

Realtime
publishers

The Essentials Series:
Virtual Security Concerns & Solutions

Understanding & Improving Virtual Machine Security

sponsored by



eEye Digital Security®

by Greg Shields

Understanding & Improving Virtual Machine Security	1
The Added Issues of Virtual Machine Dormancy	2
Agentless and Agent-Based Tools	4
New States Equals New Needs	4

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Understanding & Improving Virtual Machine Security

Article 1 of this series discusses some of the new and powerful hypervisor-based vectors for infection that arrive when an IT organization makes the move to virtualization. That article discusses how the hypervisor easily becomes a quiet risk to the unprepared organization. But the hypervisor itself is only one facet of the story. Along with its benefits, the move to virtualization brings about added risks associated with your virtual machines themselves.

Physical servers traditionally tend to operate in the *Powered On* state for essentially their entire operational life cycle. Once built, a physical server is rarely rebooted and almost never down for an extended period of time due to the always-on needs for its services. On the contrary, while virtual machines can be considered functionally equivalent with traditional physical machines, their easy-to-create nature and single-file composition makes them much more likely to exist in states other than *On and Operational*. For example:

- Virtual machine templates, which are machines themselves, are rarely powered on.
- Single-use virtual machines may linger on-disk past the point of their usefulness. Their presence on-disk may ultimately be forgotten over time.
- Virtual machines based on templates rather than built from the ground up tend to not exist in the *Build* state like what is usually required in the early stages of physical server creation.

Figure 1 shows a graphical representation of these differences in states between the two machine types.

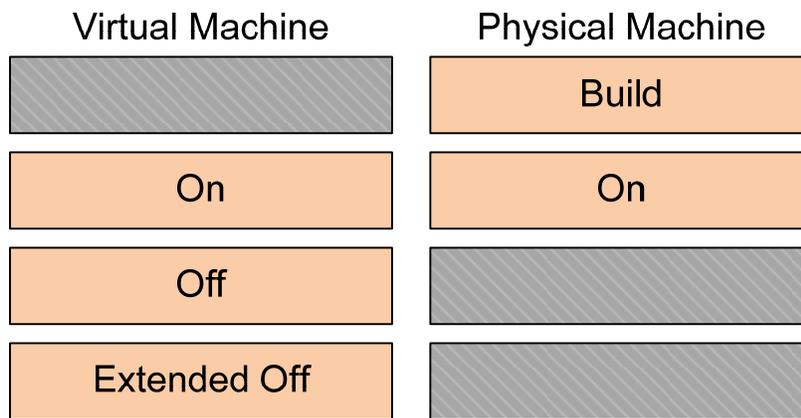


Figure 1: Virtual machines and physical machines tend to spend their time in much different states.

The most problematic of these states is the situation in which a virtual machine for one reason or another finds itself in an extended state of powered down. While powered down, a virtual machine is little more than a file on a disk. The accumulation of these files across the IT environment can grow to become a critical issue for organizations that lack the capability to inventory their state and keep them patched.

The Added Issues of Virtual Machine Dormancy

With virtualization, most IT organizations are aware of the ease of creating new virtual machines. Virtualization's "copy and paste" process for accomplishing this task speeds the process of bringing on new services to meet the demands of business. But at the same time, it introduces a set of risks to the computing environment.

First is the problem of virtual machine spread. When the creation process grows absurdly simple, IT organizations can quickly find themselves awash in dozens or hundreds of new virtual machine instances to manage. Dealing with the management and licensing issues of a quickly growing server count can be a major hurdle for the unprepared organization.

This first problem of spread is obvious but merely administrative. There is a more critical yet often overlooked security-related issue associated with virtual machine inventory growth. That issue is virtual machine *dormancy*. When virtual machines can be created quickly, there comes the increased likelihood that some will be created for short-term uses and then later discarded. These virtual machines when powered off exist as benign files in a data storage location but can later become a vector for compromise when powered on.

The ever-changing nature of security threat prevention requires that functioning computers operate with a specific and up-to-date configuration to protect them against malicious threats in the environment. Consider the situation shown in graphical form in Figure 2. There it is easy to see how a virtual machine can be created and used, then powered off and forgotten, only to be later powered on without the proper security configurations needed to protect itself from compromise.

As this example shows, protections were implemented for every operational computer in the environment. But those protections were missed on the machine that was powered off during the update. The dormant virtual machine—powered off and missing the update—when later powered on, becomes a risk for compromise.

