

Live Attack Visualization and Analysis

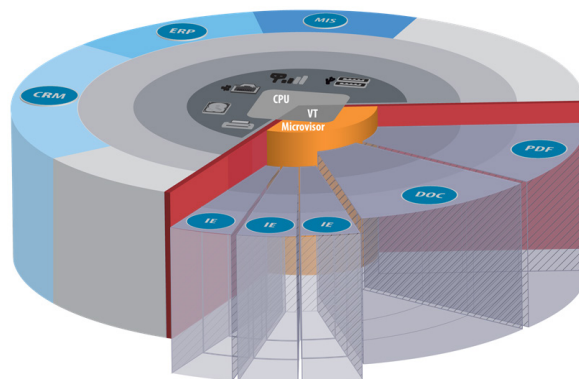
What does a Malware attack look like?



Introduction

Bromium is a virtualization pioneer whose micro-virtualization technology delivers dependable, secure and manageable computing infrastructure. Bromium vSentry™ makes every endpoint secure by design, defeating malware and protecting enterprise data and applications at all times with minimal impact on the user experience.

Bromium micro-virtualization extends the isolation, control and security principles of hypervisor-based virtualization into the OS and its applications. It does this by using hardware enhanced virtualization to dynamically virtualize and isolate vulnerable user activities. It provides a powerful, hardware-guaranteed backstop for the existing software isolation used in the OS, protecting sensitive applications and data, and allowing users to safely access untrusted networks, documents and removable media.



Micro-virtualization provides the ideal platform for observing, detecting and analyzing both known and unknown forms of malware with minimal false positives and no need for re-occurring updates.

Bromium's Live Attack Visualization and Analysis system, or LAVA delivers a unique view of malware to the security analyst that enables them to determine both the strategy and the tactics used by the attacker within minutes rather than the hours or days typically required for advanced forensic analysis.

LAVA provides comprehensive visibility into all attacks targeted at the most vulnerable applications used by modern endpoints including the web browser and associated plugins, Adobe Acrobat Reader and its plugins as well as the Microsoft Office suite and Outlook mail client.

Leveraging the unique characteristics of the Bromium Microvisor and an advanced behavioral analysis system developed for LAVA provides unmatched visibility into the most difficult types of modern malware including;

- › Advanced rootkits and bootkits that avoid all other forms of detection
- › Drive by downloads targeted at JAVA, Internet Explorer, Windows or Adobe
- › "Man in the browser" attacks used to attack high value cloud based corporate data
- › Trojans, backdoors and other forms of remote control tools and techniques
- › Keyloggers, password stealers and other forms of stealthy monitoring techniques

Bromium Live Attack Visualization and Analysis Benefits

The task isolation architecture inherent to vSentry provides protection against compromise without the need to specifically identify or block execution of malicious code. However the ability to identify and analyze unknown forms of malware delivers significant benefits to organizations beyond the protection of the targeted system.

- › **Strategic intelligence:** The ability to thoroughly analyze the specific behavior of each unique piece of malware provides insights into the strategic intent of the attacker. Knowing that an attacker's goal is stealing specific types of intellectual property versus attempting to install a keylogger to capture generic passwords enables the security team to inform both the targets of the attack and other members of the organization that an attack is underway.

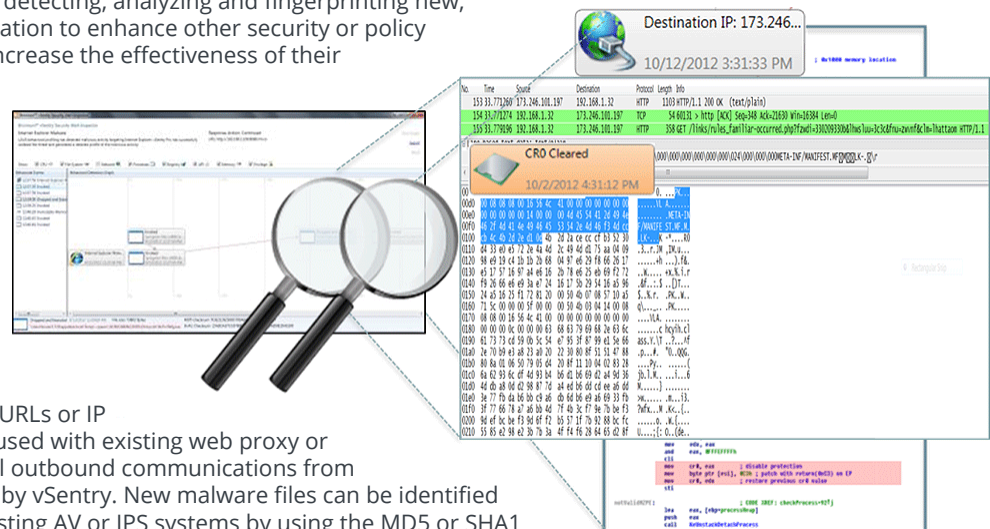
Attackers will often attempt different forms of attack to achieve their goal if their initial efforts are unsuccessful. Knowing an attack has been attempted and what an attacker is after enables organizations to have heightened awareness of a specific threat and to be on their guard for future social networking or other types of attacks.

