Symantec

SECURITY RESPONSE

Threats to virtual environments

Candid Wueest

Version 1.0 – August 12, 2014, 16:00 GMT

> *According to Forrester Research, over 70 percent of organizations are planning to use server virtualization by the end of 2015.*

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

Symantec

CONTENTS

OVERVIEW

Virtualization in enterprises has been a growing trend for years, offering attractive opportunities for scaling, efficiency, and flexibility. According to Forrester Research[1], over 70 percent of organizations are planning to use server virtualization by the end of 2015.

Often, companies delay implementing virtualization due to security concerns or adopt virtualization before deploying advanced security measures. However, virtual machines and their hosting servers are not immune to attack. Introducing virtualization technology to a business creates new attack vectors that need to be addressed, such as monitoring the virtual networks between virtual machines. We have seen malware specifically designed to compromise virtual machines and have observed attackers directly targeting hosting servers. Around 18 percent of malware detects virtual machines and stops executing if it arrives on one.

Virtual systems are increasingly being used to automatically analyze and detect malware. Symantec has noticed that attackers are creating new methods to avoid this analysis. For example, some Trojans will wait for multiple left mouse clicks to occur before they decrypt themselves and start their payload. This can make it difficult or impossible for an automated system to come to an accurate conclusion about the malware in a short timeframe. Attackers are clearly not ignoring virtual environments in their plans, so these systems need to be protected as well.

1. Strategic Benchmarks 2014: Server Virtualization, Forrester Research, Inc., March 2014.

Symantec

INTRODUCTION

> “Virtual machine hosting servers are not any less secure than any other type of server - they are just as vulnerable to malware or targeted attacks.”

Introduction

Virtualization presents organizations with many opportunities, as well as some new challenges. The concept lets companies abstract, pool, and automate all of their computing resources, such as operating systems and storage, within a data center. Businesses can access virtual environments as a service through a software-defined data center (SDDC). By letting companies access their resources from an SDDC, they can scale more efficiently and deploy new services quicker.

Virtual environments are often combined with cloud solutions and other services. SDDCs even influence the whole datacenter architecture, so some of these aspects need to be considered as a complete package. Rolling out virtualization in the data center involves a lot of planning.

Virtual machine hosting servers are not any less secure than any other type of server —— they are just as vulnerable to malware or targeted attacks. In addition to this, attackers are introducing new attack vectors to target virtual machines and their hosting servers. Unfortunately, not every company applies well-known security principles to virtual machines, despite the fact that most virtual servers are open to the same risks as physical servers are, along with a few new ones. Virtual machines need to be patched and protected just like traditional physical computers. Enterprises need to ensure that their virtual machines are included in their security strategy.

In this paper, we will highlight a few security concerns with virtualized machine environments (VME), focusing on malware targeting VMEs. Most of these concerns apply both to hosted hypervisors as well as bare-metal hypervisors which do not have a host operating system.

Security challenges with virtual machines

There are a few extra security challenges that come into play when VMEs are used. The most common issues are as follows.

Up-to-date snapshots

Companies can create snapshots of their virtual machines at a certain point in time, which can be accessed again at a later date. Often, the installed software in these snapshots is not kept up-to-date. This means that when an older image is provisioned, such as during a disaster recovery, the image is outdated. This could allow attackers to exploit old vulnerabilities until the next patch cycle detects and upgrades this virtual machine. Companies should ensure that their virtual machines' software is updated regularly, security patches are applied, and that security software is up and running. Missing or outdated licenses of virtual machines' software can also be a problem that leads to security holes. Most virtual environment management tools allow a periodical launch of the images in order to patch them. This life-cycle management is important to any security strategy. Newer SDDCs lets security reside outside of the virtual machine, allowing for an additional up-to-date security barrier. Another option to keep the software up-to-date is the use of Virtual Desktop Infrastructure (VDI) and application virtualization.

Virtual networks

Depending on the setup, multiple virtual machines may be connected over a virtual switch in order to provide a virtual network. This can mean that any traditional network security service, such as an intrusion detection system (IDS) or data loss prevention (DLP) agent, will not detect if one virtual machine attacks another on the same physical server, as the traffic never passes through the physical network. To overcome this layer of complexity, virtual machine vendors allow virtual firewalls and similar devices to be deployed. Companies need to ensure that they have accounted for this in their network diagrams.

