MessageLabs®

Be certain

The week the email security landscape shifted

Whether the pressure of virus outbreaks witnessed during the last week of January 2004 can be seen as a blueprint for things to come remains to be seen. But if multiple viruses continue to be released within such a short space of time, many organisations are going to have to change their entire approach to email security.

An interim MessageLabs white paper by Natasha Staley, Information Security Analyst

A challenging week for conventional email security

In email security terms, the month of January 2004 began like any other. There were no significant shifts in the volume of viruses, worms and trojans attempting to compromise systems and disrupt everyday business activities. It seemed that January might end that way too – until the last few days of the month.

On 23 January, MessageLabs intercepted its first copy of a new variant of the Dumaru worm – W32/Dumaru.Y. And by 25 January the number of copies caught had risen to 8,902.

The worm arrives as an attachment to an email called myphoto.zip, and spreads by sending copies of itself to email addresses harvested from an infected machine, using its own email engine. The worm also contains a password-stealing or key-logging trojan component, capable of leaving a backdoor open and allowing an attacker to gain remote access to the victim's PC. At the time of writing, 35,733 emails containing this worm have been caught.

It is also worth noting that because the attachment is a zip file, many content filtering systems deployed at the email gateway may not have been able to detect the worm.

It is also worth noting that because the attachment is a zip file, many content filtering systems deployed at the email gateway may not have been able to detect the worm.

Barely a day later, on 26 January, W32/Mimail.Q appeared. Although a relatively low number of copies have been intercepted – 1,189 to date – the latest addition to the Mimail family is possibly the trickiest to detect, due to its polymorphic capabilities.

Because the worm changes on each infection, anti-virus signatures have to be capable of detecting every variation of the worm. Whilst some vendors battled to produce their fixes, the window of vulnerability was left open for the worm to infect corporate users left with no form of protection.

Yet worse was to follow

With two notable virus outbreaks within a matter of a few days, it had already been a pretty busy week in the world of email security. But it seemed that the worst was yet to come. On the afternoon of 26 January, MessageLabs intercepted its first copy of W32/Mydoom.A, which rapidly became the fastest spreading computer virus to date.

W32/Mydoom.A is a mass-mailing email worm that spreads by searching infected machines for email addresses and mailing itself to those it finds. In addition, the worm copies itself to any available shared directories used by Kazaa. Mydoom.A also tries to generate randomly, or guess likely email addresses to which to send itself.

As part of its payload, the worm also has a remote access trojan component which, once activated, attempts to connect to a TCP port and establish itself as a route into the compromised machine. At this point it is all too easy for a remote attacker to gain access to an infected machine and steal sensitive or confidential information, lift passwords, credit card numbers, and so on.

A ploy to deceive the unwary

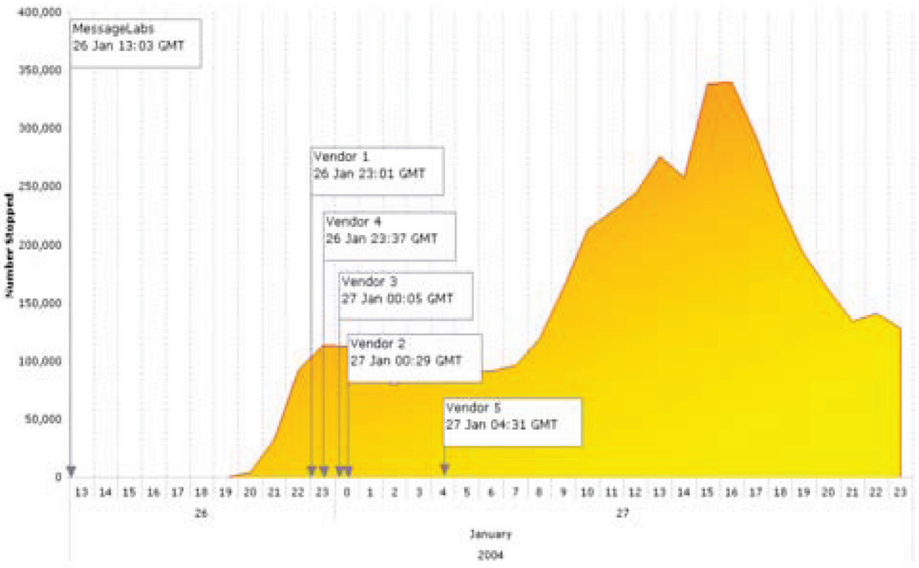
The sender and subject fields of emails containing W32/Mydoom.A are random, making it particularly difficult for email users to spot. However, the text itself suggests that the email message is in some way damaged, or has not been delivered in its entirety, and invites users to double click on the attachment in order to receive what is left of the message.