- › **Zero Day Attack Analysis:** Accurately detecting, analyzing and fingerprinting new, unknown attacks enables the organization to enhance other security or policy enforcement mechanisms in use to increase the effectiveness of their "defense in depth" strategy.

LAVA gathers intelligence directly at the point of attack, the endpoint and is effective even when the system is mobile and outside the corporate perimeter. This ensures that every alert is a valid attack against a truly vulnerable system rather than a generic piece of malware hoping to find the right target but representing no real threat to the organization.

New malware command and control URLs or IP addresses identified by LAVA can be used with existing web proxy or security gateway solutions to block all outbound communications from hosts systems that are not protected by vSentry. New malware files can be identified and fingerprinted for scanning by existing AV or IPS systems by using the MD5 or SHA1 hashes created by LAVA.

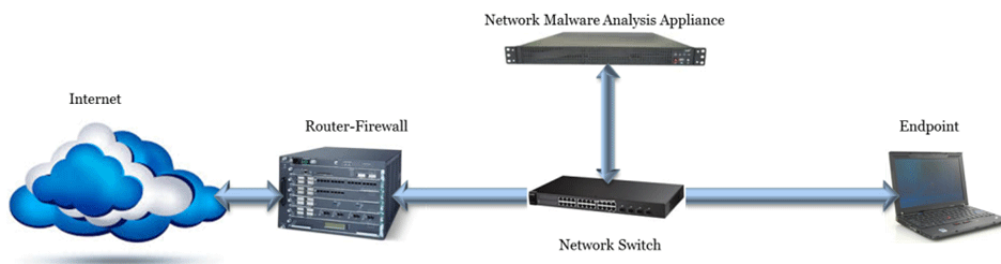
- › **Advanced Visualization:** LAVA delivers a whole new way of seeing and analyzing attacks. Every step taken by the malicious code is automatically and visually linked to show a complete "kill-chain" of the attack. This new way of looking at attacks enables security personnel to completely reconstruct and validate even the most complex attacks in just minutes rather than the hours or days traditionally required to untangle the complex web of interactions that make up a modern attack.



Current Malware Detection & Analysis Techniques

The information security industry has been moving towards network or cloud based systems that use “honey pots” or dedicated appliances for detection and analysis of attacks.

Isolated “off line” analysis systems are used to safely run and analyze samples of traffic that might contain malware that is requested by users. The potentially malicious software is still delivered to the requesting endpoint while the analysis service or appliance runs the unknown code in an “application sandbox” or a traditional virtual instance of a “typical” endpoint.



Off line systems have a number of challenges to overcome to detect and analyze a high percentage of attacks without producing an unacceptably high number of extraneous alerts.

- › Different combinations of software require different forms of malware for a successful attack. An attack targeted at Internet Explorer v8 and JAVA v6 does not pose a significant threat to a system using Internet Explorer v9 and Java v7.
- › Off line detectors need to closely emulate only those software combinations that exist within the network they are protecting. Attacks detected that are targeted at endpoint configurations that don't exist on the protected network must still be evaluated and can generate very significant workloads for the security staff without benefit to the organization.
- › Endpoint systems that do not share the same configurations as the off line detectors deployed can be compromised by attacks that the detectors are unable to identify eliminating the value of the detectors.
- › Off line detectors must be upgraded every time the endpoint systems they protect are upgraded to maintain their effectiveness. Endpoint software is upgraded and patched on a continuing basis. The requirement to constantly upgrade a large number of detector images at the same time adds a considerable burden to the security operations group.

