# Protecting against spear-phishing


Bimal Parmar

**Bimal Parmar, Faronics**

**Facing an increasing number of threats and stricter business regulations, organisations are continually challenged with ensuring that security and compliance across the IT infrastructure is sufficient. While scams and tricks are hardly new, the speed and reach of them has been magnified enormously with the world's increasing dependence on the Internet, email and social media. In particular, the proliferation of email within the workplace has not only facilitated the success of businesses, it has also opened a door to substantial security threats.**

According to IDC, there were more than 400 million corporate email boxes worldwide in 2010, with that number continuing to rise.[1] With it now almost impossible to imagine work without email, it is perhaps no surprise that hackers have come to rely on this as their principle vector of attack. And while these campaigns once focused on low-value consumers, hackers now have their sights firmly set on more lucrative targets, and are beginning to develop more and more social engineering tricks in order to find and exploit high-value victims.

***"For evidence of the effectiveness of these attacks, look at the recent spate of high-profile breaches, such as those suffered by Google and RSA"***

Judging by the almost daily news stories about the latest security breaches, it is clear that many organisations are struggling to defend themselves against these latest complex attacks. One of the reasons that their security practices have become so impotent is that they continue to be based on established technologies, which are unprepared to protect against these emerging threats. A prime example is blacklisting technology. While many enterprises invest heavily in, for example, anti-virus solutions – signature-based software to keep out known malware – the increasing sophistication of cyber-threats is now enabling attackers to bypass these defences, leaving corporate networks dangerously vulnerable to attack.

Spear-phishing is a prime example. Evolving from mass-mail phishing campaigns, which were originally spammed out to many thousands of users in the hope that some would take the bait, spear-phishing attacks are much more targeted and involve duping particular individuals within a specific organisation into unknowingly downloading malware onto their machines. These attacks are successful as they send customised, credible emails that appear to come from a trusted source. Indeed, industry statistics show that spear-phishing attacks have a success rate of 19%, compared to just 5% for standard phishing attacks and less than 1% for spam.[2] For further evidence of the effectiveness of these attacks, look at the recent spate of high-profile breaches, such as those suffered by Google and RSA. These incidents provide a stark reminder of just how easy it is for these tailored emails to evade detection by traditional security tools.

## Characteristics of an attack

Typically involving a link to a fake website or encouraging the recipient to download an attachment that is laced with malware, spear-phishing emails have grown increasingly convincing. They are designed to be highly personalised, thus enhancing their authenticity and legitimacy, and increasing the probability of the individual complying with their request. If the user is fooled into downloading malware, a likely outcome will be that the hacker will gain remote access or log their keystrokes and ultimately gain access to their machine and, even more critically, the network to which it is attached.

A recent attack that illustrates how hard spear-phishing attacks are to detect – and how easy it is for the attacker to succeed – is that experienced by Google. After identifying an individual within Google who had access to high-value information, the hacker simply monitored the target's online activity over a couple of months, gathered personal information via social media sites and then sent a web link from a friend's Facebook account that was laced with a brand new piece of malware. The user believed that this message was credible, coming as it did from a friend, and innocently clicked on the link. This simple trick ultimately allowed the hacker access to Google's mainframe server. Not only does this illustrate the difficulty in recognising an attack, but it indicates how vulnerable corporate networks actually still remain.

***"Although spear-phishing attacks are much more complex, time-consuming and therefore more costly to undertake, the rewards are much greater"***

## Rising popularity

A recent report from Cisco Security Intelligence Operations (SIO) states that

although cybercrime activity caused by mass-mail messages has decreased by more than half in the past year, highly personalised attacks are growing rapidly, tripling in number during the same period.[3]

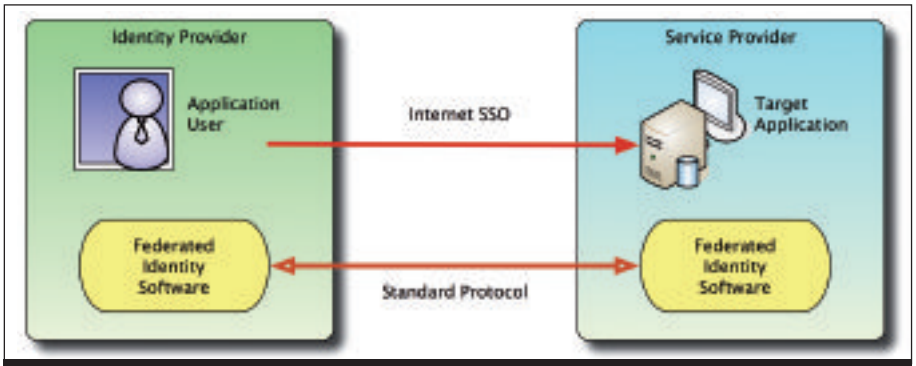
The most obvious reason for why spear-phishing has become so prominent is that it offers significantly more financial gain than traditional phishing attacks. Although spear-phishing attacks are much more complex, time-consuming and therefore more costly to undertake, the rewards are much greater. In the same Cisco report, it is estimated that while a highly targeted spear-phishing attack can cost five times as much as a traditional phishing campaign, it can yield a profit of more than 10 times.

