



>TANGLED WEB : UNDERCOVER THREATS , INVISIBLE ENEMIES

>AUTHOR: MARK SUNNER, CHIEF SECURITY ANALYST, MESSAGELABS



>CONTENTS

THE SECRET WAR	>P1
SPYWARE: AGENT OF CHAOS	>P2
EXPOSING THE SPY	>P3
WEB OF INTRIGUE	>P4
INFORMATION IS PROFIT	>P5
YOUR BUSINESS: CAUGHT IN THE CROSSFIRE	>P6
HOW TO WIN THE WAR	>P7

THE SECRET WAR

The enemy you can't see is usually the hardest to fight. And it's the adversary who doesn't operate out in the open that can often do the most damage. They move in the shadows, constantly changing tactics and repeatedly altering their point of attack. Elusive and dangerous, they may emerge briefly from their cover – only to vanish again just as quickly.

COMPUTERS ARE ATTACKED WITHOUT THEIR USERS EVER KNOWING IT.

The world of messaging and web security has seen striking growth in just this type of activity. Anonymity, deceit and subterfuge are now established weapons in the arsenal of the 'bad guys' targeting organisations like yours with profit-reducing malware, spam and scams. Increasingly, this enemy's ultimate aim is to access intellectual property and other confidential data – just the sort of information you can't afford to fall into the wrong hands. Now motivated by commercial gain rather than pure malice, these masters of disguise pose a greater threat than ever to the health of your business.

Long gone are the 'good old bad old days' when threats generally had an instant and obvious effect – when many businesses simply warned employees not to click on dubious-looking email attachments in case their computers became infected with a virus or some other unwelcome visitor. Today we are seeing a rising tide of dangers that are more cunning, harder to pin down and much more difficult to defend against.

Many of these attack computers without their owners or users ever knowing it, often as a result of visiting an innocuous-looking website. Another key trend is the delivery of malware via 'bad' weblinks rather than the traditional email attachment – a rapidly escalating trend that is proving a more efficient (and ultimately more lucrative) way for the bad guys to realise their objectives. And much of the time those objectives involve the secret pilfering of business-critical information from your organisation.

Examining recent developments in the threat landscape, this MessageLabs White Paper focuses on the emergence of the web and covert information-gathering as key battlegrounds in the ongoing war against malware propagators and the criminal gangs increasingly active in this field. Above all, the paper highlights the crucial danger points for any business that doesn't defend itself adequately against undercover threats and invisible enemies. But it also outlines a ready-made solution that can protect your business, immediately, comprehensively and cost-effectively.

**THE WEB HAS
INCREASINGLY
BECOME SPYWARE
GANGS' WEAPON OF
CHOICE.**

The information presented here is based on MessageLabs hands-on experience of providing proven messaging and web security management services for over 17,000 clients worldwide, with around 2.5 billion attempted SMTP connections processed every day on their behalf.

SPYWARE: AGENT OF CHAOS

Perhaps the best-known example of an undercover threat is spyware, which first appeared around five years ago. Essentially, spyware is software that gets onto a computer's hard drive without the user's explicit and knowing agreement. In some cases, 'permission' for spyware to install itself is buried deep in the small print of a licensing agreement. In other cases, permission is not given at all.

Once installed, the spyware secretly tracks the computer user's web browsing behaviour, logs websites visited and passes this information on to advertisers – all with the consummate skill of a professional pickpocket. The computer then finds itself flooded with a torrent of irritating pop-up adverts, pricelists etc broadly related to the user's browsing behaviour. Hence the other name commonly given to spyware – 'adware'. The user, meanwhile, remains oblivious to the fact that their machine has been infected. Pop-ups are a common feature of the electronic landscape, so it's not always obvious when spyware is to blame for their appearance.

Spyware usually gains access to a computer by camouflaging itself among other software (eg a free screensaver or a music file) which the user has agreed to download. Ironically, it's often concealed in downloadable software claimed to be 'spyware-free' or 'adware-free' – and even in many 'anti-spyware' applications! As for the actual delivery mechanism, this may be an email attachment, but weblink/ website downloads have increasingly become the spyware gangs' weapon of choice.

