Bromium®

The evolution of virtual endpoint security

Comparing vSentry® with traditional endpoint virtualization security solutions

Bromium®

Executive Summary

First generation endpoint virtualization based security solutions have struggled to have an impact on the current generation of attacks and exploits. Current products have focused on running the web browser in a separate (guest) virtual machine that is isolated from the main desktop (host) system by traditional "hypervisor" software. This monolithic approach to isolation has fundamental flaws.

Current application software is designed to increase productivity and decrease resource consumption by allowing users to perform multiple instances of a programs function using a single instance of the application such as "tabbed" web browsing. These multiple instances or "tasks" make security more difficult as compromising the parent application automatically compromises all the tasks being performed by the application.

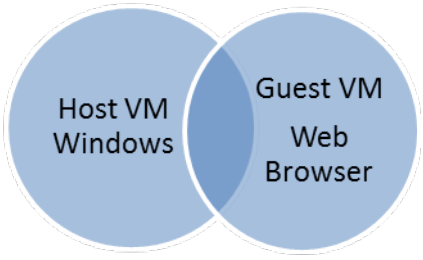
Running a full browser within a single virtual machine does not protect against new types of attacks like "man-in-the browser" that uses one browser session to compromise a second browser session running in the same virtual machine. Running potentially malicious documents or e-mail attachments in the same monolithic virtual machine presents the same problem; malware introduced in one document can compromise the entire VM and all the other documents or browser sessions within the virtual machine.

Some solutions have added a variety of malware detection mechanisms to the guest environment in an attempt to detect attacks and abort the web browser sessions, but as with all detection based systems, new or unknown attacks have a high probability of compromising the guest machine which can then serve as a host to launch other attacks against other browser sessions or applications in the guest machine.

vSentry provides a completely new level of granular isolation by automatically and instantly creating a micro VM for each task, such as opening a new browser tab, an email attachment or a PDF document. Each web domain, attachment or downloaded document is fully isolated in a separate, hardened and hardware enforced light weight microVM that has no access to any information on the host system, the network the host system is located within or any other microVM running on the system. This extreme level of granularity ensures that information and resources remain protected from theft or disruption even in the event of a successful attack against the web browser or document viewer running an individual microVM.

First generation endpoint virtualization and security

Traditional Endpoint Virtualization Systems provide a mechanism for running multiple operating systems on a single desktop or laptop computer. Migrating computing resources to a virtualized environment has little or no effect on most of the resources' vulnerabilities and threats according to NIST, the National Institute Standards and Technology. These solutions deliver no protection beyond that provided by standard desktops and incur a heavy performance penalty as they do not leverage the advanced hardware virtualization features available on today's latest processors.



At first glance, using a hypervisor platform designed to host multiple operating systems as a mechanism to isolate specific

application programs like the web browser or Adobe reader would appear to provide increased protection. The presumption is that malware inadvertently installed in the "guest" virtual machine would be separated from the information contained within the "host" Windows system and would be erased each time the user restarted their web browser, word processor, Acrobat reader etc.. In reality there are some fundamental problems to this approach that we will explore in this section.

- This model relies on users regularly closing and re-opening their browser to ensure that malware does not persist within the system. In reality most users keep their web browser open throughout the course of their entire workday, and often will not close the browser for many days at a time. The tendency for organizations to make their internal corporate intranet site the default home page for users has encouraged this behavior.
- Multiple sessions (tabbed browsing) in the web browser in the guest VM are susceptible to exploits between the different sessions. The most common example of this problem is the recent outbreak of "man-in-the-browser attacks which are not defeated by simply isolating the entire browser. In this scenario one compromised session can be used to insert a Trojan into the guest VM which monitors information entered into the 2nd session and inserts attacker generated responses to the end user.
- Adobe PDF attachments have been one of the most popular threat vectors over the last few years based on its wide spread adoption across all platforms. A successful attack via a malicious PDF, Word document, spreadsheet etc. distributed as an e-mail attachment or as a web download can compromise the guest VM exposing other documents or web browser sessions running within the isolated VM.

First generation virtual endpoint security systems attempt to counter the weaknesses listed above by including malware detection capabilities within the guest VM hosting the browser. When malicious activity is detected the guest VM is shut down and deleted and a new instance of the guest virtual machine and web browser is launched.