Mixed data sets

Since multiple virtual machines are hosted on the same physical hardware, compliance issues might arise. If a virtual machine with sensitive information is mixed with non-sensitive virtual machines on the same physical server, auditors might complain, depending on the regulations surrounding that specific data. These circumstances can make it harder to manage data. Dynamic trust zones covering workloads that share common security and compliance policies can be used to cover this. Companies should treat snapshots of these virtual machines as sensitive too and should protect them accordingly.

Covering dynamic systems

Virtual machines may be moved around quickly from one host server to another and new systems can be provisioned rapidly and may be deleted afterwards. In cases of load balancing, the server may transparently switch from one virtual machine to another. This can lead to an issue if traditional security barriers like firewalls are configured very narrowly. Virtual machines that are moved, either manually or automatically due to a fail-over feature, may end up at a different cluster with a different physical network address. Since workloads are not tied to specific physical devices, logical security policies are required. This activity needs to be addressed in the security information and event management system (SIEM) in order to have consistent logging and tracking of events. Some virtualization solutions allow for dependencies on different levels to be defined, which ensure that the correct security postures are applied at the destination. New virtual systems that are provisioned temporarily may never show up in inventory snapshots and could be left out of some security audits.

Input/output (I/O) hits

Simultaneous disk operations, such as updating software or rebooting multiple virtual machines after patching, may generate a huge I/O access spike on the physical server, which can reduce the server's performance capabilities. Because of this, many software tools allow companies to roll out changes in small batch groups or add a randomized time element for when the operations should start. Unfortunately, this can mean that virtual machines can remain unpatched for longer periods of time, opening them up to attack. For example, an attacker could deliberately use up scarce resources to carry out a denial-of-service (DoS) attack against a local server. If enough resources are bound, then this attack may reduce the performance of any other virtual machine on the same host server. Most virtualization software includes options to throttle the Input/Output Operations Per Second (IOPS) per machine.

Managed access control

Management tools for virtual environments let IT administrators make significant changes to their virtual environments. With the combination of multiple virtual systems on a single hosting server, this could increase the risk of insider threats. Virtual environments need to be protected from mistakes or malicious actions by administrators with high privileges. Setting up role-based access control across a large virtual environment can be a complex challenge.

Symantec

SECURITY THREATS TO VIRTUAL SYSTEMS

> “One of the most feared scenarios among administrators is if malware from a virtual machine breaks out and infects the host server.”

Security threats to virtual systems

There are two main scenarios which lay out how malware could specifically attack virtual systems. Either the malware exists on the host server and attacks the virtual machine or the threat is on the virtual machine and attacks the host server. All other attack vectors can be reduced to classic scenarios where a computer attacks another computer, which we already know about from the traditional IT world.

Infecting virtual machines – the Crisis malware

It is possible that an attacker who successfully breaches a host server will infiltrate virtual machines on that server or create their own malicious virtual machine and launch it.

We have seen malware that has actually automated this behavior. One example of such malware is W32.Crisis. This specific threat targets multiple operating systems, including Windows, Mac OS X, and Microsoft's previous mobile operating system Windows Mobile. The malware is dropped as a Java file through social engineering and performs various information-stealing activities. The malware also tries to spread to virtual machines that are stored on the local server, a host-to-guest infection. It does not exploit any vulnerability in the VMware software itself to achieve this. Rather, it takes advantage of the fact that all virtual systems are simply a series of files on the disk of the host server. These files can usually be directly manipulated or mounted with freely available tools.