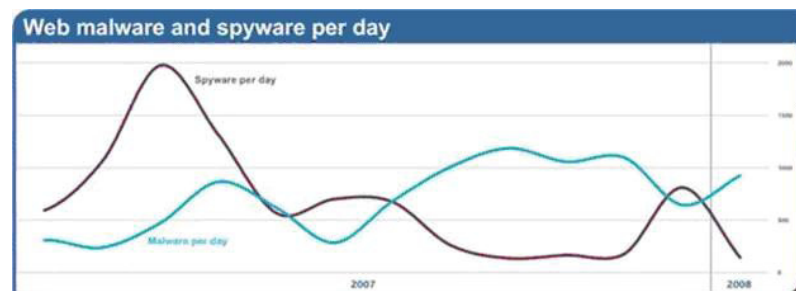
Like any good spy, spyware is designed to go about its stealthy business unnoticed, concealed from a computer's operating system and even from much of the advanced security hardware/software in use today. As well as its expertise at infiltrating computers in the first place, spyware is equally adept at staying there. Frequently, it will break itself up into a number of pieces and hide in different parts of the hard drive. If one piece is detected and deleted, the spyware will simply rebuild itself using the pieces that survive.

Spyware has developed into a multi-billion dollar global industry, often operating in the grey area between legal and illegal. In many cases, adverts for reputable companies appear on computers as a result of spyware. But those companies may be totally unaware of the fact – their adverts having been passed down a convoluted chain of distributors without their knowledge.

Of course, it's the businesses which fall victim to spyware that are left to pick up the bill. Unsolicited pop-ups are not just an irritating nuisance. Their deletion from computer screens is a time-wasting distraction from more important tasks. Moreover, as they enmesh themselves, spyware programmes act as a serious 'drag' on the functionality of individual machines and entire networks – an efficiency-compromising burden that businesses can well do without.

EXPOSING THE SPY

Despite the serious damage it can do, spyware accounts for a relatively small component of overall 'bad' internet traffic. In fact, in recent months, MessageLabs has actually detected a reduction in this proportion. In December 2007, spyware accounted for 55.7% of traffic; by January 2008, this had declined to 10.9%.



This should not be mistaken, though, for a sign that the virulence of the spyware itself is declining. Indeed, in terms of ingenuity and sophistication, spyware has continued to evolve. Some current breeds can even track the keys you press when you enter a password. Others can hijack online banking sessions after authentication has been completed.

Nevertheless, important new developments are now acting as a constraint on the spyware industry. Foremost among these is the deployment of legal machinery against the perpetrators of spyware. In particular, a current lawsuit involving New York-based spyware company Direct Revenue is causing significant ripples. The key issue at stake is whether computer users should be made more aware of the software they download onto their machines, and whether it really is satisfactory for permission for a software download to be concealed in small print.

SPYWARE REPRESENTS THE TIP OF A HUGE ICEBERG.

Fearful of being stigmatised, mainstream advertisers and leading brands are now taking greater precautions to ensure they have nothing to do with spyware. This in turn means some key markets are being choked off, making it harder for spyware propagators to operate. In response, the spyware industry is increasingly launching its attacks from countries where there are fewer (or even no!) legal and regulatory constraints on their operations.

WEB OF INTRIGUE

But the real significance of spyware is that it represents the tip of a huge iceberg. On one level, it forms part of a whole suite of weapons that have been converging over the last two years. The result has been the unleashing of new types of much better targeted, fundamentally stealth-based attacks on computer users around the world. Because such 'surgical strike'-style attacks are more likely to slip under the security radar, they are much more likely to succeed. The application of social engineering techniques has also played a key role in this evolution.

A classic instance of such convergence neatly harnesses spyware's ability to equip scammers with a sniper's rifle rather than a blunderbuss. It involves using the information that spyware gathers about individuals and organisations to maximise the chances of launching a successful 'phishing' attack. Phishers send out legitimate-looking emails designed to dupe recipients into supplying high-value, confidential data. Including authentic information about the recipient or their company can significantly increase the odds of the email attracting a 'bite'.

