

# WEB THREATS 2010: THE RISKS RAMP UP

A WHITE PAPER FROM CSC AND SYMANTEC

**CSC**

CSC CLOUDPROTECTION FOR MAIL AND WEB

**CSC.COM**

BUSINESS SOLUTIONS  
TECHNOLOGY  
OUTSOURCING



## **Web Threats 2010: The Threats Ramp Up** *A White Paper from CSC and Symantec*

### Table of Contents

Executive Summary .....	3
Introduction: Web Threats in 2010 .....	3
Headline Findings .....	4
Cyber-Criminals: Strategy and Tactics.....	4
Web Users: In the Malware Minefield .....	6
A Classic Attack.....	7
CSC CloudProtection for Mail and Web.....	9

## EXECUTIVE SUMMARY

No-one can deny the phenomenal success of the World Wide Web. But its increasing prominence and importance come at a price. Quite apart from the big risks that businesses can find themselves exposed to as a result of inappropriate web use by their employees, cyber-criminals are focusing more of their resources on transforming the web into a malware minefield. Just one visit to a website infected with a virus or spyware can have serious revenue-reducing, reputation-eroding consequences for your business.

The reality is that infected websites are no longer confined to the dark margins of the internet. There are now probably many tens of thousands of them – and 90% are perfectly legitimate, often mainstream sites that, unknown to their owners, have been compromised in some way by the sophisticated, skilled and determined gangs of cyber-criminals who now dominate the online ‘underworld’.

Equally concerning is the fact that infection techniques have become much more cunning and virulent than they were just two or three years ago. In many cases, the simple act of visiting an infected website is enough to download malware onto the victim’s PC – the so-called ‘drive-by download’. And with cyber-criminals successfully extending the lifespan of many of their threats, the odds on a user stumbling on a malware-bearing website have never been shorter.

So far in 2010, the average number of website requests blocked by the technology behind CSC CloudProtection for Mail and Web is over 20% higher than in 2009. In the face of unprecedented web threat level growth, however, CSC CloudProtection for Mail and Web delivers protection of the very highest quality for thousands of businesses worldwide.

## INTRODUCTION: WEB THREATS IN 2010

Globally, an estimated 1-1.5 billion people use the internet. Every day hundreds of millions of visits are made to websites worldwide. But as usage continues to climb upwards, some accepted truths about the web have broken down. Take ‘safe surfing’, for instance. A few years ago, common sense was all you really needed to keep your computer free from infection by the malware that lurked in the shadier corners of the internet. But today, all that has changed.

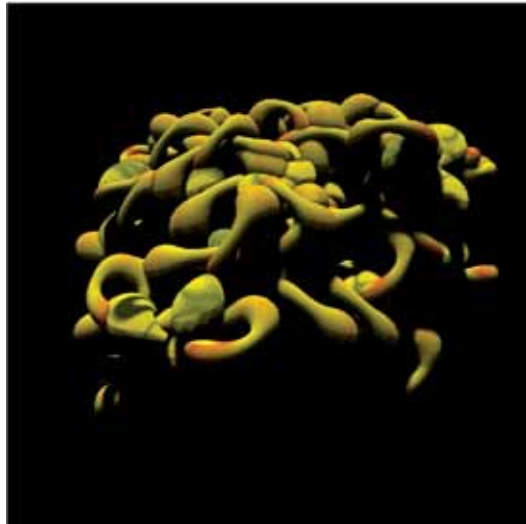
In 2010, the threat posed by the web is sharper and more extensive than ever before. Almost any website can now host malware or forward you to one that does. Indeed, an infection is much more likely to result from a visit to a perfectly legitimate website that has been compromised with a virus or spyware than from one set up specifically to spread malware. In addition, techniques such as the ‘drive by download’ – where simply visiting an infected site is enough to contaminate a PC – have become mainstream.

But getting infected is just the start. It’s what happens next that can really harm your business. For example, once the malware has breached defenses, sensitive systems and confidential data may be exposed to damage or theft, resulting in loss of revenue and/or reputation. For the increasingly skilled gangs behind the attacks, the basic aim is to seize control of computers (usually surreptitiously) and then use/abuse that control in a range of business-compromising ways.

