Spoofed Identities: Virus, Spam or Scam?

Pete Simpson, Head of Clearswift ThreatLab

Identification is becoming increasingly problematic in the halls of smoke and mirrors we call ‘cyberspace’. The identity question raises its head in the context of the origin of mass-mailing viruses and worms; the relentless avalanche of spam; electronic identity theft; Internet fraud and cybersquatters. How do we recognise and respond to email address spoofing? How should we react to the evil spammer? Why must we remain vigilant in defence of our financial details and what is our recourse in the event of identity theft and fraud? How we choose to resolve these issues could determine our future freedom of use of the Internet, and a clearer understanding should allow us to navigate safely some potentially hazardous waters ahead.

Where did this virus come from?

Faked Sender addresses are not a new phenomenon, but over the last six months this characteristic seems to have become the norm. Of the last six worms to have appeared in significant numbers on the scene recently (Sobig.C, Bugbear.B, Sobig.B, Fizzer.A, Ganda.A, Gibe.B and Yaha.P) all spoof the senders name and/or address.

By far the greatest culprit in this respect has been the infamous Klez.H. It searches for email addresses in the Windows address book and also in files with the extensions TXT, HTM, HTML, WAB, ASP, DOC, RTF, XLS, JPG, CPP, C, PAS, MPG, MPEG, BAK, MP3 and PDF. The “From” address can be either one of the addresses found in this search or one selected from a list inside the body of the worm.

Consequently, many innocent users these days may be wrongly indicated as the senders of malicious code. This can cause some confusion and even misdirected anger. Indeed Klez.H is capable of spreading using a forged email address appearing to come from Sophos, Kaspersky, F-Secure, Symantec or Trend Micro. Consequently, many AV companies were obliged to send assurances to their customers that they were not infected and were not the real senders of the Klez worm.

It is important to recognize that receiving the worm from a given address does not necessarily imply that the apparent sender is infected. Nor, indeed, does it necessarily mean that the apparent sender even exists - many are fictitious. Prior to the advent of Klez.H good practice called for an automatic notification to the sender to counter the continued progress of the worm. Now, on balance, automatic notification is likely to prove counterproductive and lead to confusion and time-wasting amongst innocent, uninfected users. It is best to disregard the apparent From address and avoid any pointless “You sent me a virus. I did not. Yes, you did!” loops.

Worms that spoof senders’ addresses:

- Sobig.C
- Bugbear.B
- Sobig.B
- Fizzer.A
- Ganda.A
- Gibe.B
- Yaha.P

Take the time to learn how to identify a spoofed email source. A quick search, on an engine such as Google, for “SMTP header” will provide many sites with primers explaining how to read an email header. At first sight, the header may seem incomprehensible, but its technical interpretation is really very simple. It may not be possible for you to track back to the real source, but it is relatively easy to determine that the address has been spoofed.

An alliance of wealthy spammers with technically-accomplished virus writers resulted in the Sobig Project.

Where did this spam come from?

In the early days, spammers saw no need to conceal their identities and sent emails from their own accounts, but were soon tracked down and expelled, after complaints to their Internet Service Providers. Next they resorted to disposable dialup accounts, which they used and abandoned after a few days, but ISPs eventually blacklisted credit card numbers (needed to open a dialup account). Spammers then found a free ride in the form of mail servers (SMTP) with open relays. Instead of sending emails one at a time, as on dialup, they could drop a single copy, with a massive distribution list, on an open relay. SMTP mail administrators, finding themselves blacklisted began to close the relays. Despite using the relays to obscure their origins, the spammer’s IP addresses could still be traced in the SMTP logs. Broadband access came along offering the spammer another means of mass-mailing but they risked black-balling by their local providers. Their options reduced to finding a way to hide their IP address completely or moving to another town.

At this juncture, the spammers took a leaf from the hackers’ book to conceal their tracks, using proxy servers. Proxies are designed to allow users on a network to gain accelerated web access, by caching popular pages, but when misconfigured, as is often the default, allow anyone, anywhere to make anonymous SMTP connections, through HTTP. Lists of anonymous proxies could be found on many hacker sites, but in the face of the increasing spam problem, many of these
Spoofing

sites became blacklisted in the way that open relays were before them.

