

Re: [Full-disclosure] The Next Super JavaScript Malware – the web has crashed

Re: [Full-disclosure] The Next Super JavaScript Malware – the web has crashed

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-05/msg00535.html>

- *From:* "pdp (architect)" <pdp.gnucitizen@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 30 May 2007 10:37:01 +0100
-

The reason, attacker will go for XSSSED.com instead of providing their own database is that XSSSED has bigger audience and the chances for someone contributing a new vector are higher. Web2.0 is all about segmenting services in small independent but very useful blocks. So, why bother create a new database when you can use whatever is already available online. IMHO, malware code that makes use of various databases online can impact the Web to an extend beyond our imagination.

For sure you can shut down the service at any given time but that won't make any difference at all. I use XSSSED.com as an example, because it is the biggest database available today. If you shut down the service, it wont take long for attackers to find another database and reconfigure the infrastructure to support it as well. In fact, attackers can submit XSS vectors to Google Base.

On 5/30/07, security@xxxxxxxx <security@xxxxxxxx> wrote:

Dear petko d. petkov,

I don't know if it was your intention, but you're giving a bad name to xssed.com, which goal is to organize the public XSS vulnerabilities, make statistics, and first of all to spread education about XSS vulnerabilities. While the scenario you describe is somehow possible, it relies on the availability of our web site, and we'd be able to stop it quickly. Anybody would be able to build such list of XSS list without the need of our site, and with their own discoveries. I wanted to clarify it. Anyway i think that everybody here on the list knows the dangers and advantages of full disclosure..

Kevin

<http://www.gnucitizen.org/blog/the-next-super-worm>

In this article I explain a technique that can be used by malicious minds to build the next generation of JavaScript based malware. The post is for education purposes and I welcome everyone who has ideas how to stop these types of attacks to do so by sending an email or

Re: [Full-disclosure] The Next Super JavaScript Malware – the web has crashed

Re: [Full-disclosure] The Next Super JavaScript Malware – the web has crashed

posting a comment. We do really need to start thinking about how to fight back and start developing strategies that can apply.

cheers

—
pdp (architect) | petko d. petkov
<http://www.gnucitizen.org>

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>

—
pdp (architect) | petko d. petkov
<http://www.gnucitizen.org>

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>