

THE MAGAZINE OF THE BCS SECURITY FORUM

iSNOW

AUTUMN 2010

www.bcs.org/security

WHO ARE WE FIGHTING?

Dealing with threats is one thing,
finding them is another

bcs

The
Chartered
Institute
for IT

06 CYBER CRIME WORLD TOUR

How one email about a watch caused a chain of events that went around the globe.

14 THE ART OF THE BLAGGER

Social engineering isn't always something that IT systems can stop, it's more of a people issue.

EDITORIAL TEAM

Henry Tucker Editor
Brian Runciman Managing Editor

PRODUCTION TEAM

Florence Leroy Production Manager

Advertising

E catherine@atalink.co.uk
T +44 (0) 20 7074 7921

Keep in touch

Contributions are welcome for consideration.
Please email: editorialteam@hq.bcs.org.uk

ISNOW is the quarterly magazine of BCS Security Forum, incorporating the Information Security Specialist Group. It can also be viewed online at: www.bcs.org/isnow

The opinions expressed herein are not necessarily those of BISL or the organisations employing the authors.
© 2010 British Informatics Society Limited (BISL). Registered charity no. 292786.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; BISL copyright notice and the title of the publication and its date appear; and notice is given that copying is by permission of BISL. To copy otherwise, or to republish, requires specific permission from the publications manager at the address below and may require a fee.

Printed in the UK by Interprint, Swindon, Wiltshire.
ISSN 1752-2455. Volume 5, Part 1.

The British Informatics Society Limited
First Floor, Block D, North Star House,
North Star Avenue, Swindon, SN2 1FA, UK.
T +44 (0)1793 417 424
F +44 (0)1793 417 444
www.bcs.org/contactus
Incorporated by Royal Charter 1984.

WHO ARE WE FIGHTING?



04 ISSG PERSPECTIVE

Gareth Niblett, Chair of the BCS ISSG, gives his view on cyber warfare.

06 CYBER CRIME WORLD TOUR

How one email caused a chain of events that went around the globe.

08 WEB ATTACK

Despite all the possible threats the internet is still the biggest source of risk.

10 SECURITY COLD WAR

How advanced persistent threats are something of concern for everyone.

12 HACK OR YOUR MONEY BACK

Modern cybercrime is big business and some tools even come with guarantees.

14 ART OF THE BLAGGER

When it comes to social engineering, IT security systems can't stop everything.

16 LEGAL

A look at security issues companies should address with cloud computing.

18 OPINION

Knowing who your enemy is and finding them are very different things.



WAR ON CYBER TERRORISM

Gareth Niblett, Chair of the ISSG, addresses the issue of cyber warfare and says we should question the motives of those who routinely raise the subject of cyber terrorism.



For a number of years there has been concern about the growth of state sponsored cyber espionage and warfare. It is believed that around 100 nations have such capabilities. Although we occasionally see news stories about the alleged activities of particular nations, attribution remains a significant challenge and most countries are looking at improving their defensive capabilities.

The UK has formed an Office of Cyber Security (OCS), to complement the Centre for the Protection of National Infrastructure (CPNI), and NATO has established the Co-operative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia, after the country was subjected to cyber attacks.

Recently it was suggested that NATO conduct joint cyber warfare exercises with Russia so that all countries can learn how to better protect critical information infrastructure. Exercises have already happened between the US, UK and others.

Beyond state sponsored activities, which seem to focus on information gathering, mapping defences, disinformation and occasionally attacking, politically and religiously motivated 'hactivism' occurs, but rarely gets beyond website vandalism and DDoS attacks, which can claim collateral impacts.

Add to this the traditional malware, spamming, hacking and commercial piracy that is so prevalent online and it is no wonder that law enforcement, such as the Police Central e-crime Unit (PCeU) in the UK, has issues with resourcing and

priorities and so many crimes fail to be reported, investigated or solved.

One thing missing from this mix is the almost always mentioned, almost never seen, cyber terrorism. My view is that unless it is visually impactful or used in support of a physical attack, this will not materialise to the level claimed by the scaremongers, whose motives should sometimes be questioned.

Gareth Niblett is Chairman of the Information Security Specialist Group (ISSG).

www.bcs-issg.org.uk

FURTHER INFORMATION

Information Risk Management and Assurance Specialist Group:
www.bcs.org/groups/irma

BCS Security Portal:
www.bcs.org/security

ISNOW online:
www.bcs.org/forum/isnow



CYBER CRIME WORLD TOUR

Mike Small CEng FBCS CITP describes how the analysis on one spam email by a security researcher at CA Technologies revealed a network of cooperating cyber criminals and fraudsters stretching across three continents.

Spam is an irritating annoyance to individuals and can be a major problem to organisations because of the volume they receive. However, spam is more than just an irritation, it is a tool used by criminals worldwide to lure potential victims to part with their money and personal details.

The email

Security researcher Mark Wade works in an office in Herndon, Virginia, just outside of Washington DC in the USA. He is one of the many unseen IT professionals who work for IT security vendors. His job is to identify potential threats and make sure

that CA's products provide protection from these threats before they do damage. He was looking through the emails that had been trapped by his spam filter and one in particular caught his eye. This was entitled 'Dreams can cost less repl1ca w4tches from r0lex here'. It is interesting to note how the author of this email substituted numbers for letters in an attempt to make it more difficult for the spam filter to detect suspicious words like watch and Rolex. This is part of the escalating arms race between cyber criminals and the IT security industry.

So who sent this email? Looking up the

domain of the sender led to a small church in Washington State and the website of this church identified the sender as the Pastor's Assistant. It seems unlikely that the sender was really the Pastor's Assistant. It is almost certain that her PC had been infected with some kind of malware that was being used to send the spam emails. This is a common method used by criminals who control a large network of infected PCs to provide a service to deliver large numbers of emails for a price.

The website

The email contained a URL linking to a

website selling watches. In fact there were a number of similar emails caught in the spam filter each from different senders and containing slightly different URLs. According to the tool whois.net the websites were all registered in China with the owner having the same name as a Chinese film star recorded in Wikipedia. Not all the websites were active – it is common for fraudulent websites to be active for very short periods of time. Just long enough to take some money before the IT security monitors around the world notice and take action against them. It also makes it difficult for victims to retrace their steps when they have been defrauded.