In the case of W32.Crisis, the malware parses the preferences.ini file in the VMware installation directory and searches for .vmx file paths in it. The threat then searches for VMware Virtual Machine Disk files (VMDK) inside the .vmx settings file.

```
.text:100218D0 S_infectVmwareGuest proc near           ; CODE XREF: sub_10021990+16C↓p
.text:100218D0
.text:100218D0 var_414         = dword ptr -414h
.text:100218D0 DstBuf          = word ptr -410h
.text:100218D0 ArgList         = byte ptr  4
.text:100218D0
.text:100218D0                 sub     esp, 414h
.text:100218D6                 push    edi
.text:100218D7                 mov     [esp+418h+var_414], 0
.text:100218DF                 call    _sub_10018C60
.text:100218E4                 mov     edi, eax
.text:100218E6                 test    edi, edi
.text:100218E8                 jz      loc_1002197D
.text:100218EE                 push    esi             ; int
.text:100218EF                 mov     esi, dword ptr [esp+41Ch+ArgList]
.text:100218F6                 lea     eax, [esp+41Ch+var_414]
.text:100218FA                 push    eax             ; int
.text:100218FB                 push    edi             ; int
.text:100218FC                 push    esi             ; ArgList
.text:100218FD                 call    S_controlDevice
.text:10021902                 add     esp, 0Ch
.text:10021905                 test    eax, eax
.text:10021907                 jz      short loc_1002197C
.text:10021909                 push    offset aMugpxAl ; "mUgpX-al"
.text:1002190E                 push    edi
.text:1002190F                 call    S_copyToStartUp
.text:10021914                 add     esp, 8
.text:10021917                 test    eax, eax
.text:10021919                 jz      short loc_10021949
.text:1002191B                 push    offset aVmwareInstalla ; "- VMWare Installation...........OK\r\n"
.text:10021920                 call    _sub_10008570
.text:10021925                 push    esi
.text:10021926                 push    offset aInf_ModuleSp_1 ; "[Inf. Module]: Spread to VMWare %S"
.text:1002192B                 push    0FFFFFFFFh      ; MaxCount
.text:1002192D                 lea     ecx, [esp+42Ch+DstBuf]
.text:10021931                 push    208h            ; SizeInWords
.text:10021936                 push    ecx             ; DstBuf
.text:10021937                 call    __snwprintf_s
```

Figure 1. W32.Crisis virtual machine spreading routine

The malware then uses the available mount service tool, vixDiskMountServer.exe, to mount the image file as a drive and start modifying it. The threat modifies the image file by copying itself to the startup folder of the virtual Windows computers in order to execute itself and infect the virtual machine the next time the virtual machine starts. The analyzed version of W32.Crisis did not attempt to infect any other OS inside virtual machines and did not target VMware ESX servers, but an attacker could theoretically do this.

For more information about the W32.Crisis malware, we have published a whitepaper detailing this threat.

Escaping virtual environments

One of the most feared scenarios among administrators is if malware from a virtual machine breaks out and infects the host server. This guest-to-host infection or virtual machine breakout could lead to widespread malware infections across many computers. This would be bad for an environment where one hosting server runs many guest virtual machines, but could also impact security professionals who are using virtual machines to securely analyze malware. It is possible for malware to escape from a virtual machine system to the host server, depending on the presence of local vulnerabilities.

It is rare, but there have been some cases where vulnerabilities in virtualization software allowed guest-to-host infection. For example, in 2009, there was the Cloudburst Attack, which allowed attackers to execute code on the host server. This attack used some invalid instructions to generate exceptions that could be hijacked. This trigger could then be cached by the emulator, establishing communications between the virtual machine and the host server.

There has been a lot of research on guest-to-host infections carried out over the years, for example by invisiblethings lab and Peter Ferrie.

Administrators should keep host servers up-to-date and should patch any known vulnerabilities. Further lockdown and hardening of the host server can limit any potential damage.

There are some other circumstances where malware might be able to spread from the virtual machine to the host computer. When shared folders between virtual machines and host servers are enabled, worms can spread from one system to the other. This requires some user interaction and should be treated like any other network sharing permission that could lead to malware spreading. Worms could also spread by exploiting vulnerabilities of exposed operating system services. Here, the host server and virtual machine act like two separate systems on the network. Just keep in mind that, depending on the setup, the network traffic might only occur on the virtual network.

Challenges in using a VME for security analysis

Security researchers and security solutions have been using virtual machines for many years in order to run and analyze suspicious files in a controlled environment. Snapshot technologies deploy quickly and can be configured for many different requirements. For example, researchers can replicate the user's computing environment, with different versions of software and third-party tools, in order to verify if exploits could successfully breach defenses.

