



## **THE MALWARE REPORT**

### ***Malware on the Rise: ESET Raises Awareness with New Campaign***

#### **Participants:**

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

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

Title: Malware on the Rise: ESET Raises Awareness with New Campaign

Episode: 138

Location: [http://www.eset.com/podcasts/090809\\_ESET\\_SF\\_Campaign.mp3](http://www.eset.com/podcasts/090809_ESET_SF_Campaign.mp3)

September 10, 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 joining us today.

Randy Abrams: Hey Matt, it's great to be back.

Matt Grant: You know, I wanted to chat about data that was recently released by ESET's research team and I was hoping that you could tell us a little bit more about some of the new data you found as it relates to the average number of malicious files that are found on a system and some other great data points. I guess, maybe you could first start by telling us a little bit more about how you came about the data and then we could go through some of the highlights.

Randy Abrams: Sure. ESET has the ThreatSense.net system and what happens is when a computer encounters malicious software, it sends a tiny bit of

information back to ESET and this is an opt-in thing. When ESET Smart Security or ESET Antivirus is set up, the user is prompted “Do you want to participate in ThreatSense?” and if they click “Yes” which many users do, then we get sometimes the actual infected file; it depends on what the file is. And we get statistics about, “Is this brand new? Is this unique?” And also, you can’t be on the Internet without your IP address (the address of your computer) being transmitted. Every time you go to a webpage that’s transmitted, so we get the IP address as well. And what we found is that about 33 out of 1,000 users of ESET’s software will encounter malicious software. So, it doesn’t sound like a lot, but it is a significant amount of attacks. This doesn’t mean that the 3.3% of the computers or, I think it’s .33%, are infected. Some of them are infected, but it means that they’ve at least encountered malicious software.

Matt Grant: Interesting. Yeah, I think you’re right, I think it is the 3.3%. So, basically you are looking at, if a company has 1,000 individuals, then 33 of those are susceptible to attacks and that’s obviously if they weren’t running antivirus software like ESET, they would be vulnerable to those attacks and that is a high percentage especially when you think that, you know, from what I see here in your report that you released, that is on a daily basis – which is pretty incredible. When did this data and research take place? Was it over the past couple of months?

Randy Abrams: Yeah, our research department actually decided to look into this and say, “Hey I wonder what these numbers actually come out to?” just a few weeks ago. So, this is pretty current research and there’s more information at [esetonline.com](http://esetonline.com), so people can run the ESET Online Scanner and see if they’re one of these people encountering this malicious software. But, yeah, the 3.3%, it sounds like a small percentage, however, when you consider how much malicious

software is out there, that's really a lot of people. You know, if 3.3% of the time you got in your car you were going to be in a wreck, you wouldn't drive anymore.

Matt Grant: Absolutely. So, going back to that [esetonline.com](http://esetonline.com), I understand that's a free tool from ESET. What does that do exactly?

Randy Abrams: That's the ESET Online Scanner. So, people shouldn't be running multiple antivirus products on their computer and if you're running another antivirus product for whatever reason – some people like the free ones – you can use the ESET Online Scanner to check your system, get a second opinion. This does not give you real-time protection so if you go to a website that's got malicious software, the Online Scanner is not going to protect you from it, but it might help you clean up after the fact.

Matt Grant: Interesting. Now, you guys also released that, on average, when a computer is infected, 13 malicious files are found on the system after that one infection. What does that really mean?

Randy Abrams: Well, that's interesting because what we found is there are 13 on average, 13 malicious files on the system. But that doesn't mean 13 viruses or 13 Trojans because much of the malicious software nowadays has more than one file associated with it and I believe what we found was usually there's three malware families found on infected computers. So, each of those three infections will have approximately four, just barely over four files associated with it. But, what that means is what we're seeing is the people doing the malicious software now aren't all about "I just want my malicious code installed on your computer;" they're getting paid to install malicious code. So, three people might pay them and they'll install all three at once if they're able to infect your computer. So, for a long long time, security experts have said, if your computer gets infected, the best thing to do is flatten it and rebuild it, because when your computer gets infected, all you

know is what you found, you don't know what else might be there and this data really supports that conclusion.

