Bromium®

# Practical Threat Intelligence

*with Bromium® LAVA*

# Practical Threat Intelligence

## Executive Summary

Threat intelligence today is costly and time consuming and does not always result in a reduction of successful attacks. Bromium has addressed these problems by applying Micro-virtualization technology to threat intelligence with the goal of achieving the following results.

1. Reduce threat analysis time and associated costs
2. Provide timely, accurate and actionable intelligence
3. Increase Security Operations Center effectiveness by decreasing successful attacks

This paper details how Bromium™ Live Attack Visualization and Analysis allows organizations to achieve these goals.

## Introduction

Threat intelligence is a hot topic in security today. Numerous tools, products and solutions are available to help security professionals gather cyber threat intelligence. Information is power, and there is a seemingly limitless amount of information available today. A quick Google search of the term "cyber threat intelligence" returns more than 2.5 million hits containing information ranging from the latest patches being issued by software vendors to the most recent political developments in far flung corners of the globe. Most of this information is very interesting, and some of it can be very useful in increasing the security of your organization. The real challenge is focusing your efforts and resources on the practical threat information that has a direct impact on your organization and allows you to perform your job more quickly, more easily and with measurable results.

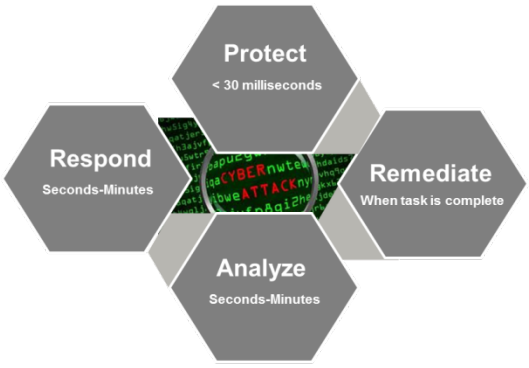

**Traditional Threat Intelligence**

## Practical Threat Intelligence

The type of threat intelligence needed by an organization depends on a great extent on the type, structure and goals of the organization. It is obvious that a national defense organization would focus on different types of threats than a commercial organization, and that a large financial organization might need different information than a mid-sized consumer products manufacturer. However all organizations share a common need for practical and actionable intelligence on the cyber threats they are facing. The following is a list of fundamental questions that all organizations need the intelligence to answer.

1. Am I being attacked? While the answer to this is almost certainly "yes" in today's connected world it is important to be able to accurately identify you are facing an attack that has a chance of compromising your systems versus a random piece of malware that poses no threat.
2. What kind of attack am I being subjected to? Understanding what an attacker is attempting to achieve is an important fact to consider when determining if and how you need to respond.
3. How does the attack work? Understanding how a specific attack or piece of malware works (the kill chain) provides critical insights into both prioritizing the threat and crafting a response.
4. Is this an isolated incident or part of a pattern? Being able to positively identify and record and correlate the details of all of the attacks against the organization enables you to adjust your response appropriately.

5. Do I have information I can use to respond to the threat? Having reliable information in a simple and understandable form enables you to act immediately to counter the attack.
6. Can I share the information with other people, tools or partners? Information has greater value when you can easily share it with other people and systems.




**Practical Threat Intelligence**

## Bromium Live Attack Visualization and Analysis (LAVA)

Bromium has developed a new technology, Micro-virtualization, which enables the type of practical threat intelligence outlined above. All Bromium products are built on the Bromium Microvisor™, a security focused, purpose built version of the Xen hypervisor. Bromium vSentry uses the Microvisor to leverage advanced CPU hardware capabilities and isolate the execution of untrusted tasks from the protected endpoint in "micro-VMs". Bromium LAVA analyzes and records malware trapped within a micro-VM using a technique referred to as "Microvisor based introspection". Introspection is the process of monitoring a virtual machine from the hypervisor, a vantage point "outside" of the virtual machine. Microvisor based introspection extends this concept to the myriad of micro-VMs that may exist on a protected endpoint running vSentry.

