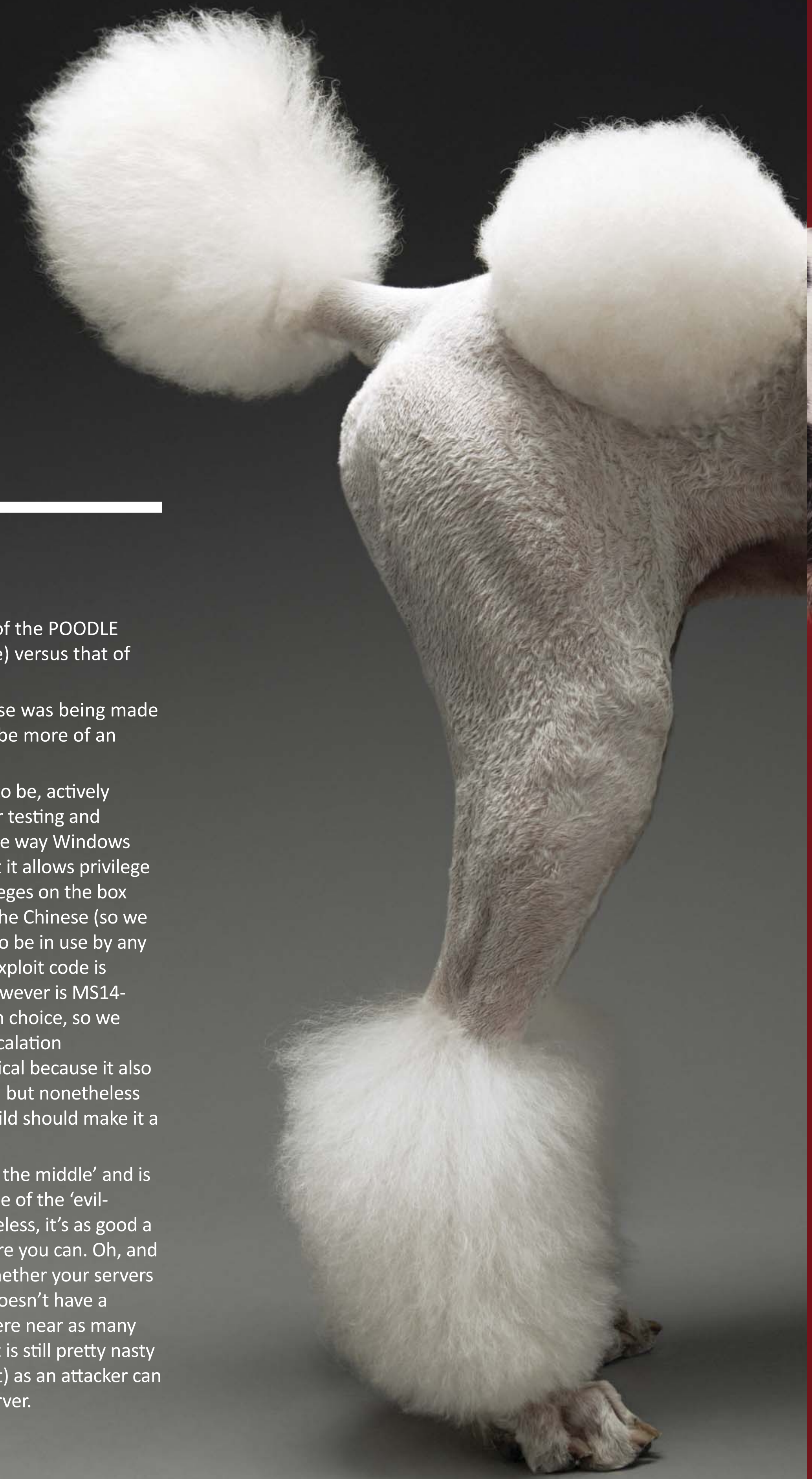
This is NOT April 1st, we aren't kidding and if your mouth has just gone dry and your hands have started shaking, that's a very good start.

You will notice this is bad, really bad and that it affects most of the stuff you are running. The only redeeming factor is that only users with domain accounts can do this, and of course you know and trust every user with a domain account on your system, don't you?

You must apply the update as soon as you can. This is currently being exploited in the wild and all the script kiddies and wannabe hackers (the ones with that live with their Mum especially, you know who these people are) are all over this like it's the last slice of pizza on the planet.

Microsoft's remediation advice makes for very chilling reading, so please get on with the updates before this becomes necessary: **'The only way a domain compromise can be remediated with a high level of certainty is a complete rebuild of the domain'.** No biggy, then.

By the way, our money is on this being a little backdoor for Microsoft's friends in Washington DC, but we wouldn't put our lives on it. Either way we know all of you have patched against it, haven't you?



THREAT #1

SANDWORM VS POODLE

This report discussed the potential impact of the POODLE vulnerability (which impacted old Unix code) versus that of the Sandworm (Microsoft) vulnerabilities.

The conclusion was that although more noise was being made about Poodle, the Sandworm issues would be more of an issue if left unpatched.

