IEDR Statement:- **9** November 2012

IEDR has concluded an investigation by the company and external security consultants of an unauthorised intrusion into the company's systems which was discovered on 9 October 2012. A criminal investigation by the Garda Bureau of Fraud Investigation is continuing.

IEDR's investigations have confirmed that during the 25 day period prior to 6 October 2012 the public-facing web server of the IEDR was subjected to repeated attempts at unauthorised access from external sources. On 6 October 2012 the attempts were successful through the exploitation of vulnerability in IEDR's configuration of the web application "Joomla!" (a popular and widely-used open source web content management system) which was exploited to allow the uploading of web scripts using the PHP language. These PHP scripts were then used to access a backend database and this database access subsequently provided access to the IEDR control panel and permitted unauthorised modifications to an account with the Domain Name Server (DNS)[Note1] details which resolves domain names such as "Google.ie" and "Yahoo.ie".

IEDR's investigations have concluded that, whilst the result of the attack has been severe in terms of allowing access to change name server records, it should be noted that the scope of the attack was limited to this single public web server, and that no personal financial information was accessed.

The IEDR confirms that it has implemented all of the recommendations of the external security advisers. As a precautionary move, IEDR has also reset the passwords of every contact, account and service, both internal and external, across its systems. The impact of this security measure is to invalidate any credentials which may potentially have been compromised.

The IEDR investigation also confirmed that neither the Registrar of the affected domains nor its systems had any responsibility for this incident.

The IEDR technical team was assisted in its investigation and analysis of this incident by several external firms, namely Cernam, BCC Risk Advisory and the Digital Forensics Team from one of the 'Big Four' accounting firms. Cernam is a specialist digital investigations firm with a focus on online evidence and digital forensic investigations. Owen O'Connor, managing director of Cernam, has assisted IEDR in assessing the root cause of the incident and co-ordinating other aspects of the investigation. Cernam's experience in investigating incidents of this type brought a forensic rigour to the investigation and to the collection, preservation and analysis of the digital evidence. BCC Risk Advisory is a specialist Internet, network and management security services company. Eoin Keary, CTO of BCC Risk Advisory, provided software security assistance including penetration testing services prior to the resumption of IEDR services. The accounting firms's Digital Forensics Team is a unit of its Fraud Investigation and Dispute Services division. A team from its London office assisted IEDR in confirming and detailing the scope of the breach, identifying which systems were impacted and determining what information was accessed.

Separately, IEDR has made a criminal complaint regarding this incident to an Garda Síochána. The Garda Bureau of Fraud Investigation (GBFI) is conducting an investigation into this external attack on the .ie namespace. That investigation commenced on Wednesday 10 October and is continuing at this time.

The IEDR regrets the incident and assures consumers and registrants that the security of the .ie nameserver network and the services infrastructure is of paramount importance. IEDR thanks its Registrars in particular for their patience and forbearance. The IEDR also regrets the inconvenience which some customers would have experienced during the service interruption but notes that taking systems off-line as a precaution was the first and most important of a series of security measures taken in response to this incident. In restoring service, IEDR has built new servers, reviewed and enhanced application controls and tested each application prior to service restoration.

IEDR is refining its Security Plan for 2013 which will include a Domain Lock service for customers' valuable .ie domains. The IEDR has recently appointed a new Technical Services Manager who will immediately place an increased emphasis on security policies, processes and procedures. The steps the IEDR has taken, together with its actions in 2013, will enhance the safety, security and resilience of the .ie domain.[Note2]

Issued by:- IE Domain Registry Limited (IEDR) **9 November 2012**

Note1:-

DNS - The **Domain Name System** (**DNS**) is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment (for the purpose of locating and addressing these devices worldwide). An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, *www.example.com* translates to the addresses *192.0.32.10* (IPv4) and *2620:0:2d0:200::10* (IPv6).

The IP number can be compared to a phone number: When someone calls http://www.example.com/, your ISP looks at the DNS server, and asks "how do I contact example.com?" The DNS server responds: "It can be found at 198.105.232.4". As the Internet understands it, this can be considered the phone number for the server, which houses the http://www.example.com web site. The DNS records for your domain are kept on your hosting server in the place called DNS zone. When you register a domain with a hosting provider, all DNS records are automatically created for you, but in some rare cases you may need to add custom records to your DNS zone. An example would be when you want all email to be processed by an external mail server.

Note 2:-

IEDR’s **Managed Registry** model – McAfee Inc., the security technology company, conducts regular surveys (“Mapping the Mal Web”) which measure the level of malware (virus or spyware) and spam (unsolicited mail) which a consumer receives following a visit to websites in various TLDs. On these measures, Ireland’s TLD, the .ie namespace, has consistently featured in the Top 5 safest namespaces in the world. This is partly attributed to the IEDR’s Managed Registry model, whereby the Registry has authentication processes and procedures at the point of registration, and can therefore provide consumers with traceability of who is behind a website, if required by the authorities.