



THE MALWARE REPORT

Legitimate Sites Hosting Dangerous Malware

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: Legitimate Sites Hosting Dangerous Malware.

Episode: 89

Location: http://www.eset.com/podcasts/ESET091708_Legitimate_Malwa.mp3

October 2, 2008

[Begin recorded material]

Matt Grant: Hi, my name is Matt Grant and you're listening to The Malware Report with Randy Abrams. Hi Randy, thanks for being here.

Randy Abrams: It's great to be back again.

Matt Grant: I wanted to spend some time today discussing this idea of legitimate sites unknowingly hosting malware. There have been more sites recently like BusinessWeek and USA Today that are legitimate websites, yet they're coming under attack and becoming hosts to malware. Is this something that you're seeing as a growing trend – folks targeting legitimate sites?

Randy Abrams: Absolutely. The reason is because people are beginning to get a little bit more savvy. They're, in some cases, not opening e-mail attachments at all, which is oftentimes a good thing. In some cases they're even slowly beginning to understand that instant messenger can have risks if there's an attachment or even a link that tells you to go somewhere. So, the bad guys are looking to "how can I get in? How can I get malware on the user's machine?" The most effective way to do it is to attack the user when their guard is down; when they're visiting a site that they have every reason to believe is legitimate. So there's a lot of effort focused on hacking the legitimate websites.

Matt Grant: How difficult is it? Do these legitimate websites have a high level of security to protect themselves as well as their readers? Or do they see themselves as sites that aren't necessarily going to come under attack so they don't have as much security as they maybe should?

Randy Abrams: It really varies from site to site. I think most of the sites have a fairly good level of security relatively speaking. The problem that they run into is when there are unknown vulnerabilities that they haven't patched. Also, the sites become massive and making sure that you've done everything absolutely correctly across the board becomes a pretty big job to manage. It just takes one small mistake to let the bad guys in. Additionally, the bad guy can use things like insider attacks. If you can get to someone on the inside that's a little bit greedy, then you don't need to use vulnerability, you can get a password that you shouldn't have with a little bit of money.

Matt Grant: You bring up a good point. These sites, for example India Times a large news site that was recently attacked, they have so many pages that one page could be compromised and it would be very hard to tell immediately that that particular page was compromised. So what should users do then to protect themselves while visiting these sites? If they're just going about their business and using sites that are legitimate, what should they be looking for?

Randy Abrams: Your basic security steps are in order. Keep your operating system patched, keep your applications patched; things like iTunes and instant messenger client, keep them patched. Use a high quality antivirus product that includes anti-spyware. I use Sandbox IE; there are other sandboxing technologies that will sandbox the browser. That's another level of defense. Sticking with the well-known reputable sites is a good precaution, it exposes you to less risk, but you have to understand that there still is some risk.

Matt Grant: What about the sites? What do they need to do to protect themselves? If the user does have a strong antivirus or security solution on their machine that will protect them, is there anything that the sites should be doing?

Randy Abrams: They should be doing security audits on themselves quite a bit. They might want to have penetration testing -- a professional firm constantly trying to hack into their site. One big growing area of concern is with online advertisements, oftentimes they don't actually know how good the advertisements they're getting are. The advertisements aren't hosted on their sites; the advertisements are on remote websites. They don't control the actual content on their own website. That's a growing area of concern that groups of people within Microsoft are trying to deal with; they've got to figure out how to control this threat factor. They know it's a growing problem.

- Matt Grant: That's really interesting, if you are visiting a legitimate site and there are banner ads on that site, that doesn't necessarily mean that those ads are hosted by that site.
- Randy Abrams: No, they aren't hosted by that site actually. The banner is hosted, but the content of the banner is coming from a remote site and you have no idea where that's at.
- Matt Grant: So would you recommend then that folks not click on the banner ads, ever?
- Randy Abrams: It's not a matter of that, by the time they've viewed the banner ad it's too late. The banner ad itself is serving up scripts; that's why they are so dangerous.
- Matt Grant: Who holds the responsibility here? Is it the website to make sure that they are not hosting the content, or is it the user to make sure that they are up to date and protecting themselves?
- Randy Abrams: There's a combination of responsibility. The user is responsible for learning how to use some reasonable security precautions. The website has a responsibility to screen their clients and trying very hard to make sure that they only have legitimate advertisers. Google is notorious for having banner ads that point to sites hosting malicious software.
- Matt Grant: This is a very interesting topic, and I know as more and more folks come under attack from legitimate sites that this is a topic that we'll be revisiting and looking at often. Last question, can a user assume that any site is safe anymore?
- Randy Abrams: Can a person assume that they get in their car and drive to the movie theater and they won't be in an accident? There is no true security, you do what you can to manage risks and you live your life. If you stick with better

known legitimate sites your risk is reduced, but you can't eliminate risk entirely.

Matt Grant: Very good point; good way to sum it up Randy. I definitely appreciate you taking the time to speak with us today. This has been Matt Grant and you're listening to The Malware Report.

[End of recorded material]