## Hitting the human weak spot

The success of spear-phishing is down to a number of factors. First, it takes advantage of basic human psychology. When taking into account that the email is likely to appear to be from a known, trusted source, such as a bank, work colleague or friend, it is perhaps inevitable that there will be some individuals who will respond, no matter how aware they are of the danger of security threats. Take, for example, the case of an employee at international publisher Condé Nast. After receiving what appeared to be a legitimate email from its print supplier requesting that all future payments be paid into an alternative account, Condé Nast ended up forwarding almost $8m in just 44 days to the account of a scammer.

***"Users are continuing to trust social networking sites such as Facebook, LinkedIn and Twitter with large amounts of personal and sensitive information"***

This example may be extreme, but it illustrates just how costly cyber-attacks can be. Organisations are consequently paying a high price, with figures showing that the average cost of a cyber-attack in the UK was £1.9m in 2010, and that's without taking into account the increasingly heavy fines being issued for lax security.[4] This was evident in July 2009 when HSBC, the largest bank in the UK, was fined £3.2m for losing confidential customer information.




Overall organisational costs per affected user, per attack. Source: Cisco.

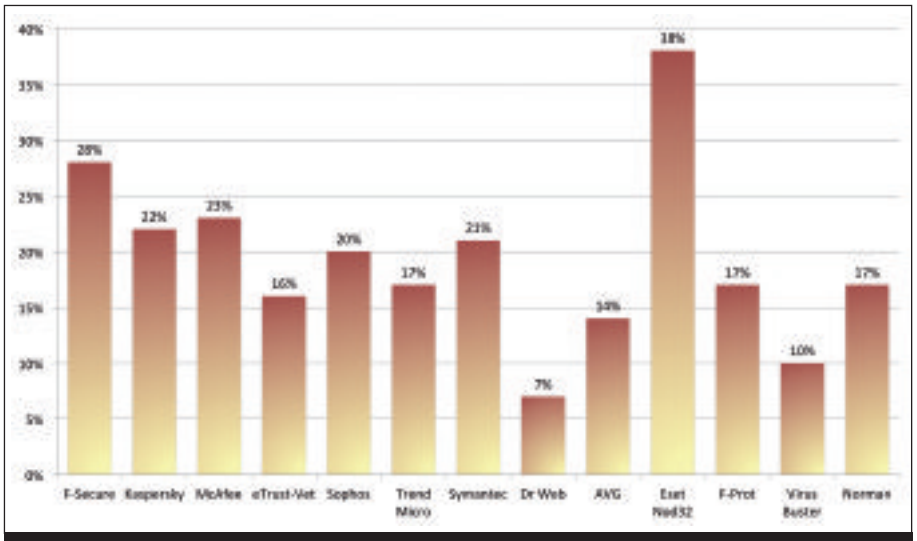
Adding to the overall security challenge is the proliferation of mobile devices. Employees now regularly open and reply to emails on the move, with little regard for security. With high volumes of email and greater chances of distraction away from the office, users are more likely to scan an email as opposed to scrutinise it for potential threats. At the same time, network boundaries are becoming more indistinct with the growth of remote working and use of mobile devices. Perhaps unsurprisingly, the Ponemon Institute has also found that 29% of data breaches were linked to mobile phone usage. This lack of attention to security only reinforces the need for more stringent security policies and defences. With hackers exploiting human – as well as technological – weaknesses, organisations can end up spending thousands of pounds investing in the latest firewalls or anti-virus software, only for it to end up completely redundant if an employee is deceived into co-operating with the cyber-criminals.

## Social media drawback

Spear-phishing attempts are made even easier with the wide availability of information being placed on the Internet for all to see. Users are continuing to trust social networking sites such as Facebook, LinkedIn and Twitter with large amounts of personal and sensitive information, such as where they live, what they do, their date of birth and hobbies. This type of information can easily be harvested by cyber-criminals without any technical know-how and with very little effort. Status updates readily provide hackers with all the materials they need to construct an email that is personal and relevant to the targeted individual.