This White Paper assesses web threats today. Its headline findings are based on the latest data gathered by Symantec’s Message Labs technology. The technology utilized by the CSC CloudProtection for Mail and Web service delivers comprehensive message security and simplifies IT management. Every week, this technology blocks over 100 million requests to visit websites infected with malware or whose content contravenes clients’ web usage policies. The paper then outlines what those findings tell us about the current tactics being used by cyber-criminals – and their implications for web users. But it also demonstrates how, in the face of web threats of unprecedented severity, your business can protect itself against them comprehensively and cost-effectively.

HEADLINE FINDINGS

- Finding 1:** 99.96% of blocks by MessageLabs Technology protect the user from inappropriate content, as defined by their employer’s usage policy. Pop-up adverts and auto-forwarding to adverts account for most of these blocks, but sites containing sexually explicit, violent and other offensive material or related to criminal activity also feature strongly. The other 0.04% of blocks protect users from malware-infected websites (‘malicious sites’), which still equates to many tens of thousands of blocks a week – representing a serious danger to business.



**Image : CIMUZ Trojan ;** allows a remote user access to and control of your computer

- Finding 2:** Looking at malicious sites, so far in 2010 the average number of blocks per client per month has increased by over 20% compared with 2009. The overall upward trend is evident in the graph below:

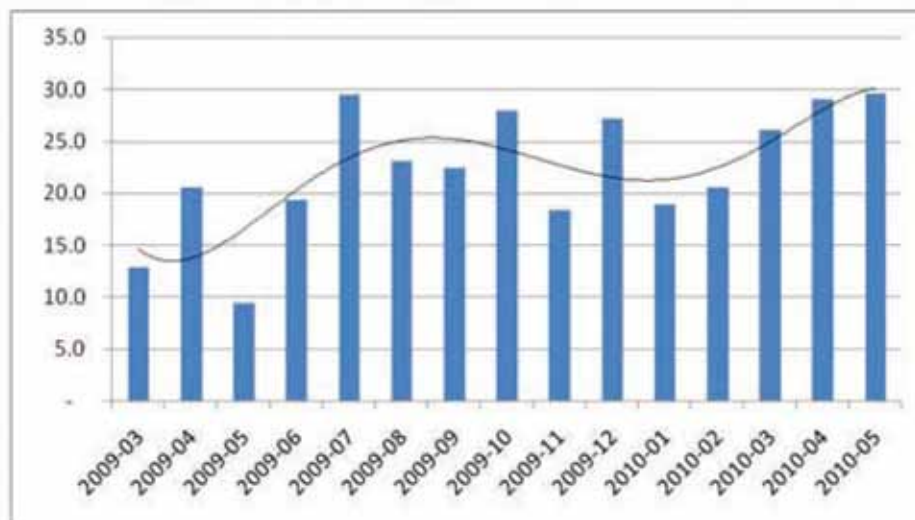


Figure 1: Average blocks by MessageLabs Technology (per client per month)

In March 2010, for instance, 42% of clients had at least one block. Clearly it is now much more likely that, within any business, at least one web user will stumble on an infected website than it was 12 or 18 months ago.

- **Finding 3:** 96% of malicious blocks are triggered by viruses and 4% by spyware (pop-up adverts, programs that track browsing behavior, programs that try to change the way browsers operate etc).
- **Finding 4:** In 2010, based on an analysis of the age of blocked domains, it can be concluded that almost 90% of malicious websites are legitimate ones that have been compromised by malware without their owners' knowledge or complicity. This compares with around 80% in 2009. The remaining 10% (20% in 2009) are malicious sites created by cyber-criminals themselves.
- **Finding 5:** As the graph in Figure 2 shows, the percentage of domains that are newly malicious each day is higher than the percentage of malware that is new each day. In other words, the domains serving up malware change faster than the malware itself. This indicates a tendency for the same viruses and spyware to be used multiple times across a number of malicious websites - the reason being that it's easier and cheaper for cyber-criminals to infect domains with malware they already have in hand than it is for them to develop new malware (or pay someone else to develop it).