To take another example, controllers of 'botnets' – networks of internet computers that, unknown to their users, have been set up to forward spam, viruses etc to other computers – now frequently install spyware onto their victims' machines. This generates incredible amounts of data on the users' passwords, online purchases etc, which can be used to target them with 'phishing' and other attacks.

Today, though, one of the biggest icebergs of all relates to the web. As noted earlier, spyware typically downloads itself when a victim clicks on a hyperlink leading to a rogue website. But now we are seeing this approach extending to other forms of malware too. Three years ago, almost every virus was disseminated via an email attachment. Over the last 18 months or so, however, traditional viruses have begun to appear in web traffic as well. Increasingly, hyperlinks are the preferred delivery mechanism. Why? Because most security solutions don't follow such links. Instead, they simply read them as body text. Threats

SPOOFING IS ALREADY RIFE IN CORPORATE CIRCLES.

hidden behind 'bad' weblinks are therefore not identified, unwary users quickly fall prey to them – and the bad guys enjoy a higher rate of success.

A key development that underlined this sea change in the threat landscape was the emergence of the StormWorm virus in early 2007. Building on the earlier SpamThru virus, StormWorm harnesses a whole host of phenomenally clever and incredibly sophisticated techniques to propagate itself. For instance, it switches the botnet computers it uses every three minutes (so called 'fast flux' or 'bullet proof hosting'), making it virtually impossible to thwart a StormWorm attack once it's under way. And the emails sent out during an attack always contain a hyperlink to a website, where the primary payload – the StormWorm virus itself – is contained.

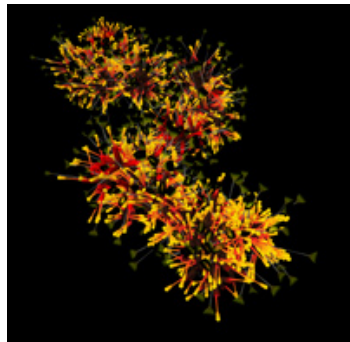


Image generated from actual source code

Image 1: A keylogger Trojan,

As StormWorm demonstrates, the web is becoming a new front line, a key territory to be fought over by scammers and security vendors. Volumes of spyware may be going down, but the overall problem of which spyware is a part is heading inexorably in the opposite direction. Indeed, by February 2008, around half of all the bad email traffic detected by MessageLabs contained a hyperlink.

INFORMATION IS PROFIT

Spyware can also be seen as the advanced guard of another kind of surreptitious web-based threat with the potential to deal enormous damage to business. The primary aim of spyware has always been to gather data – without the victim being aware of the fact. It's this desire to obtain unauthorised and illicit information (plus the knowledge that the information can be turned directly into financial profit) that has become a key driver of criminal activity in the world of the 'underground internet'.

**MESSAGELABS
LINK-FOLLOWING
FEATURE IS
ABSOLUTELY
UNIQUE .**

It's no exaggeration to say the internet overflows with opportunities to dupe people into sharing privileged information or making unguarded, indiscrete comments about themselves or their employers. And there's no shortage of scammers queuing up to exploit those opportunities.

The comparatively new phenomenon of social networking is a classic case. Almost 50% of all UK web users now participate in this activity, with social networking websites such as Facebook, MySpace and Bebo proliferating in the last couple of years. A rapidly growing number of business-oriented sites, like LinkedIn, Viadeo, Huddle and BT Tradespace, are also competing for attention.

Undoubtedly, social networking offers many potential business benefits. But the underlying and overriding problem remains – it's impossible to know if the people you converse with in this medium are really who (and what) they say they are. Spoofing, where impostors pose as authorised users to gain access to (or credibility within) a social network, is already widespread in corporate circles. Even so, it's incredible just how much confidential information is exchanged and how many risks with sensitive data are taken as a result of social networking. Again, it's business that pays the price.

YOUR BUSINESS: CAUGHT IN THE CROSSFIRE

Make no mistake. Although they and their effects are not always immediately visible or obvious, the undercover – and increasingly web-based – threats now rife across the internet pose a significant commercial risk to businesses. No organisation can afford to believe it won't become a casualty in this particular dirty war. No business can rely on email security measures alone and ignore or underestimate the dangers also posed by the web.

