



The convergence of viruses and spam

Lessons learned from the SoBig.F experience

The SoBig.F outbreak has comprehensively demonstrated the accelerating convergence between the burgeoning threats of email viruses and spam. So what do you need to know in order to protect yourself from what is undeniably the biggest menace that electronic communications has yet faced?

An Interim MessageLabs white paper by Paul Wood, Chief Information Security Analyst

Contents

- 3 SoBig F. - so how big was that?
- 4 What's in it for the perpetrators of the SoBig menace?
- 4 SoBig - a case in point
- 5 How does the SoBig virus work?
- 6 Evolution of the SoBig virus
- 7 SoBig.F ultimately failed – but what's to follow?
- 7 The explosion of the SoBig.F virus
- 8 How MessageLabs protects against email viruses, spam and porn
- 8 MessageLabs advice to customers

Most vitally, it tells you how you can protect yourself and your business from the SoBig.F virus – and all future outbreaks of viruses as they gain in malevolence and guile.

SoBig.F – so how big was that?

First let's consider some hard facts relating to the recent SoBig.F outbreak, the fastest-growing email virus ever:

- MessageLabs stopped more than a million emails carrying the Sobig.F virus during the first 24 hours of the outbreak.
- And in excess of 6.4 million further copies during the first week. Typically we stop between one and two million viruses a month. To see this many copies of one particular virus is absolutely unprecedented.
- MessageLabs scans, on average, between 16 and 18 million emails for customers each day. During the first 24 hours the volume rose by more than 60% to over 25 million emails. At peak we were stopping 12 SoBig.F viruses every second!
- The ratio of virus to emails topped 1:17. After a week this had slowed to 1:48 – still huge by any standards.
- It took conventional anti-virus software vendors a full 13 hours to come up with a signature, or 'fix', for SoBig.F after it first appeared. This meant non-MessageLabs customers were wide open to the virus for at least 13 hours. It's not hard to see how the most intrusive virus in history was able to gain such a devastating grip.

The facts in terms of SoBig.F's extraordinary proliferation tell only a part of an alarming story, however. What is less well known – and what concerns those unprotected from this menace most – is the knock-on implications for those who have been infected. Whether they yet know it or not.

This white paper explains the emerging history of the SoBig virus in its various incarnations. It explains how the virus is designed to work and why its payload is potentially so much more sinister than most previous viruses.

It also explores why the profile of a typical virus writer has shifted. While earlier virus outbreaks have been initiated chiefly by computer geeks with a yen to test their programming skills, today's threat comes from explicitly criminal elements who seek to make fraudulent profit by exploiting the potential of email viruses.

What's in it for the perpetrators of the SoBig Menace?

While many past viruses have been designed to create nuisance, at best, and wholesale corporate embarrassment at worst, viruses like SoBig have a more sinister purpose.

This underlines a significant shift in both motivation and authorship behind these new virus strains. Indeed, the email security community now faces an entirely new enemy. In the past, the typical virus writer was an individual or group of computer geeks whose motivation was not so much driven by malice as by a desire to show off their programming skills and ability to outwit the system.

That has changed. The authors of viruses such as SoBig, Fizzer and Bugbear are not geeks. They are highly-skilled programmers in the pay of criminals who recognise the potential of viruses for fraudulent activity and gain.

Viruses and spam used to be parallel threats to email security. Now we are seeing a rapid convergence between them. Virus writers are starting to use ratware to seed initial copies of viruses. Spammers are including trojans and automatic connection to porn sites in spam messages.

SoBig – a case in point

The principle objective of SoBig is to create spam proxies – that is to establish a worldwide network of subtly infected PCs that can be used to flood the Internet with millions of spam emails (unsolicited junk email).

The capability to mass-mail spam from proxy domains provides spammers with a variety of options:

- They can 'spoof' unsuspecting email users' addresses, sending out spam so that it appears to come from those individuals – without their knowledge.
- They can use those IP addresses also to host web servers, typically pornography websites.
- They can use a hijacked address to launch denial of service (DoS) attacks. This involves the deliberate crashing of the victim's servers by flooding the system with millions of spam emails. Domains affected have included several not-for-profit providers of spam blacklists, effectively disabling a key source of anti-spam capability.
- They can launch socially engineered spam emails that encourage recipients to enter personal details, enabling spammers to steal identities for criminal purposes. Just a tiny percentage of success could generate enormous profits from fraudulent use of innocent people's identities, theft from bank accounts and so on.

This was demonstrated very recently by the appearance of a spam campaign which purported to advise customers of a major high street bank that their online banking details needed updating.

