MessageLabs

SYMANTEC
HOSTED
SERVICES
™

TARGETED TROJANS: TAKING AIM AT BUSINESS

JANUARY 2010

AUTHORS:

DAN BLEAKEN, MALWARE DATA ANALYST,
MESSAGELABS HOSTED SERVICES

MAT NISBET, MALWARE DATA ANALYST,
MESSAGELABS HOSTED SERVICES

TONY MILLINGTON, MALWARE DATA ANALYST,
MESSAGELABS HOSTED SERVICES

MARTIN LEE, MALWARE DATA ANALYST,
MESSAGELABS HOSTED SERVICES

CONTENTS

EXECUTIVE SUMMARY

Even in a world where internet threats present an ever-evolving and increasingly sophisticated danger to business, targeted trojans pose a particularly potent threat that can deal devastating short and long-term damage to their victims.

Aimed and delivered with sniper-like precision, the targeted trojan's objective is to slip through an organisation's defences and cleverly dupe the recipient into downloading a malicious 'trojan' program onto their computer.

Expertly concealing itself from detection, the trojan then hunts down key confidential data and leaks it back to the trojan's controller – almost certainly a professional cyber-criminal located anywhere in the world.

Organisations falling foul of an attack can be faced with crushing bills running into thousands or even hundreds of thousands of dollars. Lost business, bad publicity, plunging share price – these are just some of the potential consequences of a successful attack.

Sometimes the damage will be noticeable almost instantly. But at other times it may not. The trojan may, silently and secretly, lie hidden for weeks, months or years, slowly but surely undermining the targeted organisation and imperceptibly eroding their performance and ability to compete.

Unfortunately, it's only too easy to become a victim of a targeted trojan. That's why MessageLabs hosted services provide businesses with industry-leading protection based on unique proprietary threat detection and prevention technology.

INTRODUCTION: DECEPTION AND DISASTER

Imagine you're a cyber-criminal. You know businesses keep all kinds of confidential and sensitive data on their computer systems. Intellectual property. Product designs. Strategies. Specifications. Customer records. Bank account details. Data you could use, abuse and monetarise – if only you could access it.

All you need is a way of infiltrating those systems, pinpointing valuable data and leaking it out undetected for as long as possible. You could then use the data yourself or sell it on, perhaps to your victims' competitors. Either way, you win – while your victims take a huge hit to their revenue, reputation and competitive edge.

Alarmingly, a weapon of precisely this kind is now firmly established in the sinister arsenal wielded by the increasingly formidable and professional cyber-crime industry. It's known as the targeted trojan. And it's one of the most invidious, insidious online threats ever devised.

Usually borne by email, a targeted trojan attack is crafted with care, harnessing trickery and cunning to win your confidence and break through your defences, before feasting on your business-critical data. In other words, it's the internet threat that invites itself round to your place – and then steals your jewellery.

Moreover, it's a threat which absolutely no organisation can afford to ignore. Initially, its sights were trained on big corporations and public sector organisations. But now it's evolved into a genuinely mainstream danger, afflicting small and medium-sized businesses too. Indeed, such is its ingenuity, even compliance with recognised data security Standards is no guarantee of immunity.

This White Paper explains exactly what targeted trojans are, how they strike – and just how easy it is to fall prey to this form of industrial espionage. It underlines the scale of the potential losses that may result. But it also describes steps you can take to keep your organisation safe from this callous and cold-blooded threat.

The information presented here is based on MessageLabs hosted services' experience of providing messaging and web security management services for over 29,000 clients worldwide, with approximately 3 billion attempted SMTP email connections and 1 billion web requests processed each day on their behalf.

KEY CHARACTERISTICS

The quirky term 'trojan' was inspired by the Trojan horse of classical mythology. Ostensibly a gift to the people of Troy, the horse concealed warriors who infiltrated the city and helped consign it to oblivion. In some ways, then, 'trojan' is an extremely apt name for a malware program that lies hidden with evil intent.

In other ways, it's very misleading. There was only one Trojan horse – and it stood out a mile. But key to a targeted trojan's success is its ability to merge into the ocean of emails constantly circulating on the internet. It's like spotting a pickpocket in a rush hour crowd. And with 'off the shelf' trojans now available online at modest prices, there's no lack of criminals queuing to use them.

First appearing on the internet security radar around five years ago, targeted trojan attacks rely on two key components: an infected file concealing an embedded trojan and a covering email designed to carry the infection into the heart of your organisation.

The aim is to make both components look innocent and innocuous. So the attachment is likely to be a .pdf, .doc, .xls or .ppt file with a name that suggests it's a legitimate business document or something of topical interest. Similarly, the covering email appears to come from a trustworthy (but actually spoofed) source.