The actual presentation of the website was very professional. There was a shopping cart built into the site, a privacy policy, a testimonial section and a Contact Us link. The About Us link claimed that the company had a four-year track record of being the #1 online retailer. There was a raving testimonial from a customer identified as Sara Berry. Examination of the website source code revealed no hidden threats of malware. According to the privacy policy the website used SSL (secure socket layer), which encrypts traffic over the internet.

The purchase

Mark decided to buy a nice pair of earrings for \$59 plus \$29 shipping. Mark used specially created email account and a pre-paid cash card – a smart move to minimise risk when using a suspect website. During this purchase Mark had a packet sniffer running on his PC. This showed that, in spite of the claim that SSL was used, all the payment card details as well as his personal details were sent in plain text over the network.

Confirmation email

Following the purchase an email was received confirming the order and thanking Mark for his purchase. The confirmation even provided an email address to contact if needed further help was needed.

Using Whois.net to check the domain from which the confirmation email had been sent led to an organisation registered in Las Vegas, Nevada. Using a Google search on the name of this organisation returned a warning referencing a database of Fake Sites. Telephoning the City of North Las Vegas established that the address that was listed in the Whois.net database was false. The company had gone into default in April of 2007. The head of the company was a resident of Seattle, Washington and had been accused by the Department of Financial Institutions Securities Division of running several fraudulent financial websites that had

Looking up the domain of the sender led to a small church in Washington State and the website of this church identified the sender as the Pastor's Assistant.



Using Whois.net to check the domain from which the confirmation email had been sent led to an organisation registered in Las Vegas, Nevada.

tricked large numbers of people into sending in money. Over \$2 million dollars had been seized by Las Vegas police.

So who got the money?

Examining the cash card account showed a debit of \$77 mentioning the vendor and giving the phone number of a company registered in Nicosia in Cyprus. The earrings had still not arrived so after calling the number five or six times it was finally answered and tracking information for the shipment of the earrings was provided. According to the shipper's website the earrings had been dispatched by air from China to Herndon, Virginia. Of course the earrings never arrived.

Criminal World Wide Web

This shows how criminals are cooperating across the world to use the internet to

perpetrate fraud and commit crimes. Researchers in the IT security industry, like Mark Wade, and IT security companies, like CA Technologies, form the first line of defence against these criminals.

The full story of this analysis can be found here:

<http://community.ca.com/blogs/securityadvisor/archive/2007/10/23/operation-greendot-following-the-spam.aspx>

About the author

Until 2009, Mike worked for CA where he developed CA's identity and access management product strategy. He is a frequent speaker at IT security events around EMEA and contributor to the security press.

For more articles go online to: www.bcs.org/articles



WEB ATTACK

Peter Komisarczuk CEng MBCS, Professor of Computing, School of Computing and Technology, Thames Valley University explains that when it comes to malware the web is still the prime source of risk.

The web is a key means of attack for organised crime. Recent figures indicate around 1 in every 150 websites is compromised (i.e. has been subverted in some fashion) and acts maliciously to attack the systems that browse to them. Web-based exploits are currently the fastest growing attack on the internet with around 0.24 per cent of websites advertising at least one compromised webpage based on a Microsoft study published in December 2009. Other sources show higher infection rates, for example Kaspersky Labs identified almost 120 million servers in the first quarter of 2010 of which 0.64 per cent were malicious.

These web servers typically deliver what is called a 'drive by download' which is an exploit that occurs, for example, when your web browser or other web application visits a web page or artefact such as a QuickTime video clip. Your browser can receive malicious content, which is usually obfuscated to avoid detection and attempts to compromise the users system. For example, a key-logger program could be installed without the users permission in order to gather sensitive user name and password data.

Web servers can be compromised by a variety of means and can continue to be malicious for some time, even though the

exploit itself may have completed its life cycle. A recent study from AVG indicates that these compromised sites can be active for as little as 24 hours, although the server itself may not be cleaned up by system administrators for some time. The attackers deploy exploit kits such as the well-known Mpack server-side PHP-based malware kit that can be purchased over the internet. It is sold commercially, with support and regular updates and can be offered with professional services for bespoke attack or obfuscation features. The hosting web server is often just one part of an attack that can be made up of several exploit servers working together using

redirection. Furthermore the exploit servers used can be changed to avoid detection and countermeasures.

Once servers are compromised the attacking organisation can develop campaigns to target certain exploits and groups of victims. The compromised web server is set to craft exploit code targeted to the client system based on the browser and operating system data passed as part of the HTTP exchange. The attack tests various vulnerabilities looking for a means to intrude and deliver malware. Once delivered the user's system is exploited for the organisation's goals to be fulfilled.

Dead famous

Other attack vectors are well developed such as the use of social networking to spread links to compromised web artefacts. For example malicious spam can advise us of the death of some celebrity and recently web surveys have been used to entice victims with the promise of winning a gadget. Web content is also being specifically developed to target users of search engines, for example content is crafted based on the top search data from Google. The crafted content is created and put up on the web and its ranking manipulated so that victims searching for topical content are able to easily find the attackers content.

As hinted at above there are many cycles involved in this web malware jungle. The attack itself can be very short lived; it can be targeted specifically, using social networking, spam and highly topical content. These are often quite short life cycles requiring a large-scale rapid detection mechanism to discover, study and counter threats. The after effects can be long lived, with the compromised user systems forming part of a botnet that can live and grow for months.

Anti-virus vendors such as AVG and Kaspersky, provide solutions for end users to protect against drive-by-downloads. For example, the linkscanner from AVG currently has 110 million deployments acting as a large internet sensor, which identifies online threats. Search-Shield scans search results from Google, Yahoo, MSN, etc. to provide a safety ranking for websites. Search engines such as Google and Bing provide a ranking system for websites and Google provides an API through which third parties can ask whether a particular website is malicious or not.

The web servers and artefacts can be specifically developed and deployed for an attack or can compromise existing servers and content. Behind these are a shifting set of exploit servers that can change rapidly. Various projects or services, such as HoneySpider run by the Dutch, Polish

The attack space has widened further with the availability of smart phones with capable browsers and rich featured operating systems.