- The primary problem with this approach is that an attacker only has to evade the detection mechanism once to compromise the guest image and gain a foothold within the system. The sophisticated attacks that cause the most concern today, Advanced Persistent Threats and other forms of advanced targeted malware often exploit unknown vulnerabilities within an ever increasing number of browser helper apps and plugins to compromise the system.
- Even purely behavioral detection systems rely on a profile or signature of "good" and "bad" behavior to detect unknown attacks. "Good" and "Bad" behaviors are generalized representations of potentially millions of different software processes and interactions and as such are notoriously prone to "false positives" which incorrectly identify benign behavior as malicious and conversely to "false negatives" where truly malicious behavior is identified as benign.
- Behavioral detections systems must attempt to detect malicious behavior as early in the attack cycle as possible to ensure that attacks do not complete successfully and disable the detection

system. This approach can lead to false positives which can result in a loss of confidence in the system, or to less aggressive detection tuning which can miss legitimate attacks.

- Most current implementations of virtual desktop security products are based on open source or "free" hypervisors. These systems are generally designed as general purpose platforms to address the problem of running incompatible software applications rather than as a security platform. As a general purpose platform these types of systems have not been optimized to present the smallest possible attack surface and generally lack the support resources need to identify and fix vulnerabilities in a timely fashion.

In today's increasingly sophisticated threat environment the only safe assumption to make is that ALL applications will eventually be compromised by an attacker without detection beforehand. Clearly a different approach to deploying vulnerable applications on a monolithic, general purpose hypervisor that relies on traditional detection technology is needed to combat the increasing sophistication of threats today.

Micro Virtualization: A New Approach to Secure Endpoint Computing

vSentry offers a completely new approach to endpoint security that relies on extremely granular, secure isolation of risky tasks performed by the user rather than detection and blocking of threats. Bromium has developed a revolutionary new technology, micro-Virtualization, that addresses the fundamental shortcomings of the monolithic hypervisor virtualization model by executing each vulnerable task in a tiny, hardware-isolated micro-VM. This next generation virtualization technology harnesses the power of the industry's latest microprocessors to address the fundamental architectural flaws inherent in today's computing systems. Bromium optimized design drastically reduces the typical operating system attack surface. In addition, protected tasks have only "need to know" access to data, networks and hardware devices, so if a task is compromised, the system still protects the enterprise and the user. Finally, micro-VMs can be instantly created and destroyed, automatically discarding malware and ensuring that the desktop always remains in a "golden" state. These capabilities are implemented automatically, in milliseconds, unseen by the user, and with no impact on the user experience

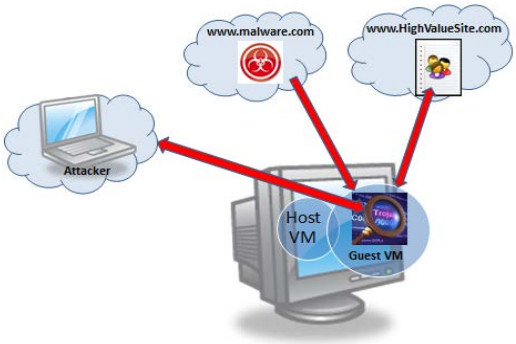
A practical Demonstration of first generation virtual endpoint security systems shortcomings

The following section is designed to highlight the pitfalls of using traditional virtualization technology to provide a secure browser environment.

The goal: Steal sensitive account name and password from a virtualized web browser

The plan: The attack plan consisted of the following steps:

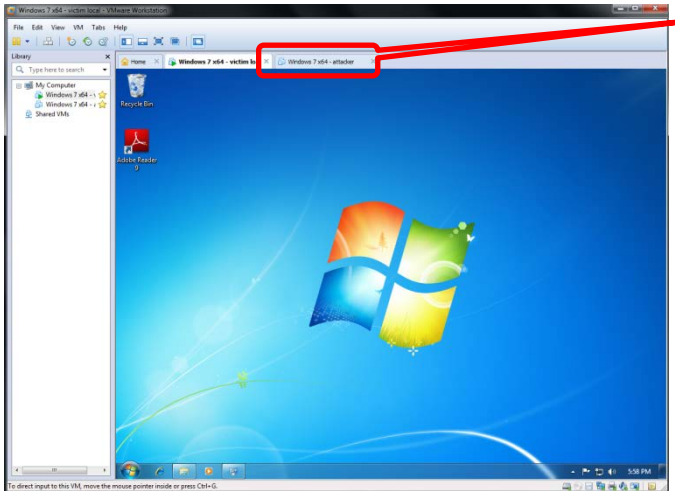
1. Target a user with an e-mail containing a malicious link
2. Exploit the web browser using a Java exploit contained within the malicious site
3. Download a Trojan to the victim
4. Monitor other browser sessions to access to the high value web site
5. Steal account info and password being transmitted to the web site being accessed by a second tab in the browser



