



Issued: 17/01/2008

Malicious Domain Advisory

GovCertUK have detected a number of systems downloading malicious software from the IP address **58.65.238.59**. The malware can be detected by analysing web traffic logs for outbound traffic to this IP address. Evidence of the IP address **58.65.238.59** within web traffic logs may indicate an infected computer on the network.

Other identifying features of this malware include:

- On occasion the IP address may resolve to the domain name of **dorifora(dot)com**.
- The HTTP GET request to the IP/domain in question will not have an initial referrer listed.
- Once the malware is present on the network, it beacons out to the domain **here4search(dot)biz** – this domain may also be present within the web logs.

GovCertUK recommend that the IP address **58.65.238.59** is blocked on the network as well as the domains **dorifora(dot)com** and **here4search(dot)biz**.

GovCertUK is responsible for Computer Security Incident Response within UK Government, and provides an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents.

The CESG GovCertUK Incident Response team provides 24 hours a day, 7 days a week operation and can be contacted by the following methods:

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	enquiries@govcertuk.gov.uk
Incidents & Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
Website:	www.govcertuk.gov.uk