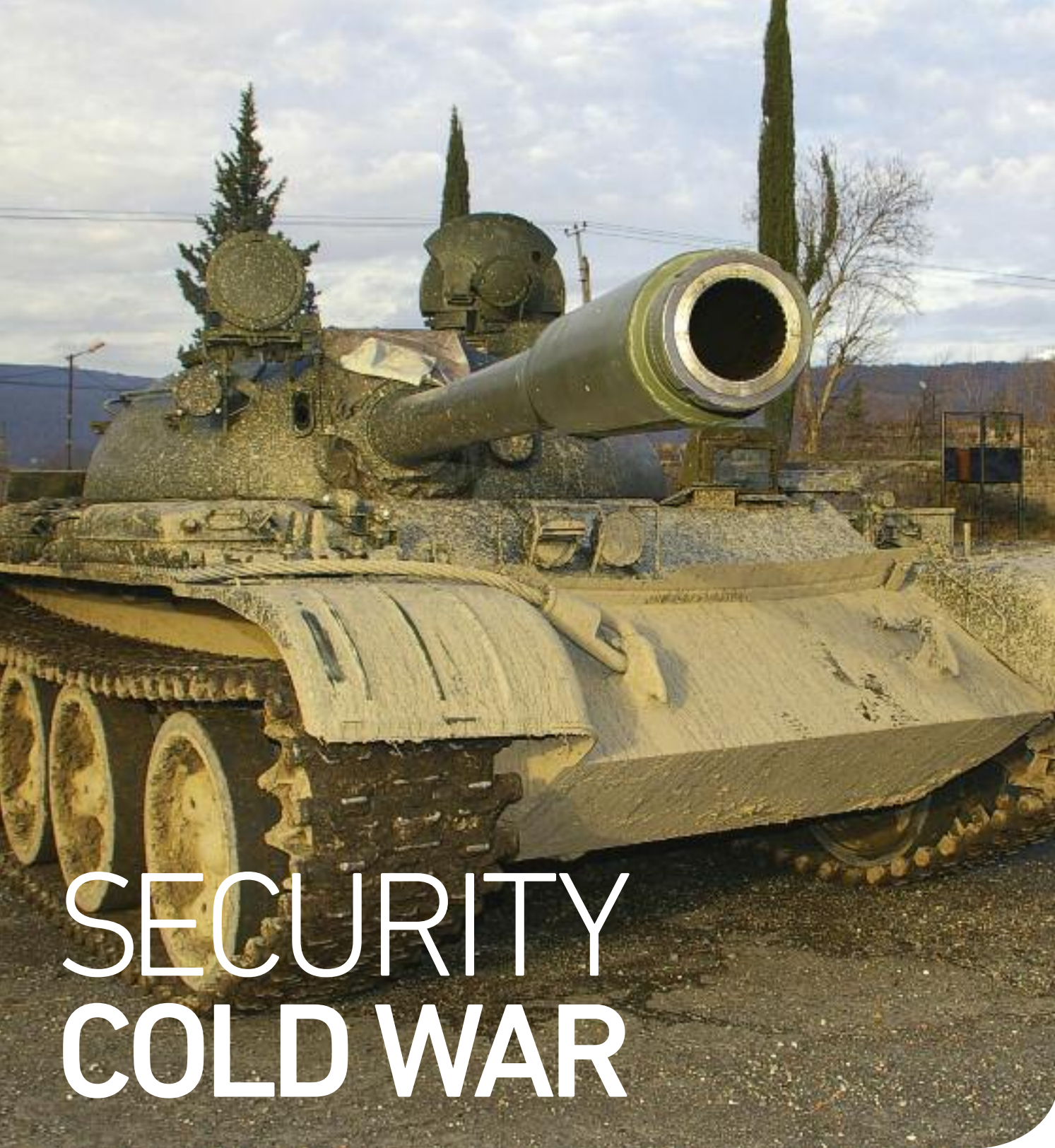
and Norwegian CERTs routinely survey their clients to detect for signs of malicious activity so that system administrators can clean up their systems. The malicious nature of the content can be detected in various ways and used to create blacklists, provide feedback in web search results or website rankings to web users. However, some exploited web pages remain compromised for long periods and are simply inactive because the exploit servers have been redeployed, rather than the attackers cleaning up after their attack.

The user and their computer system is also a moving target. The attacks are based on exploiting some vulnerability in applications and operating system and often the attack is done through a web browser and its helper or plug-in applications. These components have their own development, patch and upgrade cycles that counter various attack vectors, whilst the attackers seek new means to exploit their prey. In recent years there has been an explosion in the number of browsers in widespread use causing more

work for the attackers. For example in June 2010 Firefox was the most popular browser, with 46.6 per cent of the market but the browser space includes significant deployment of IE 6, 7 and 8, and Chrome. New browsers have developments to provide greater security whilst browsing, such as sandboxing and cross-site scripting mitigation techniques. Likewise the number of host operating systems deployed by users has changed over time, however, Microsoft Windows XP still makes up 56.4 per cent of the measured systems in June 2010. The attack space has widened further with the availability of smart phones with capable browsers and rich featured operating systems.

The drive-by-download continues to be an expanding threat making the web a dangerous place but countermeasures from anti-virus systems to search engines and application development cycles are playing their part in fighting the problem.

For more articles go online to:
www.bcs.org/articles



SECURITY COLD WAR

One of the biggest security risks to businesses and individuals are advanced persistent threats according to **Joe Hancock**, Senior Consultant, Information and Technology Risk at Deloitte.

Some people refer to the current state of threats as a 'cyber cold war' or as an arms race likening the challenges we face now as security professionals to those faced when dealing with the international threats of the 20th century.

What started out as hobbyist hackers accessing systems for the thrill of the act itself quickly moved to criminal enterprises with lucrative global markets to the now state and organisation sponsored advanced persistent threats.

As technological capabilities advance to

protect our electronic and physical information assets so do the capabilities of those who have a need to access or disrupt them for gain.

When business models began to move to better leverage technology, information became a tangible asset to be bought, sold and used. With its increase in tangible value the threats against it grew and adapted.

Criminals began to exploit the interconnected nature of the internet evolving acts such as extortion and protectionism in new ways. If you can't

extort money by threats to physically prevent a shop or business trading because its customers are now online, can you make money from denying them access to it electronically?

