



THE MALWARE REPORT

Virtualization: Security Risks You Must Know

Participants

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

Amir Ben-Efraim, CEO, Altor Networks

The Malware Report Transcript

Title: Virtualization: Security Risks You Must Know

Episode: 98

Location: http://www.eset.com/podcasts/120108_ESET_Altor_Virtualization.mp3

December 4, 2008

[Begin recorded material]

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

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

Matt Grant: We also have a special guest on this week's edition of The Malware Report. We have Amir Ben-Efraim who is the CEO of Altor Networks, a virtual firewall provider. Hi Amir, thanks for being here.

Amir Ben-Efraim: Thank you, Matt, nice to be here.

Matt Grant: We wanted to spend some time today talking about malware becoming smarter or more virtually aware. Randy, maybe you can give us some background with your expertise in the security industry. What's your experience with malware becoming smarter, if you will, or more virtually aware?

Randy Abrams: There's a long history of malware becoming much more aware of what it's interacting with, and this goes way back to the DOS days when the malware would just simply look if there was antivirus and try to delete it. As the malware became more complex, researchers used virtual machines to analyze the malware. So the malware authors started checking to see if they were running in a virtual environment, so that they wouldn't be detected – they just wouldn't do what they're supposed to do. However, along with that realization the bad guys realized that there's a lot more to virtual environments than just antivirus running. We're currently seeing over 200,000 files a month that use VM-aware techniques to check and see if they're running in a virtual machine. It's kind of a stunning realization when you consider how rapidly the use of virtual machines are growing.

Matt Grant: Amir is this something that you are seeing or hearing from your customers who are using virtual environments?

Amir Ben-Efraim: I think there is a lot of education that's taking place on that front right now. First of all, virtual machines are just as vulnerable as physical machines, so steps must be taken to protect them. Because virtualization is still so new, many IT organizations fail or just simply forget to architect in advance to ensure security best practices carry over into their virtual domain. So things we take for granted such as antivirus and firewalls must be given due consideration to make sure that they can address the unique security needs of many virtual machines hosted on a single physical host.

Matt Grant: Interesting. Randy, how has malware really evolved to recognize virtual environments? And how's the AV industry trying to combat this problem?

Randy Abrams: Well right now, from an AV pure perspective, what we're dealing with is malware that is trying not to be detected by antivirus software. The malware sees AHA and running in a virtual environment and that

means that probably someone's trying to reverse engineer me. So, the malware will then do things to avoid detection, as long as it realizes it's in a virtual environment. We also know from history that the bad guys are trying to exploit anything they can. What we know now also is that virtual with environments becoming widespread, you can have one server hosting several VMs and that could represent several Web sites that the bad guys want to exploit so that they can get their malware out there; that's pretty concerning. You couple the VM-awareness with respect to malware, with the bad guys' knowledge that there's a huge juicy target out there and you really need to consider taking defense-in-depth into perspective when you're implementing a virtual environment. Running multiple virtual machines on a single server actually increases your attack surface, it doesn't make you safer.

Matt Grant:

Interesting. Amir, do you agree with that? From the virtualization perspective, what are you most concerned about when it comes to virtually aware malware?

Amir Ben-Efraim:

Yes, I guess today malware can infect a VM in much the same way it can infect a physical server. And as Randy had described, unfortunately once a VM is infected it makes an excellent launch pad for spreading around to other neighboring VM's inside that same virtual server. Given the consolidation of VM's that's going on, it's very easy for one infected VM to infect twenty or thirty pure VM's that are all riding on that same physical host without anyone even recognizing that something bad is going on. And, what's really concerning is how malware can already spot that it's inside of a VM as Randy had just mentioned. So it's easy to extrapolate and see that we're quickly heading towards malware that will leverage the facilities of virtualization against itself to actually cause more damage. For example, a VM that's infected by malware could intentionally trigger Live Migration and move itself around a virtual data center and

circumvent any security that's in place; such as firewall that are installed as physical appliances. The malware could essentially just simply walk around them by triggering VMotion or Live Migration.

Matt Grant: It seems like more and more organizations are turning to virtual networks and virtual environments. For both of you, what would you recommend to IT managers who are looking to virtualize their environments?

Randy Abrams: I'd recommend first off recognizing that running multiple VMs on a single box means that you've got a larger attack surface. Virtualization is not security. Recognize that your attack surface is greater, and then deal with it by having much stronger defense in depth.

Amir Ben-Efraim: I'd like to add to that, companies need to start preparing for zero-day protection by looking for security tools that were designed with virtualization in mind and are capable of detecting and stopping virtualization attacks. For example, virtual firewalls or antivirus capable of detecting virtual malware are excellent starting points as people consider using virtualization in production and places like that.

Matt Grant: Well Amir, I definitely appreciate you being a guest on our show this week; and taking the time to speak with us about this concern and the growing need for security within virtual environments. To learn more about Altor Networks visit www.altornetworks.com. And to ask Randy additional questions on this topic e-mail him at askESET@ESET.com. This has been Matt Grant, and you're listening to The Malware Report.

[End of recorded material]