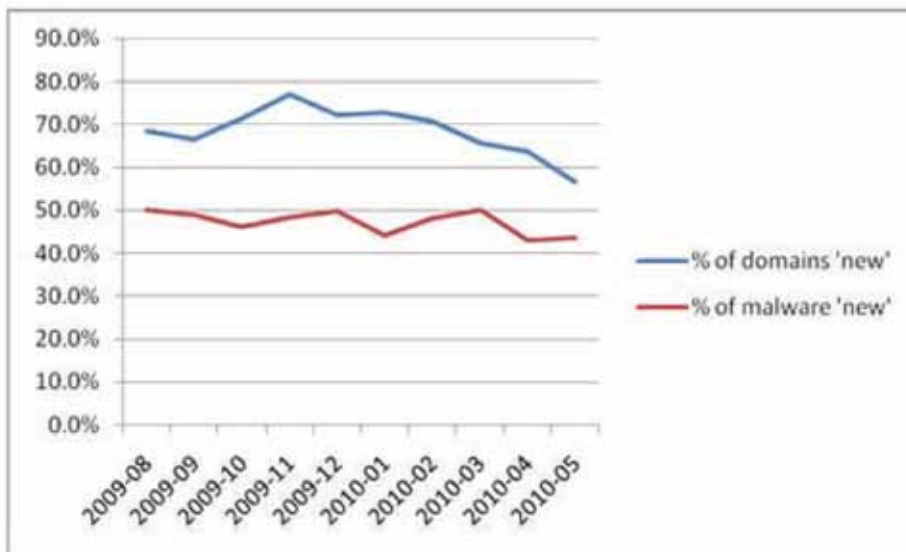


Figure 2: Proportions of domains and malware that are new each day

### Cyber Criminals: Strategy And Tactics

In the world of the internet, everything happens for a reason. So to understand web threats properly, it's vital not just to comprehend what those threats are but also to dissect the cyber-criminals' thinking in devising them.

To further their strategy of infecting as many PCs as possible, cyber-criminals frequently set up and host their own malware-infected sites. Perhaps tens of thousands of these currently litter the internet. Potential victims may be lured to such sites through blogs and social networking websites, or by spam emails and IM messages - there are all kinds of possibilities. Some malicious websites are deliberately designed to look very similar to legitimate sites and so tempt visitors to hand over personal/financial data or take actions that lead to malware being downloaded onto their machines. Or they may redirect the visitor to another website where malware is concealed.

But as Finding 4 shows, cyber-criminals are now showing a clear preference for polluting other people's sites with malware rather than setting up and hosting their own. Again, compromised websites may themselves harbour malware, with content changed by the insertion of malicious code that performs certain actions when someone visits the site, or they may redirect victims to the malware's location – perhaps via a malicious advert introduced to the site by the cyber-criminal and using a number of intermediate 'stepping-stone sites'. Unfortunately, there are plenty of techniques in the bad guys' toolkit, e.g. Structured Query Language (SQL) injection, cross-site scripting (XSS) attacks and use of stolen File Transfer Protocol (FTP) credentials, to help them compromise legitimate websites. So why has this become the preferred tactic? Key reasons probably include:

- The attraction of knowing that legitimate sites often come fully furnished with regular users and a good level of traffic in general, providing a ready pool of instant victims and eliminating the need to stimulate from scratch a flow of visitors to a newly established domain.
- The fact that visitors to legitimate websites – sites that those visitors may already be very familiar with – are more likely to have lowered their guard and are less likely to maintain the level of care and suspicion that might otherwise have helped protect them from infection.
- Measures introduced in 2008 by ICANN (the Internet Corporation for Assigned Names and Numbers) to tighten up on so-called 'domain tasting', where a new domain could be set up and deleted within five days at no cost; these measures have almost certainly acted as a brake on the establishment of bespoke malicious sites.

