MessageLabs

Monthly Report January 2005

Business in the front line

Statistics for January

- In January MessageLabs scanned more than 90 million emails a day on behalf of its clients.
- 83.1% (1 in 1.2) were stopped as being spam.
- During the same period, 2.86% (1 in 34.9) were intercepted because they contained viruses, trojans or other malicious content.

Business in the front-line

How cyber criminals can specifically target your business to defraud, steal intellectual property and extort money by menace

There was a time when the popular perception of a virus writer was a young adolescent male, beavering away at a PC in a bedroom somewhere, with perhaps too much time on his hands. To most of us, his intent seemed only on making mischief, malevolent perhaps, in order to gain notoriety within his chosen community. As a consequence, the 'script-kiddies' were able to cause a lot of trouble — but it was nothing in comparison to more recent developments in cyber crime.

Indeed many hackers and virus writers are now lured by the monetary gain that can be realised through the creation of bespoke viruses and trojans. These are now being made to order, with the specific objective of creating global networks of compromised computers, or botnets. These botnets are then hired out for use by spammers and other criminal gangs who, for example, may attempt to extort money from an organisation by means of a distributed denial-of-service (DDoS) attack.

This prevailing trend in electronic exploitation is no longer about wire-heads playing games to impress their friends. The overtly commercial motives of spamming make it clear that unlawful manipulation of the Internet is becoming a serious and highly profit-driven business.

The destructive union between spam and viruses remains a very hot topic. Convergence came about as spammers began to lose the initiative when filtering systems — in particular MessageLabs' highly effective anti-spam service — blocked the delivery of most of the unsolicited email being sent to businesses. Meanwhile, virus writing techniques have evolved into a far more menacing threat. For those inclined to such malicious practices, it is now a simple matter to compromise systems by secretly planting trojans, spyware and other intrusive software on individual PCs.

Enter the racketeers

Traditional organised crime is very structured and highly hierarchical and operates along rigid lines of discipline, and online crime is no different in that respect. However, online criminal groups need to conduct themselves along different lines, because the parties involved often don't even know each other. To be accepted, each person needs to have established a track record within a community where the relationships are largely based on trust alone.

Small wonder that organised crime has moved in on the opportunities presented by the cyber sphere. And as a result, the rules of engagement are changing radically. From now on, malicious manipulation of the Internet will be almost exclusively about fraud, theft, blackmail and extortion.

As the technology has changed, so too has the nature of the target. While the old-style virus proliferation tended to be an indiscriminate shot-gunning of the e-world at large, new criminal methods show a preference for selecting a particular target, whether an individual or an organisation.

Indeed, the motivation behind today's email-borne threats is altogether more sinister. That is why every business organisation urgently needs to review its email security policies and provision. No longer is the threat simply one of being caught up in collateral virus damage; now it is the possibility of your organisation itself being deliberately targeted.

As we shall see, a pattern is emerging that betrays a modern technological exploitation of some traditional activities favoured by organised crime gangs — protection racketeering, extortion, money laundering, fraud and blackmail.

Distributed denial of service attacks

A growing menace is the distributed denial of service (DDoS) attack, where someone targets your web site or email system by deliberately swamping your servers with thousands of simultaneous connections from a botnet army under their control. It could be hostile action by a competitor wishing to damage your business or, increasingly likely, an act of old-fashioned extortion that threatens a DDoS attack unless a ransom demand is paid.

And this menace is everywhere. You may not immediately associate the Scottish Highlands with organised crime, but a recent operation by the British and US law enforcement officers has uncovered what appears to be a sophisticated extortion campaign, launched and managed exclusively through the email system, at least a part of which originated in Scotland.

Another recent case involved a US businessman, charged last summer with deliberately launching DDoS attacks against three of his competitors who, he claimed, had stolen material from him and had launched DDoS attacks against his own business.

The perpetrator allegedly hired criminally-motivated hackers to flood the target e-commerce web sites with thousands of requests for image downloads. The result was that one competitor's site was forced to go offline for 12 hours, another for two weeks.

Significantly, the hackers-for-hire were reported to have networks of between 5,000 and 10,000 zombie computers at their disposal, through which they could coordinate massive pressure on the target sites. Botnets, as they are called, are networks of compromised PCs that have been hijacked surreptitiously by hackers, unbeknown to their owners. These PCs can then used to launch spam transmissions in massive volume.

Botnets now represent a huge asymmetric risk to businesses because the defence mechanisms required to mitigate such an attack are hugely expensive, whilst renting a botnet remains a negligible cost.

A $100,000 bill for defence

It was suggested that one particular group which targeted a number of bookmakers in 2004, were initially hired by a rival bookmaker to disrupt a competitor's online business. Apparently, once the group realised how vulnerable the industry appeared, they shifted their sights towards other similar targets.