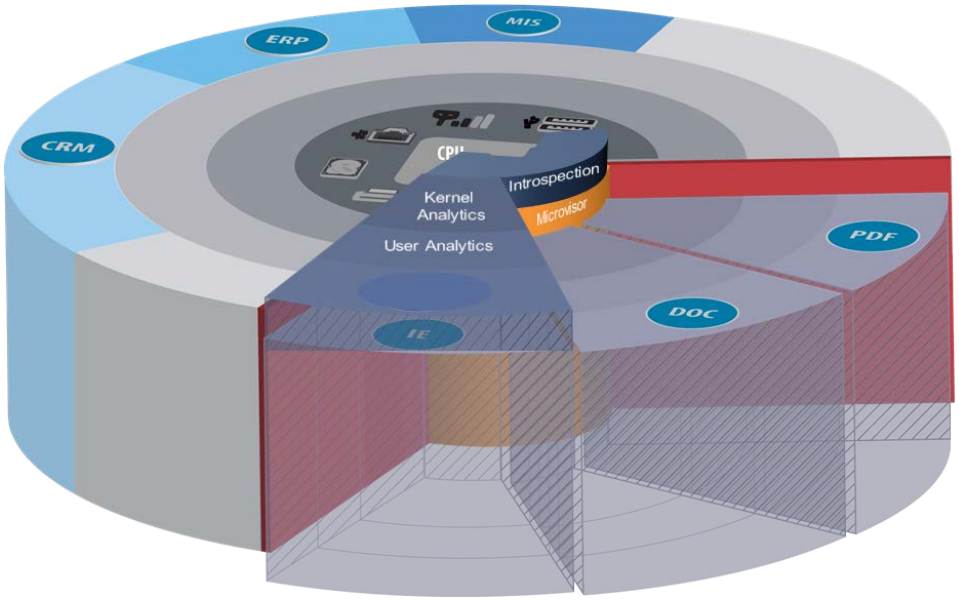
## Am I Under Attack?

Microvisor based introspection has profound implications on the current Threat Intelligence "state of the art". Threat Intelligence is a "strategic" conclusion based on correlating and summarizing a number of different low level "tactical" data points. The more accurate and relevant the individual data points, the more accurate and relevant the intelligence will be.

Microvisor based introspection provides extremely accurate and relevant "tactical" information that is then assembled into practical intelligence that can be used to immediately to improve the security of an organization. Assembling accurate data points on the existence of an advanced, unknown or zero-day attack presents a number of problems that have made it difficult for the industry to deliver practical threat intelligence. Bromium address these challenges with Micro-virtualization.

Micro-virtualization simplifies the complexity of recognizing malicious behavior as each micro-VM contains only one user initiated "task" or instance of an application. Any suspicious" behavior observed can thus be directly attributed to a specific application and an accurate judgment as to the legitimacy of an activity can be easily made. For instance a document opened in Adobe Acrobat Reader would not generally be expected to communicate with a web server located in a different part of the world. However this type of behavior generated by a web browser or an application update utility would be perfectly legitimate. The task isolation aspect of Micro-virtualization thus has a huge impact on the accuracy of one of the key elements that any practical threat intelligence system must provide and that is the ability to accurately and reliably determine if you are under attack by an unknown type of malware.

Microvisor based introspection runs directly at the point of attack, the endpoint system. Being installed directly on the system ensures that attacks detected are actually a threat to that particular machine and ensures that y ou will know if you are under attack no matter where the machine is located.