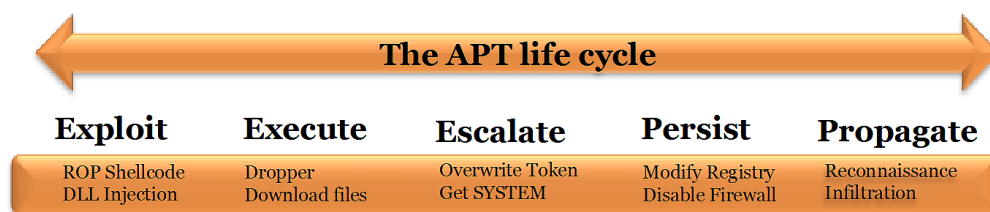
Only by allowing a sample to fully execute and observing its behavior on the targeted endpoint itself can an accurate assessment be made as to the safety of a document, e-mail attachment or web site content etc. without generating a high number of extraneous alerts.

Off line analysis systems, whether they are located in a security vendor's malware lab, in an appliance on the target network or in a cloud based system are inherently reactive systems. Detection only takes place after a target endpoint system has been exposed to unknown, potentially malicious software. The security staff must react to every alert by manually analyzing the targeted system and remediating the system if the attack was successful.

The advantages of microvirtualized detection and analysis

Micro-virtualization as implemented by Bromium delivers truly unique and powerful capabilities, not least of which is the ability to provide a secure, hardware isolated container located directly at the point of attack with just a single task running within it. This provides the perfect laboratory to identify and analyze an attacker's effort to penetrate a system. Following is a description of the key features that micro-virtualization enables;

- › **Multi-phase attack detection:** The inherent protection against system compromise offered by vSentry enables LAVA to observe the entire life cycle of the task, and any malware that has been introduced to it within the micro-VM without risk.



As the malware runs through its entire attack sequence a series of behavioral analytic engines located both within the microvirtual container as well as in the Bromium Microvisor which is located outside of the container observe and record the behavior. A full event or "kill-chain" is built documenting the complete behavior exhibited by the malicious code as it interacts with the system user and the software image contained within the container.

Observing the full malware execution cycle is the first step in eliminating false positive alerts. The user is able to safely interact with the task (and the malware) within the container by typing in keystrokes, moving the mouse etc. This is an important factor in detecting advanced attacks as many new forms of malware monitor the system they are running in to ensure that an actual human is controlling the system and that they are not executing in an automated "honeypot" or offline detector located in a separate analysis appliance or in the cloud. Only when the malware has confirmed that it is running in a "real" system will it trigger its payload and begin the attack which can then be analyzed and reported to the security team.

LAVA provides granular correlation of individual computing events across multiple phases of the task to ensure that the behavior is malicious before alerting and logging the data. This enables security personnel to focus on real incidents rather than false alarms and increases their effectiveness and efficiency.

- › **Isolated task execution:** Bromium vSentry isolates each user task in a dedicated micro-virtual container. A user task is a single instance of an application which is initiated by the user of the system. For instance when a user opens a new tab in their web browser vSentry creates an entire microvirtual container running a completely separate instance of the web browser than that used by the web site displayed in the first tab.

This granular isolation eliminates much of the "noise" that is encountered when using behavioral detection techniques within a standard endpoint system. The average Windows desktop system can have dozens of applications and hundreds of different processes running concurrently. This makes it difficult to attribute a specific operating system level event with a specific application program.

For instance a behavioral monitoring analysis routine might see that the system registry received a request from a process to create a new entry. While this is a legitimate operation for many applications, it would clearly be an indicator of malicious activity if it originated from a different application.

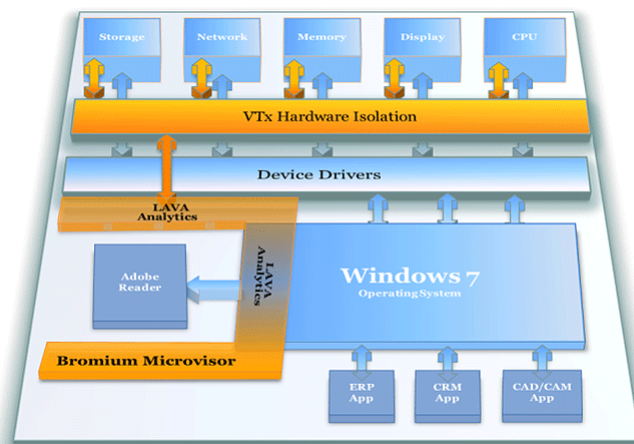
With only a single application running in each micro-VM, every event can be directly attributed to the specific iteration of the application. Taking the example above, seeing a registry modification request in a micro-VM containing only Adobe Acrobat Reader would be a very strong sign of compromise as PDF files would not normally attempt to modify a systems registry entries.