Components: The components required to execute the attack

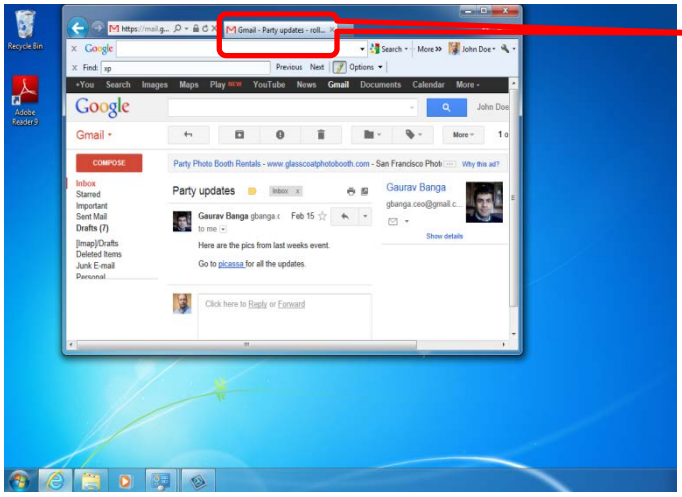
1. Metasploit open source console for generating and controlling the required exploit code.
2. A reliable browser exploit, in this case one targeting a vulnerability in the Java Rhino interpreter used by virtually all popular web browsers
3. DarkComet Remote Access Tool, a popular shareware Trojan horse application
4. Victim Machine, Windows 7 host with Windows7 Guest virtual machine running under VMware Workstation
5. A victim e-mail account
6. A web server hosting the attack
7. An attacker machine hosting the Metasploit Framework console and the Dark Comet Trojan command and control software

The following section details the step by step process of launching and completing this attack plan.



The Defense: A Windows 7 system is installed within an isolated virtual machine using VMware Workstation (guest machine). Internet Explorer and it's typical add-ons like Adobe Reader, Adobe Flash etc. were installed within the virtual machine. No other applications were installed within the VM as is commonly the case when configuring a traditional desktop virtualization system for isolation.

The browser is launched in a separate virtual system



The Lure:

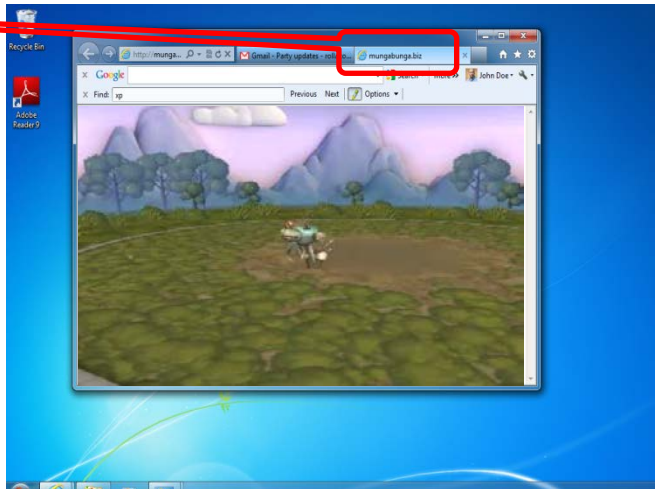
An e-mail is created and sent to the target victim containing a link to our malicious web site. The e-mail is crafted using information gathered using standard surveillance techniques to ensure that the mail will be read and that the embedded link will be activated by the target victim.

For maximum effectiveness the malicious code of the attack can be embedded in an existing web site that we have compromised in advance. This approach defeats most web

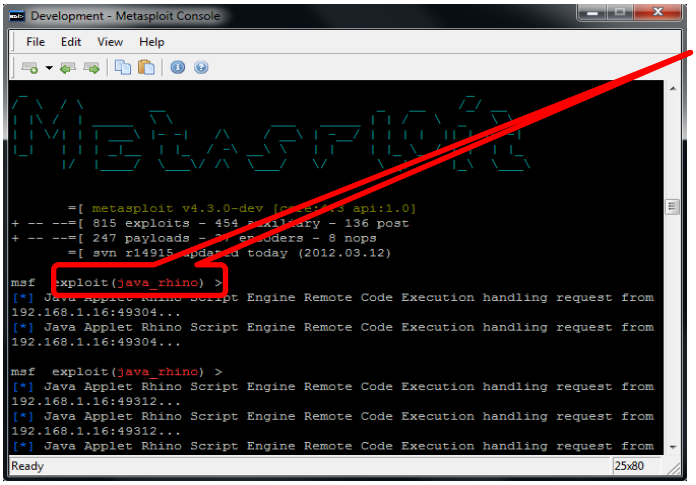
The victim receives an e-mail with an embedded link

gateway filtering systems that rely on the reputation of the linked site for detection of potential malicious activity.