Electronic lives

This threat evolution has continued as society has moved almost totally online and has begun to use electronic means to carry out every aspect of our daily lives.

The criminal world also began to use electronic means to attack end users,

exploiting lack of awareness and technical know-how coupled with the increased reliance on technology to directly target end users for financial gain.

Criminals today have a sophisticated economy of service providers and high tech expertise to fully take advantage of their current targets. A threat that was once focused on single criminals is now focused on major organised crime crossing international boundaries and jurisdictions.

Hidden threats

Alongside this threat maturity has been a more hidden class of threat that many would not have been exposed to previously. These threats are an information technology aware trend in state sponsored and supported espionage and intelligence that has always been a problem in its more traditional form to the manufacturing and defence industries.

Given the name advanced persistent threats, these are becoming a major issue for many business and industry sectors today.

There is now more than circumstantial evidence of a new threat model emerging for both the criminal and intelligence exploitation of systems containing information of economic, defence and intelligence value.

This new class of threat is distinct and by breaking down the terms used to describe these threats we can clearly see the themes that underpin this new model.

Advanced

These new threats use advanced technical attacks including 'weaponised' versions of system exploitation code often used very close to their exposure date if not before it is even identified.

Persistent

Once access has been gained to a system the attackers will covertly maintain a presence in the target system and exfiltrate information over a period of time taking steps to avoid detection.

Threats

Neither the attacks are random nor the information assets targeted. The sources and types of information attacked are chosen deliberately based on their perceived value for commercial, economic or intelligence gain.

A major part of these new threats is the support network behind them – command and control channels for malicious software are becoming increasingly sophisticated and complex challenging a defender's ability to detect and remove the threats once installed.

What can defenders do to prevent these

As an industry we need to see a move to designing and building secure systems that are easily and safely used as well as raising user awareness to what threats are present.



A major part of these new threats is the support network behind them – command and control channels for malicious software are becoming increasingly sophisticated.

attacks or to eradicate them once found? In my opinion no new solution is needed – implementing good security practice at every step of the business and technology process involved will lessen the chance of a threat being realised if it is detected and reacted to quickly.

In the home

The same solutions apply to home users. As an industry we need to see a move to designing and building secure systems that are easy and safe to use as well as raising user awareness to what threats are present and how they can prevent

themselves becoming a target.

Once security concepts become embedded in both our business and personal lives the arms race will undoubtedly continue but with defenders perhaps leading the field. It may even push these attackers into another unprotected area of our business and personal lives.

The next step is not to predict the new threats but the targets they will be looking to access.

For more articles go online to:
www.bcs.org/articles



HACK OR YOUR MONEY BACK

Exploit kits can be easily bought online and in some case even come with a money back guarantee, says **Michael Montecillo** Senior Threat Analyst at IBM Security Services.

For decades information security professionals have been engulfed in battle with anonymous adversaries referred to as hackers. These hackers had long been influenced by the mystique of computer intrusion and sometimes an innocent and curious mind. Unfortunately, this computer hacker environment has largely fallen by the wayside. Today's maliciously minded hacker has shed the mystique previously associated with computer intrusion and the innocence of curiosity in lieu of monetary

profit. Malicious hackers are no longer fueled by curiosity or technical prowess but rather by the competitive edge of business.

In place of the basement hacker bragging about the number of systems their virus was able to infect are profitable underground businesses. As a direct result, a new market for malware creation software, often referred to as exploit kits, has emerged. The majority of malware and virus outbreaks in the world today are no longer generated by individual hackers but

rather manufactured by malicious software kits vendors. This software is later used by these vendors' customers for nefarious purposes including fraud and government sponsored information thievery.

Exploit kits

Additionally, the availability of software capable of creating highly effective malware allows less knowledgeable, less technical criminals to wreak havoc within IT infrastructures. Exploit kits, also

sometimes referred to as crimeware, such as Mpack (\$1,000), Icepack (\$700), Neosploit (\$1,000), Fragus (\$800), Phoenix Exploit Kit or the Eleonore Exploit Kit (\$599) can all be purchased in underground markets. Many researchers have cited exploit kits such as these at the heart of all too familiar botnets such as the Zeus Botnet (zBot).

Malware tech support

Each one of these commercial exploit kits is supported by increasingly sophisticated organisations that in some cases offer technical support and guaranteed effectiveness for their malware creation software. In fact, the sophistication of the Fragus malware kit is such that the authors actually offer customers version updates to increase the effectiveness of evading security countermeasures such as anti-virus solutions. In addition, global communities have arisen to allow users of malware kits to discuss the effectiveness and support of particular exploit kits.