About 90% of spam received in North America and Europe derives from a hardcore of professional spammers, numbering about 200 individuals, often forming loosely-grouped ‘spam gangs’. In general, spammers are not particularly technically competent – most still use the age-old technique of moving from one ISP to the next. Some, however, have accumulated considerable wealth, mainly by combining their aggressive spamming activities with a ruthless disregard for copyright, ripping thousands of images from competitor websites to establish porn empires.

The financial stakes are very high, culminating in January 2003, in the alliance of wealthy spammers with technically-accomplished virus writers in the Sobig Project. The first signs of the project appeared in August 2002, when researchers noticed a backdoor trojan listening on unusual ports. This was followed by six variants of the Sobig virus released into the wild in 2003, each as a controlled experiment, with a self-imposed lifetime, typically of one or two weeks. In a highly surreptitious manner, which for quite some time evaded the attention of the antivrus research community, the virus checks a remote website for the presence of a file pointing to another website, from which to download the latest version of the backdoor trojan. Once this is accomplished the original virus is removed from the PC. The rapidly mutating backdoor trojan then installs an illegal copy of the Wingate proxy server – the spammers’ dreams come true.

The escalation of spam since late 2002 has been associated, particularly in 2003, with the infection of home PCs with the Sobig virus. Silent installation of the proxy, sometimes over a period of days, is often followed by spam emanating from the IP addresses of the victims. Thousands of home PCs are now ‘owned’ by the spammers. One would expect telltale signs of a PC having been hijacked by the spammers with an excess of non-delivery notifications, from addresses unknown to the user. Unfortunately this is not the case, as the from addresses are spoofed denying the victim any indication of the ongoing misuse of their PC.

To the delight of some spam-haters, these spammers can no longer hide behind a façade of ambiguous legality. The act of uploading unauthorised code and use of an individual’s PC without permission for the purpose of sending unsolicited email is clearly criminal under many jurisdictions. However, identifying the guilty parties is now no trivial matter, depending upon successful forensic examination of the victims’ PCs.

How should we respond to spam? The simple answer is that we should never respond to the spammer. Any invitation to unsubscribe from the unsolicited mail is really an attempt to verify that the recipient’s address is valid and in use. Ironically, we should learn from the spammers and, in part, emulate their ways. Personally, I receive no spam whatsoever. How come? In the first place, I maintain multiple identities. My business identity, I use strictly for work purposes and never divulge in any other context. I have a separate identity I use to communicate with friends and family only. Then I adopt disposable identities, which I use for all other purposes. In the second place, I am protected at work with an anti-spam solution.

Identity theft and fraud

Spam is not the only game in town: ebanks are fair game for attack. Whenever Internet Explorer, on a Sobig infected PC (and then trojanised with the Lala backdoor), opens a page containing the text “bank”, “ebay”, “PayPal” etc. a keystroke logger captures passwords and account details and sends them to one of the websites hacked by the authors of the virus. It is not yet known how many may have suffered financial losses following infection with Sobig and theft of banking credentials.

The project opens the door to possible impersonation and identity theft. With luck, one constant can alert us to the next Sobig variant (G) should it land in our mailbox. So far, all email message text has been limited simply to “Please see the attached file for details” and in the last case “Please see the attached zip file for details.”. If variant G follows the same

### Top Ten Tips for Managing Email Identities

1. Keep tight control over your professional email identity and use it strictly for work purposes only. Employers should make this an essential requirement of your organisation’s email use policy.

2. Never be tempted to ‘unsubscribe’ from spam: you merely confirm that the spam has hit a valid address.

3. Use a separate identity for personal communications with family and friends.

4. Adopt disposable identities for all other purposes on the Internet - particularly on Usenet groups. Select long (over 8 characters) email names, to escape brute-force guesswork. The first letter of each word in a poem or saying is ideal, especially with some letters transposed to numbers.

5. Obtain your disposables from a trustworthy source, such as yahoo, hotmail, netscape, etc., as some free email services will sell your ‘free’ address to spammers.

6. Never divulge financial details and passwords in email forms or at email-linked web pages. Contact the financial service provider and confirm whether or not it is a scam.

7. Never put your email address on a web page in machine-readable form, as spammers use scavenger programs to harvest these.

8. Use a search engine, such as google, to find a primer on how to interpret the from details in an email header. Learn how to spot a spoofed address.

