

Re: A serious threat to our national security

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2008-09/msg00525.html>

- *From:* Guy Macon <<http://www.GuyMacon.com/>>
 - *Date:* Sat, 06 Sep 2008 06:15:17 +0000
-

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.

| http://www.theregister.co.uk/2008/09/02/zombie_surge/

| Zombie network explosion: long shadow cast by SQL injection surge?

| Published Tuesday 2nd September 2008

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

| Shadowserver tracks botnet activity and the number of command and control servers. It uses a variety of metrics to slice and dice its figures based in part on the entropy of botnet infections. The clear trend within these figures is upwards, with a rise in botnet numbers of 100,000 to 400,000 (if 30 day entropy is factored into equations) or from 20,000 to 60,000 (for five day entropy).

| Entropy of botnets is calculated on the basis that if no activity is seen from a specific IP for a number of days – either 30, 10 or five – then it is removed from the botnet count.

| Shadowserver figures suggest the number of command and control servers has actually decreased over the last month, following a spike in activity back in July.

Re: A serious threat to our national security

| Security watchers at the Internet Storm Centre have a number of
| explanations for the rise in the zombie population.

| It could be that experienced botnet herders have got better at keeping
| control of compromised machines, or that more machines have been
| infected. Not much by way of email malware activity has been
| monitored, so if the latter explanation is true, then drive-by
| download attacks are playing a bigger role in spreading botnet client
| infestation. The recent rise in SQL injection attacks that plant
| malicious scripts on vulnerable servers could be to blame, but there's
| no hard data to support this plausible theory.

| Improved detection of web-based attacks may be needed to gauge the
| extent of the problem, according to security watchers at the Internet
| Storm Centre.

| "We are very good at tracking email-based malware (including
| lead-the-user-to-the-bad-website variety) and certainly network based
| attacks," writes ISC staffer John Bambenek. "Short of spidering the
| web on a consistent basis, it gets difficult to find infected sites
| for that malware. We at the ISC, and I'm sure many others, are working
| on ways to honeypot pure web-based attacks to capture this malware,
| but much work is left to be done."

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