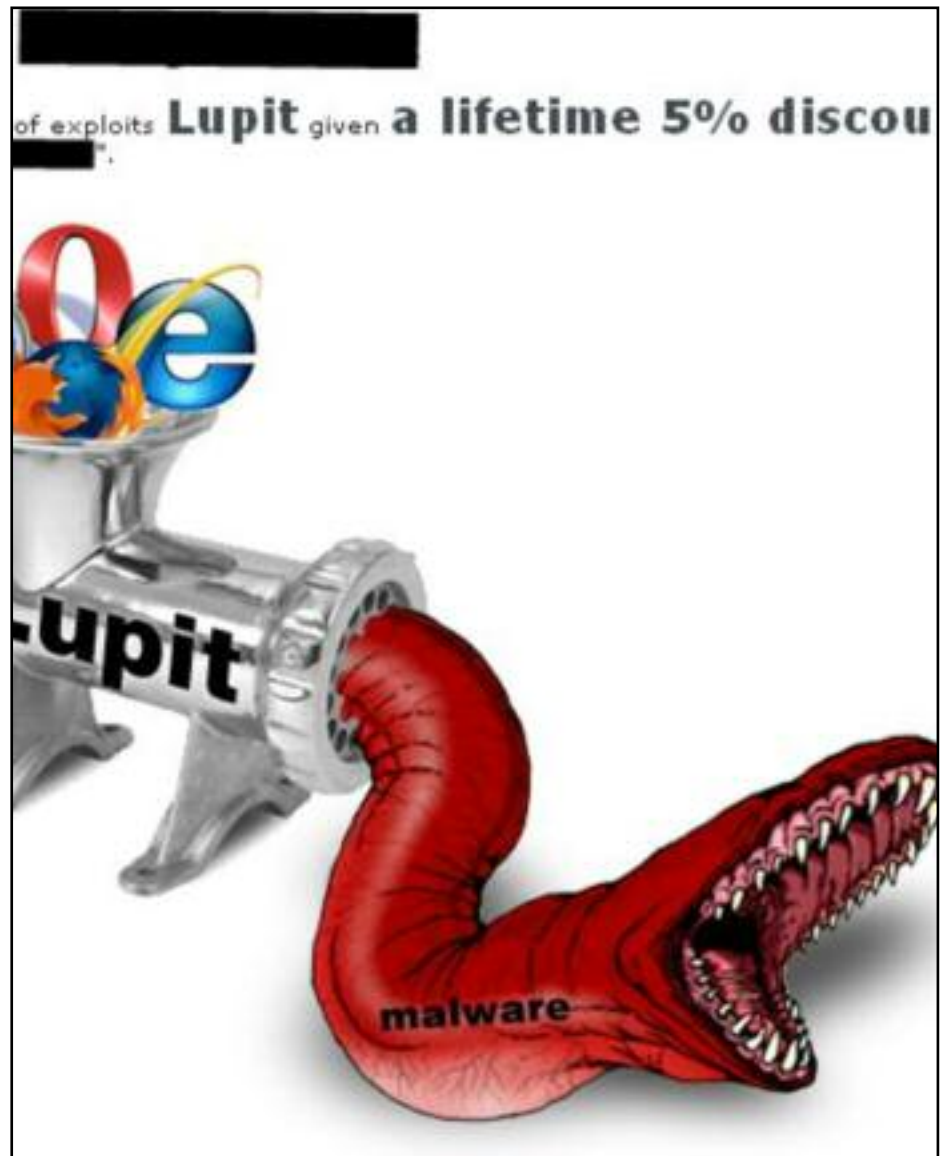
In one example, the Lupit Exploit pack actually offers potential buyers a coupon code for receiving a discount price on the malware kit.

For the security professionals attempting to thwart attacks backed by exploit kits, the increasing popularity and quality of the kits themselves signals a troubled future. The use of a kit to create effective and constantly evolving malware functions as a force multiplier for attackers. In other words, the number of issues and the amount of damage that can be caused by the malware is amplified by the relative simplicity of its creation and spread. This causes a severe imbalance between the amount of investment required to damage a business via computer intrusion and the amount of investment required to protect a business from computer intrusion. This imbalance translates to higher security costs and by extension higher business operating costs, which of course has a direct effect on any business's overall revenue.

Sharing the burden

There is some hope for security professionals in the growing maturity and heavier adoption of consolidated security strategies, such as those supported by managed security service providers (MSSPs). These security strategies share the burden of security investment across multiple organisations in order to create a unified front against the rapidly rising tide of highly effective kit created malware. In addition, these strategies also create a force-multiplier for security professionals by pooling together some of the best talent in the security industry to allow them to effectively apply their knowledge across

In one example, the Lupit Exploit pack actually offers potential buyers a coupon code for receiving a discount price on the malware kit



thousands of environments as opposed to focusing on a single entity. This reduces the timeframe with which a piece of malware can operate and ups the ante in the arms race between attackers and defenders.

Many organisations are already reaping the benefits of a unified approach to security strategies. However, there are still a large number of businesses who have not even begun to explore the possibility. In order to better combat the emerging market for exploit kits, it is imperative for businesses to offset investments into malicious software with an investment into effective security capabilities. In particular every organisation with a stake in IT security must make an investment in creating a unified front against the

increasingly sophisticated threat environment. Without this type of unification businesses will be forced to take on increasing costs in creating effective security strategies alone. It is in this type of environment, where there exists little or no ability to reduce the costs of an effective IT security strategy, that exploit kit vendors are poised to thrive. Until the vast majority of businesses are properly leveraging the benefits of a unified approach to IT security, trends in the maturing market for exploit kits are doomed to continue.

For more articles go online to:
www.bcs.org/articles



THE ART OF THE BLAGGER

One morning a few years ago **Ralph O'Brien** MBCS of IT Governance Ltd walked into a police station and easily walked back out again with some very sensitive information, without going past reception.

Of course this was ethically done, with agreement from all concerned. But as an information security professional you would think that I utilised some sort of hi-tech attack on the corporate network to steal information via the latest IP spoofing or crafted Trojan attacks. But the truth is I've always found it much easier to rely on getting the staff to do my work for me. To simply ask for the information I need, a bit at a time, until I have enough to potentially access anything I need. Simple. The weakness is ordinarily never the automated IT systems themselves, but the people who use them, operate them and have legitimate information access.

Social engineering is a common term with many definitions. As an avid watcher of BBC's *Hustle* and C4's *Derren Brown*, I can't help but compare social engineers, or people who 'blag' information over the phone, to con-artists, grifters or simply students of human psychology and neuro-linguistic programming. For what this subject is really about is the abuse of human trust and of their desire to help their fellow man.

Reliance on IT security

Whilst it is never unwise to invest in IT security, the problem with this approach is it simply isn't holistic enough. Unfortunately

you have to trust somebody – people. These people you give legitimate authorised access to. And unfortunately 99 per cent of people are too easily conned. Perhaps the most famous social engineer is Kevin Mitnick - a 'phreaker' (person who uses the phone and phone exchanges to commit fraud and gain access). He is now a well respected 'poacher turned gamekeeper' in this field after being caught carrying out high profile attacks on US defence and central government organisations. His famous quote from Security Focus sums it up well.

'You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable

to old-fashioned [human] manipulation.'

In fact the over reliance on IT security and its' disconnect from the business can sometimes be a great asset to the social engineer. Often pretending to be someone who is from the IT department, or even in need of IT support can be the most effective tool in their arsenal.

Unauthorised access

The basic goals of the social engineer are the same as for all hackers in general. This is to gain unauthorised access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.

Typical targets will include telephone companies and answering services, big-name corporations and financial institutions, public services, legal and research. Particularly vulnerable are call-centres and customer facing roles, where the role is based around access to information and the desire to help is strong.

Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of an easy and natural relationship.

The psychology of persuasion

So let's return to my example of the ethically agreed attack on the police HQ.

I dressed in a smart, but not stand out, business suit, and carried a laptop case. On arrival I approached the public reception area and asked for the chief constable and/or the head of IT, names of whom I had researched earlier on the internet and via phone. I watched the receptionist actually physically 'switch on' at the mention of the chief. I then claimed to be an hour early for the meeting, "so please don't disturb these busy and important people yet". Instead I was looking for somewhere I could quietly work until the correct time. She showed me to a meeting room near reception and I said I'd pop back out nearer the time.

Valuable tools

The meeting room had an internal phone line, an internal telephone directory, and a network point. So far so good. I now knew all the staff names, extensions and roles in the business, probably the most valuable tool the social engineer can find. I phoned someone in IT, claimed to have the wrong number and asked to be redirected out to another caller. Coming through on an inter-

The weakness is ordinarily never the automated IT systems themselves, but the people who have legitimate information access.

nal line it was a simple matter to convince any recipient that I was indeed new in the IT department and the head of IT had given me the boring job of checking that not too many users had the same password – a clear security risk (when actually it's not a risk unless they know they have the same password). If too many people had the same password we would of course ask them to reset, so it's of no risk to tell.

In a few calls I had several individuals' log on credentials. Usernames are easy to establish (first initial surname, or firstname.surname, and nobody minds confirming these). Using the handy network point supplied in the meeting room I was able to browse their accesses and leave when I had what I needed. Equally I might have tried to talk the information out of them, getting them to log in whilst on the phone, getting them to do the technical work as well. Telling the receptionist I'd left something in the car, I left with the information I wanted and returned to base to write my report.

Know your enemy

On site a social engineer is a consummate actor, the pregnant woman carrying a heavy box, the maintenance engineer who has lost his badge or a new member of staff who is lost. Off site, they are the poor wife of the customer who must have the information or bad things will happen to her, the disgruntled customer who must be

The receptionist and security guards in an organisation are often one of the first lines of physical defence, so these people need to be educated to spot possible physical social engineering attempts.

Staff should be trained to attempt reverse social engineering in that if they are suspicious of a caller, for example, they should try and gather information about the caller. One of the best defences is simply to ask for the caller's land line number to either check against your records, or to call them back to check that they are who they say they are. Secure authentication methods such as passwords on accounts and shared secrets can be employed too. However, be aware that national insurance numbers, addresses, telephone numbers, mothers maiden names and other details can be easily found by research on the internet, especially through social networking sites.

Creating a culture of security

The company policy should be highlighted through training and enforced. The situation should be monitored and even suspicions reported to management. Audits and measurements of this area should be carried out for management assurance. An ISO 27001 or other management system framework can assist.

Temporary staff will also need training in the company security policies and should only be employed in sensitive

On site a social engineer is a consummate actor, a pregnant woman carrying a box, a maintenance engineer who has lost his badge.

placated, the member of staff working remotely who has lost their access or the senior management who must have that information now or we will lose the big deal. Staff should be aware of the issue and how to defend against it.

Training

Employees should be trained in spotting the social engineering techniques and should be made aware regularly of the latest tricks and scams being employed by tricksters. Particular staff that are more vulnerable, include customer services personnel, help desk staff and receptionists – these roles should be made a training priority.

positions once their authenticity is verified. Remote workers need to be made aware of the risks. Their main contact with the parent company is via email or telephone, both classic social engineering tools. These staff need to ensure they verify any request for information and the identity of the requester.

Social engineering is a dangerous tool, mainly because investment is often in IT technologies, rather than on training staff to guard against old fashioned manipulation. Investment priorities should always be the staff, second to the machines they use.

For more articles go online to:
www.bcs.org/articles



DEALING WITH CLOUD THREATS

Charlotte Walker-Osborn, Partner, and Laura Friend, Solicitor, Eversheds LLP, discuss cloud computing security concerns.

By the end of 2010, Deloitte's 'Technology Predictions' expect the cloud computing market to be worth approximately \$70 billion. However, many corporates still have material concerns with the use of cloud computing.

Discussions at the Council of Europe's Octopus Interface Conference in Strasbourg, held in March 2010 highlighted that data security remains a real concern in terms of potential weakness of cloud computing.

The focus of the conference was on harmonising global cyber laws, to give enforcement agencies the legal basis to gather cross-border evidence. Francesco Pizzetti, President of the Italian Data Protection Authority, declared that 'it is not possible to continue to guarantee the protection of citizens' data without very strong international rules accepted by all countries around the world'.

The Cloud Security Alliance (CSA), a non-profit organisation that promotes best practices for data security in the cloud, stated that the top threats are abuse and nefarious use of cloud computing, insecure interfaces and application programming interfaces (APIs), malicious technologies, shared technology issues, data loss or leakage, account or service hacking and unknown risk profile.

Relatively weak registration systems which facilitate anonymity, and providers'

limited fraud detection capabilities contribute to providers being actively targeted. These organisations are further exposed to various security issues related to confidentiality, integrity, availability and accountability due to a reliance on a weak set of interfaces and APIs.

Insider threats

CSA stated that 'it is critical that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.' According to the CSA, 'attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalisation.'

CSA reports that data compromise increases in the cloud 'due to the risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.'

Another concern of the CSA is account and service hijacking, where 'stolen credentials can be used by attackers to access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services.'

They continue that often issues with compliance of internal security procedures, configuration hardening, patching, auditing and logging 'are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.'

During the 2010 DEF CON Hacker Conference, the Fortify Software sponsored poll revealed that 96 per cent of respondents believed the cloud increased hacking opportunities, with 45 per cent of hackers admitting they had tried to exploit its vulnerabilities. Furthermore, 89 per cent of respondents stated cloud vendors are not doing enough to address security issues, as noted by Fortify's Barmak Meftah in his Business Computing World article (24 August, 2010).

The Octopus Interface Conference recommended that existing instruments on international cooperation, e.g. the Data Protection Convention, should be applied much more widely and efficiently. Additional international standards may also be necessary, alongside training of and greater cooperation between law enforcement agencies, internet service providers and the IT industry generally, and the establishment and strengthening of high-tech crime and cybercrime units.