**Microvisor Based Introspection**

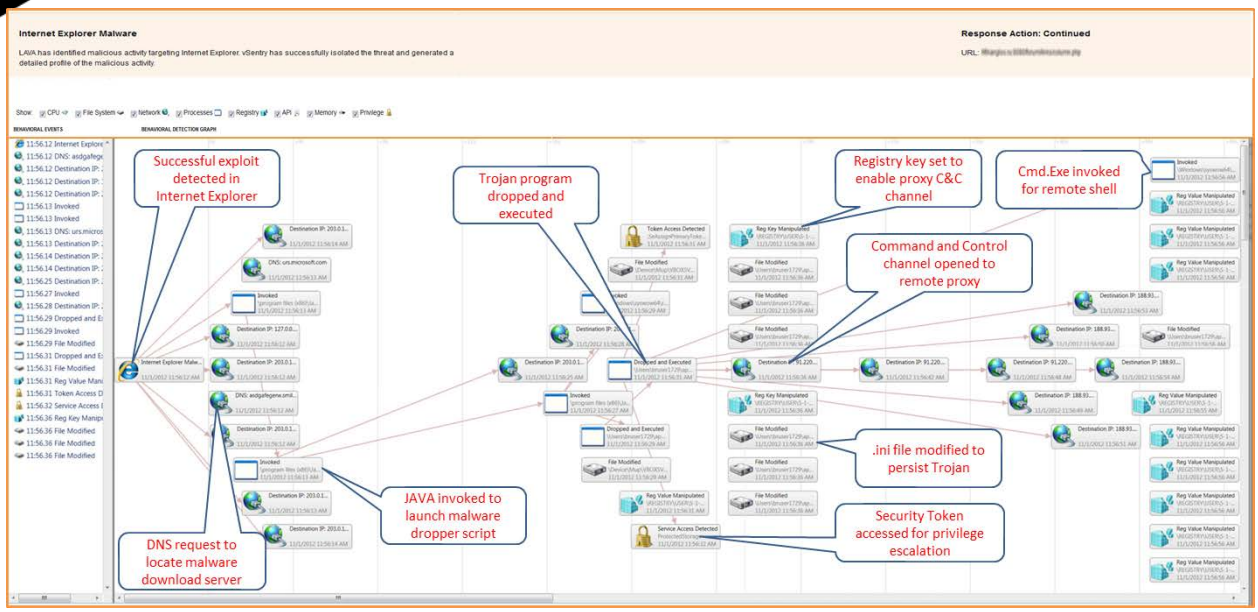
## What Kind of Attack Am I Under?

Understanding the type of attack being targeted at the user is another important strategic consideration. There are a broad range of goals pursued by attackers today. There are personal types of attacks such as “click fraud” or “banking fraud” and then there are more organizational types of attacks such as “password stealing” or the installation of a “remote access Trojan” that may pose a greater concern to the organizations security team. Answering this question with traditional security intelligence tools can be one of the most time consuming and expensive aspects of the process. To understand the type of attack under way generally requires the malware itself to be analyzed by a forensics or security analyst. Attackers have been going to great lengths in recent years to obfuscate or hide the intentions of all aspects of their malware. Analysts may have to try dozens of different tools to unpack and de-obfuscate malware once they receive a sample which can consume many hours or days of time.

Bromium LAVA analytics observe and record the interaction of the malware with the micro-VM after the malware has “detonated”. This approach completely bypasses all of the time consuming unpacking and de-obfuscation tricks implemented by the attacker as the malware itself must perform these functions before it is able to run. LAVA monitors, correlates and visualizes a large range of parameters within the micro-VM enabling quick identification of the specific type of attack being observed.

## How Does the Attack Work?

Knowing how the attack works allows the security operations center (SOC) to quickly judge the vulnerability of other systems in the organization. The unique visualization of the complete “kill chain” provided by LAVA “connects the dots” and enables the SOC to respond in minutes rather than days to mitigate the overall risk to the organization and without having to wait for a detailed analysis by the specialists.