The vantage point of the Microvisor, and LAVA – outside the micro-VM, allows it to associate every resource accessed by the micro-VM against a behavioral template for the task. This includes a specification at the task level, of the network traffic that a micro-VM may legitimately send and receive: For example a micro-VM protecting access to a trusted SaaS application should be forbidden from sending data to untrusted sites on the public web. Similarly, untrusted micro-VMs cannot resolve DNS queries for any enterprise sites, or send traffic into the enterprise Intranet. No untrusted document should ever communicate over the Internet, and only documents that have been created securely and kept on the Intranet should ever be able to communicate over the network, and then only with specific sites or stores.

Being able to attribute low level events directly to a single instance of a specific application enables LAVA to virtually eliminate false positives or generate alerts on extraneous attacks that pose no direct threat to the system. This level of accuracy is a key element in enabling an analyst and the security organization in general on focusing on significant events rather than “back ground” noise.

Virtual Introspection

The Bromium Microvisor is a highly specialized hypervisor which has a unique perspective on the software executing within its virtual task environment. The Microvisor runs outside of the task environment which it controls and owns all virtual memory and manages virtual page tables, controls network and storage I/O as well as CPU allocation to the code executing within its environment. The industry term used for a hypervisor's ability to inspect the state of code executing within its execution environment is “VM introspection”, and substantial academic and industry literature exists on its use for detection in traditional legacy full-OS virtualized environments.



Advanced rootkits and bootkits operate in a somewhat similar fashion to hypervisors and attempt to insert themselves as an invisible layer between the operating system and the underlying hardware. From this vantage point the rootkit controls the entire operating environment and is able to hide itself from security software executing under the normal operating system. By its inclusion within the Microvisor, LAVA is able to detect a rootkit's attempt to install itself and is able to ensure that malware is not able to disable or evade the LAVA analytics engines.

Enterprise-Wide Insight

As detailed earlier in this paper, traditional behavioral analysis systems are not deployed widely within an organization due to the resource and performance impact of traditional hypervisors on endpoint systems as well as the other factors outlined above. Network based analysis systems typically capture and sample a very small subset of the overall network traffic due to both performance challenges as well as the ever increasing amount of encrypted traffic encountered in modern networks. These restrictions make it difficult to gather a truly comprehensive view of the attacks targeted at the organization.

The Bromium Microvisor with its ability to run on industry standard desktop systems enables the organization to achieve a truly enterprise wide view of attack activity in real time.

LAVA provides the capability of correlating detailed information across the enterprise, and to export these insights into systems such as Security Incident Event Managers (SIEMs) from major vendors, or IT management systems such as Splunk or traditional event managers.

LAVA Analytics

LAVA monitors, correlates and displays a large range of behaviors that may be exhibited by malware isolated within the micro-VM. Each of the different aspects can be visualized individually or can be “layered” to achieve a full view of the entire malware chain in the LAVA trace.

Following is a list of the individual LAVA event categories that are monitored for malicious behavior. The goal is to monitor and correlate the following behaviors and compare them against a behavioral template specific to each type of micro-VM to identify malware.

CPU: These events are typically generated by advanced rootkits and bootkits that attempt to manipulate CPU hardware registers directly. LAVA monitors this type of activity using the introspection capabilities only available to a hypervisor based environment.

File System: FS events track modifications to files within the micro-VM. Malware often modifies .ini files, .bat files and other file types to allow the malware to persist on the system or to facilitate execution of the complete attack.

Network: Network events such as DNS lookups or remote connections are identified and tracked. Both TCP and UDP protocols are monitored for outbound communications with remote command and control servers or malicious downloaders.

Processes: All events incorporating various types of system process manipulation are displayed and parent/child relationships are tracked and indicated in the LAVA trace. New DLL files that are dropped on the system and executed by the malware are identified and fingerprinted as well as attempts to inject code into common system process to ensure the malware persists on the system.

Registry: Registry manipulation events are often associated with setting up a covert communication channel, disabling existing protections such as the Windows Firewall or anti-virus systems and allowing the malware to persist after the system is re-booted. Each registry manipulation is documented and linked to the originating process.