But perhaps the biggest reason for the emergence of compromised legitimate websites as the weapon of choice in the web war is the longevity of the threats they pose. It's a survival tactic. Cyber-criminals are hugely aided in this by the complexity of many sites, which now often consist of 100-200 components harnessing a range of media and drawing data from multiple external sources, prompting the evolution of web browsers from simple HTML viewers into full-blown software platforms. In this complex terrain, a compromise can now duck under the radar comparatively easily and stay there, unnoticed and unmolested, for some time. Even when detected, it can be a lengthy process to identify, flag up and eradicate the threat without damaging the way the website functions, especially if the threat has deliberately been made difficult to remove. And the longer the threat exists, the more likely that web users will stumble upon it.

Such durability contrasts dramatically with the fate of many new domains that serve up malware, which are often spotted quickly by the internet community and by internet security providers and then taken down comparatively quickly and easily. In fact, around 12% of these sites don't even last more than a day. Cyber-criminals are responding to this by registering more of their domains with registrars who are known to make it harder for a domain to be taken down. Overall, then, it now takes longer to deal with a malicious website – whatever its age – than in 2009:

	Bespoke malicious websites		Compromised legitimate websites	
	2009	2010	2009	2010
Threats removed within 7 days	25.4%	22.0%	8.8%	6.9%

Figure 3: Elimination of web threats

Economy of effort is one of the hallmarks of the cyber-criminal's trade. This is reflected in their quest for effective ways of extending the lifespan of threats and milking the maximum benefit from them. Hence the increasing tendency not just to pollute legitimate sites and use stepping-stone sites that add an extra layer of protection to bespoke malicious domains (bolstered by so-called 'referrer checks' to prevent probing by internet security providers), but also to make malware itself work harder and longer (thus cutting the cost of producing new families of rogue programs), as seen in Finding 5. This whole 'economy philosophy' is reflected too in the cyber-criminals' increasing reliance on and use of:

- **Funneling:** Although the number of blocks per client per month has risen by 20% this year, the average number of domains blocked per client is unchanged at 3.6. Evidently, more users are using each malicious domain – probably because cyber-criminals are focusing particular effort at widening the funnel that leads visitors to those domains (e.g. by distributing more spam, 'malvertisements', pop-ups, forwarding iframes/javascripts etc) and so increasing 'footfall' there.
- **Automation:** Cyber-criminals have access to many highly automated techniques and systems that need little or no monitoring and work day and night both to scour the web for legitimate sites that can be compromised and to register new ones. Similarly, FTP credentials stolen from previous victims can be used to compromise vast swathes of websites as part of a large-scale automated process.
- **Converged threats:** Threats are increasingly being mixed and matched, e.g. with malicious URLs appearing in emails or IM messages. This blurring of lines, with the same malware often appearing across all vectors, is further evidence of an intent to squeeze maximum value out of every threat devised.

However, we shouldn't mistake economy of effort for laziness. Cyber-criminals invest huge energy in their malevolent activities, not just at the tactical level but at the strategic level too. For example, 2010 has seen a significant increase in the average number of blocks per month performed for clients in the EMEA (Europe, Middle East, Africa) region – an increase unseen in other parts of the world. Indeed, the EMEA increase is driving the overall global rise outlined in Finding 2. All the evidence points to deliberately increased targeting of EMEA-based organizations by the cyber-criminals orchestrating web threats today.

Furthermore, as seen in Finding 5, although the number of new malicious domains (both compromised legitimate sites and bespoke malicious sites) shows a downward trend, the majority of malicious domains are still 'new', i.e. not previously encountered by MessageLabs Technology. Indeed, MessageLabs Technology blocks over 100 such domains every single day. A proportion may be well-established domains that previously went undetected, but most are almost certainly brand new malicious domains. Clearly, the gangs continue to work hard to lay new traps and create as many opportunities as possible for web users to infect their machines.

#### Web Users: In The Malware Minefield

From the user's point of view, the web isn't just a potential minefield. It's a minefield where new threats appear literally overnight and where it's impossible to know where a mine is located until it's too late. As noted above, with threats now tending to last longer than before, the probability of encountering one is greater than ever. But what has really elevated web threats to new heights is the disturbing truth that even restricting browsing to the websites of reputable organizations – sites visited every day by thousands of business and/or home users – and avoiding the temptation to click on tempting buttons or links are no guarantee of immunity.

