



## **THE MALWARE REPORT** *40,000 Websites Infected: Is Yours?*

### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

### **The Malware Report Transcript**

Title: 40,000 Websites Infected: Is Yours?

Episode: 126

Location: [http://www.eset.com/podcasts/060309\\_ESET\\_Attacked.mp3](http://www.eset.com/podcasts/060309_ESET_Attacked.mp3)

June 18, 2009

[Begin recorded material]

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

Randy Abrams: Good to be back here.

Matt Grant: Fantastic, great to have you. I wanted to get your thoughts on a recent article I read on thousands of websites that have been stung by a mass hacking attack. They're saying more than 40,000 websites have been hacked. Can you tell us more about this attack and are you familiar with this particular attack?

Randy Abrams: Yes, I've seen the reports on this and it's a significant attack. Not only is it 40,000+ websites, but they silently attempt to infect the computers of the people who visit them with other malicious software. The site is called Beladen.net – which translates to “loaded” in German. It is a “loaded” website. It's actually using 20 different vulnerabilities and

browser plug-in attacks that target older and unsecure versions of third party applications such as QuickTime and WinZip. People out there are using old versions of applications – which many people use – it’s a really good time to go out to the vendor’s website and check and see if there are security updates or new versions and get with the newer software.

**Matt Grant:** Interesting. The report I was reading mentioned that the sites were redirecting to a fake Google analytics website which then was redirecting to another bad site. Was this the only site it was redirecting to or were there multiple sites that it was redirecting to?

**Randy Abrams:** I think it was just contacting this fake Google analytics site – which was spelled a little different than the real Google analytics site and that site was then, I think it was another site that was redirecting to the Beladen site. I don’t think Google analytics itself (which wasn’t really Google analytics – instead of an “I” you know, they’ve got another character in there) I haven’t dug in to it enough to know exactly the point of contacting Googleanalytics.net is other than I know it’s not a site people want to visit, it’s not a good thing right now, but it checks the name of the referring website. The bad guys are doing tracking to find out what’s working because it’s recording the date and time stamp of the visit and then the victim is forwarded to the Beladen site and that’s where all the exploitation of the browser vulnerabilities are occurring from.

**Matt Grant:** This just seems like it really underscores the success that some hackers have had with hosting dangerous code on poorly secured websites. How important is it for all websites, small or large, to understand the importance of securing their website and what should they be doing so that they don’t fall victim to this?

**Randy Abrams:** That’s a difficult one. It is very important for people with websites to they make sure they’ve secured the websites, but it’s hard for the home

users to do who doesn't know anything about it. Then, what happens is, you get people doing the right thing and that's having professionals host their websites and the problem is, if the professional makes a mistake, they might have several hundred or even thousands of hosted websites in the virtual server farm and if they made a mistake, all of those sites can be compromised simultaneously. It's really important, especially for people that host sites, to make darn sure that they've got good security and from time to time have external penetration testers testing their site. If a company is going to host their own website, it's a good idea for them to have professional penetration testers from time to time check and see what the security of their site is because a good website can turn bad very quickly if it gets hacked.

Matt Grant: Now, do we know at this point at all what the hackers are doing with these compromised PCs? Are they just part of a Botnet?

Randy Abrams: Actually, I'm not exactly sure on this hack what they're doing with it. I've got some of the code of the exploit in front of me. Typically, what happens is they want to either sell you fake antivirus software and/or take control of your computer, create a Botnet out of your computer. Once they've installed a bot onto your computer, they can do anything they want. Today, they could use it to send spam; tomorrow, they could use it for distributed-denial-of- service attack. They can use it to host illegal software; they can use it to steal your confidential information. The fact that they can exploit a vulnerability on your computer makes it irrelevant what they're trying to do today because anybody can do all of these things all of the time if you're vulnerable that way.

Matt Grant: Good point. I guess they have a lot of different options once that PC is infected. Could you tell us a little bit, how can a website know if they've been attacked and if they've been victimized and part of these 40,000+ websites that have been attacked? Obviously, at that number,

it's very hard to contact them all; is there anything that those website owners can do to see that they've been affected or that PC users can do?

Randy Abrams: One of the things that PC users can do is disable scripting, but that makes it pretty difficult to use most of the web. The most important thing for the PC users in this case is to make sure that all of their applications are current and up to date. If they've got plug-ins for browsers, make sure it's the most current like the Adobe plug-in for Firefox or for Internet Explorer, the Sun Java application, QuickTime plug-ins, anything like that. Any plug-ins for the browsers as well as the applications themselves, stand alone applications like iTunes, Adobe Acrobat, Flash, all this stuff needs to be kept current and up to date. That's the most important thing for the users to do. Website owners, what's really important, is to know what you have on your website. There are examples of some of the code that appears on hacked websites that owners can look at and then search for that code on their website, but probably this is a really good example of where whitelisting is at its best. Understand what your website is supposed to look like and monitor it so that if it changes when it shouldn't change, it doesn't matter what the change is, any change is bad in that case. Be alert, if it changed – there are programs that will monitor that – if it changed, you've got a problem.

Matt Grant: Absolutely, very good point. It's always important to be conscious of knowing where you're going and knowing what that page is supposed to look like.

Randy Abrams: If my house isn't where I left it, it doesn't matter what someone was doing – I know there's a problem. Sometimes just change alone is enough to flag a problem.

Matt Grant: Absolutely, good point. Thanks so much Randy. We appreciate you taking some time to further explain this particular attack with us. This

is Matt Grant and you're listening to the Malware report with Randy  
Abrams.

[End of recorded material]