API: The Windows API is a programmer's interface which is used to access the Windows system resources, files, processes, network, registry and all other major parts of Windows. User applications use the API instead of making direct system calls and thus this offers great visibility for behavioral analysis of malware executing in the user space. LAVA transparently hooks the API functions to ensure malware is not aware it is being monitored.

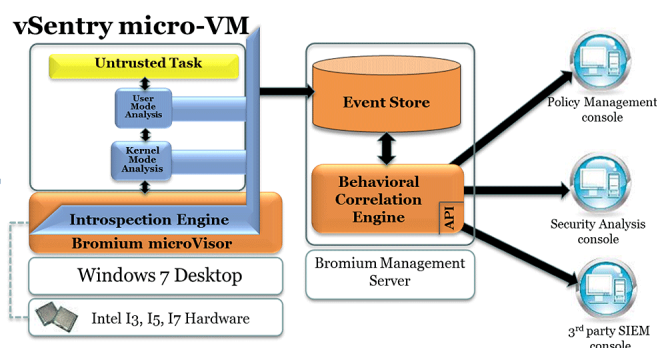
Memory: One of the key advantages to analysis of malware in a "live" system is the ability to monitor the dynamic memory of the system. Malware authors often avoid using techniques that leave a record of their efforts for future analysis by traditional forensic tools and execute their attacks in volatile memory, or attack the sensitive memory constructs directly. This analytic monitors any attempt access or change the kernel memory within the micro-VM which can be used by advanced kernel mode exploits targeted at systems using application sandboxing for protection.

Privilege: Security tokens are a mechanism used by Windows to determine the security privileges of a user to grant or deny access to resources within the system. Attackers often attempt to access and modify these security tokens to escalate their privileges and gain higher levels of access to system resources. LAVA monitors and displays the activities as they are a strong indicator of malicious behavior.

How it works

When a user initiates a task that interacts with unknown or untrusted data, such as launching a new web browsing tab, a new micro-VM is created by the Bromium Microvisor to host the task.

LAVA analytics monitor and record all aspects of the behavior of the operating environment during the lifetime of the micro-VM. Once the task is completed and the micro-VM is destroyed, LAVA's correlation and analytic engines compare the behavior observed within the micro-VM against a data base of legitimate or typical behaviors generated in the specific type of micro-VM being analyzed.



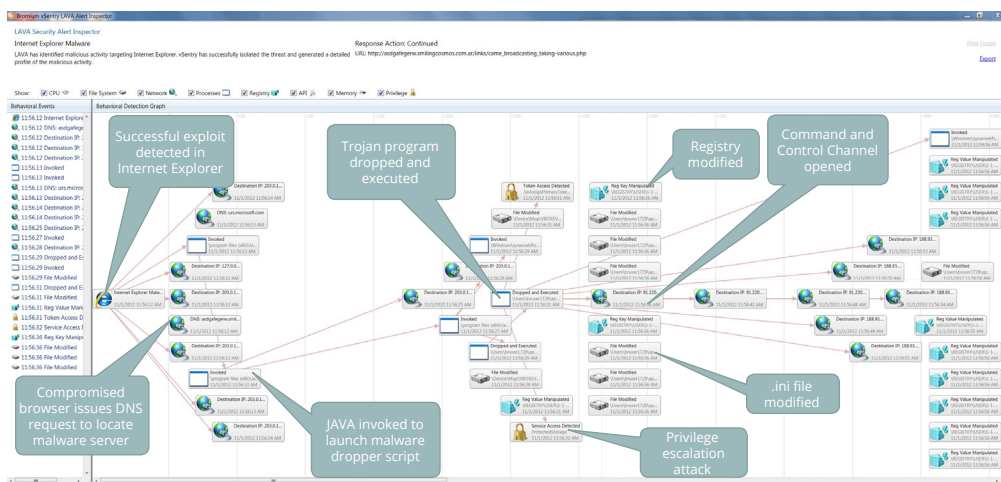
Each variation recorded from the behavioral template is weighted and fed to the correlation engine which uses advanced heuristic algorithms to determine if malicious behavior has occurred. If a verdict of malicious activity is reached, a summary file of the events occurring in the micro-VM is created for display by the LAVA visualization engine and an alert is generated. Both the detailed behavioral information and the visualization summary files are retained locally or forwarded to the Bromium Management Server based on the policy set by the administrator.