In January last year the operators of an online gambling site received an email demanding that they pay up or face concerted DDoS action. In the event, the gaming business lost just one day's business before fending off the attacks with superior technology — but the incident cost them $100,000.

Many demands were between $10,000 and $60,000, and some bookmakers were tempted to pay up, for fear of losing out to their competition, especially in the run-up to a major sporting event. Correspondingly, companies in the UK began to coordinate their responses more effectively and decided their official position was to not reply to blackmail demands, and the would-be attackers seemingly moved on.

A recent survey by Carnegie Mellon University in conjunction with *InformationWeek* discovered that 17 out of 100 US businesses polled had experienced extortion-driven DDoS threats. The courts are seeing an increasing number of actions brought against the perpetrators too. For example, an individual in Maryland now faces a long sentence after pleading guilty to threatening to launch DDoS attacks against a law firm unless he was paid $17 million.

From the political angle

And it's not just avarice that drives the DDoS threat. Attacks by email are being used increasingly for political and social purposes. At the time of writing, it was clear that animal rights activists were planning a concerted DDoS attack on specific businesses in the fur and vivisection industries to which they take exception, timed for St Valentine's Day.

Through means of 'electronic civil disobedience', their plan is to severely disrupt the targets' email systems by setting up a chat-room and encouraging everyone to log on and 'chat' at the same time. For each word typed, an email would be sent to the target organisation. All that participants needed to do was to follow instructions on the website to find out how to join in the online protest.

The intention behind the campaign, said the organisers, was to ensure that the target companies would 'experience problems with communications for a few days' and would 'realise just how expensive the animal abuse business can get'.

There may be nothing illegal about this sort of activity in the UK, although the government is planning legislation under which anyone could be prosecuted for 'economic damage' brought about through intimidation to organisations carrying out, or connected with, animal research. Presumably this type of planned action could thus be outlawed in future.

A run on the banks

Phishing attacks by criminals on major banks have already been well documented (see MessageLabs Intelligence Report for November). By creating fraudulent look-alike web sites and encouraging customers to log on to them, the swindlers have been extraordinarily successful in acquiring personal information from customers that enables bank accounts to be cleaned out.

To date the cost of these activities has been borne by the banks, but there is now a suggestion that more responsibility will be placed on customers who inadvertently divulge passwords, PINs, *et cetera*, in the future.

MessageLabs Intelligence has witnessed an unprecedented run specifically on Brazilian banks in recent months, with between 10 and 20 attacks per day. The motivation is unclear; it could be that criminals regard Brazil's banks as a soft target — or that this is some preparatory exercise as the prelude to much wider operations on banks internationally.

It has been reported that more than 50 people in Brazil, evidently all part of the same criminal organisation, have been arrested on phishing charges in the wake of this phenomenon. A series of specialist gangs had planted trojans on e-commerce web sites and transmitted thousands of emails from networks of compromised PCs to lure unsuspecting customers into divulging personal security details.

New type of trojan

As security has been tightened to fend off phishing attempts, the criminals have had to raise their game. The conventional way for phishers to harvest personal account details can be to draw the victim towards a decoy website and capture whatever they enter, or to install a trojan that can capture keystrokes, mouse movements or screen-shots and upload the information to the criminals.

Online banking systems are already edging towards adopting two-factor authentication schemes. These don't just rely on something you know — such as a username and password — but also something you physically have, which may be a key-fob with a number that changes every minute, and only the bank's systems know what that number is at any time. Other schemes include a list of one-time passwords that can be sent to the customer each month, perhaps along with their statement — and each password can only be used once.

Having two passwords resolves a number security concerns. For example, if a key-logging trojan captures your password, it won't matter as it cannot be used again. At least that was the established wisdom before the development of a new type of trojan, which is able to employ the victim's own web browser to siphon funds from his account after he has logged in, a method which sidesteps the bank's authentication processes. E-Gold account holders have recently been targeted with spam emails in this way.

The email carries an attachment with a Visual Basic Script Encoded attachment (.VBE), designed to wait until the victim has completed the authentication process before making the browser session invisible and creating another window for the user to continue, unaware that he has just been hijacked. Thus, the fraudsters can bypass the bank's authentication processes and personal accounts can be looted at will.

Anti-virus software sometimes has problems detecting key-logging software — some of which may be perfectly legitimate, such as that used by parents to monitor their children's online activities — so from a legal standpoint it can be very awkward if they identify these products as suspicious. From time to time, anti-virus software may be able to detect some trojans, but these signature-based solutions will never achieve 100 per cent detection.