Crucially, these attacks are preceded by often painstaking research about the victim – even down to the level of a specific individual in a target company. Using easy-access sources (e.g. the internet), the attacker builds up a profile of their victim and then decides how best to dupe them into opening the infected attachment – and inadvertently downloading the hidden malware onto their machine.

It's the made-to-measure threat with the personal touch. And it's this degree of targeting that makes the targeted trojan so adept at achieving its objectives – be they data leakage, keystroke logging or amendment/deletion of critical business files.

The deception may be so successful that the recipient forwards the email to colleagues, propagating the attack further. Moreover, the perpetrators often monitor their victims in search of legitimate files or emails that can be used as the basis for attacks on other individuals or organisations – a warped form of recycling by any standards.

Targeted trojans, then, represent the cutting-edge in covert surveillance. And while some have essentially short-term objectives, many aim to deal out smaller-scale but longer-term damage without attracting attention. In fact, this can be a highly lucrative tactic, enabling the attacker to siphon off valuable data, unimpeded, over weeks, months or years, leaving the victim none the wiser why their organisation is underperforming.

KEY STATISTICS

So how likely is it that your organisation will become a victim? Although, in percentage terms, targeted trojans are rare compared to other internet threats (e.g. spam), this rarity actually makes them less obvious, less liable to detection and therefore more dangerous. What's more, there are still an awful lot of targeted trojans in circulation. Figure 1 illustrates how MessageLabs hosted services block hundreds or thousands of these attacks each month:

2005	2006	2007	2008	2009..	Recent Peaks
2	1	10	50	60	357
per week	per day avg.	per day avg.	per day avg.	per day avg.	per day

Between May and Octover 2009, targeted trojans were launched at 2.7% of MessageLabs clients. If left unblocked, each one could have inflicted crippling damage on its victim.

The exact picture, though, varies from region to region: 1.9% of clients in Europe, the Middle East and Africa were targeted, compared with 3.6% in the US and 4.8% in the Asia-Pacific region.

Figure 2, which breaks down the attacks by type of attachment, shows that pdf (41.2%) is currently the format of choice. One key reason for this is likely to be that pdf readers are freely available to download onto PCs. Another is that the cyber-criminals behind the attacks probably hope to exploit the widespread and long-held – but now, sadly, outdated – perception that pdf is a 'safe' file format.

In terms of the most targeted sectors during this same period, Government/Public Sector (19.5% of clients), Minerals/Fuels (17.4%) and Telecommunications (13.6%) topped the list. However, September and October 2009 saw a marked increase in the targeting of IT service companies.
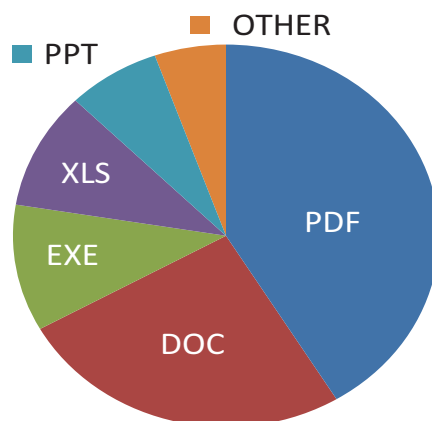

Figure 2: File types used in targeted trojan attacks blocked by MessageLabs hosted services, May to October 2009.

Significantly, those 19.5% of Government/Public Sector clients were the targets for a massive 34.7% of attacks launched. In other words, the same organisations were often repeatedly targeted. Similarly, in the Finance sector, 4.3% of clients were attacked but these accounted for 10.6% of all attacks. Again, a number of organisations appear to have been selected as special targets by the cyber-criminals.

Analysis also shows that certain words tend to crop up more frequently than others in the subject lines of targeted trojan emails. Among the most common over the last two years have been 'China', 'Obama', 'North' and 'Industry'. Moreover, their peak usage has tended to tie in with particular news events (e.g. 2008's US Presidential Elections saw a huge upsurge in what might be termed 'Obamail').

The evidence, then, clearly points to attackers taking the trouble to stay abreast of current affairs, in much the same way as spammers do. But the key difference is that, with targeted attacks, the selected news events are almost always of a political nature – fairly predictably in view of the fact that Government/Public Sector bodies are the most popular target.

As Figure 3 shows, 60% of targeted trojan attacks are directed at senior or medium-level staff within the targeted organisations (e.g. Director, Executive Director, Senior Commercial Manager, Head of Research, Chief Political Correspondent, Manager – Global Marketing Communications etc.).

