



April 2008 Update

Summary

This month there has been a widespread website SQL injection attack, with many thousands of legitimate websites affected. The malware uses JavaScript to attack visitors' computers using a number of vulnerabilities for which patches were previously released. Maintaining up-to-date patching levels is a key strategy in reducing exposure to such attacks.

Other significant incidents include a new variant, known as "Kraken", of a morphing botnet and the discovery of further flaws in a Mifare chip used in RFID cards. Important patches released this month include patches for Adobe Flash Player and the imminent release of Windows XP Service Pack 3.

Trends and alerts

Websites compromised by the SQL injection attack have an inserted script tag that uses malicious JavaScript to silently install the malware from a malicious domain on unsuspecting visitors' computers. GovCertUK have released an [advisory](#) detailing the domain to block, while a technical summary is available from [SANS](#), amongst others. Database and website administrators may find the [Microsoft guide to protect against SQL injection](#) helpful to assess and secure the systems for which they are responsible.

Malicious software ("malware") has been a recurring theme of the month. There has been much press discussion, including the increasingly business-like approach of malware authors and the criminal fraternity intent on using their products. Identity theft is of growing concern, as is the increasing exploitation of cross-site scripting (XSS) vulnerabilities; Symantec's [six-monthly reports](#) give one overview of developing trends, while MessageLabs have highlighted [Olympic Games-themed targeted email attacks](#). Another issue is the evolving transfer mechanisms for malware, such as the use of USB and social networking sites.

The botnet dubbed "Kraken" has been called the largest zombie network discovered to date. It is a particular menace as this malware regularly alters its code to evade detection and attempts to prevent detailed analysis. It is not clear what the infection mechanism is, although some suggest it is

[camouflaged as an image](#). The Emerging Threat wiki has a [summary](#) of technical details and further reading.

GovCertUK recommend reducing exposure to such attacks by maintaining all systems to current patch levels wherever possible, after suitable testing, using anti-virus software, enabling a software firewall or installing a firewall device and disabling unused browser functionality such as JavaScript and ActiveX. CERT has published [comprehensive advice](#) on web browser security with practical tips to harden many popular browsers. Administrators are advised to follow CESA best practice, published in the IA Bookstore CD and the CESA GSI website. If not a GSI user or Bookstore recipient, please contact your local IT Security Officer or WARP administrator for further details. GovCertUK has published advice on [common XSS techniques and suggested mitigations](#).

Further research into the encryption of the MiFare chip, used transport ticketing and access systems, has demonstrated [further issues](#) with the security mechanism. GovCertUK recommend that those responsible for such systems should review their exposure to this vulnerable card type if they have not already done so.

In addition to the usual [monthly Microsoft patches](#), Windows Vista Service Pack 1 was released in March and Windows XP Service Pack 3 is to be published imminently. A GovCertUK [advisory on the Vista Service Pack](#) is already available.

Critical vulnerabilities in Adobe Flash Player have been recently addressed with a new update; further details are available in the GovCertUK [Flash Player advisory](#). GovCertUK recommend that all systems should be maintained to current patch levels wherever possible, after suitable testing.

Contact us

We welcome any queries about this report. Please contact us via one of the following means:

Email	enquiries@govcertuk.gov.uk
Telephone	01242 709311
Fax	01242 709113
Postal address	GovCertUK A2f P.O. Box 144 Cheltenham Gloucestershire GL51 0EX