Such sandbox-like technology can be used to log artifacts that are generated during code execution as well as any system changes that have occurred. Different security systems use different approaches. Some use system emulation while others use virtualization or sandboxes. In the case of virtualization, the code runs on the actual underlying hardware, as opposed to emulation, which can run programs that are written for different CPU architectures as well. Furthermore, simple virtualization systems take snapshots before and after code execution and compare them. More advanced virtualization systems log all system changes made by the code or can even trace the complete code.

Depending on the methods used, the results may be more or less granular, providing different benefits or drawbacks. For example, a snapshot delta analysis will not see memory changes, so any memory-only threat might be unnoticed. Also, it is difficult to say if the threat has performed all of its action during the snapshot window. Many attackers use different methods to make it harder for security researchers to analyze these threats on virtual machines.

Evading analysis

One of the most basic analysis evasion method encountered in the wild is to detect if code is running in a virtual machine. There are many freely available code snippets that will help malware detect the most common virtual machines. If a VM is detected, the malicious code can act accordingly, which in general means stopping code execution and exiting the system. This might lead a lesser skilled observert to believe that the suspicious sample does not perform any malicious activities and classify it as a benign application.

The following evasion techniques worked on certain virtual machines at some point in time. The vendors of virtualization technologies are constantly upgrading their software to make them more robust. As a result, not all of these techniques still work. In addition, extra tools and scripts are available to let researchers modify static attributes of virtual machines in order to keep malware from detecting that it is running in a virtual machine.

Techniques for checking the presence of a virtual environment:

- Check the MAC address of the virtual network adaptor to try and reveal the virtual machine vendor.
- Check the BIOS brand and version to reveal the virtual machine vendor.
- Check certain registry keys that are unique to virtual machines. Often, the virtual machines leave traces in different registry keys. For example the existence of "HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__" reveals the presence of VirtualBox.
- Check if helper tools, such as VMware tools, are installed.
- Check for the presence of certain process and service names.
- Check for the presence of specific files, like drivers specific to virtualization.
- Check for communication ports for guest-to-host communication.
- Execute special assembler code and compare the results. Some commands are not implemented or can behave differently than on physical computers. Other commands take longer to execute and can show a timing difference.
- Check the location of system structures, such as the interrupt descriptor table (IDT). Virtual systems typically store the IDT at a higher register than a physical computer does.
- Check for static OS licenses.
- Check dmesg or dmidecode log for entries from virtual devices.

These checks are frequently integrated into runtime packer applications, which can be used to encapsulate the malware code. These sometimes legitimate packer tools can offer many options for checking for the presence of virtual systems.

In some rare cases, we have encountered malware that does not stop code execution in a virtual machine, but instead sends false data. These "red herrings" might ping command-and-control (C&C) servers that do not exist or check for random registry entries. These tactics are meant to confuse security researchers or trick the automation process into believing that the malware is a benign application.

We conducted an analysis in order to see if malware authors are frequently using techniques to detect virtual machines. We randomly selected 200,000 customer submissions since 2012 and ran them on both a real computer and on a VMware virtual machine. We then compared the results. Some samples had to be filtered out due to unrelated crashes before leaving traces. We also tried to remove any sample that generated fake "red herring" traces. The result is that for the last two years, the percentage of malware that detects VMware hovered around 18 percent, with a short spike at the beginning of 2014 where it reached 28 percent. On average, one in five malware samples detect virtual machines and stop