This is a fairly common technique known as social engineering, although it is far subtler than previous viruses have used. Instead of luring users in with the promise of scantily clad celebrities or raunchy photos, W32/Mydoom.A encourages users to double click using the ruse of a technical error. This is a shrewd move on the part of the author, who perhaps realised that users have begun to wise up to the more outlandish and obvious claims, and would need something less obvious to hook them in and aid the worm's spread.

Whether this was deliberate or not, it certainly worked. Within the first 24 hours of the emergence of Mydoom.A, MessageLabs had intercepted 1.2 million copies of the worm. Perhaps a more accurate reflection of the degree of penetration achieved by the worm is that fact that, at its peak, 1 in 12 of all emails scanned contained the worm.

This compares to the infamous SoBig.F worm, of which MessageLabs had caught one million copies with the first 24 hours, and at its height accounted for 1 in 17 of emails scanned. Mydoom.A had officially knocked SoBig.F off the top spot and claimed its place as the most rapid spreading virus of all time.

Within the first 48 hours, 2.2 million copies of Mydoom.A had been intercepted, and at the time of writing.



The rapid proliferation of Mydoom.A:MessageLabs had the instant solution,while the first of the anti-virus software vendors could only provide customers with a signature nine hours later. Some took even longer.

MessageLabs data shows that its scanners have stopped more than 16 million copies of the worm – and that number continues to rise.

Another telling statistic is the sheer volume of email processed between 26 and 27 January. On a normal day, approximately 25.6 million inbound email messages would be scanned, but during this period MessageLabs processed more than 38 million inbound messages. This is an increase of 49%.

There was also some confusion over what Mydoom.A should be known as. Whilst one security vendor referred to the worm as W32.Novarg.A, another named it W32/Mimail.R – although it doesn't appear to be another Mimail variant. The majority of security companies, however, decided upon Mydoom.A.

Though on the surface it may seem as though naming issues amount to nothing more than a battle of egos between vendors, for the IT or security manager this lack of uniformity can be highly confusing.

As soon as a company hears of a new virus, and particularly one that is spreading at such an alarming rate, its first priority is to download and roll out protection. Once that is done, and assuming that no infections have occurred, the IT department can breathe a sigh of relief – until they hear another name for the virus.

Then the confusion begins. Is it the same virus? A new variant? Does the update already downloaded protect against it? Is it something completely new? If so, where can they find protection? Verifying whether or not several different names actually refer to the same virus can be a time consuming and worrying process.

It can only take a couple of hours for a virus to travel the globe, during which time an exponential number of systems may be hit.

The window of vulnerability
MessageLabs intercepted its first copy of Mydoom.A at 13.03pm GMT on 26 January. At this point no anti-virus vendor had issued a signature. As the hours passed, each vendor pushed out an update file to protect against the virus. In some cases, this took more than 10 hours. During this window of vulnerability, MessageLabs had already captured around 165,000 copies of the worm, which gives some indication as to the sheer number of businesses that may have been caught unawares.

It is this window of vulnerability that becomes ever more critical, as virus authors find more ways of launching almost instantaneous attacks. It can only take a couple of hours for a virus to travel the globe, during which time an exponential number of systems may be hit.