Clearly, the cyber-criminal community has cynically calculated that these individuals are the most likely to have direct access to the most lucrative data. Sometimes, however, the attacker adopts the opposite approach, mailing staff of low seniority (secretaries, general enquiry, recruitment and other mailboxes etc.) – quite possibly in the hope that they will be less likely than their higher-level colleagues to recognise an attack.

An interesting footnote to Figure 3: it was extremely easy for MessageLabs analysts to find job titles and seniority details for most of the staff targeted, simply by using internet search engines. This underlines how simple it is for cyber-criminals to mine the internet for data that can help focus their targeted trojan attacks.
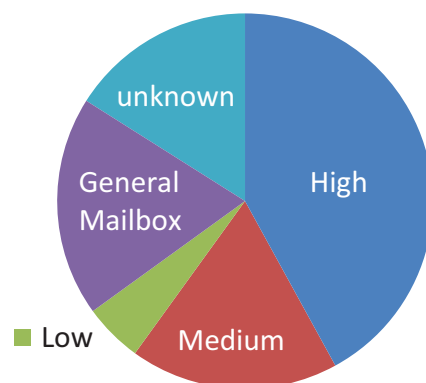

Figure 3: Seniority of intended targeted trojan recipients, May to October 2009, based on MessageLabs hosted services data.

BECOMING A VICTIM: THE THREE C'S

Credulity, curiosity, complacency. These are the key human characteristics that the cyber-criminals who orchestrate targeted trojan attacks try to exploit to lure their victims into taking their poisoned bait.

All it needs is for a target to drop their guard and suspend their critical faculties for a few short seconds – and irreparable damage could be done to their organisation.

Cyber-crime has developed into a sophisticated and well-organised growth industry. And as part of this development, its expertise now extends well beyond purely technical know-how and encompasses a genuine understanding of human nature and how to manipulate it.

It's simply a question of finding the right button to push. Some victims might respond to emails purportedly containing important corporate data. Others might be more enticed by messages referring to high-profile local, national or global news stories. Others might respond to something more personal.

From the criminal's viewpoint, there's really no shortage of options. Last autumn, for example, MessageLabs detected a trojan-bearing email pretending to come from a well known search engine and inviting the recipient to open the attached file to fix a (non-existent) software bug.

Furthermore, the fact that many attacks are purpose-built 'one-offs' makes it extremely difficult for conventional anti-malware defences to ward them off. Plus, of course, cyber-criminals are all too ready to vary their tactics in their quest to find a weak spot.

In November 2009, for instance, MessageLabs detected a new breed of 'machine gun style' targeted trojan attack. Unlike the usual pattern, where two or three emails are sent to a company and thorough research ensures they reach appropriate, legitimate email addresses, this type of attack sends hundreds of copies of the same email to a single organisation – hitting both legitimate and non-legitimate addresses. Just like a machine gun, some bullets will miss but others will find their target.

Whatever the means of infection, the scale of the damage done can be truly eye-watering. One US-based financial company recently saw almost half a million dollars siphoned from its bank account by a trojan concealed in an email attachment. Clearly, the stakes for business are phenomenally high.

STEP BY STEP: UNLEASHING AN ATTACK

So what exactly is involved in setting up and launching a targeted trojan attack? Although the details may vary from one attack to another, the basic shape generally conforms to the following tried and tested four-step methodology:

1. The cyber-criminal identifies the organisation which will be their target – perhaps a successful company with a particularly popular product. The internet will frequently be a key tool in this identification process.

2. The cyber-criminal tries to pinpoint individuals within that organisation who are likely to have access to key corporate, product-specific or other valuable data. Again, much of the required information is likely to be freely available on the company's website or in its publications, although 'innocent' telephone enquiries to the company can also generate target names and detailed data about them (including their email addresses).

3. The cyber-criminal then shapes the attack to give it the best chance of success. Fundamentally, this means tailoring the message/attachment to the responsibilities and interests of the intended victim. A vital part of this process typically involves setting up an email account which will generate a 'sender' address not likely to arouse suspicion – especially in the context of the subject line contained within the message.

    Depending on the level of social engineering applied (and social networking websites, in particular, are a goldmine of information in this respect), it may even be possible to include in the sender address the name of someone the victim actually knows – and possibly even within their own organisation. This vastly improves the cyber-criminal's chances of success.

    Of course, the closer the email subject and the purported sender correlate, and the more relevant and interesting the subject line and attachment name, the better the odds of the trojan getting through. Email messages entitled 'Draft Figures for the AGM', 'Customer Complaint' or 'Invoice', for instance, are in themselves unlikely to raise many suspicions.

