

Re: A serious threat to our national security

Re: A serious threat to our national security

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2008-09/msg00526.html>

- *From:* Guy Macon <<http://www.GuyMacon.com/>>
 - *Date:* Sat, 06 Sep 2008 06:17:29 +0000
-

Content-Transfer-Encoding: 8Bit

Guy Macon <<http://www.GuyMacon.com/>> wrote:

Guy Macon <<http://www.GuyMacon.com/>> wrote:

I was just reading that right before Russia invaded Georgia, there was a cyberattack on Georgia's basic network infrastructure launched from the Botnets that Bill Gates created through the above policies. I can only conclude that Microsoft's ongoing refusal to make a version of windows that cannot be remotely controlled by criminals is now a serious threat to our national security.

| The number of compromised zombie PCs in botnet networks has quadrupled
| over the last three months, according to figures from the Shadowserver
| Foundation.

| http://www.channelregister.co.uk/2008/06/05/scansafe_web_malware_survey/

| 'Legit' website compromises reach epidemic proportions

| 05 Jun 2008 12:53

| Once upon a time surfers could stay unmolested by malware by staying
| away from warez and smut. Those days are well and truly over as
| changes in hacking tactics mean that compromised content on legitimate
| website has become the main conduit for so-called drive-by download
| attacks.

| Web security firm ScanSafe reports that two in three instances of
| web-based malware (68 per cent) it blocked last month came from

Re: A serious threat to our national security

Re: A serious threat to our national security

| legitimate sites. ScanSafe blames the increase on attacks that have
| planted malicious scripts, often exploiting iFrame web browser
| vulnerabilities, on pukka websites. Hacked sites are commonly used to
| deliver password-stealing Trojans and other strains of malware onto
| compromised PCs.

| For example, ScanSafe reported earlier this week that some pages on
| the Wal-Mart website were compromised in the latest phase of an
| ongoing series of SQL injection attacks. The attack was used to plant
| exploits of recent Flash vulnerabilities onto Wal-Mart's site.
| High-profile victims of malware attacks in May alone included
| Nature.com, Foofighterslive.com, Acer.co.th, Webster.edu and
| Photopass.com.

| Large-scale SQL Injection attacks started around six months ago in
| October 2007 and are affecting mom and pop website operations as well
| as household names. Attacks based on stolen FTP are also playing a
| significant (albeit secondary) role, according to ScanSafe.

| This evolution in tactics by black hat hackers means that miscreants
| are able to quickly 'colonize' thousands of legitimate sites with
| malware. ScanSafe reports a 220 per cent increase in the amount of
| Web-based malware over the last twelve months. The volume of backdoor
| and password-stealing malware blocked by the firm increased by an
| order of magnitude (855 per cent) between May 2007 to May 2008.

| "Over the last year malware authors have moved away from direct
| attacks ? attacks in which they directly interact with victims, via
| social engineering for example ? to indirect attacks accomplished
| through compromised websites," said Mary Landesman, senior security
| researcher at ScanSafe.

| "Currently, thousands of legitimate sites are being compromised daily.
| The net result is that you absolutely cannot assume that because you
| are on a brand name or well known site that it is a safe site," she
| added.

--
Guy Macon

<<http://www.GuyMacon.com/>>