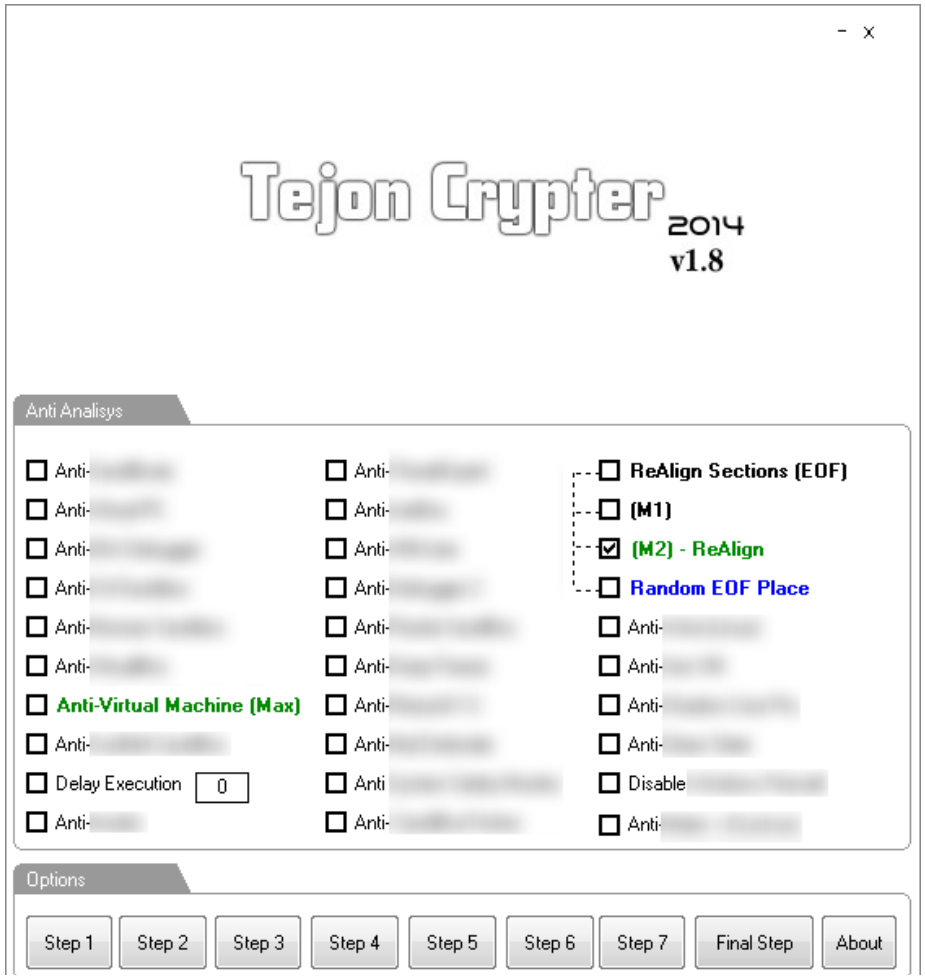

Figure 2. Packer tool virtual machine detection options

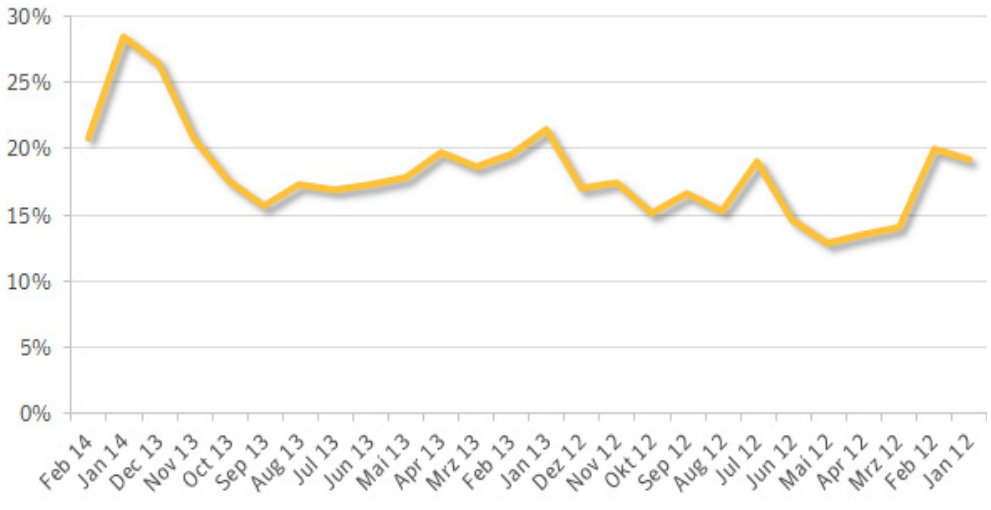

Figure 3. The percentage of malware samples that detect VMware virtual machines per month

executing completely if they arrive on one. This means the majority of malware will happily continue to run in virtual machines.

