



THE MALWARE REPORT

Virtualization is Not Security!

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Virtualization is Not Security!

Episode: 88

Location: http://www.eset.com/podcasts/ESET091708_Virtualization.mp3

September 29, 2008

[Begin recorded material]

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

Randy Abrams: Thanks for having me.

Matt Grant: I wanted to take some time today to talk about virtualization security, given the VMWorld tradeshow recently took place, and there was a lot of buzz coming out of this show regarding securing virtual environments. What's the main concern here with regards to securing the virtual network?

Randy Abrams: Well there are a couple concerns. One of them is users misunderstanding the difference between virtualization and security. Virtualization in itself is not security and can actually lead to a less secure environment, because you're kind of putting all your eggs into one basket when you virtualize multiple machines and have them all on the same physical machine. So if a user thinks that they are gaining security by virtualization, they're really misleading themselves. Virtualization is great for saving energy -- for being more green. It can be good for helping to manage multiple machines as well, but it's not security itself. The example I like to use is, if you're using a virtual machine and you get a keystroke logger installed on it and then you open up your browser and go to your online bank site and log in, well, it's real money that you're going to lose. I was at a security conference at Microsoft and one of their leading virtualization developers was saying, "Actually, when you use virtualization and have many machines on the same server there is a little decrease in your overall security". You have to be careful what kinds of applications and machines you put together on the same virtualized environment.

Matt Grant: I had an e-mail come in to askeset@eset.com from Steve who is an IT Manager with about 30 employees at his organization. They are thinking of virtualizing their environment. What should he do to secure that environment and what should he look for in terms of security solutions for a virtual network?

Randy Abrams: It's a really good idea to read up on the virtualization issues and security issues. Education cannot be overemphasized; you're still going to want all of

the traditional security measures, and you're going to want a hardware firewall that's protecting the virtual machines. As well as personal firewalls within each of the virtual computers in most cases. You're also going to want different levels of security, including anti-malware software. Malware frequently will run just fine in virtual environments, although in some cases, malicious software will detect that it's running in a virtual environment and then refuses to do what it normally would do. Occasionally, you can gain a benefit inadvertently. You don't want the malware there in the first place, that indicates that there's a problem in your security measures.

Matt Grant: Is it as easy to protect a virtual environment as it is a physical network?

Randy Abrams: For the most part it's just as easy, but you have to understand that you're reducing your security level by having multiple machines in the same virtualized server. Just like using the same password for multiple accounts is dangerous, having the same virtual machine with a bunch of servers or workstations on it is somewhat analogous to using the same password in multiple locations.

Matt Grant: So do you see this as an area where folks know there's some security risks involved, or not?

Randy Abrams: Right now a lot of people mistake virtualization for security, and generally security is not the right reason to go to virtualization. If you want to use virtualization to enhance security then you have to understand certain techniques that need to be used to achieve that. For example, I use a product called Sandbox ID where it virtualizes the browser, but I religiously empty the Sandbox between websites. That's one of the fundamental issues with Google's home browser, they're sandboxing tabs; however, if you use the same tab for multiple sites you can create the effectiveness of the virtualization – the sandboxing.

Matt Grant: Well, Randy, I definitely appreciate you taking time to speak with us about this topic. I think that's extremely beneficial as more organizations are looking to virtual networks and virtual environments. If you have any questions for Randy, please feel free to e-mail him at askeset@eset.com. This has been Matt Grant, and you're listening to The Malware Report.

[End of recorded material]