The CSA produces a 'Security Guidance for Critical Areas of Focus in Cloud Computing', available on their website for download now. Furthermore, on the 1 September 2010, the CSA launched online testing of the industry's first user certification program for secure cloud computing. The Certificate of Cloud Security Knowledge (CCSK) aims to ensure that a broad range of professionals with cloud computing responsibilities have a demonstrated awareness of the security threats and best practices for securing the cloud. Many companies have expressed their commitment to the CCSK including eBay, ING, and Symantec.

In light of the above threats and the strong indication that hackers may target cloud computing, some businesses will remain reluctant to move to the cloud model without detailed understanding as to how the cloud provider will address security threats and risks. It will be interesting to see what further developments transpire and how the recommendations of the Octopus Interface Conference work in practice as the market continues to grow.

Please note that the information provided above is for general information purposes only and should not be relied upon as a detailed legal source.

www.bcs.org/legal

BOOK REVIEWS

Virtualization and Forensics

Diane Barrett, Greg Kipper
Syngress Media

ISBN 978-1-59749-557-8

£36.99

8/10

Virtualisation is a buzz word that seems to be gaining momentum daily.

Virtualisation improves the availability of IT resources and applications by running several virtual machines on a single hardware, thereby reducing cost and promoting energy efficiency.

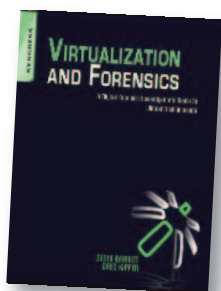
Yet for all its projected benefits, there are drawbacks that needs addressing.

This book is a useful resource that provides adequate coverage of virtualisation and security to readers who are new to this topic.

The authors introduce the readers to the various virtualisation architectures giving the reader an overview of the different virtualisation environments.

In part two of the book the authors look at forensics and the implications virtualised environments have on forensic investigations.

In the past the practice for investigation has been to mount an image of the



suspected environment that allows investigation to be carried out while preserving the affected system.

The technological changes brought about by virtualisation present new challenges, however there are a multitude of ways in finding evidence in a virtual environment.

For example the use of snapshots, memory analysis, log files, system registry and configuration files in system folders. In this part of the book the authors present some brief investigation and provide notable findings.

However, these are not as detailed as most readers would hope for.

In part three compliance and various challenges of virtualisation are introduced. A great concern lies with data centre architecture as well as with data retention and security. However, the book only covers very little detail.

The book is a theoretical introduction to virtualisation rather than a practical reference handbook. The authors provide a basic, easily understandable introduction combined with some practical examples.

Uma Kanagaratnam MBCS

Network and System Security

John R. Vacca (ed.)

Syngress Media

ISBN 978-1-59749-535-6

£36.99

8/10

Network and System Security is edited by John Vacca, an information technology consultant and well known best-selling author based in the USA. The thirteen chapters in this book are provided by experts in their own field and cover a diverse range of topics.

A comprehensive introduction to each segment is provided at the start of the book. The content of each chapter is fully described and its relation to the overall topic of network and system security is explained in detail.

The first chapter sets the scene for the remainder of the book. It deals in depth with the issues likely to be encountered when attempting to build a secure organisation and provides an insight into how to go about building a secure organisation.

Subsequent chapters deal with: system intrusion; UNIX and Linux security; internet



security; intranet security; LAN security; wireless network security; cellular network security and RFID security, all in the same manner as the first chapter.

The only exception is the chapter entitled 'A Cryptography Primer', which explains the role and development of cryptography from its beginnings through to the present day.

This a desk reference volume that provides wide-ranging coverage of the subject matter along with methods of analysis and problem solving techniques to help the reader understand the material.

Whilst aimed primarily at network security professionals, the book also contains valuable information and guidance for project managers working alongside security staff, possibly as part of their wider project responsibility.

There is a small amount of duplication between the chapters that could have been eliminated by the editor exercising more rigour over the individual contributions. However, I have no hesitation in awarding the book eight out of ten for its approach, treatment of the subject matter and coverage of the material it contains.

Jim McGhie CEng MBCS CITP

BOOK OF THE MONTH

Information Security Risk Management

Edward Humphreys

BSI

ISBN 978-0-580-60745-5

£38.95

9/10



Author Edward Humphreys is well placed to write this book, since he is recognised as the 'father of the ISO/IEC 27000 family of ISMS standards'.

Having some experience of the 27001 standard I found the book very easy to read, but I wouldn't say this is a prerequisite for the book. The author presents the sections of the standard in a logical manner, giving the reader sufficient understanding of what is required for an information security management system.