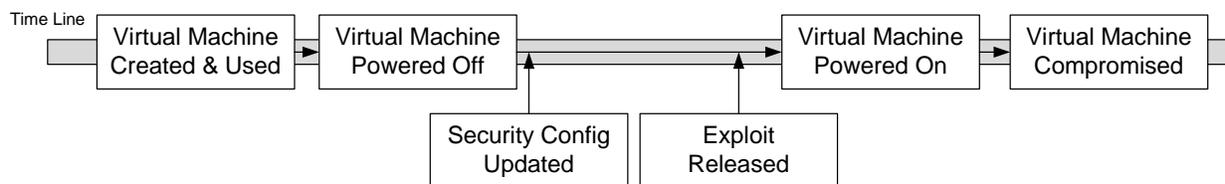


Figure 2: In the timeline of virtual machine dormancy, forgotten virtual machines are likely to be powered down during the period when critical security configurations are updated. This results in the virtual machine being unprepared for an exploit should it later be powered on.

When thinking about this issue of virtual machine dormancy, consider the answers to five questions that probe how your environment handles security and configuration updates in support of security:

- *How are you patching?* When your organization undergoes its regular patching process, is that process done using manual tools or through automated systems? More importantly, are those systems regularly probing all endpoints on the network to identify computers that have missed the deployment of a particular patch? Effective patching systems have the capability to regularly scan endpoints across the environment without the need for installed agents on each computer. By not relying on the need for installed clients, rogue computers that are not built to specification can be quickly identified and patched when they arrive in the network. For dormant virtual machines, regular scanning and patch updating ensures that any offline virtual machine is quickly updated before it can be exploited.
- *How are you updating security configurations?* Security for computer systems is more than simply ensuring that the correct vendor patches are correctly installed. Firewall configurations, file system permissions, desktop and application lockdowns, and allowed/disallowed executables are all examples of security configurations that must be set and maintained over the life cycle of each computer in the environment. As with patches, your process for updating security configurations must have the capability to quickly identify and resolve areas of gap.
- *How are you monitoring your baseline?* For both of the previous needs, there is the critical necessity of creating and maintaining a baseline across all computers. The process to monitor for that baseline and individual machine alignment with that baseline must include regular scanning irrespective of location, directory services membership, and operating system (OS) type.
- *How are you verifying that entitlements are current?* One major factor in ensuring that baseline is in validating the users and entitlements on machines in the environment. For security as well as compliance purposes, IT organizations must ensure that dormant virtual machines are not hosting expired users or entitlements assigned to those users. Your management solution must have the minimal capability to peer into virtual machines as they power on to identify and remove expired accounts before they can be exploited.
- *How are you identifying when machines are powered on?* The most crucial component of all these questions is in identifying when computers are brought online in the environment. When machines both virtual and physical can be identified and adjudication actions completed at the point of their power on, much of the risks associated with dormancy disappear. Active identification of machines going from Off or Extended Off states to On and Operational is a key need for environments that leverage virtualization.

Agentless and Agent-Based Tools

In answering these questions, IT environments that make use of virtualization must incorporate tools that assess the risk of dormant virtual machines. That assessment requires two separate but linked phases. First, the location of dormant virtual machines—those that exist only as files on a disk—must be identified and inventoried prior to being powered on. By identifying dormant virtual machines while they remain benign, it is possible to move to the second phase.

In the second phase, virtual machines must be protected from the point they are powered on until they are considered healthy. This protection prevents the effect of external attacks from impacting the unprotected machine until the proper protections can be put in place. In accomplishing this mission, both agentless and agent-based tools can be used. Agentless management platforms provide a mechanism to scan entire network environments irrespective of location. Agentless management platforms integrate with common management frameworks at the OS level as well as the virtual platform level to interrogate network endpoints for specific information. When otherwise unmanaged network endpoints become active, only through the use of agentless mechanisms can these endpoints be quickly identified.

 Part of that risk identification process should include the mapping of environment elements—virtual machines being only one example—to their relevance to the business. Best-in-class tools provide the ability to map network elements such as virtual machine composition to business applications. This gives the IT organization an easy way to identify potential threats and prioritize them based on risk, impact, and business priority.

Agent-based tools enable richer management capabilities of predetermined IT assets. With agents installed to virtual machines at the time of their build, the agents have the onboard ability to identify when they have been powered on. They can provide protections from within the virtual machine while incorporating the necessary configuration updates as identified by management servers.

New States Equals New Needs

With the potential for entirely new states of operation associated with virtual machines comes the need for new tools. These tools ensure the proper configuration of machines even during extended periods of being powered off. Only by leveraging the right set of tools that enables monitoring for dormant machines can IT environments truly protect themselves against the accidental exposure that can occur by simply powering on a forgotten or expired virtual machine.