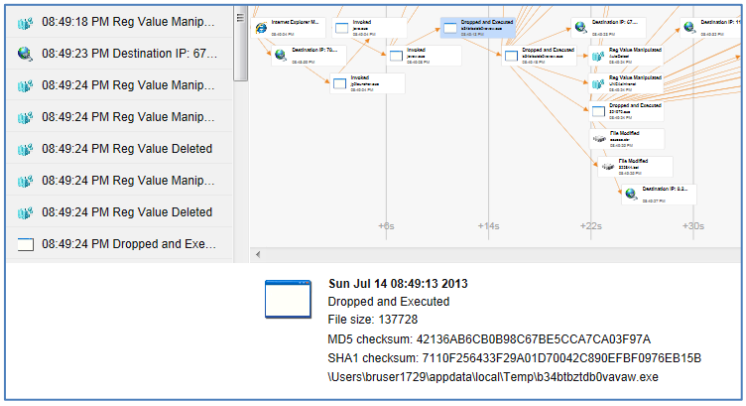

**Advanced Visualization of the Malware Kill-Chain**

## Is This an Isolated Incident or Part of a Pattern?

Understanding the relationship between a unique or unknown attack and the numbers, names and roles of targeted victims enables the SOC to quickly determine if an attack is being targeted at a specific area of the organization. For instance a unique form of malware that contains file stealing capabilities detected in one system is a cause for concern. If the identical piece of "unknown" code is detected in 3 machines, and the users involved are all members of the engineering development team for a secret new project, the implications of the attack are much greater. LAVA provides full integration with the organizations Active Directory infrastructure enabling the SOC team to determine the implications of a new attack just by comparing the system users with their place within the organizational structure. This level of strategic threat intelligence enables to security team to take additional mitigation steps, both technical and non-technical within minutes.

## Do I Have Information I Can Use to Respond To the Threat?

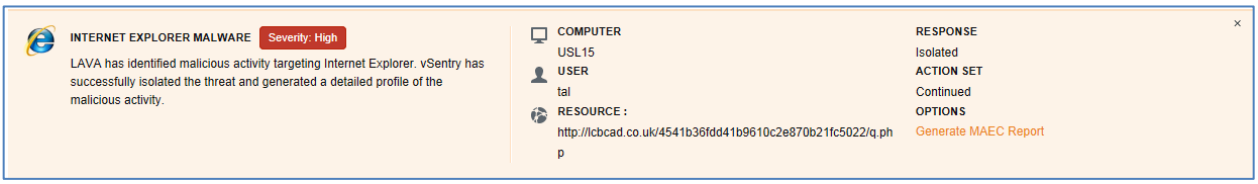
LAVA automatically generates cryptographic hashes of binaries it observes that can be automatically exported as "signatures" for use by other security systems in the organization such as a network IPS.




**Automatic Malware Signature Generation**

All network traffic is observed and recorded including the addresses and URLs of malicious servers and command and control server. This information can be used by perimeter defenses such as web security gateways, next generation firewalls or by the web browsers installed on other endpoints to automatically block access.

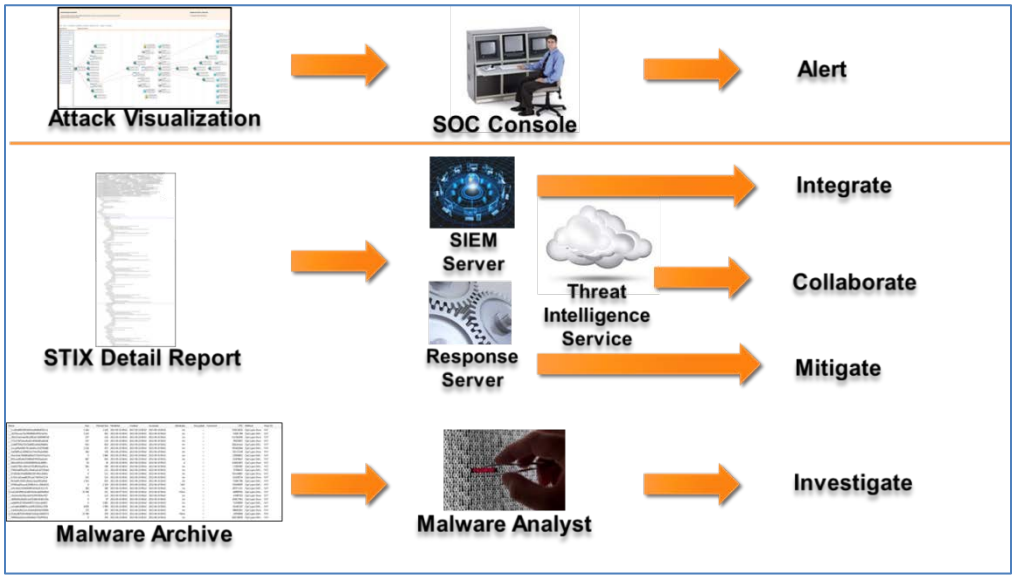
In short LAVA actually generates signatures for use by other systems rather than consuming signatures after an attack has successfully compromised an organization.