Two issues in particular were, and continue to be, actively exploited and should have been a priority for testing and deployment. MS14-058 is concerned with the way Windows handles fonts and is particularly nasty in that it allows privilege escalation (i.e. you can get local admin privileges on the box with this one). It's been used in the wild by the Chinese (so we hear) in targeted attacks, but doesn't seem to be in use by any wider audience just yet. The one for which exploit code is definitely kicking around on a wider scale however is MS14-060, aka the 'Sandworm' exploit (the Russian choice, so we hear). This one doesn't have the privilege escalation component and Microsoft only rate it as Critical because it also involves user interaction (i.e. opening a file), but nonetheless the fact that it's more prevalent out in the wild should make it a priority for desktops in particular.

POODLE requires an attacker to be a 'man in the middle' and is thus relatively hard to actually pull off outside of the 'evil-hotspot' public WiFi type scenarios. Nonetheless, it's as good a reason as any to finally switch off SSLv3 where you can. Oh, and whilst you're doing that, be sure to check whether your servers are vulnerable to CVE-2014-3513 (this one doesn't have a catchy name yet). This doesn't affect anywhere near as many versions of OpenSSL as HeartBleed does, but is still pretty nasty as an effective DOS (Denial Of Service exploit) as an attacker can cause memory exhaustion on an affected server.

THREAT #2

HOW MUCH IS THAT DOGGY IN THE WINDOW, THE ONE WITH THE WAGGLY TLS?

There are some nasty issues dealt with by Microsoft this month (December 2014). Yet more privilege escalation issues, including another vulnerability in Visual Basic. How long will it be before we find out that you can become a domain Administrator by typing XYZZY into notepad? (If you got that joke, you are old!)

You might remember the POODLE vulnerability. Hot on the heels of the big bad boys ShellShock and HeartBleed it's a vulnerability in SSl 3.0 which enables a dog-in-the-middle attack to decrypt your stuff.

'So what?' you cry, 'we've disabled SSl 3.0 and are using the more funky TLS stack exclusively'. Bad news, I'm afraid, TLS v1.2 is also vulnerable to a very similar exploit designated CVE-2014-8730.

'Yeh, yeh but these dog-in the-middle attacks require well, err a dog in the middle don't they?' Yes they do. Have you ever been to Dubai, or China, or Iran, or the USA or even Brentford? There are dogs-a-plenty, as revealed in exquisite detail by Mr Snowden.

We recommend that you test your websites using this brilliant tool from our friends at Qualys:

https://www.ssllabs.com/ssltest/ If you are vulnerable apply your vendor's patch, which they will have out either now or very shortly we would hope.

THREAT #3

OLÉ! FINALLY, AN INTERESTING POWERPOINT PRESENTATION

After years of boring everyone to tears, the worm has finally turned, PowerPoint officially went rogue. Power with a Point to prove, scary.

So scary in fact that Microsoft released an advisory about a bug in the Object Linking and Embedding (OLE – see what we did there?) library – the code that sometimes (on your birthday maybe) lets you embed Excel Spreadsheets in PowerPoint spreadsheets and Word Documents hassle-free.

Obviously this wasn't the first vulnerability against OLE; however this zero day is being exploited right now out in the wild. Attackers can run code on your machines at will and at the same level of privilege as the exploited user (at least).

Microsoft recommended some actions before they patched the issue. These included a workaround and a recommendation to not open PowerPoint files from untrusted sources (like your boss). Additional workarounds include deploying User Account Control or the enhanced mitigation experience toolkit, which seem severely onerous in an Enterprise environment.

THREAT #4

END OF SCHOOL REPORT FOR ITC THREAT OF THE WEEK

Wow. A year went by in a whirlwind of hacks, cracks and fracks.

At the end of last year we made some predictions about what would happen in the security world. Let's take a moment to see how we did in the second half of the year.

Malware: Malware, especially mobile malware is rife. In September, Alcatel-Lucent reported that 15 Million mobile devices (mostly Android) were infected with malware. As for Malware targeting desktops, laptops and servers, according to all industry analysts the trend is only going to be upwards, so get used to it.

Cryptolocker: Symantec reported a 700% increase in Cryptolocker in 2014. Enough said. The fact that the delivery comes hand in hand with the Zeus credential stealing botnet means we must remain vigilant when opening any links from people we don't know, mustn't we? (You know who you are).

Windows XP exploits: It seems that most sensible people have now upgraded from XP. Hallelujah.

Enterprise private clouds: BOOMING!

Behavioural based security: From the McAfee Network Threat Behaviour Analysis product, through Veracode's mobile behavioural analysis to Alien Vaults 'behavioural monitoring', the hype builds and real results may follow. LinkedIn Users have been targeted by Phishing attacks after breaches.

Mobile Security increasingly provided by vendors of device or OS – Compartmentalization and security features, such as always on VPN (based on IKEv2) are features of Windows8.1, iOS8 and Android Lollypop. This is only going one way.

The message remains clear. Malware and information security breaches are becoming more mobile, more targeted, more accurate and more effective. You have little chance of identifying or dealing with attacks using point technologies, let alone understanding your risk profile.