The motivation behind the worm?
A possible explanation for the creation of W32/Mydoom.A is offered by the fact that the worm is scheduled to perform a denial of service attack on www.sco.com between 1 and 12 February 2004. SCO Group recently began a litigation campaign in which it claims that some of the Unix source code in use actually belongs to SCO Group. The company has been advising those using Unix source code to purchase a licence from the company in order to prevent legal action.

It is therefore possible that whoever is behind this worm had a point to make to SCO Group about its claim to 'own' portions of Unix source code, and is possibly an open source advocate. Whether this is true or not, SCO Group is obviously taking the threat seriously and has offered a $250,000 reward to anyone with information leading to the arrest and conviction of the perpetrator of the worm.

On 1 February, SCO Group confirmed that the denial of service attack had been successful. According to a statement made by the company, Internet traffic began building momentum on Saturday evening and by midnight EST www.sco.com was unable to cope with the volume of requests. SCO also said it expected the attack to persist and was putting in measures to deal with the threat.

The hint of an apology
By mid-week, two further worms had appeared. W32/Mydoom.B and W32/Mimail.S were both intercepted by MessageLabs on 28 January. Neither of these worms is comparable to Mydoom.A, being classified as low and medium threats respectively. Nonetheless ensuring the organisation is protected has added to the average IT department's already heavy load.

In the midst of the chaos caused by Mydoom.A, a new variant of the worm, plus yet another Mimail variant, emerged.

It also appears that the author or authors of Mydoom.A and Mydoom.B may have tried to apologise. Both worms contain the signature 'Andy' in the source code and in Mydoom.B the following message appears: 'I'm just doing my job, nothing personal, sorry.' Such an apology is unlikely to offer much comfort to those who have been hit by the worms.

Mydoom.A has become the fastest spreading worm to date, which alone is a significant event. However, instead of focusing on Mydoom.A in isolation, it is necessary to step back and view the week as a whole.

There has never been a week like it in email security terms. While businesses were still in the process of defending their systems from Dumaru.Y and Mimail.Q, Mydoom.A struck and instantly pushed itself to the top of the priority list. In the midst of the chaos caused by Mydoom.A, a new variant of the worm, plus yet another Mimail variant, emerged.

For many IT departments the past week will have been one of the busiest and most challenging. Ensuring that a company is protected against a single outbreak is disruptive enough, and can divert the attention of staff from core business activities. A continual stream of outbreaks amplifies the issues and places additional pressure on administrators – especially for companies using traditional anti-virus solutions whereby individual signature files have to be downloaded and rolled out to the entire organisation.

So is there any indication as to why this has happened? It is impossible to know whether this rash of virus dissemination was planned, although it can of course be assumed that the person or persons behind the different variants of both Mydoom and Mimail released them at particular times deliberately.

However, for it to have been decided that the group of viruses – Mydoom.A and B, Mimail.Q and S, Dumaru.Y – would be released in some sort of pattern, would take a degree of coordination within the virus writing community that is unheard of to date.

It has certainly never been easier to write, disseminate and even make money from viruses, so such a situation is not unrealistic. Whether this week is the blueprint for things to come remains to be seen, but if we continue to see multiple viruses released within a short space of time this will lead many companies to change their approach to email security.

Pressing need for managed email security services

For most organisations, the function of the IT department is to support the core activities of the business and facilitate new initiatives by which competitive advantage can be gained. Many businesses cannot afford to have IT resources regularly diluted by groups of virus attacks.

As a result, we could see an increasing number of businesses adopting a managed email security service – not only to protect them from email security attacks, but crucially to alleviate the burden on their IT staff.

www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000

Europe

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
1 Great Portland Street
London, W1W 8PZ
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastraße 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

Americas

AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 830 1000
F +1 952 831 8118

Asia Pacific

HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia

T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 6232 2855
F +65 6232 2300