If no malicious activity is observed the LAVA behavior data base is either deleted, or retained and forwarded to the Bromium Management Server for historical reference as determined by the policy implemented by the system administrator.

This two stage recording system conserves both local and network resources by ensuring that only valid alerts and the associated activity records needed for detailed analysis are retained.

LAVA Visualization

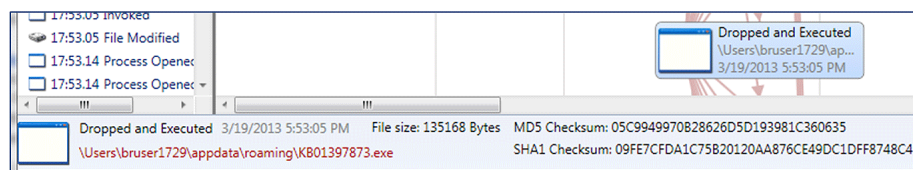
The LAVA visualization graph is designed to provide an “at a glance” view of the entire malware execution cycle and determine the specific links in the “kill-chain” that can be used to counter the attack when using other security enforcement devices like web gateways and signature scanning engines line network IPS appliances or endpoint AV engines.



LAVA trace with explanatory call out boxes added

The LAVA graph displays the sequence of the individual events on a timeline from left to right. The relationships of the individual elements to each other are indicated by lines connecting the child and parent processes, or the process or application that initiated an action on a different element.

The different categories of events are indicated by different icons within each event box. The trace is interactive and the analyst can select which specific event types to display by checking the appropriate box at the top of the chart.