Today, there are a phenomenal number of ways that a web user may inadvertently infect their PC, as the following – far from exhaustive – list of examples illustrates:

- **User action required** (i.e. to allow malware to run or download): following ‘click here to install’ prompts for ‘important’ software updates; accessing malicious files placed alongside legitimate music, software, movie files etc; clicking on fake adverts; responding to ‘scareware’ that claims the user has been infected with malware and tries to sell them useless or damaging virus-removing software to ‘repair’ the problem; following weblinks to malware in spam and IM messages, or on blogs and social networking sites; ‘clickjacking’ that alters the actions performed by buttons/links on legitimate webpages; etc.
- **No user action required:** the dreaded ‘drive-by download’ (see Introduction); iframe/javascript redirects; exploitation of browser/software/plugin vulnerabilities; redirected search engine queries (usually as a result of a previous infection); etc.

Unfortunately, the list of potential consequences of infection is no less extensive. Whether the victim becomes aware of the problem almost immediately (e.g. because their PC starts to run more slowly) or they remain in the dark for some time, the outcome will certainly *not* be to their advantage and may include:

- Loss of personal information.
- Financial fraud.
- Compromised computing resources/capabilities.
- Recruitment of the infected machine to a ‘botnet’, enabling cyber-criminals to control it remotely and use it to distribute spam, malware etc – in other words, the victim becomes part of the problem.

Arguably the biggest danger of all is posed by ‘trojan’ programs that secretly download themselves onto the victim’s PC. Silently and effectively, they can then gather personal data, edit or move files, modify email, browser or other software settings, change registry values, stop the PC functioning altogether, or open ports allowing cyber-criminals further access to the infected machine in order to unleash yet more damage and disruption.

### A Classic Attack

Web-based attacks are characterized by variety and variation. But the following real-life example displays many of the classic features of the web criminal’s art:

- **Step 1:** A user using a search engine (e.g. to find information on oil spills) clicks on a link that looks relevant. But they are taken to a fake YouTube page placed on a legitimate (but compromised) site selling paper shredders.

- **Step 2:** The user clicks to play the video, but it doesn't play and a pop-up invites the user to install a media codec:



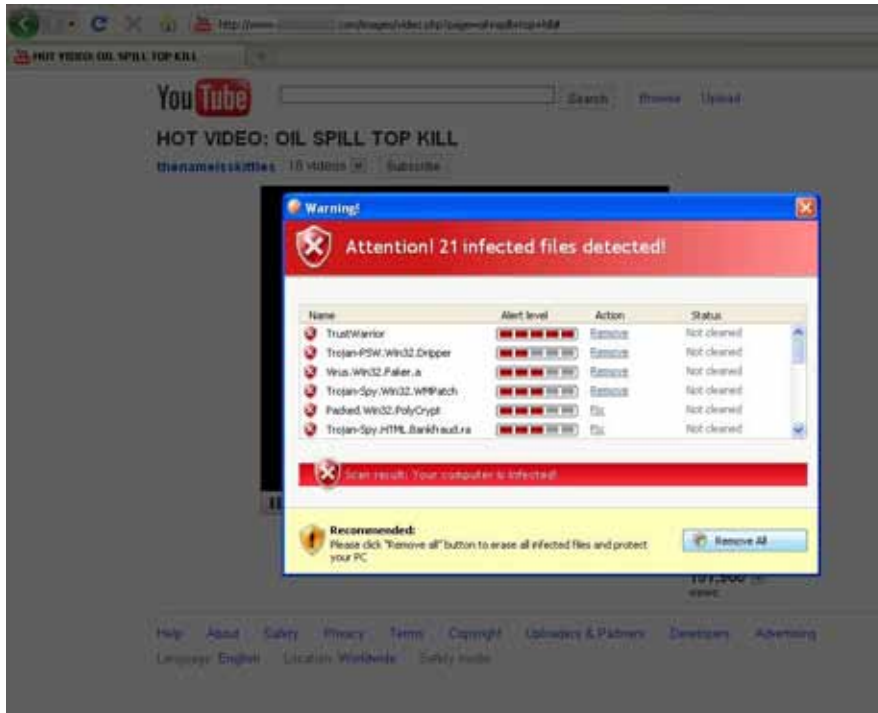
Clicking on 'ok', however, downloads an executable file from yet another legitimate but compromised website belonging to a company selling eco-friendly, money-saving products.

