# Media shock stories about GameOver Zeus are not helpful

June 6 2014, by Bill Buchanan


Don’t click on links and you’ll be all right. Credit: Atlaspix

We need to watch out for headlines like the ones earlier this week warning that people had two weeks to protect themselves from a "powerful computer attack". It can end up scaring people who have little idea about how these threats actually work.

There's very little that can be done about stopping GameOver Zeus and all the associated botnets: the group of infected computers carrying out the instructions of a remote master. The key thing is that users look after themselves better online.

There's no single piece of software that can thwart all the Zeus-related threats, which essentially involve ransacking infected computers for financial information and then, if nothing is discovered, using Cryptolocker ransomware to lock up personal information and refusing to release it unless the owner pays a ransom.

Unlike less sophisticated botnets, in the Zeus botnet a master controller can be created at any place on the internet and start rallying their troops on information-harvesting exercises. So grabbing hold of a few bot masters and strangling them is not really going to cause any long-term damage to their infrastructure. It almost feels like the internet is becoming alive, with its own in-built ecosystem.

## The internet is filled with botnets

Indeed, botnets and the associated Cryptolocker ransomware have been running happily on the internet for quite a while now. If you look at any internet traffic, you'll find a whole lot related to botnets, who are blindly harvesting data such as bank login details in order to steal from the victims. While the FBI's moves this week to take over the Zeus botnet are good, botnets have been used for many years and have been going up and down, with very little that can be done to stamp them out.

In times gone past you switched your computer on, and if someone on the network had been infected with a virus, there was a good chance that you were too. But it's not really like that now, as infection tends to be through a phishing email, where there's a link to follow; or through a trojan contained in a software download.

These threats are mainly fixed by users downloading security updates for their systems – "patching" in the jargon – not necessarily people rushing to update their virus scanners. Take away patching for the Windows XP operating system and you create a new risk from a threat that has been around for a while. This makes Zeus different from Heartbleed, which was real and new when it struck in April. As long as we have unpatched systems, we'll have botnets.

If a user has an unpatched system, they can be exposed to the three major threats, which are due to vulnerabilities in Adobe Flash, Adobe PDF and Java. The threats are fairly easy to implement for script kiddies using exploit kits such as Phoenix, which has all the scripts required to create the documents and code necessary to exploit the user's machine.

## Blame the old viruses

The way the Zeus headlines put it, we are going to get hit, no matter where we are, and it's coming to get us, just by connecting to the internet. This is far from the truth. The old-fashioned worms and viruses have a lot to answer for, since they have created a sense that computer infections still spread in this way.

The attack that is coming in two weeks is mainly related to phishing emails that will request you to submit your tax return online. If you click on the link, there will be a PDF, a Flash file or a Java program which then exploits your system by running some code and dialling back to the main master botnet controller, which downloads the latest data harvester

for your machine.

Most people can now spot these emails a mile off. (Strangely our spam checkers often let these though, as they often have an email address of a person who might actually know you.) Not clicking on the link in the first place protects you. If you are stupid enough to click on it, then a patched system will often stop the exploit from working.

So a stronger message for the authorities to put out there would have been to define what a phishing email looks like; tell people not to click any email links unless they are fully trusted; and tell them to patch their systems.

To conclude, don't be frightened by the headlines but be careful. Thethreat is not new, and it won't explode in two weeks time, like Heartbleed did, but you are at risk, and you have been for quite a while.

The media need to be careful that they don't desensitise the general public. The internet and the cloud are two of the greatest things that have happened in the history of mankind. We need to educate and inform, rather than frighten. So the bottom line is still: patch your system, and be safe.

Organisations such as the NCA are doing good work in disrupting crime gangs, but users too need to be part of the fight, and broadcast media also have a key role in not only alerting users of threats, but to also inform and educate.



Provided by The Conversation