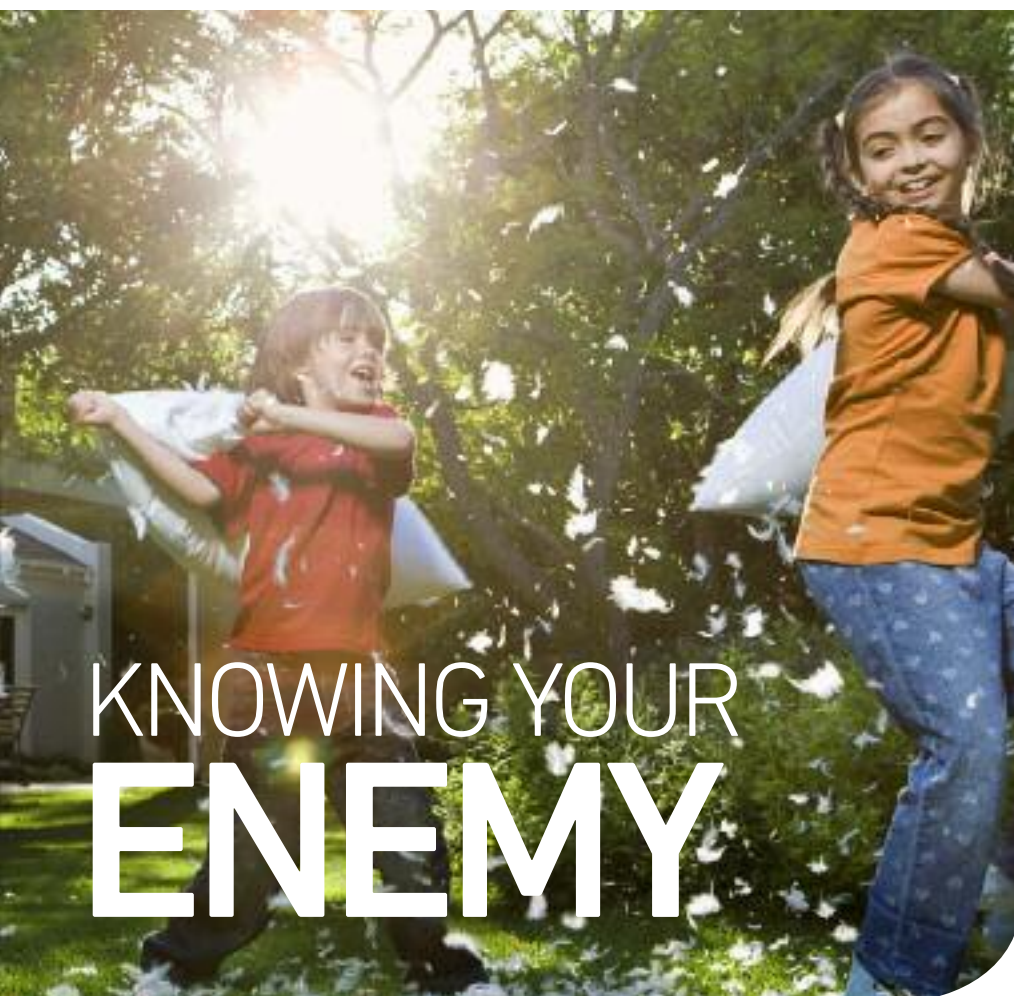
Sections include creating a risk management framework, carrying out a risk assessment, options for managing risks, selection and implementation of risk controls, monitoring and reviewing risks, improving risk controls and a documentation system. Annexes include definitions, examples of compliance, examples of assets, threats, vulnerabilities and risk assessment methods and selection of risk management tools.

Each section is pretty complete and presented in an easy to understand manner. The combination of the standards-based content supplemented with clear explanations and illustrated with brief case studies works well to make it very readable.

Whatever your level of experience with information security risk management, the handbook provides a methodical approach to risk management, with clearly defined outputs from each stage, illustrating how these are used as inputs to the next stage of the process. Although many parts of the handbook are duplicated from the standard's documentation the author brings the standard alive with additional explanations and examples.

Overall a very complete book, with key stages and concepts explained clearly and presented in a methodical manner.

Mehmet Hurer CEng MBCS CITP



KNOWING YOUR ENEMY

John Mitchell has been thinking about separating myth from reality.

Anyone who has read Stieg Larsson's *Millennium trilogy* will know about a group of fictional hackers who can target the computers of undesirable elements at will. Nothing can prevent them from breaching even the best of protection systems.

However, this group of hackers have a huge advantage over the rest of us. They know who their enemy is and where in cyberspace they reside. My company's server is constantly being pinged to ascertain if there is a live computer at that particular internet address. We know through using tracing software that the majority of these queries appear to come from two universities: one in Europe and the other on the Indian sub-continent. I use the word 'appear' simply because we don't know whether these universities are unknowing conduits from another downstream source, or whether the address we see is a spoof.

Not knowing your enemy is unnerving, but as our firewall does not respond to the pings they don't know about us either. In much the same manner that naval submarines operate in stealth mode we

tend to do the same, which is why I have never bothered to contact the universities concerned. Our firewall neutralises their pings, our anti-spam filters limit the amount of junk mail we receive, our anti-spyware protects us from Trojans and the anti-virus software prevents infection.

Firewall pings

In much the same way that the alien in the film *Predator* was invisible and could only be seen indirectly, we have the same challenge with the blackhat hackers. I mentioned that we had traced the pings against our firewall to a couple of universities, but all we really know is that someone out there is sniffing around. Who, and ultimately from where, remains a mystery, which is one of the problems associated with taking away people's internet access if they are deemed to be illegally downloading copyright material. Is it really them? So we offer passive resistance to an unknown enemy.

But isn't attack sometimes the best means of defence? Firstly we don't know who they are and secondly we are law abiding.

The UK's Computer Misuse Act makes it impossible to conduct legal offensive action. My passive defensive stuff is OK, but any move into offensive action could result in me spending up to 10 years inside. So in practice I am dependant on the government to take action. The thought of a cyber 007 slipping silently into the spammer's base, wrecking their systems and just as silently departing is comforting, but naïve, so I have to rely on commercial products to defend myself and hope that there are secretive white-hats out there who are taking the battle to the enemy.

Well, if this is happening they appear to be losing. Simply having right on your side is no protection against 13 year-old kids who subvert computers and are then able to carry out DDoS attacks. Only when governments suffer a really severe disruption will they take things seriously.

Interestingly, the US has a cyber warfare school, but it still wide open to a hacker from the UK seeking information on aliens.

If Gary McKinnon was able to break into those 97 military computers and if he was able to do the \$800,000 damage claimed, then the world's only superpower has pretty much wasted the last 10 years of its much publicised cyber warfare capability.

Unknown enemy

Electronic warfare is cheap, can be launched from anywhere and leaves little in the way of hard evidence. The unknown enemy, operating from an unknown base who can strike at the speed of light. The Chinese supposedly have 100,000 people researching and developing cyber warfare techniques. In May this year the Americans created a 'Cyber Command' within its Department of Defence with a total staffing of around 90,000. We have a few dozen.

Size may not be everything and quality is the prime requirement, but statistically you are bound to have more quality people in a large population than from a small one. If you are not worried by this, then you don't really understand the problem and if you don't understand the problem, then to quote Malcolm Forbes, 'it's so much easier to suggest solutions when you don't know too much about the problem'. On balance I prefer the George Orwell quotation that 'people sleep peaceably in their beds at night only because rough men stand ready to do violence on their behalf'.

I started my last column along the lines that ARPANET, the predecessor to the internet, was designed to survive an atomic war. A reader pointed out that this is an urban myth, for which I apologise.

For additional articles please visit:
www.bcs.org/articles