It was pretty slick. Users who fell for the scam clicked on what looked like a perfectly legitimate link and arrived at a login page which looked passably like the interface page through which they normally managed their account. Here they were asked to enter details such as account numbers, passwords and so on.

You can imagine that a few bank accounts got rapidly cleaned out. And of course, the whole spamming campaign had been launched by criminals from proxy addresses which they'd hijacked to cover their tracks.

FACT: more than 80% of global spam originates from fewer than 200 known spammers in the USA. Many are based in the small town of Boca Raton in Florida, one of three states in the US which have no spam legislation in place.

And yet there is a further twist to the unfolding convergence between viruses and spam as email threats. The development of worms such as Fizzer, SoBig and Bugbear has also created new challenges for the geek virus writing community. They like to reverse-engineer existing viruses and create their own variants, a factor which poses additional new dangers to unprotected email systems.

SoBig.A first appeared in January 2003. Since then the perpetrators of this virus have been refining the capability of their insidious worm through subsequent releases, from SoBig.B through to the most recent release of Sobig.F.

The good news is that, thus far, they have failed in their ultimate purpose (see page 5). The bad news is that these people learn fast and won't make the same mistakes again. It's a certainty that SoBig.G will not be long in coming.

How does the SoBig virus work?

At MessageLabs we are able to correlate data from the viruses and spam that we have intercepted. From this we can determine the convergence between the two threats.

The data shows that between 60 and 70% (around two-thirds) of all spam is delivered via an open proxy. In other words, the spammers hijack the computers of innocent people, without their knowledge, and channel huge volumes of spam through those addresses.

As soon as this fraudulent use of the proxy is identified and measures are taken to stop it, the spammers simply move on to another open proxy which has previously been set up.

A number of viruses, such as Fizzer and Bugbear, as well as SoBig, are designed to create open proxies by planting a 'backdoor' entrance, also known as a trojan. It's estimated that around three-quarters of spam delivered by open proxy comes from domains infected in this way.

Each strain of the SoBig virus, from A to F, has been refined by the authors. Previous SoBig viruses have spread by sending out emails singly. Part of the reason why the F strain has proved to be so virulent is that it uses threading techniques to send out seven emails simultaneously.

The virus installs a backdoor component, the deployment of which is controlled via a number of IP addresses belonging to domestic users who have always-on broadband connections to the Internet. And, of course, the object is that the victim will have no idea that his or her computer has been hit by the virus.

A further concern is that the new strains of virus have been engineered to circumvent anti-virus and anti-spam software. This is done by creating a communication that has its own SMTP email engine, sending emails directly from the infected PC and thus bypassing the internal email structure.

That is why we recommend that firewalls are locked down to prevent this kind of traffic entering, except from designated email servers (further detail, see page 7).

The convergence between viruses and spamming techniques is also underlined by the manipulation of potential weaknesses in the configuration of target companies' MX records. Some domains are configured with a final backup MX record that points directly at the company's email server, rather than the spam-filtering email servers that are in place at Internet level.

SoBig is designed to target the last address in the MX record, so that the email is delivered without being scanned and intercepted. That is why we also advise caution in configuring your MX records (see page 7).

Evolution of the SoBig virus

Virus Name	Number Intercepted	First Intercepted	Expiration Date
WS32/SoBig.A-mm	856,416	9 January 2003	Ongoing
WS32/SoBig.B-mm	409,735	17 May 2003	31 May 2003
WS32/SoBig.C-mm	180,560	31 May 2003	8 June 2003
WS32/SoBig.D-mm	4,365	18 June 2002	2 July 2003
WS32/SoBig.E-mm	359,008	25 June 2003	14 July 2003
WS32/SoBig.F-mm	16,670,849	18 August 2003	10 September 2003

FACT: the initial seeding of SoBig.F was posted on an adult oriented website, using an account created with a stolen credit card.

SoBig.F ultimately failed – but what's to follow?

The unprecedented speed with which the SoBig.F virus spread certainly created disruption on a substantial scale for non-MessageLabs customers. But ironically it was SoBig.F's extraordinary proliferation which ultimately led to its failure to achieve its real objectives.