**Malicious URLs Automatically Recorded**

## Can I share the information with other people, tools or partners?

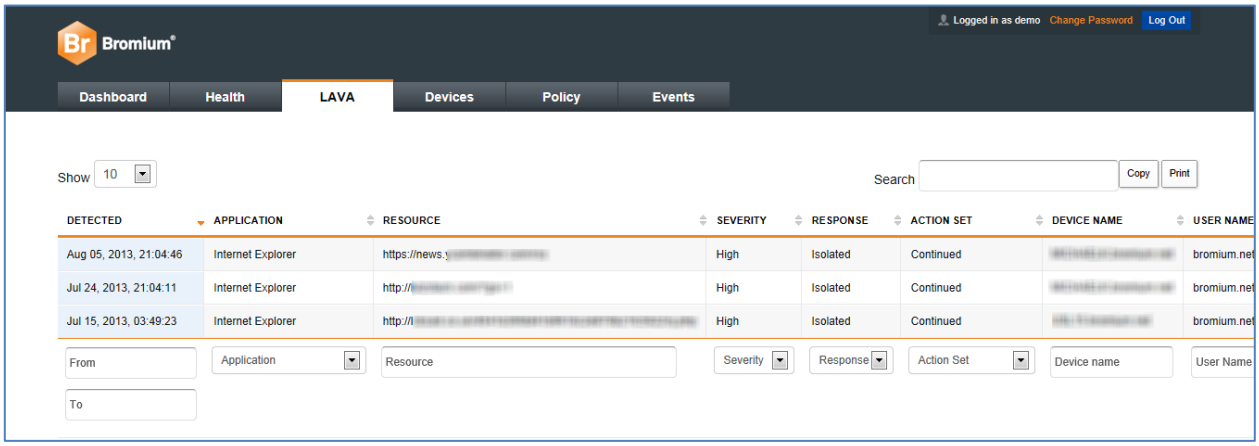
Because the malware executes within the confines of the micro-VM under the full control of the Microvisor, LAVA is able to record all of the information, including complete executable images of scripts and executable droppers during the course of the attack. These images are forwarded to the Bromium Management Server (BMS) where they form a comprehensive Malware Archive that analysts can use to completely reverse engineer the malware, validate samples against public attack information services or forward to partners and vendors for further study.




**LAVA Integration Capabilities**

The full intelligence gathered by LAVA can be automatically formatted and exported in the STIX/ MAEC format developed by NIST to enable high level intelligence sharing with other organizations of government agencies.

Comprehensive reporting on incidents, their severity and the outcome of the attack are provided within the BMS dashboard. This information can provide a valuable audit trail when endpoint security policy compliance data is needed within the organization.




LAVA Event View

## Conclusion

Micro-virtualization is a key component of a practical threat intelligence solution.
Bromium LAVA enables an organization to;

1. Reduce threat analysis time and associated costs
2. Provide timely, accurate and actionable intelligence
3. Increase Security Operations Center effectiveness by decreasing successful attacks

Bromium LAVA provides rich integration capabilities and enables organizations to enhance the effectiveness of their existing security infrastructure and share information with partners and other stake holders while reducing the overall risks to the organization.