- **Step 3:** Another pop-up then prompts the user to run the executable file:



Clicking 'run' runs the executable and connects to a botnet.

- **Step 4:** The malicious web page instructs yet another pop-up to appear. This aims to dupe the user into believing that infected files have been detected. ‘Scareware’ attacks like this may be designed to generate money, lock the victim’s PC then hold them to ransom, or work in some



- **Step 5:** Clicking the ‘remove All’ button takes the user to a payment page. But even if they pay, they will get absolutely nothing of any use or value in return. More pop-ups may even return at a later date – and the process may then start over again.

### CSC CLOUDPROTECTION FOR MAIL AND WEB

So has the concept of safe web browsing become totally outdated? If avoiding the web altogether just isn't a realistic option for most businesses, how can web threats be neutralized and how can using the web be made as risk-free as possible?

First and foremost, organizations need to adopt basic ‘best practice’ such as ensuring software, operating systems, plugins, browsers and so on are kept up to date, and to choose strong passwords and change them regularly. But gone are the days when this would have been sufficient. In 2010, web threats are more ubiquitous, imaginative and potentially damaging than they have ever been. They don't just skulk in murky corners but also lurk in the places that organizations must go each day to conduct business, access information, and communicate with customers, colleagues and partners. That's why the protection offered by CSC CloudProtection for Mail and Web, is proving critical for an increasing number of businesses all over the world.

CSC CloudProtection for Mail and Web provides advanced email antivirus, antispam, and web content filtering capabilities eliminating the need for on-site hardware or software. This approach to secure communications is designed for those organizations who value the highest levels of security, but are also looking to focus on core competencies and outsource specific non-core security functions. CloudProtection for Mail and Web cost effectively protects networks from web and email-borne attacks before they are able to reach the enterprise. This approach offers many advantages that

translate directly into unprecedented protection against all internet-borne dangers, including today's virulent breed of web threats. For instance, by running a large number of pro-active checks, even new threats never previously seen can be blocked before they can get near your network or individual PCs. Moreover, operating 'in the cloud' means that threats can be identified and stopped in fractions of a second, before they even reach your network.

Underpinning these capabilities are CSC experts, along with powerful policy-based controls, that help assure secure messaging and web access. CSC Global Security and Compliance Specialists work with you to configure and test the service based on your specific enterprise security policy and practices. In addition, CSC Security Engineers enable rapid onboarding of the service, and provide consistent ongoing management and support globally, 24x7x365.

While Web threats are still ramping up, so are your options for outpacing them by choosing CSC CloudProtection for Mail and Web. See how your business can go on harnessing the full benefits of the web – without running unacceptable risks to the success and well-being of your organization.

#### ABOUT CSC

CSC is a recognized global leader in providing technology enabled business solutions and services. CSC delivers enterprises cloud solutions to capture and accelerate realizable gains in business agility, innovation and cost reduction by transforming business processes and applications with the right cloud, the right way. Our portfolio includes a full lifecycle of cloud services. We offer cloud advisory services to shape cloud strategies and identify the ideal cloud workloads. Our cloud implementation and integration services transform your business processes and create new opportunities. On and off premise CSC cloud delivery solutions support private, hybrid or public clouds with enterprise-class service levels. Customer-centric and platform independent, we help you select the best technology to meet your needs. Security is an integral component of all our offerings, processes and systems. For 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

#### FIND OUT MORE ABOUT CSC CLOUDPROTECTION FOR MAIL AND WEB

<http://www.csc.com/cloud>

##### **NORTH AMERICA**

**Email:** [trusted\\_cloud@csc.com](mailto:trusted_cloud@csc.com)

**Call:** +1 866 255 0832

##### **EMEA**

**Email:** [eur\\_busdev@csc.com](mailto:eur_busdev@csc.com)

**Call:** +44 (0)845 602 4204

##### **AUSTRALIA**

**Email:** [talk\\_to\\_us@csc.com.au](mailto:talk_to_us@csc.com.au)

**Call:** +61 (0)2 9034 3000