



Weekly Brief, March 8, 2010

InfoSecurity.com

March 8, 2010

<http://www.infosecurity-us.com/view/7871/weekly-brief-march-8-2010/>

Infosecurity US rounds up the significant events from the last week.

The big news event last week, of course, was the RSA conference. Newly appointed government cyber czar [Howard Schmidt said that cyber war doesn't exist](#), which will comfort all the private sector organizations – including McAfee, whose executives sat on the CSIS advisory panel for cybersecurity – who [think that it does](#).

Talking of cyber warfare, a pair of researchers with [TippingPoint](#) created a weather application for jail broken mobile phones that [co-opted them to a botnet](#), and collected 8000 iPhones and Android phones as part of their infection process. This is a particularly significant event, given that the recent [cyber warfare simulation conducted](#) by the [Bipartisan Policy Center](#) used a similar scenario as the basis for an attack.

Unfortunately, botnets created by security researchers were not the only ones to be unveiled at the RSA conference. [BlackEnergy 2](#), a Russian banking trojan, was unmasked by the ever-insightful Joe Stewart, security researcher at Atlanta-based SecureWorks. The trojan developed out of the original BlackEnergy, which he said was involved in the cyber attacks against Georgia during the conflict with Russia.

As one new botnet thrived, another bit the dust this week. Mariposa (which means butterfly in Spanish), was dismantled, stopping its controllers from stealing bank and password and conducting other nefarious online activities. Spanish authorities have arrested three men accused of controlling the botnet's 12.7 million PCs.

Not content with appointing a new senator, the [State of Massachusetts](#) also added a new data privacy law. 201 CMR 17 went into effect on March 1, and stipulated preventative measures, rather than focusing on data breach disclosure after the fact.

Blogs and news outlets are suggesting that in 2004, [Facebook](#) CEO and anti-privacy urchin Mark Zuckerberg hacked into the email accounts of two journalists using data obtained from Facebook's logs.

Here's a new approach to destroying evidence: according to excellent crime and punishment blog [The Smoking Gun](#), a New York City man swallowed a flash drive while in the custody of Secret Service agents during a federal raid. After failing to pass the offending item for four days, he was somewhat ironically charged with obstruction of justice. It's certainly a novel way to bung up the judicial system.

What is it with USB devices and security this week? [US-CERT](#) issued an advisory warning that the Energizer DUO USB battery charger contains a backdoor that allows unauthorized remote system access.

12 000 patients had their personal information exposed after a former employee of the [University of Texas Southwestern Medical Center](#) was found in possession of patient billing data.

Oh, the irony – according to a study from wireless security company [Motorola AirDefense](#), 116 wireless clients were found to be associated with 315 ad hoc networks. Ad hoc networks, which you'll often find with names such as "Free Public WiFi", are client-to-client networks, rather than wireless access points, and they represent a security risk if a malicious client wants to pose as a legitimate network. Most networks using encryption were also vulnerable to attack. Almost two-thirds were using the now defunct WEP security standard.