



THE MALWARE REPORT

Department of Homeland Security Attacks Cybercrime

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Department of Homeland Security Attacks Cybercrime

Episode: 123

Location: http://www.eset.com/podcasts/032409_ESET_DHS.mp3

May 28, 2009

[Begin recorded material]

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

Randy Abrams: Thanks for having me back again.

Matt Grant: We've been spending some time recently talking about sites online that can be a resource for folks to educate themselves on cybercrime and other malicious attacks that have to do with online security. One of the sites I wanted to talk about today is the Department of Homeland Security's website. Can you tell us a little more about the website in particular and what it offers?

Randy Abrams: Sure, I'd be happy to. The part that's particularly relevant is their National Cybersecurity Division. The Department of Homeland Security oversees a massive security network; these are the guys who are in charge of TSA at the airports along with a variety of security

projects. One of their mandates is cybersecurity. Cybersecurity is critical to the world; not only to our national defense, but to world stability. We've seen cyber attacks against Estonia, cyber and physical attacks against Georgia. The DHS recognizes that not only do government computers need to be secured, but businesses need to be secured because commerce is essential in our world. The DHS has launched programs to help secure the entire country, if you will. For example, I've been working with the U.S. Chamber of Commerce and DHS on a couple of panel sessions where we are working with local Chambers of Commerce. I've been on several speaking panels and there have been people from organizations such as DHS, Stay Safe Online or OnGuard Online and met with business people to help them improve their cybersecurity. One of the key partners at DHS is the United States Computer Emergency Readiness Team (US-CERT). If you go to the National Cybersecurity page for DHS, you'll find a link to US-CERT as well.

Matt Grant: Who in particular is this website targeting or most appropriate for?

Randy Abrams: It's appropriate for anyone. This is information that people need to have. They have specific sections that target different people. For example, the cyber cop portal is in accordance with law enforcement that helps capture those responsible for attacks. If you're a business person, you will not be interested in the cyber cop portal. There's the national cyber response coordination group that has 13 federal agencies. I'm sure there are many federal employees who don't know about the federal resources they have. For most users, the US-CERT page is most important because it has security alerts; you can sign up to get alerts on security issues such as Windows security or other kinds of vulnerabilities. There's a page dedicated to cybersecurity tips, general information, why cybersecurity is a problem, guidelines for publishing information online and understanding internet service

providers – most people don't even know that they need to understand them. The list of information and topics is extensive. There's about ten sections under general security, eight or ten or more under different types of attacks or threats, a whole section on dealing with cyber bullies, understanding hidden threats, Botnets, links to information on securing email and communication and mobile devices and privacy. Most people probably don't realize they aren't as anonymous they think they are.

Matt Grant: It seems as our technology continues to advance, the number of attacks on different online vectors increases. The government is starting to do more and step up the effort to combat cybercrime – are they doing enough? What do we need to do to combat cybercrime?

Randy Abrams: I'm not sure we can do enough, but the government has certainly stepped up the efforts in combating cybercrime. The survey ESET did where well over 60% of users thought the government should do more to fight cybercrime shows that the government is getting support in that citizens actually want them to tackle the challenge. It's a huge challenge, the government can't do it alone and private industries can't do it alone either. Fundamentally, it comes down to users becoming more secure. Without that the link in the chain, you won't get a grasp of the problem.

Matt Grant: Good point. You are absolutely right. There's always more that can be done. Well Randy, I appreciate you taking the time to talk to us today and point out these websites. We will continue to highlight particular websites we feel will be of value for our listeners. If you would like a list of sites or have additional questions, you can ask Randy at askeset@eset.com. This has been Matt Grant and you're listening to the Malware report.

[End of recorded material]