Open Web Application Security Project (OWASP)

Response to Consultation on a New .UK Domain Name Service

F. About you

Name:	Submitted by Colin Watson on behalf of OWASP
Position:	Member, OWASP Global Industry Committee
Organisation:	The Open Web Application Security Project (OWASP)
Email:	NA
Telephone:	NA
Postal Address:	OWASP Europe VZW, Leinstraat 104A, B-9660 Opbrakel, Belgium
Area:	Civil Society
Sector:	ICT

G. Security

1. As outlined above, we are proposing that the direct .uk service offers routine monitoring and notification to registrants of viruses and malware on sites associated with the domain. Do you have any comments on this proposal?

Malware on a site cannot always be attributed to the primary host domain. With cloud services, data mashups, advertising and shared hosting, it is possible for malware to originate from another included source, possibly outside the control of the site's owner. Malware may also be related with spam email from a particular domain, even if there is no website as such.

Conversely, some parts of sites may not be easily examined by external monitoring. This includes functionality that is not linked to, role and channel-specific content, some Ajax interactions, and areas of a website requiring authentication (by customers, citizens, administrators, etc) where some of the most critical business logic is often found.

It is also noted that enterprise-scale organisations could use a single .uk domain for multiple sites, some perhaps with user-generated content, and it may not be reasonable to take down all the sites due to a single problem in one area.

But more importantly monitoring of viruses and malware, even with subsequent action to resolve the effects, is not at all a sufficient measure to protect business systems, business data, users and users' data. Threats target a wide range of vulnerabilities[1] in websites and their supporting systems; the vast majority of which would not be detected by the suggested monitoring. Many attacks use a combination of actions[2].

[1] http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

[2] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-

Although some successful attacks might lead to malware and viruses being hosted on the site, but the purpose of an attack is more likely to be to view confidential information, to steal data, to misuse business processes for personal benefit, to commit fraud, to cause damage to the site, to facilitate other e-crime[3], or to link to more malicious material elsewhere.

If Nominet intends to encourage secure sites, OWASP recommends that instead of monitoring for malware, organisations consider security is throughout the lifecycle of the site – from initial concept, right through to deployment, operation and disposal. This has been shown[4,5] to be the most effective way to reduce the occurrence of exploitable vulnerabilities in deployed sites, and is widely adopted[6]. OWASP's Software Assurance Maturity Model[7] (SAMM) provides a simple method to assess an organisation's overall maturity to generate a scorecard for 12 practices.

An individual website's software security controls could also be assessed using the OWASP Application Security Verification Standard[8] (ASVS) which defines a range of security controls, including data protection, for different assurance levels.

2. As outlined above, we are proposing that the direct .uk service offers a trust mark to registrants. Do you have any comments on this proposal?

OWASP is concerned that the proposed security and registrant identity verification requirements underpinning the trust mark would provide very little actual protection to users of such websites and is not sufficient to establish even a limited level of trust. Therefore it may mislead users into a false sense of security. One or a small number of public failures, such as breaches in confidentiality, would undermine the trust mark and all other websites using the proposed new .uk domain service. Trust marks can easily be faked and generally they are implemented using third-party hosted JavaScript, meaning the site's content is no longer under the owner's complete control (this is why similar trust marks are not displayed on banking websites and rarely on e-commerce checkout pages for example).

3. As outlined above, we are proposing that the direct .uk service requires a digital signature known as DNSSEC as mandatory. Do you have any comments on this proposal?

Agree.

OWASP suggests that Nominet also considers other measures such as requiring that all communications between the user and the site are undertaken using robustly-configured transport layer security (also known as “SSL”).

2012_en_xg.pdf

3 http://dpalliance.org.uk/wp-content/uploads/2012/09/20120910-eCrime_Reduction_Partnership_Mapping_Study.pdf

4 http://www.microsoft.com/en-us/download/details.aspx?id=2629

5 http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=6968

6 http://bsimm.com/facts/

7 https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

8 https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

N. General Views on the Proposed Service

11b. Are there any other points you would like to raise in relation to this consultation or about the proposed new service?

This official response has been created by volunteers and is submitted on behalf of the Open Web Application Security Project[9] (OWASP) by the OWASP Global Industry Committee[10], following our own consultation process with the local OWASP chapters in the UK. The response addresses a subset of Nominet's consultation questions – only those which relate directly to OWASP's remit[11].

OWASP would be pleased to work with Nominet to progress any security-related aspects.

OWASP is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a U.S. recognized 501(c)(3) not-for-profit charitable organization (EIN 20-0963503), that, and OWASP Europe VZW is a registered non-profit organisation (VAT number BE 0836 743 279).

[9] http://www.owasp.org/

[10] http://www.owasp.org/index.php/Global_Industry_Committee

[11] https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project