For security researchers who are concerned that they might miss 18 percent of the threats with their security analysis, we advise them to use real physical hardware in a controlled network for security analysis. Once the analysis is complete, the computer can be reimaged with a clean image. Of course, this might not always be feasible, but it will provide reliable results.

Evading automated systems

Virtual systems or sandboxes are also commonly used to automatically execute suspicious samples, in order to produce a verdict about the sample.

Malware has one huge advantage when executed on an automated virtual machine analysis system — time is on its side. The automated analysis system needs to make a decision in a reasonable timeframe, because the user is waiting for their connection. If the sample does not behave maliciously within the first five to ten minutes the analysis system will most likely deem the file as harmless. This has caused attackers to develop other methods to detect a virtual machine or rather, evade automated analysis on virtual machines, such as focusing more on the user's interaction. The following examples show that the attackers have found ways to evade automated analysis and are still capable of executing sophisticated spear-phishing attacks without getting detected at the gateway.

System delays

Malware can wait for the virtual machine to restart twice before the software starts acting maliciously. On normal client virtual machines, this will happen in a reasonable timeframe, so it is not too much of a burden for the malware to wait until this occurs. Some analysis systems monitor autostart hooks, like the registry run key or the startup folder. If a sample registers itself so that it will execute if the client virtual machine restarts, the analysis system will notice. In order to speed things up, the automated system can execute the registered payload straight away and continue its analysis. Unfortunately, this opens the virtual machine up to attack, as the malware can use other means to verify whether the virtual machine has really restarted or not.

The same applies to sleeping loops and delays. Whereas a simple two-hour sleeping loop might have worked for older analysis systems, newer implementations will simply speed up the analysis system in order to skip over such loops. This is basically the old problem of detecting garbage loops and ignoring them. But attackers have come up with techniques to hide the malicious activity from the automated scanner.

Some of the delays are outside the control of the virtual analysis system itself. For example, a downloader threat can deliberately have a slow responding C&C script, that uses a small TCP window size of five bytes. This stalls the download of the configuration file so that it takes ten minutes to complete. This length of time cannot be reduced by the virtual machine and as a result, it might generate a timeout issue on the automated analysis. Essentially, this will lead the automated analysis system to misclassify the threat as a non-malicious file.

User interaction

Another evasion method that we have seen used in the wild is the monitoring of user interaction. For example, any normal client virtual machine would commonly experience mouse movements and mouse clicks. A malicious sample can, for example, wait for three left mouse clicks to occur before any payload is decrypted and executed. Of course, such a threat would not work on a normal server which has no user logged on, so attackers will only be able to attack an end user system.

Any kind of user interaction can work in the attacker's favor. Even a dialog box with a CAPTCHA could be deployed before the payload is executed.

Such checks are harder to patch on virtual machines and require some background monitoring to generate the necessary interaction triggers.

Hide from hooks

In order to detect any malicious modification of the virtual machine, most analysis systems install their own tools and create some system hooks. Clever malware can try to bypass these hooks by executing its own low-level function calls or unregistering itself from certain calls. For example, it could unregister from the CreateProcess notification in order to create a new process that is not monitored by the analysis system. The malware may also fool snapshot-based tools by executing code straight from memory without writing any files to disk.

Environmental checks

Since analysis systems are custom built and modified, they may contain additional artefacts which can give the malware a clue as to whether the system is a client virtual machine or an analysis tool. For example, if the analysis tool is using predefined file names for the suspicious files that get analyzed, then the malware can simply look at the file names and determine whether it is running in a VM or not.

Symantec™

BEST PRACTICE

Best practice

Virtual environments need security solutions that go beyond traditional protections in order to cover the different requirements of its dynamic and application-centric approach. This holds true for standalone virtualized servers as well as for modern SDDCs. Of course, different setups and architectures might require different implementation approaches. In any case, virtual machines need to be integrated into the security strategy of the IT.