This was exactly the case with the recent RSA breach. Here, cyber-criminals targeted an HR employee by sending an email containing a fake 2011 recruitment plan, after researching the individual on LinkedIn. Although the mail was caught by a spam filter, the employee actively retrieved the email from their junk mailbox, believing it to be sorted incorrectly, and subsequently downloaded the attachment. A piece of malware was then installed on the machine, giving remote desktop control to the hacker who then had free range to steal data within the network. Although the full impact of the RSA breach has yet to be determined, it could potentially impact more than 100 million users, while several large customers have since announced breaches of their own systems following the RSA breach, which they claim stem from the RSA attack.

This is a perfect example of how an organisation not only faces financial loss, but also runs the risk of jeopardising its reputation and customer loyalty. Inadequate security practices no longer just cost organisations time and money, but



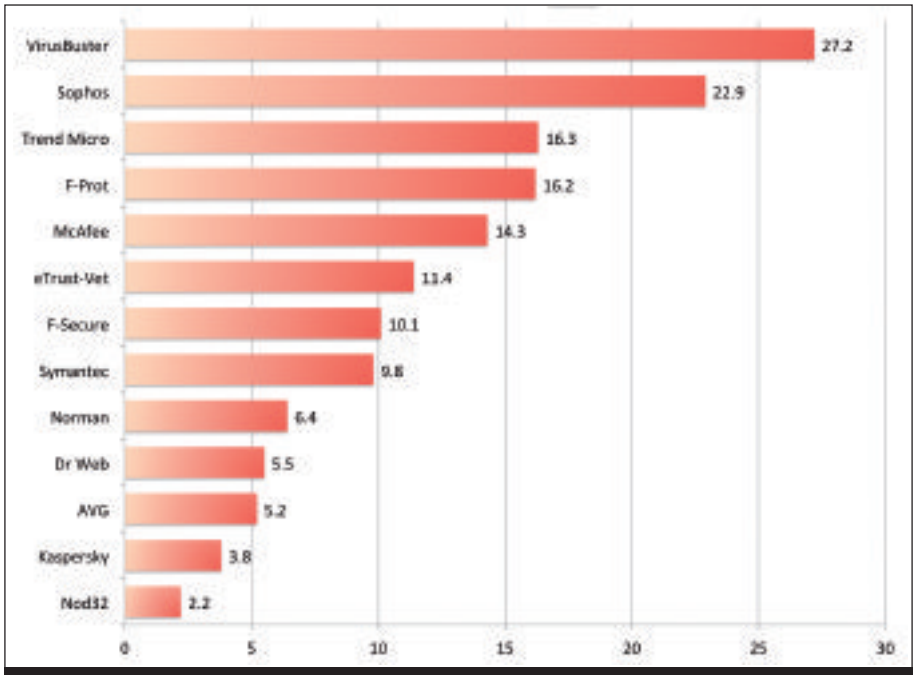

Anti-virus solution detection rates upon initial discovery, 20-22 April 2010. Source: Cyveillance.

can result in bad public relations, loss of future revenue, customer churn and even damaged share prices. With the European Commission expected to beef up legislation around the compulsory disclosure of data breaches in the near future, bad publicity, and all its knock-on effects looks set to have an even greater impact.

## Education, education, education

To counter these threats, organisations need to increase awareness of the dangers of spear-phishing and continually educate their customers and employees on how to avoid cyber-fraud. Education, or 'common sense' defence, is a key component in combating these cyber-threats. Spear-phishing is simply a 21st Century equivalent of traditional, non-technological tricks such as pick-pocketing; therefore the smarter and more street-wise users are, the less likely they are to become victims.

This point is perfectly illustrated by William Pelgrin's exercise. Director of the New York State Office of Cyber Security and Critical Infrastructure Co-ordination (CSCIC), Pelgrin sent a carefully crafted spear-phishing email to 10,000 New York State employees requesting they click on a link that asked them to fill in their email address and password. Around 15% tried to enter their passwords before being stopped and sent a note explaining the exercise and the error of their ways. When a similar message was sent four months later only 8% attempted to interact with the fake website.




Average lag time in days between new threat being detected and anti-virus vendors providing protection through new signatures. Source: Cyveillance, 2010.

***"Not only is the endpoint where much of the data on a network resides, but it can also provide a hacker with a direct route into the organisation's entire network"***

Exercises like these show that users can learn to be more vigilant. But the fact of the matter is that it only takes one person to unknowingly click a malicious link or download an infected attachment, for an entire organisation to be at risk of suffering major reputational and financial loss. This, and the ever-evolving threat landscape, makes it clear that education is not a sole solution. Organisations must also ensure that they have a solid endpoint security strategy in place. Not only is the endpoint where much of the data on a network resides, but it can also provide a hacker with a direct route into the organisation's entire network. By compromising just one PC it is possible to bypass all network level security.