4. The email is sent. If the recipient is successfully duped into opening the infected attachment, the trojan program downloads itself, completely undetected, and can begin to seek out and harvest confidential data – and then transmit it to the cyber-criminal via the internet. The attack may comprise an immediate 'big hit' or a more low-key, surreptitious but equally destructive leaching of data over an extended period. Whatever the case, the criminal turns the data to a quick profit while the compromised company is left to pick up the bill.

HALL OF INFAMY

There's really no end to the different forms an attack can take. But here are just a few examples of targeted trojan emails, which serve to illustrate the extraordinary variety of tactics employed by those pulling the strings.

This first example employs a whole range of classic tactics common to many targeted trojan attacks. Its subject is phrased in authentic 'business-speak' and is likely to stir the recipient's curiosity and interest. The title of the attachment dovetails perfectly with the subject and aims to amplify that initial interest. Finally, the email message itself is short, enticing and ostensibly originates from a sender on first name terms with the recipient – adding to the email's apparent authenticity.

This second example tries a different approach. It uses a long and detailed message on a very specific topic, and tries to entice the recipient into opening the attached 'letter' in a number of ways.

First, it includes a tight deadline for response, creating a sense of urgency. Second, it includes the phrase "the connection between this and climate change is evident if you read the letter" to entice the recipient to click on the attachment. Third, yet more urgency is added by telling the recipient their organisation will have to opt out of the list of signatories referred to ("if we
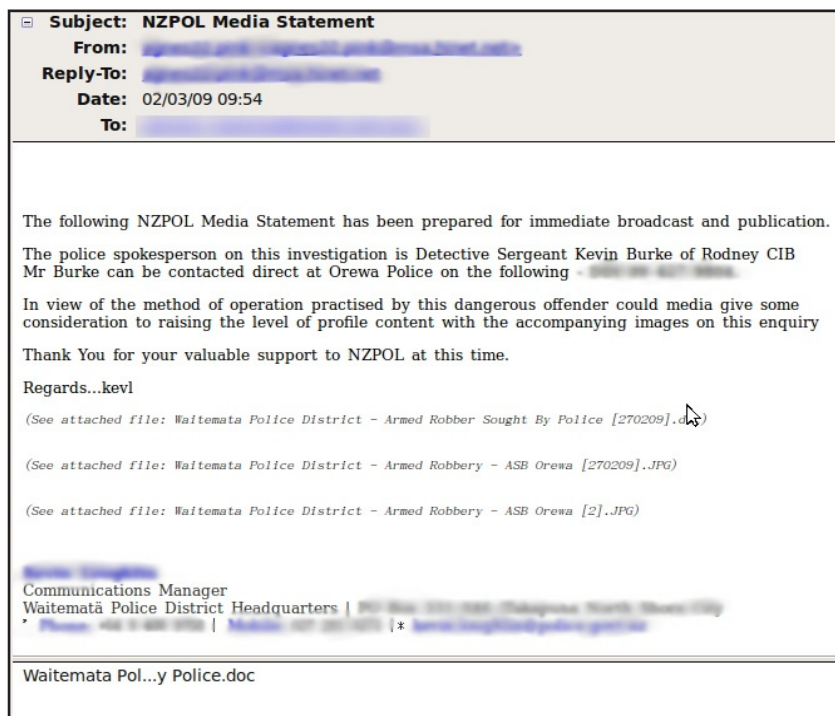
do not hear from you, your organisation will be included"). The cyber-criminal clearly hopes the recipient will check immediately whether their organisation really is listed in the attachment.

The third example addresses the recipient about a personal matter – pensions. But again a note of urgency ("last opportunity…") is injected to coax the recipient into rashly opening the attached file, even though the email originates from a freemail account.

Subject: Very Important:Last opportunity for commutation of additional pension for defence personnel

From:

Date: 20/09/09 15:06

To:

Very Important:Last opportunity for commutation of additional pension for defence personnel who retired between 01-01-2006 and 02-09-2008