It's not just a matter of minor inconvenience or modest financial cost. These threats have the potential to undermine your operations and damage the very foundations on which your performance is built. Intellectual property and other confidential information may leak out or be lost completely. Your ability to demonstrate compliance with ever more stringent data security regulations will be compromised. Vital electronic communications may be impeded and employee morale and productivity may take a major hit.

Trying to combat these threats can be a huge challenge. The level of expertise deployed by scammers today is every bit as high as that found in the upper echelons of the messaging and web security industry. Confronted with this reality, it's clear that in-house IT specialists, budgets and facilities face an impossible struggle in terms of tackling the challenge successfully. However much is invested in software, appliances and upgrades, it's never going to be enough to provide the level of security and peace of mind that business needs.

HOW TO WIN THE WAR

Little wonder, then, that outsourcing the problem is growing in popularity. But of the many vendors offering 'comprehensive messaging and web security solutions', which is the best one to choose? Which has the right weapons to fight back against the rise of web-based threats and clandestine data gathering? Above all, which is best-placed to deal with the disorienting world of deception and illusion that the threat landscape has become?

MessageLabs offers integrated web and email security services proven to stay a step ahead of the bad guys. Its Web Security service, for example, includes anti-spyware and anti-virus protection, as well as industry-leading converged threat analysis which ensures that threat intelligence learned from email is also applied to web security. The service's state-of-the-art URL filtering capabilities also enable businesses to develop low-risk web usage policies that precisely meet their needs.

Moreover – and absolutely invaluable given today's shifting threat profile – MessageLabs Email Anti-Virus service incorporates a unique link-following feature designed to detect links in emails that lead to harmful web content. No other vendor can match this capacity to check every single incoming email for bad weblinks, which in turn, can further bolster web security.

Armed with capabilities like these, MessageLabs is superbly equipped to carry the fight to scammers all over the globe – and to reassure its millions of clients that the good guys really can overcome the bad guys in this particular war.

For a free trial of MessageLabs Web and Email Security services please visit [**www.messagelabs.co.uk/trials/free**](http://www.messagelabs.co.uk/trials/free)

>WWW.MESSAGELABS.CO.UK
>INFO@MESSAGELABS.COM
>FREEPHONE UK 0800 917 7733

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 20 7291 1960
Fax +44 (0) 20 7291 1937
Support +44 (0) 1452 627 766

>NETHERLANDS

De Geelvinck, Office 5.06
Singel 540
1017 AZ
Amsterdam
Netherlands
Tel +31 (0) 20 5 222 393
Fax +44 870 238 4401
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Cullinganlaan 1B
B-1831 Diegem
Belgium
Tel +32 (0) 2 403 12 61
Fax +32 (0) 2 403 12 12
Support +44 (0) 1452 627 766

>DACH

Feringasträße 9a
85774 Unterföhring
Munich
Germany
Tel +49 (0) 89 189 43 990
Fax +49 (0) 89 189 43 999
Support +44 (0) 1452 627 766

>AMERICAS

>AMERICAS

HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Tel +1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>CENTRAL REGION

7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
Tel +1 952 886 7541
Fax +1 952 886 7498
Toll-free +1 877 324 4913
Support +1 866 807 6047

>CANADA

First Canadian Place
100 Kings Street West, 37th floor
Toronto, ON M5X 1C9
Tel+1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>ASIA PACIFIC

>HONG KONG

Unir 1601, 16F
Lippo Centre, Tower 2
Tower II
89 Queensway
Admiralty
Hong Kong
Tel +852 2111 3650
Fax +852 2111 9061
Support: +852 2111 3658

>AUSTRALIA

Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia
Tel +61 2 8208 7100
Fax +61 2 9954 9500
Support +1 800 088 099

>SINGAPORE

Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
Tel +65 6232 2855
Fax +65 6232 2300
Support +852 2111 3658

>JAPAN

Bureau Toranomom 3rd Floor
2-7-16 Toranomom Minato-ku
Tokyo 105-0001
Japan
Tel +81 3 3539 1681
Fax +81 3 3539 1682
Support +852 2111 3658