When it came to it, a bug in the trojan planted by criminals in the E-Gold example prevented any wide-scale fraud being perpetrated. Nevertheless, it's a development that the banks are watching with concern.

Unauthorised access hazards

While enterprise security used to be the concern purely of IT departments, it has now become the responsibility of every individual within the organisation. Theft of the log-in name and password of just a single employee can give criminals access to internal corporate networks, whether for theft of identities or intellectual property, or to access sensitive financial information and personnel data.

A well-worn technique is for the criminal to target individuals indiscriminately by sending what appears to be a genuine email from a bank or other organisation. The email will typically request confirmation of security codes, passwords, PINs and so on. Using spamming techniques to transmit thousands of such emails simultaneously, the phisher aims to harvest victims who are unwary enough to comply with the request.

The rise of spear phishing

Essentially, phishing is just spam being used to trick people into revealing some information to the phisher, and relies very heavily on social engineering to succeed. By blocking spam effectively, the bait never reaches its target, and the opportunity for deception is crushed.

2004 was the year of the phishing scam, and now more sophisticated attacks exploit phishing techniques in order to gain access to corporate networks. Rather than using the 'traditional' approach of casting their large nets far and wide, and then waiting to see who bites, phishers are now sending more targeted emails to businesses.

Such emails are designed to appear as though they were sent by another member of staff at the same organisation, typically from the IT or HR departments. A number of recent surveys suggest that people are content to share their passwords in return for small rewards, such as bars of chocolate or pens.

In the same way, a phisher can try to persuade employees into revealing some private information, when perhaps they should know better. Moreover, there are still many businesses that also provide a rich harvest of personal email addresses on their website, which may then be easily spoofed.

In a recent US example, a phisher bluffed his way into the network of a port authority by spoofing an internal email address. Once on the inside, with an apparently genuine email identity, he was able to fool employees into revealing passwords for applications.

This sort of attack has been termed 'spear' phishing, designed to bamboozle unsuspecting 'colleagues' into revealing information that will give the perpetrator access into secure areas of corporate networks.

By spear phishing one company at a time, a phisher need only send emails to a single domain, spoofing the sender address and requesting usernames and passwords to validate some information, or providing a link to a spoofed version of the company's website or intranet — or perhaps that of a business partner or supplier.

Many people often use the same username and password for different applications or websites, and the phisher may try and use that to their advantage in their social engineering.

It is surprisingly easy to use existing spam-sending software to dynamically generate the target email addresses, for example by combining databases of first names and last names with letters and numbers. Furthermore, it would only take a few hundred such permutations to provide a valid email address in a large organisation.

Additionally, a sustained attack of this nature can quickly become a huge drain on the company's email server, sapping its resources as it attempts to handle several hundred or thousand connections for emails that can never be delivered to recipients that don't exist.

Nevertheless, a successful spear phishing expedition can reduce the effort required to break into a company's network without too much difficulty.

Not only are the individual's details potentially compromised; it can also lead to theft of intellectual property and other sensitive corporate information. Spear phishing is certainly set to be a growth area in Internet fraud techniques.

The managed solution to email security

The growing emergence of organised crime in the Internet fraud arena further endorses the need for businesses to protect themselves comprehensively from email security threats.

We have seen the continuous development of viruses, the burgeoning menace of spam — and then the convergence of the two. Now organised criminals are exploiting techniques developed by virus writers and spammers in wide-scale fraud scams.

Email security can no longer be regarded as adequate when applied on a piecemeal basis; rather organisations must to a multi-layered approach to protection. Particular attention must be paid to the first line of defence at the Internet level, which is where managed email security services play a crucial role. Enterprises can benefit from the solutions offered by MessageLabs in many ways.

Managed email security services protect organisations at the Internet level, outside of the corporate network, without the hassle, inconvenience or additional cost of traditional software or hardware solutions.

Managed services can free up in-house IT resources, increase employee productivity and enhance the efficiency and operability of email systems by combating the threats that place them at risk. This in turn can raise network utilisation levels through reduced email volumes and less demand on Internet bandwidth.

These services ensure the integrity of electronic communications, helping businesses to manage and reduce risk while securing their critical infrastructure and business information.

About MessageLabs

MessageLabs is the world's leading provider of email security and management services with more than 10,000 clients and offices in 12 countries. For more information, please visit http://www.messagelabs.com

About MessageLabs Intelligence

MessageLabs Intelligence is a respected source of data and analysis for email security issues, trends and statistics. MessageLabs provides a range of information on global email security threats based on live data feeds from our control towers around the world. The information relating to MessageLabs' services contained in this report, is based on data generated internally by MessageLabs and has not been subject to an independent review by a third party.