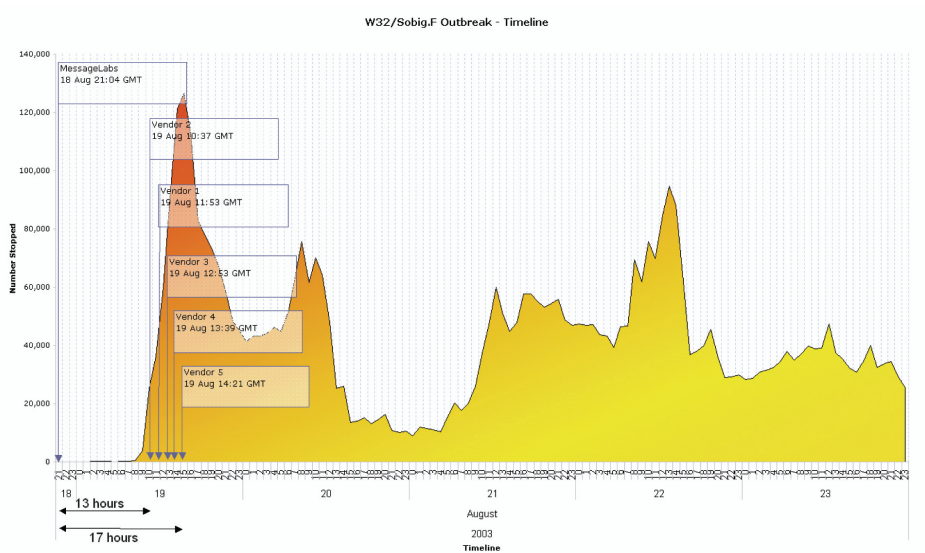
Success in planting trojans relies significantly on stealth, since the key requirement is that the 'cuckoo in the nest' should not be noticed. But SoBig.F attracted so much media attention that the authors' plans went awry before its staged progress could be implemented.

SoBig.F was released into the wild on Monday August 18. Within 24 hours it had spread worldwide. However, its second download stage was designed to activate five days later – giving time for the master servers, the IP addresses of which were encrypted in the body of SoBig, to be shut down and made safe before the download could activate.

This is why a further release of the SoBig virus is expected imminently. And it's a racing certainty that the authors won't be making the same mistakes again.

We expect that the design of SoBig.G will schedule the second-stage download to begin much sooner after the initial spread, rather than waiting five days. We also anticipate that the authors will use another route to control the IP addresses of the master server, possibly through an insecure DNS server.

The explosion of the SoBig.F virus



The graph shows the proliferation of SoBig.F by numbers intercepted by MessageLabs. It also illustrates points in the time-line where conventional email security vendors were able to provide a signature – the first of which became available only 13 hours after MessageLabs intercepted the first copy.

How MessageLabs protects against email viruses, spam and porn

It is highly significant that MessageLabs identified, named and stopped the SoBig.F virus as soon as it appeared. And the first of the conventional AV software vendors was only able to provide a signature fix for the virus 13 hours later.

That 13-hour difference demonstrates why MessageLabs is the leading provider of managed email security services for businesses worldwide. Our global infrastructure acts as the first and strongest line of defence by scanning email and eliminating threats such as viruses, spam and other unwanted content before they can reach customers' internal systems.

At the heart of our email security system is Skeptic, MessageLabs' unique predictive technology architecture. Skeptic uses patented artificial intelligence and learning from an ever-expanding knowledge base of email security threats to identify viruses, spam and pornography – without the need for those time-delayed updates which hamper the effectiveness of conventional software.

The lesson of SoBig experience shows that the integrity – and therefore the vital usefulness – of email has never been more seriously compromised than it is at present. It also underlines how crucial it is for today's business email systems to be properly protected against these threats.

The MessageLabs Email Security System protects against viruses, spam, pornographic attachments and other harmful or unwanted email content. We urge any business or other organisation which is not adequately protected to act now.

But in the meantime...take the following precautions

Ideally, we trust that awareness of the dangers posed by new strains of virus like SoBig will go some way to create more permanent behavioural changes that make future versions of this and other similar viruses less pervasive.

Regardless of the next strain's impact, businesses can adopt quick and specific measures to defend against the new type of threat that SoBig presents, which uses virus and spam techniques to increase system infection rates and ultimately disrupt business in today's global information economy.

A full list of security recommendations is given on page 7. However, in general, MessageLabs advises companies to adopt basic security measures:

- 1. Changes at the user level:** Update or implement email security policies that instruct employees to refrain from opening suspicious emails and attachments. Circulate and post virus alerts to intranets so that employees know what physical forms viruses are taking.
- 2. Changes at the network level:** Ensure any machine connected to the Internet is secured through a firewall that does not permit connections on ports that are unused or unnecessary. Properly configure firewalls to block access through these ports to prevent worms from spreading.
- 3. Changes at the Internet level:** Implement an Internet level email scanning service, such as the MessageLabs Email Security System, to stop email-borne threats before they reach the corporate network.

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