pension.doc
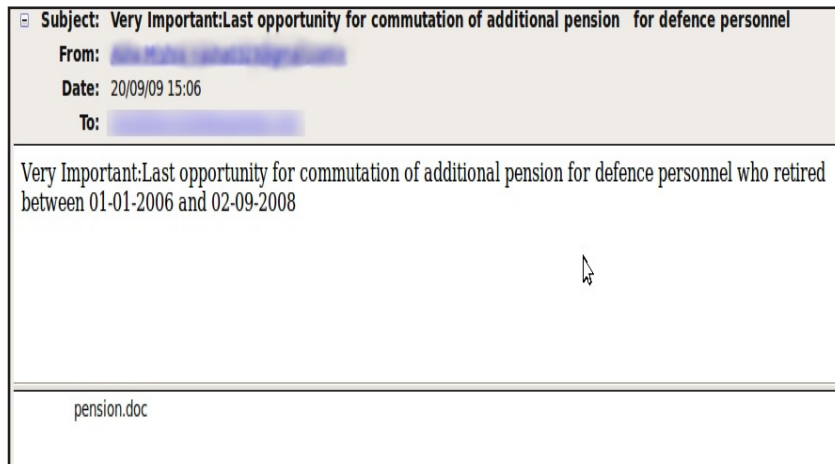
This final example plays on the recipient's sense of good citizenship, as well as their media instincts and plain human curiosity, by claiming to come from the police. To enhance the feeling of authenticity, the message incorporates a wealth of legitimate-looking contact details.

Subject: NZPOL Media Statement

From:

Reply-To:

Date: 02/03/09 09:54

To:

The following NZPOL Media Statement has been prepared for immediate broadcast and publication.

The police spokesperson on this investigation is Detective Sergeant Kevin Burke of Rodney CIB Mr Burke can be contacted direct at Orewa Police on the following -

In view of the method of operation practised by this dangerous offender could media give some consideration to raising the level of profile content with the accompanying images on this enquiry

Thank You for your valuable support to NZPOL at this time.

Regards...kevl

(See attached file: Waitemata Police District – Armed Robber Sought By Police [270209].d)

(See attached file: Waitemata Police District – Armed Robbery – ASB Orewa [270209].JPG)

(See attached file: Waitemata Police District – Armed Robbery – ASB Orewa [2].JPG)

Communications Manager
Waitematä Police District Headquarters |

` **Phone:** | **Mobile:** | * `

Waitemata Pol...y Police.doc

BLOCK THE THREAT, BEAT THE BAD GUYS

Not surprisingly, given its guile, ingenuity and precision, the targeted trojan is one of the hardest of all internet-borne security threats to thwart effectively. Not only is it custom-made to fool even the most vigilant of computer users; it also finds it relatively easy to slip though conventional internet security solutions and set about its pernicious work.

Traditional security solutions dissect the characteristics of the rogue programs they detect – in other words the viral genetic codes or 'signatures'. The information acquired can then be used to identify and block further occurrences. But this only works for malware which is already starting to circulate widely and whose characteristics can be properly analysed and understood.

An obvious parallel is the development of a flu pandemic vaccine, which is only possible once the disease has begun to spread. Such a vaccine is very good at safeguarding anyone who hasn't yet caught the disease – but no use at all to the unlucky people who have already contracted it.

In the face of a targeted trojan attack, this approach simply doesn't work. By definition, each attack of this kind is essentially a very tightly focused assault extremely limited in extent, although potentially enormous in destructive power. So it probably won't even appear on traditional security solutions' radar in the first place.

The only sure way of derailing a targeted trojan is to put each and every email attachment under the microscope, study it in depth to detect any tell-tale trojan characteristics and block any attachment that tests positive. And all in less than the blink of an eye, to avoid holding up business-critical email traffic.

Capability of this kind is far from standard issue, even in the high-tech world of messaging security. But MessageLabs hosted services are far from being standard. From its world-leading global network of state-of-the-art data centres, MessageLabs deploys its unique predictive Skeptic™ technology.

Skeptic™ specialises in blocking targeted attacks at zero hour – even those originating from previously unknown sources. Constantly learning and growing in strength, Skeptic™ is specifically designed to stay a step ahead of targeted trojans (and other threats), drilling down to analyse email attachments' encoding format in minute detail.

Crucially, you can't buy MessageLabs protection in shops. So it's just not possible for the purveyors of targeted trojans to test their creations' ability to outwit MessageLabs defences. Moreover, with its worldwide presence, MessageLabs is perfectly placed to pinpoint local and regional variations in the pattern of targeted trojan attacks – and to act swiftly and appropriately to tackle them.

Targeted trojans, then, pose a unique threat to business. But MessageLabs hosted services provide the unique protection capabilities needed to stay ahead of that threat – and to ensure your organisation doesn't join the ever-growing roll-call of victims.

Find out more about MessageLabs hosted internet security services – call us today or visit www.messagelabs.co.uk

>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
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
Munich, Aschheim 85609
Germany
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

>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
170 University Avenue
Toronto, ON M5H 3B3
Canada
Tel :1 866 460 0000

>ASIA PACIFIC
>HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8200 7100
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

✸ symantec™

Confidence in a connected world.