## Blacklist flaws

Though popular, the problem with traditional blacklisting solutions is that companies need to know exactly what threats they are facing if they are to adequately protect against them. Known as a zero-day attack, if the piece of malware is brand new, there is a good chance it will be allowed to run and cause damage before it makes the anti-virus publisher's blacklist. With anti-virus vendors estimating that around 60,000 new pieces of malware are created daily, it is not hard

to see how difficult it is for traditional defence methods, such as anti-virus, to keep pace.

Organisations also need to take into consideration the fact that malware often evolves, allowing it to continually evade anti-virus blacklisting technologies. In the same way that the email from the spear-phishing attack is customised, the piece of malware that is downloaded is also bespoke. When considering that top anti-virus vendors take an average of 11.6 days to recognise new malware, it can be extremely dangerous to rely solely on this one solution.[5] Indeed, a recent report from NSS Labs stated that anti-virus products missed 10-60% of the threats created by cyber-criminals, often due to the fact that malware caught via one entry point is not always detected when introduced via another vector.[6]

## A layered approach

Traditional technologies based on blacklists are therefore no longer a suitable sole defence against cyber-attacks. Instead, organisations need to ensure that they have a layered approach to endpoint security. That is not to say that firewalls and anti-virus solutions do not have a role to play – they are still good baseline securities to have. However, they have limitations. While they are valuable tools against known threats such as viruses, worms and trojans, with sophisticated threats such as spear-phishing attacks becoming more and more prevalent, it is essential that organisations take action to bolster their layers of defence.

***"Unlike blacklisting, the malicious files do not need to be caught first and so application whitelisting does not rely on updates from the anti-virus publisher's database"***

The concept of a layered protection strategy, or 'defence in depth', is fairly well known. However, many IT managers overlook some of the strongest layers of defence available – application whitelisting and system restore methods. Working in the opposite way to blacklists, whitelists enable IT managers to identify exactly which programs should be permitted to run, thus providing greater reassurance that unknown malware and viruses will not infiltrate the network. Unlike blacklisting, the malicious files do not need to be caught first and so application whitelisting does not rely on updates from the anti-virus publisher's database of known threats. This is important to endpoint security as, unlike anti-virus solutions; it doesn't depend on definition updates. Crucially, this means that mutating viruses and executable threats that would normally bypass your anti-virus protection and attack your networks, are now stopped in the second line of defence. Another critical, and final, defence layer is a method for restoring systems to their original settings. Essentially this allows the user to reboot a computer at the touch of a button and delete any unwanted or malicious malware that may have slipped past other security tools.

With more advanced, targeted cyber-attacks and new malicious code constantly being created, there has never been a more appropriate time for organisations to conduct a serious risk assessment of their infrastructure and ensure that they are prepared for evolved threats, such as spear-phishing. Applying a layered security strategy combining blacklisting and whitelisting solutions brings added value by not only helping to keep employees productive and minimising compliance risks, but by providing the ultimate safety net for corporations, should individuals fall victim to a convincing attack.

### About the author

*Bimal Parmar is VP marketing at Faronics and, with more than 18 years of industry experience, he oversees the management of all Faronics products to ensure they continue to solve security and operational challenges. Faronics helps businesses manage, simplify and secure their IT infrastructures, and offers a comprehensive layered security solution consisting of anti-virus, application whitelisting and instant system restore protection.*

### References

1. Erin Traudt. 'Worldwide Email Usage 2010–2014 Forecast: Email Adoption Remains Despite Continued Spamming and Rise in Social Networking Popularity'. IDC, May 2010.
2. 'Ready for some spear-phishing'. SearchSecurityChannel, September 2006. Accessed Jan 2012. http://searchsecuritychannel.techtarget.com/feature/Ready-for-some-spear-phishing.
3. 'Email attacks: This time it's personal'. Cisco, June 2011. Accessed Jan 2012. www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.
4. '2010 Annual Study: UK Cost of Data Breach'. Ponemon Institute, March 2011. Accessed Jan 2012. www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.
5. 'Malware Detection Rates for Leading AV Solutions'. Cyveillance, August 2010. Accessed Jan 2012. http://www.cyveillance.com/web/docs/WP_MalwareDetectionRates.pdf.
6. 'Corporate Endpoint Protection Group Test Anti-EvasionQ3 2010' and 'Corporate Endpoint Protection Group Test Socially Engineered Malware via Multiple Attack Vectors Q3 2010', NSS Labs, 9 March 2011. Accessed Jan 2012. www.nsslabs.com/company/news/press-releases/av-industry-fails-to-cover-the-basics.html.