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