



## **THE MALWARE REPORT**

### ***Fake Antivirus Products Generate \$34 Million a Month!***

#### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

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

Title: Fake Antivirus Products Generate \$34 Million a Month!

Episode: 134

Location: [http://www.eset.com/podcasts/073009\\_ESET\\_Fake\\_AV.mp3](http://www.eset.com/podcasts/073009_ESET_Fake_AV.mp3)

August 13, 2009

[Begin recorded material]

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

Randy Abrams: Excellent, thanks. How are you?

Matt Grant: Pretty good, thanks. Thanks so much for joining us on the show today. You know, I've been noticing recently that there's been a lot of media attention about the rise in fake antivirus software. Is this something that ESET has been seeing as well?

Randy Abrams: Yeah, it's actually kind of a bit of a sore point for us; it's become a really huge problem. You know, I was just reading on the Tech Herald, Steve Ragan wrote an article that rogue antivirus earns almost \$34 million a month and you know it's something that sometimes our users ask us about, they say, "What happened? You didn't catch this program." But, according to Dark Reading, there's 640,000 new

variants of fake antivirus just in the third quarter of the fiscal year. So, we can catch a bunch of them and if we miss a small percentage it's still a lot of them, and all of the antivirus companies are struggling with this. It's a big, big problem and the most effective defense really is education. People need to understand what they're looking at.

Matt Grant: Yeah, absolutely. What are they or what should they be looking for and why the recent spike?

Randy Abrams: Well, it's actually been growing for quite a long time. I don't think the spike is recent; it's been coming on for quite a while. And what happens is the bad guys realize that security companies are making money and it's a lot easier to make money selling a security product that doesn't do anything than actually make it do something and so you've got these fake products that claim they do something, and they use intimidation oftentimes to sell the product. So, a user will go to a webpage and it'll say that it's scanning their computer for threats, and what they have to realize is if they did not consent to having their computer scanned, it's just a picture, it's just a video, it's not actually happening. The fake antivirus comes up and says it found all these threats on your computer and it's just a lie, it's completely not true and they say to clean them off, you need to download and buy this program.

Matt Grant: So, what's the best way I guess to spot the fake antivirus software; where can consumers go or businesses go to make sure that what they're purchasing is legitimate?

Randy Abrams: Well, they should never buy a product, I think, if it's not either tested by Virus Bulletin or certified by ICSA labs or West Coast Labs, who have check mark certification. You want to look and see that the company is actually certified or tested by one of these three organizations. You can also check and see if they're tested by [avcomparitives.org](http://avcomparitives.org) or [avtest.org](http://avtest.org). You know, they're not out there

testing the bad guys, they're testing legitimate products. So, you want to look for these organizations to endorse the products, not in terms of "We think this is a good product," but say we know we're testing something legitimate anyway. So, that's one of the big keys to it. Typically, if you do a Google search on the name of whatever product is trying to install on your computer, if it's a fake one, you're gonna find a lot of hits telling you this is bad stuff. Sometimes they make it really hard to escape the webpage; you click "Cancel" or "No" and it keeps coming back and coming back and you need to learn how to use task manager to end the process in which case it's Internet Explorer, iexplorer.exe or Firefox or whatever the name of your browser is and just end it and get out of there. You don't want to click on the file and save it or buy it.

Matt Grant: With the amount of fake AV that's out there, do you think there are a small number of groups behind all of these rogue antivirus solutions or do you think that there are a lot of different people behind these?

Randy Abrams: I expect there's quite a few different people behind these. I mean, there's probably a couple hundred different families of these threats out there and there's a lot of criminals out there that are happy to steal money. So, you know, if someone sees something making money, they're gonna copycat it as quick as they can.

Matt Grant: Right. Do you know from the top of your head, is there a handful of these rogue antivirus software that seem to be dominating the market, any names that we should warn our listeners about?

Randy Abrams: You know, I'm not sure if any are dominating and I really, I hate going for names because they get popular, they'll just change the name. It's better for consumers to understand the concepts because then they can avoid all 200+ families of this malware instead of looking out for the name of one. It doesn't matter what the name is if you've done your

homework and you've gone and checked and see 'is this a certified product, has it been tested by virus bulletin?' That's really crucial.

Matt Grant: Absolutely. No, that certification is definitely key and I think that's a good point for our listeners to be aware of when they're looking for antivirus software to help protect their PC against malware. Do you expect we're gonna start seeing more of this or do you think as consumers and users become more aware of the fake antivirus, if there's no money in it I can't see the bad guys continuing down this route or do you think we're gonna see more of this in the near term?

Randy Abrams: I think it'll be a long time before we have enough people educated enough that there's no money in it, so it's going to be here for quite a while to come.

Matt Grant: Right. Well, Randy thanks so much for discussing this topic with us. Obviously, it's an issue that listeners need to be aware of to help protect themselves against. If you have any other questions about fake antivirus or if you're unsure if the antivirus you're using or about to purchase is fake, feel free to e-mail Randy and ask him a question at [askeset@eset.com](mailto:askeset@eset.com) and feel free to follow the ESET research team on Twitter @esetresearch for the latest updates. This has been Matt Grant and you're listening to the Malware report with Randy Abrams.

[End of recorded material]