The Attack:
The victim clicks on the embedded link and the browser is redirected to the site hosting the attack code. In this case the attack consists of Java code that is automatically executed in the target web browser which exploits a wide spread vulnerability in the Java Rhino scripting engine. This attack does not require the user to click on any additional links or download any files.



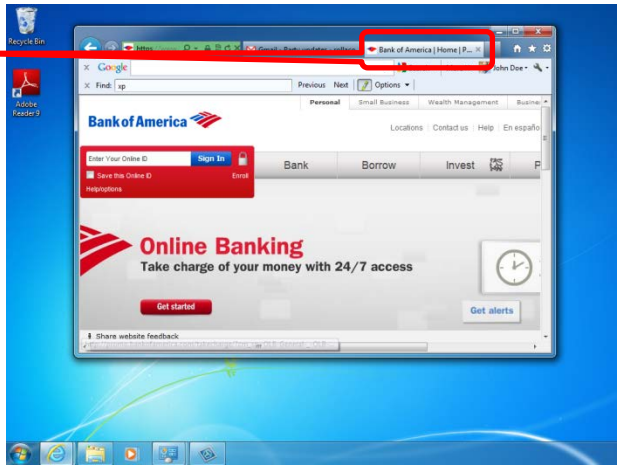
The victim is redirected to the malicious web page



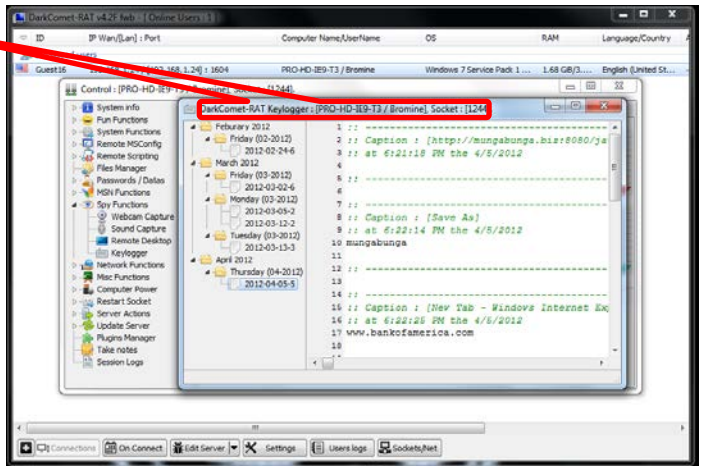
The attack executes and installs a Trojan program

Installing the Trojan:
The successful Java Rhino attack allows the attacker to run remote commands on the system at will. The Trojan remote control program is transferred to the victim and is started. This activity is transparent to the end user and the Trojan remains active in the guest system until the entire virtual machine is shut down, hours or days later and the guest virtual system is re-launched.

Multi Tab Browsing in the "Protected" Browser
During the course of the work day the user opens a second tab in the browser and navigates to a high value site like Salesforce.com, the internal corporate web site or in this case a bank to accomplish another task.



Successfully Completing the Attack
Once the second browser tab has been opened to the high value site, the targeted information is successfully captured via the key logger function of the Trojan application installed earlier and transferred to the attacker.



Conclusion

The concept of virtual isolation is valid but first generation virtualization technologies do not provide the isolation granularity needed to successfully protect against current attacks. Trying to compensate for the monolithic nature of legacy virtualization technology by adapting current malware detection mechanisms of is clearly doomed to failure as evidenced by the large number of attacks that evade and succeed against all current security solutions based on detection.

To fulfill the promise of isolation as the ultimate form of defense requires the ability to virtualize and granularly isolate individual tasks rather than applications or operating systems. Bromium vSentry delivers on this vision through the use of uVirtualization which fuses the next generation of virtualization, security and hardware technology to solve the most critical problems facing organizations today and in the future.