9. Keep your antivirus defences up to date and be alert for non-delivery reports for mail you never sent - you may be playing unwitting host to a trojan spammer.

10. Organisations - implement a multi-layered content filtering solution and use it to enforce policy and educate your employees.

Remember, the final victor in this war is the spam-savvy user.
pattern, be alert and delete the mail, even if it appears to come from a known source. One thing we can be sure of is that the project it not over and we can expect a series of further short-lived experiments.

Emails purporting to come from ebanks or PayPal should be treated with the utmost suspicion. Often, these are cleverly designed to coax or intimidate the victim to go to a replica of the real website and enter account details and passwords, under the pretext of routine security checks or replacement of lost data, following some technical error. In a recent twist, some eBay customers found themselves accused of violation of the site's policy and threatened with removal if they failed to update their details.

Interestingly, there appears to be some evidence to suggest that the recent PayPal scam email may have originated from the same source in Russia, as the Sobig worm. The link, in the email, to the fake website may be disguised using HTML formatting. Right-clicking on the HTML in Outlook will present the ‘View Source’ option, which displays the HTML text in Notepad. This will expose the fake site URL sitting beneath the displayed value of the real site. Remember any URLs beginning with “http” are insecure: secure sites begin with “https”. If you do click on the apparent URL visible in the HTML, compare this with the URL displayed in the Address bar of the browser. Although the latter represents a simpler method of checking the URL, the site may harbour other dangers in rogue pages. In any event, do not delete the email: it represents evidence. Go to the real site and get the ‘About’ or ‘Contact’ details. For example, PayPal have a page for reporting fraud, spam and fake sites.

According to the Identity Theft Resource Center, a non-profit organisation, based in San Diego, identity theft is the fastest growing crime on the Internet, often facilitated by email scams or careless online shopping and banking. Typically, victims may remain unaware of their predicament for several months and recovery can be a long and painful process. The ITRC site provides useful advice and victim resources.

The impersonation of an individual is one matter, but the impersonation of large multinational corporations has also recently become an issue, with the entry of the ‘cybersquatters’. Vast amounts of cyberspace real estate have been hijacked by using forged email and false business fronts to trick the non-profit organisations responsible for the allocation of address spaces. Los Angeles County had it’s /16 (pronounced ‘slash sixteen’) block of sixty-four thousand IP addresses stolen in this way. The ‘land grabs’ have opened up new territory, and pornographers and spammers have not been slow to move in.

Identity in cyberspace has, indeed, become a murky issue. Some such as Eugene Kaspersky, of Kaspersky Labs antivirus, have called for the introduction of an Internet driver’s licence, as proof of identity. The ePrivacy Group have recently published a standard for email digital signatures, and ‘assertions’ about the sender’s intent and integrity, as a proposed means to combat spam. Perhaps, prompted by such initiatives, some spammers have taken to displaying bogus PGP signatures in their mail. However, any such encryption schemes are liable to suffer the same drawbacks as PKI infrastructures and browser certificates: great in principle, but largely unworkable in practice.

As we have seen, some spammers are in league with a number of highly inventive individuals, technically knowledgeable in Internet security, who will continue to find new tricks and channels, such as the pop-up Windows messaging. Also, demanding some scheme for proof of identity would allow some authority to deny the spammer use of email: but then anyone could be denied its use. This raises serious civil rights implications, particularly for those resident in countries keen to curtail those rights. On balance, we may well be better served by adapting to meet the challenges of spoofed identities, as well as learning to use multiple aliases to our own advantage.

---

Balancing the Security Budget

Matthew Pemble

Regardless of the prevailing economic climate and, especially when, as now, the outlook is reasonably poor, the budget and time allocated to information security are never going to be enough to allow you to do everything you want to (or think that you want to) do. It is therefore incumbent upon all of us to maximise the effectiveness of the way we spend the pittance our masters decree unto us.

Concentrate on what you must do.

There are far too many different ways to skin the security cat and a never ending variety of tasks, each that appear to be vital for the future wellbeing of humanity (or, at least, your organization and employment.) However, we need to look hard at what we are actually here for – to protect and maintain the business function. Or, as my current employer has it, “Keep the Show On the Road.” This means that the focus of our