Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Malicious web pages: What if hosting providers could actually do something…

Huw Fryer [b,*], *Sophie Stalla-Bourdillon* [a], *Tim Chown* [b]

[a] *Institute for Law and the Web, University of Southampton, UK*
[b] *ECS, Faculty of Physical Sciences and Engineering, University of Southampton, UK*

Keywords:
Web security
Drive-by download
Malware
E-Commerce directive
Immunities
Internet intermediaries
Hosting providers
ISP
Search engines

ABSTRACT

The growth in use of Internet based systems over the past 20 years has seen a corresponding growth in criminal information technologies infrastructures. While previous "worm" based attacks would push themselves onto vulnerable systems, a common form of attack is now that of drive-by download. In contrast to email or worm-based malware propagation, such drive-by attacks are stealthy as they are 'invisible' to the user when doing general Web browsing. They also increase the potential victim base for attackers since they allow a way through the user's firewall as the user initiates the connection to the Web page from within their own network. This paper introduces some key terminology relating to drive-by downloads and assesses the state of the art in technologies which seek to prevent these attacks. This paper then suggests that a proactive approach to preventing compromise is required. The roles of different stakeholders are examined in terms of efficacy and legal implications, and it is concluded that Web hosting providers are best placed to deal with the problem, but that the system of liability exemption deriving from the E-Commerce Directive reduces the incentive for these actors to adopt appropriate security practices.

1. Introduction

The ability of cyber criminals to compromise networked computer systems through the spread of malware allows the creation of significant criminal information technologies (IT) infrastructures or 'botnets'. The systems compromising such infrastructures can be used to harvest credentials, typically through keylogging malware, or provide a cover for illegal activities by making victim computers perform criminal acts initiated by others, such as distributed denial of service (DDoS) attacks. A single compromise may result in an infected system that is used in multiple criminal activities, and the cumulative effect of these activities and the resources dedicated to prevention can be considerable.[1] This paper explains how the phenomenon of drive-by downloads has evolved to become a significant threat to both Internet users and third party systems.

To effect a compromise via a drive-by, a criminal will create a malicious Web page which, when visited, attempts to

* *Corresponding author*. ECS, Faculty of Physical Sciences and Engineering, University of Southampton, Highfield, Southampton, SO17 1BJ, UK.
E-mail address: hf1g10@ecs.soton.ac.uk (H. Fryer).

[1] See e.g. Ross Anderson and others, "Measuring the Cost of Cybercrime", Proceedings (online) of the 11th Workshop on the Economics of Information Security (WEIS), Berlin, Germany (2012).

http://dx.doi.org/10.1016/j.clsr.2015.05.011

exploit vulnerabilities on the user's computer automatically. In contrast to email or worm-based malware propagation, such drive-by attacks are stealthy as they are 'invisible' to the user when doing general Web browsing. They also increase the potential victim base for attackers since they allow a way through the user's firewall, as the user initiates the connection to the Web page from within their own network. The phenomenon of drive-by downloads is not a new one, but remains one of the significant threats to the security of the Web, with the prominent malware variants being distributed in this way.[2]

The perception that malware only resides on 'suspect' sites such as file sharing sites, or those carrying pornography is now far from reality. Commonly, an attacker will seek to compromise an otherwise legitimate website and use that to distribute malware. They may also attempt to place malware on a cheap throwaway domain name, but it is harder for ISPs or authorities to take measures against a legitimate website, and it also increases the probability of a potential victim visiting it. Where the target is a website on a trending topic, the risk of exposure is even greater. With the rise of blogging and similar content creation, there is also a significant risk of vulnerabilities in common blogging platforms, such as WordPress, exposing visitors to such sites to potential drive-by malware.

This article provides a review of the existing strategies being used to mitigate this problem, and explains why they are not enough. We suggest that simple actions by Web intermediaries, in particular companies providing hosting services, could significantly impact upon the amount of malicious web pages, and force the criminals to use a smaller, more readily identifiable set of platforms to spread their malware. We conclude that laws excluding liability for intermediaries such as the E-commerce Directive in the European Union do not necessarily give an incentive to hosting providers to engage in such security practices and legitimate use of the Web suffers as a result.

2. Background

Like any other technology, computers have turned out to have a significant amount of use by criminals as well as legitimate use. The problem has been more severe than with previous technology, due to the combination of two factors. Firstly, computers have increased the speed at which a task can be automated. Secondly, the Web has got rid of the majority of the geographic limitations towards finding more victims so this automation can be put to good (or rather malicious) use.

An example of this automation in action comes from the volume of spam, which despite having reduced considerably from a high of 92.6%, still represents 75.2% of all emails.[3] The main way that criminal groups are able to maintain infrastructure which can send this volume of spam, or perform other undesirable actions is through the use of malicious software (malware). Malware takes over a victim's computer, and having done that can either attack the users directly, or recruit them into a botnet, i.e. a distributed network of computers which is of great to value to an attacker. Targeting the users might include something as simple as altering search results to gain advertising revenue, or spying on the browsing habits to target adverts. More seriously, it can steal credentials to online banking; or render a user's computer unusable (e.g. through encrypting all their files) unless they pay a ransom. Distributed computing offers the opportunity to conduct distributed denial of service attacks; sending spam; and more recently mining bitcoins.[4]

Over the years, the tactics that criminals have used to distribute malware have evolved and now different strategies are required to combat them. This section provides some background of this evolution, up to the primary focus of the paper: that of "drive-by" downloads. The distinctions between different types of malware are often unhelpful, since a lot of them do not fit neatly into one category, and in corporate elements of different types of malware. The reason for the distinctions in this section is to emphasise the differences in propagation methods, and the differences in strategy which are required to combat them.

2.1. *Exploitation vs social engineering*

In order to work, malware needs to be able to run on a victim machine. One method to infect a victim is known as **social engineering** which is to simply make the user voluntarily run the malicious code.[5] This can be accomplished through the use of **Trojan** style malware. Like the name suggests, this is a reference to the Trojan horse from Greek legend, which was let into Troy and allowed the Greeks hiding within to sneak out and open the gates of the besieged city from the inside. In the context of security, this might comprise an application purporting to perform a certain task, whilst at the same time an application hidden within would simultaneously attempt to subvert the machine it was run on.

Another method is to **exploit a vulnerability** on the machine. A **vulnerability** is a flaw, or bug in a piece of software which amounts to a security weakness. Vulnerabilities will have a greater or lesser degree of severity, but the most serious are those which allow Remote Code Execution (RCE). These vulnerabilities allow an attacker to run their own code rather than the code intended by the application. This is done by confusing the program into accepting input as commands to be executed, rather than as data to be manipulated. An **exploit** is a piece of code which takes advantage of the vulnerability, in order to run the desired code. In traditional computer based applications, this will be done by corrupting

[2] Chris Grier and others, "Manufacturing Compromise: The Emergence of Exploit-as-a-Service", *Proceedings of the 2012 ACM conference on Computer and communications security* (2012).

[3] Trustwave, "Trustwave 2013 Global Security Report" (2013) <http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf> accessed July 22, 2014.

[4] Bitcoins are a virtual currency, a part of which relies on solving a "hard" mathematical problem, for which the miner is compensated. The power requirements for doing this are significant, so using a network of victim computers can save a considerable amount of money.

[5] In this context, code refers to the series of instructions written by the programmer which gets converted into "machine code" (a series of 0s and 1s) that the computer can understand.