IN SUMMARY

It is clear that attacks are becoming smarter and also inevitable. The bad guys will be analysing your business processes for weaknesses, as well as your technology, and you should be doing the same.

What are your crown jewels? Which of your assets deserve the highest level of protection? What would you do if they were compromised in any way?

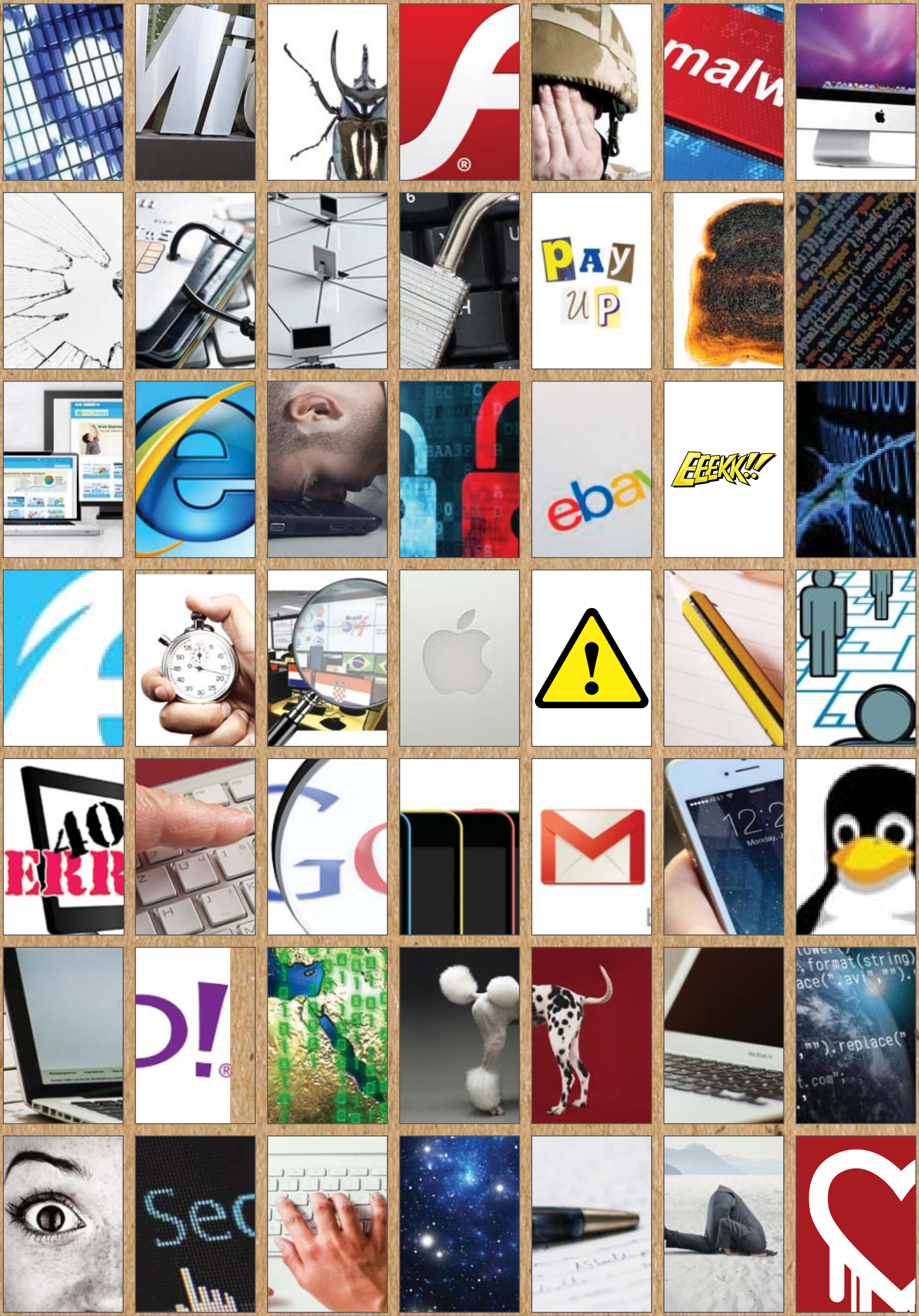
2015 should see the introduction of compromise planning as part of business continuity. Likely incidents should be analysed, with a 'playbook' prepared in case should they occur. The playbook should be ready, up to date and above all tested.

**We will continue to keep you abreast of security developments in 2015 through our Threat Of The week blog, by direct communication with our customers. We will be using our Threat Intelligence services and partners to ensure that this years' Threat of the Week blogs maintain our impressive record of accuracy and timeliness.
We wish you well.**

- **Consider analysing your business processes for weakness – because the bad guys will.**
- **Think about common / likely types of incidents – do you have the capability to spot them**
- **Prepare your 'playbook' should an incident or breach occur – prepare and test it**

"PLANS ARE WORTHLESS, BUT PLANNING IS EVERYTHING"

WINSTON CHURCHILL



ITC
SECURE NETWORKING

Threat of the Week 2015
www.itcsecure.com/itc-security-threat-of-the-week/