

## NC Company Discovers the "Obama Worm"

Articles / dBNews Charlotte

**Date:** Friday, January 30, 2009 10:23:08

Is it any surprise hackers have taken advantage of President Obama's online popularity?

Hickory - President Barack Obama is the First U.S. President with a Facebook page, and a YouTube channel. In addition, the President has 1 million "MySpace" friends, 3.7 million Facebook supporters and his campaign database boasts the e-mail addresses of 13 million supporters. President Obama is truly the nation's first "wired" president.

So is it any surprise that hackers have taken advantage of the new president's online popularity?

Claremont, NC-based Walling Data, North America's top distributor of AVG Internet Security Products, discovered a new computer threat this week that exhibits interesting symptoms, including a pop up of the President's face in the bottom right hand corner of infected computers. Ironically, the worm was discovered on the network of a K-12 school in the President's home state of Illinois.

"From what we can tell so far, the good news is that this worm is nothing more than a major nuisance. This threat spreads via external devices, such as flash drives, attacking where a network is typically most vulnerable – from the inside" said Luke Walling, President of Walling Data.

"We first discovered the worm in the course of some support work we were providing to the school," Walling added. "It seems this threat was developed in an off the shelf development environment often used for the production of simple games, the version we have seems to have last been modified in December 2008."

Walling also noted that the threat is unlikely to be an isolated incident, as it can be easily spread through the use of external devices, like USB flash drives. Schools are especially susceptible because they often allow the use of such devices to move class work back and forth from home and school.

As of today, the worm is not detected by any security product worldwide based on data obtained from virustotal.com and internal testing.

"We have isolated the components of this threat and have provided samples to security vendors to ensure it is properly and quickly detected by popular security products."

"This is one instance when seeing our President's face on your computer screen is not a good thing," joked Walling. "You have to admit, no matter your political affiliation, this proves even hackers have a sense of humor."

Are you infected?

Walling reveals what it knows about the "Obama worm" so far and what has been submitted to security vendors.

1. The threat appears to have been introduced to the school's network via the use of a USB flash drive or possibly from e-mail.
2. The Obama worm replicates via USB storage devices and network shares.
3. The worm's behavior indicates that it is more of a nuisance than a threat to sensitive data as there are changes to exe/bat/vbs shell extensions (i.e. breaking exe files) and it replicates to a large number of folders on the local computer.
4. On Mondays only, it will depict President Obama's face in the lower right corner.

## Lessons Learned

Walling suggests two things that could prevent this threat and others like it from wreaking havoc on a network:

1. Make sure all machines are "patched up."

"Because this threat is not yet detected by any security product, it is critical that any machine with a Microsoft operating system is completely and always 'patched up'. The threat exploits machines that lack critical Microsoft updates and trust only anti-virus software to catch threats," Walling said.

2. Prohibit the use of external devices. Define and enforce usage policies diligently.

"It is difficult for many small businesses and schools, who often have limited manpower and resources, to prohibit the use of external devices like flash drives and external hard drives. While these devices are convenient, they are also the easiest way for threats to enter your network. We always recommend that network administrators disable a machine's ability to use external devices via Group Policy or at a computer level for small workgroups. The ban on these devices should be a part of any organizations' Internet usage policy, and of course, must be strictly enforced."

For more information on Walling Data, visit [www.wallingdata.com](http://www.wallingdata.com) or call 828-459-7340.

### About Walling Data:

Walling Data represents a group of divisions that offer technology distribution and support services throughout North America, traditional break/fix repair services from its two office locations in Catawba and Iredell Counties in North Carolina, as well as Virtual IT department outsourcing via its Guaranteed IT managed services program. Walling Data is also the largest distributor of AVG Ant-virus products in the US and Canada and is an authorized distributor of Cymphonix, Cyber Patrol, and other security products. Learn more at [www.wallingdata.com](http://www.wallingdata.com).

---

This article comes from dBusiness News

<http://charlotte.dbusinessnews.com/>

The URL for this story is:

[http://charlotte.dbusinessnews.com/shownews.php?newsid=175651&type\\_news=latest](http://charlotte.dbusinessnews.com/shownews.php?newsid=175651&type_news=latest)