Matt Grant: Interesting. So, I mean this is really debilitating for a computer. So, if you are infected it sounds like there are multiple vectors that these pieces of malware can attack and then have multiple types of malicious content that could be downloaded on your machine in places you probably couldn't even find.

Randy Abrams: Exactly. And to give you an analogy of this, if you leave your front door unlocked on your home, many people can come in through the front door, it's not just a burglar who could come in. A burglar could come in; an arsonist could come in; a murderer could come in. There's all kinds of bad guys that can come in if you've got a vulnerability – which, having the front door unlocked leaves you vulnerable. So, it's the same with computers. If you've got a vulnerability, it doesn't mean just one piece of malicious software can come in; anything out there can exploit it.

Matt Grant: Now, are we seeing an increase then overall in malicious attacks these days especially with people investing so much in their computers and relying on them more than ever; how important is it to stay protected? Is this problem only getting worse?

Randy Abrams: Well, the problem is getting much worse. You know, I'm not sure if we're seeing an increase in the absolute number of malware attacks, but what we're seeing is about 100,000 new pieces of malware every day and in many cases it's old malware that's been modified to evade detection. So, yeah, you can say it's new malware, but it's not some brand new attacker. It's a seasoned attacker doing what they need to do to make sure that they keep on infecting computers and so yeah, if you're not protected, you're going to get nailed.

Matt Grant: Yeah, it sounds like there are certainly a lot of vulnerabilities out there. So, if a person, if a user, does buy that new computer, what are kind of

the first couple of steps that they should take to make sure that that machine is protected and then what, as a user, should they also do as a user do that's key to continue to stay protected?

Randy Abrams: That's a really good question because people, kids, have just gone back to school and gone to college and sometimes have their first computer of their very own and that computer often comes with antivirus software pre-installed on it. So, one of the things you want to do is check and see if this is an evaluation copy that's going to expire in three months or six months and make that sure you don't let it expire. Either purchase the full product that doesn't expire or purchase brand new antivirus software that you like and run it on your computer. Make sure you've got a firewall, and software suites generally will include a firewall. Windows has a very basic firewall which is a heck of a lot better than nothing. Don't ever turn off the firewall. I've encountered cases where an ISP support person will say, "Well, to do this you need to turn off the firewall" and they forget to tell the user, "You need to turn it back on." Generally, turning off the firewall is not the answer, but if you ever do that, make sure you turn it back on and by all means, especially with high-speed Internet like cable or DSL, have a router. You probably would have one anyway if you wanted to do wireless, but even if you're plugged right into the wall, put a router between your computer and the Internet and that helps protect you as well. And then use some good judgment. Free usually isn't free, it usually costs something. So, if you're surfing the web for free desktop wallpaper and free smileys and stuff like that, especially for free antivirus software, do some research and make sure you're dealing with a credible site. There are good free antivirus software products, but there's a lot of bad ones out there as well.

Matt Grant: Great advice Randy and before I let you go, it certainly sounds like this problem is getting worse and there's a lot that users should be

aware of. ESET recently released a campaign in San Francisco during the month of September to try to generate awareness of this problem.

Can you tell us quickly a little bit about that campaign?

Randy Abrams: Yeah, it's actually a rather lighthearted and fun campaign. People tend to be more visually oriented. I mean, words start running together when you're just reading things over and over. So, we've got some videos up there to kind of demonstrate by analogy what happens to your computer when it gets infected. The website is [www.esetsecures.com](http://www.esetsecures.com) (plural) eset.secures.com. Check out the snowboarding turkey on the lower left side, it's a pretty funny video. But, you know we have a variety of videos, and people are interviewed, and there's some gags pulled and it's just to raise awareness and make people understand that this malicious software really does stuff to your computer.

Matt Grant: Randy, as always thanks so much for taking the time to chat with us today. If you have any questions for Randy, feel free to e-mail him at [askeset@eset.com](mailto:askeset@eset.com). You can also learn more about ESET's San Francisco campaign at [esetsecures.com](http://esetsecures.com). Feel free to follow Randy and the ESET research team on Twitter @esetresearch and you can also learn more about the San Francisco campaign by following @esetpr at Twitter. This has been Matt Grant and you're listening to the Malware report with Randy Abrams.

[End of recorded material]