Here are some best practice guidelines that should be considered when securing virtual environments.

- **Hardening:** The host server needs to be well protected as it provides access to multiple virtual machines. Besides updating and patching, the server can be protected against attacks with the help of lockdown solutions and host IDS. Administrators can adjust policies and whitelisting to only allow trusted system applications to run.
- **Advanced malware protection:** The host server, as well as any virtual machine running on it, needs to be protected against malware. To achieve this, advanced malware protection with proactive components that go beyond classical static antivirus scanner, needs to be in place. Depending on the setup, threat protection can be deployed on each virtual machine separately or agentless from the hosting server in order to maintain a high level of performance.
- **Access control:** Administrators need to apply proper access control management to virtual machine hosting servers in order to ensure that only eligible users can perform changes. These are crucial servers that should use strong login processes, like two-factor authentication. These processes should include a proper logging of successful and failed logins for accountability.
- **Disaster recovery:** Virtual machines need to be integrated into the disaster recovery and business continuity plan. Administrators should apply high availability and backup strategies for the data.
- Virtual network protection: Administrators should ensure that network security tools like IPS/IDS have access to traffic in the virtual network between multiple virtual machines on the same host server. Most vendors provide access to hooks that can be used.
- **Updating:** Snapshots and images of virtual machines need to be included in the patch and upgrade cycle, so that they are up-to-date when deployed.
- **Logging:** Virtual machines need to be integrated into the security logging and SIEM visualization systems just like any other IT device. Since virtual machines can dynamically be provisioned and moved around the network, these activities need to be consistently logged as well.

Some security solutions combine multiple protection features, such as Symantec's Data Center Security (DCS) for virtual environments, which provides hypervisor-based security controls. This includes agentless or light agent protection for guest virtual machines, hardening of the host server and protection against exploits.

Conclusion

Most companies have already implemented virtualization or have it on their roadmap for the future. The use of virtualized systems in a corporate environment can provide a lot of benefits, but these systems need some special attention paid to security. This is why virtualization needs to be included in the security strategy and strong security measures need to be adapted for these resources. Along with applying traditional security practices, administrators need to pay particular attention to virtual connections between guest virtual machines themselves. These connections might be invisible to traditional network security devices as they are not aware of them.

Virtual machine host servers should particularly be hardened and protected. If an attacker manages to gain control of these servers, they will have access to all the hosted virtual machines. This also applies to insider threats who might leverage their privileged access rights.

In the past, we have observed attackers targeting virtual machine host servers as well as malware specifically designed to compromise virtual machines. Attackers are able to infect guest virtual machines starting from the host server. There are also vulnerabilities that can allow malware to escape from the virtual machine and compromise the host server.

Newer malware frequently use detection techniques to determine if the threat is run in a virtualized environment. We have discovered that around 18 percent of all the malware samples detect VMware and will stop executing on it. The converse argument shows that four out of five malware samples will run on virtual machines, meaning that these systems need regular protection from malware as well.

With the move of virtual systems to the field of automated analysis and the detection of unknown malware, we noticed that attackers have created new checks to evade such analysis. For example, some Trojans will wait for multiple mouse left clicks before they decrypt themselves and run the payload. This can make it difficult or even impossible for an automated analysis system to come to an accurate conclusion in a short timeframe, leaving a window open for attackers. The groups behind targeted attacks are well aware of this and create sophisticated threats that will evade automated detection systems.

References

Strategic Benchmarks 2014: Server Virtualization, Forrester Research, Inc., March 2014.

http://eval.symantec.com/mktginfo/downloads/21187913_GA_WP_SecuringtheCloudfortheEnterprise_05%2011.pdf

http://www.symantec.com/security_response/writeup.jsp?docid=2012-081606-2200-99

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/crisis_the_advanced_malware.pdf

http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf

http://www.invisiblethingslab.com/resources/2011/Software%20Attacks%20on%20Intel%20VT-d.pdf

http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

http://www.symantec.com/connect/blogs/malware-authors-using-new-techniques-evade-automated-threat-analysis-systems

Author
Candid Wueest

About Symantec

Symantec Corporation is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings - anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

July 16th 2014, v. 2.01