



GovCertUK Brief Summary - August

Storm Worm

Storm Worm (also known as Trojan.Peacomm and others) is still being detected. It was first observed in January 2007 and is distributed predominantly through socially engineered emails that entice a user to either open an attachment, or click on an embedded link to a website that hosts malicious code. More recently evidence has shown that Storm is being spread via a link claiming to be YouTube.

Updates and command and control are achieved using peer-to-peer networking.

GovCertUK wish to remind its constituency of the need to warn users of the dangers of opening unsolicited emails, following embedded links and opening executable attachments. These are common tactics used for the distribution of all forms of malware. Additionally peer-to-peer networking and file-sharing protocols are not recommended across domain boundaries due to inherent risks.

Cross-Site Scripting

GovCertUK have been alerted to an increased number of sites vulnerable to a Cross-Site scripting (XSS) attack. GovCertUK monitor open source resources and will contact Departments that have been identified.

Briefly, XSS is a vulnerability within Web applications that allows code injection by malicious users into the web pages viewed by other users. This could be exploited for example to run malicious code, in a Phishing attack, or for information disclosure.

Methods of avoiding XSS include encoding all user supplied HTML special characters, using content filtering, performing input validation or disabling client-side scripts on the browsers.

Detected Attacks

The majority of attacks that GovCertUK identify are web based. These come from either redirects from compromised legitimate web sites, hidden IFRAMES or browsing non-work related web sites.

The vulnerabilities exploited are numerous and include MS07-017 (ANI files), MS07-009 (Adodb.Connection), MS06-014 (RDS.Dataspace), MS06-071 (XMLHTTP) and MS06-057 (WebViewFolderIcon). A regular patching policy, and user education combined with detailed content filtering will help mitigate this threat.

Brief Summary - August

Targeted email attacks are also still being detected. Regular patching will also help mitigate this threat, however users should be reminded to be vigilant.

Other Comments

Microsoft released 9 patches as part of its regular patch cycle in August. Details can be found at the GovCertUK website or from Microsoft direct

Apple released three security updates addressing 45 vulnerabilities in Mac OSX, 4 vulnerabilities in Safari 3 Beta and 5 vulnerabilities in the iPhone. Details available from the Apple Website.

General

If you have any questions about this report, please contact us at:

enquiries@govcertuk.gov.uk

If you need to report an incident to GovCertUK, please follow the guidance at

www.govcertuk.gov.uk/reporting.shtml