



## **THE MALWARE REPORT**

### ***BBC Buys and Uses a Bot Network to Highlight Vulnerabilities***

#### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

#### **The Malware Report Transcript**

Title: BBC Buys and Uses a Bot Network to Highlight Vulnerabilities

Episode: 113

Location: [http://www.eset.com/podcasts/031709\\_ESET\\_Bots\\_BBC.mp3](http://www.eset.com/podcasts/031709_ESET_Bots_BBC.mp3)

March 19, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams.

Matt Grant: Randy, I wanted to spend some time today talking about the recent news that the BBC bought a botnet, can you tell us a little more about this?

Randy Abrams: Yes, I'll start off with an analogy. I thought that there was a problem with people not locking their doors to their homes. Tell me if this is sounds like a good idea. Grab a camera crew let's go around the neighborhood and check the doors on houses, if they're unlocked go inside the house and leave a note, come back out and leave the door unlocked. Does that sound like a good idea?

Matt Grant: Not necessarily.

Randy Abrams: The BBC bought a botnet which means they bought access to a bunch of computers that are infected with the program that allows them access to the computer. And then they use the computers to send spam to their own addresses. It's not like they are spamming your friends, family, or you. Also, they proved they can do what's called a distributor denial of service attack which cripples the Web site. The Web site they cripple, the owner agreed to cripple the Web site. And they changed the wallpaper on the computers. They actually changed the desktop wallpaper on people's computers without their consent. They went into the people's computer without their consent and used the people's computer to make the point that botnet is a problem.

Matt Grant: How did they get their hands on the botnet in the first place? Do you know the back story?

Randy Abrams: Yes. With the help of security experts, they went through the back channels, "dark net channels," to contact a Napster and pay a few thousand dolls to use 22,000 computers - the bots. That's how the bad guys do it, buy access to the botnets to send spam and do distributed denial of service attacks and steal information off computers. The BBC did it the same way everyone does it. But the BBC claims since they didn't have criminal intent, it was legal. But there are other experts who disagree. Since the infected computers are located all over the world, it doesn't mean it's legal in every country that they did it in. Quite likely, it was illegal in many countries, potentially in Great Britain too.

Matt Grant: Yes, that's what's interesting to me. You would think that no matter what the purpose is, purchasing a botnet would be considered illegal in its typical use.

Randy Abrams: I'm not sure if purchasing is illegal, but using it is illegal.

Matt Grant: Right, using it in any regard. Your opinion, was it a good idea/bad idea?

Randy Abrams: It was a bad idea. It's a good idea to raise awareness, it's very important. But the implementation was not within the ethics of most people. And it's interesting to see if there's any fallout because a well known security firm was potentially included. A well known security firm allowed the BBC to perform the distributed denial of service attack on their own Web site. They allowed to allow their own Web site to be attacked, but that means they knew the BBC was going to use other people's computers without authorization and it's really shocking that a security company would be party to this kind of abuse.

Matt Grant: Is this the first type of campaign like this that would raise awareness in this fashion?

Randy Abrams: It's the only one I'm aware of by an entity that did not wish to remain anonymous. There's long been a debate going on about whether there is a good virus or worm and most of the experts agree there is no such thing, but it keeps coming up. There was a virus called "Cruncher," it was a Goss virus written years ago that was an attempt to prove there could be a good virus. It would compress files so you would save disk space - which in that time hard drives were expensive and disk space was at a premium. That still didn't give the author the right to modify another person's program regardless of whether or not it broke them. I'm not aware of any legitimate or any other companies doing something like this per say.

Matt Grant: Do you think that if someone were to do this, should it have been a news organization like the BBC or should it have been someone with more experience in the realm?

Randy Abrams: I suspect the BBC got some competent experts to help them with it, but I don't think this should have been done. If we decide this is the approach for how we want to alert users that their computers are infected, then that's the kind of thing where laws need to get set up and there's got to be monitoring. Perhaps we'll get to the point where

we say we can find out what computers are infected, alert the users and, if they're using the internet, their ISP has an agreement that gives them buy-in where the consumer has been notified that if you have a bot in your computer, we have the right to notify you that there's a bot by doing such and such actions. I can see where something along these lines might be feasible in the future, but for right now taking control of the person's computer without their authorization is not a good idea.

Matt Grant: Well Randy, we certainly appreciate you taking the time to explain this further detail in a way you need to understand exactly what happened here. If you would like to learn more, please feel free to e-mail him at [askeset@eset.com](mailto:askeset@eset.com). This has been Matt Grant and you've been listening to the Malware report.

[End of recorded material]