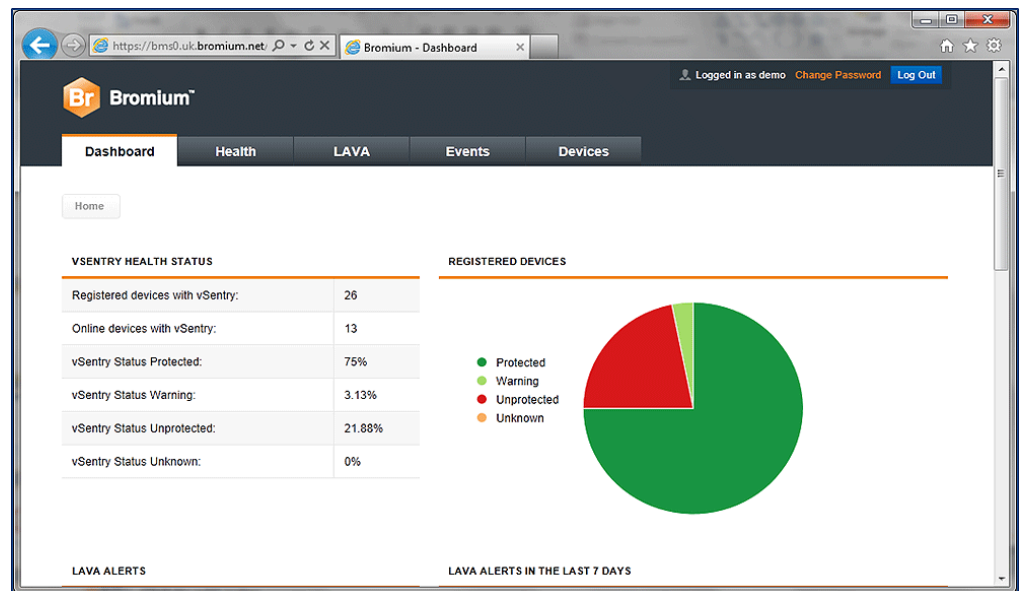


Clicking on specific event boxes brings up details at the bottom of the trace

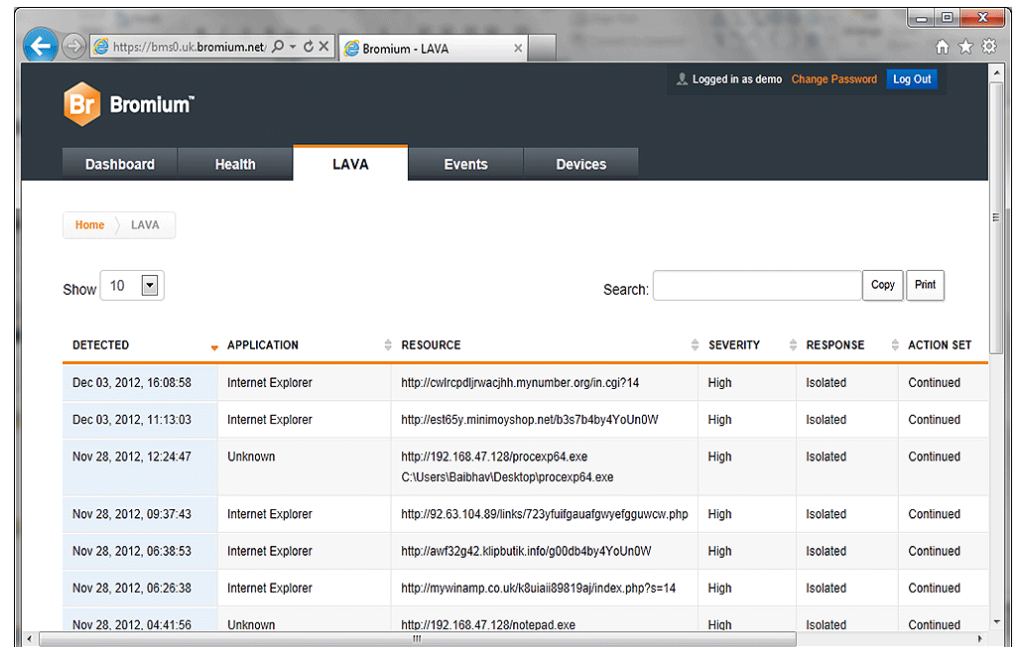
Details provided such as a file fingerprint (MD5 hash) the external IP address or URL of a command and control server etc. can be exported or simply cut and pasted by the analyst to augment existing defenses elsewhere in the organization.

Bromium Management Server

The Bromium Management Server (BMS) provides enterprise wide visibility for the security analysis team by providing a centralized repository for all LAVA alerts and traces. BMS provides a web interface allowing analysts to select and view traces from any LAVA enabled endpoint.



BMS provides multi-role access capabilities for management of vSentry and LAVA enabled endpoints and for centralized alerting and attack analysis.



LAVA

Home > LAVA

Show 10

Search: Copy Print

DETECTED	APPLICATION	RESOURCE	SEVERITY	RESPONSE	ACTION SET
Dec 03, 2012, 16:08:58	Internet Explorer	http://cvtcpdjrvcjhh.mynumber.org/in.cgi?14	High	Isolated	Continued
Dec 03, 2012, 11:13:03	Internet Explorer	http://est65y.minimoishop.net/b3s7b4by4YoUn0W	High	Isolated	Continued
Nov 28, 2012, 12:24:47	Unknown	http://192.168.47.128/procexp64.exe C:\Users\Baibhav\Desktop\procexp64.exe	High	Isolated	Continued
Nov 28, 2012, 09:37:43	Internet Explorer	http://92.63.104.89/links/723yfulgauafgyefgguwcv.php	High	Isolated	Continued
Nov 28, 2012, 06:38:53	Internet Explorer	http://awf32g42.klipbutik.info/g00db4by4YoUn0W	High	Isolated	Continued
Nov 28, 2012, 06:26:38	Internet Explorer	http://mywinamp.co.uk/k8uiaii89819aj/index.php?s=14	High	Isolated	Continued
Nov 28, 2012, 04:41:56	Unknown	http://192.168.47.128/notepad.exe	High	Isolated	Continued

Conclusion

Malware continues to evolve at a rapid pace as evidenced by new variations that are designed to evade automated analysis systems. At the same time the emergence of highly damaging attacks targeted at specific individuals or groups within an organization has made effective intelligence a higher priority than ever.

Bromium LAVA uses the latest developments in virtualization hardware and software technology combined with leading edge visualization and behavioral analytics to deliver a more effective method of detecting and analyzing malware and attacks than anything available in the past.

Deploying LAVA in an organization can significantly increase the security teams' ability to identify and respond to the most advanced forms of attacks in less time and with a smaller investment in instrumentation and tools than any other solution available today.

Bromium HQ

20813 Stevens Creek Blvd, Suite 150
Cupertino, CA 95014
info@bromium.com
+1.408.598.3623

Bromium UK Ltd

Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44 1223 314914

For more information refer to www.bromium.com,
contact sales@bromium.com or call at 1-800-518-0845

Copyright ©2013 Bromium, Inc. All rights Reserved.
#Bromium-wp-LAVA-0413a