Bromium LAVA

Live Attack Visualization and Analysis

Key Benefits

STRATEGIC INTELLIGENCE

Accurately identify targeted attacks as they occur to enable more effective response

ZERO-DAY ATTACK INSIGHT

Quickly analyze and respond to who, what, when, where, and how you are being attacked to minimize impact and costs

ADVANCED VISUALIZATION

Identify and act on attacks in minutes—not days or months—saving time and money

Key Features

AUTOMATIC ANALYSIS

Instantly understand the specific tactics and goals of any attack. LAVA details the precise set of malicious steps down to the registry, external IP addresses, and files changed by malware

STANDARDIZED COLLABORATION

Automatically create standardized indicator of compromise reports in STIX/ MAEC format for collaboration with other security tools

Every day, enterprises and government organizations are confronted with malware attacks that evade firewalls, network protection devices, and traditional endpoint security. What if there was a way to safely record and analyze the complete attack, without risk to the organization? Now there is.

Transform your security operations

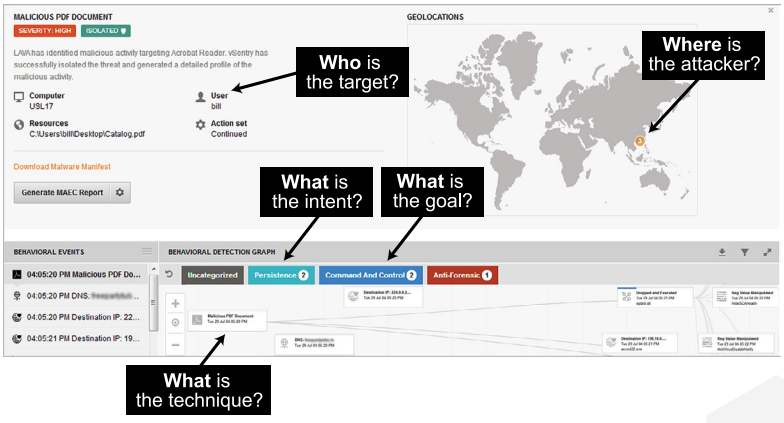
Security teams spend valuable time reacting to hundreds of routine events every day. These can be minor or a truly serious attack—and sometimes it is difficult to tell the difference.

Bromium® LAVA™ enables you to quickly identify real attacks from the rest and determine who within the organization is being targeted. This level of insight allows for immediate implementation of technical and user policies to counter malicious activity.

Empower your security staff. Unmatched threat intelligence.

LAVA's advanced visualization techniques enable security personnel to understand complex attacks in minutes rather than hours or days.

LAVA shares detailed attack information with your current infrastructure. You can automatically export security incidents to the most popular SIEM, next-generation firewall, or other systems to deliver a new level of visibility and control.



Supported Platforms

ENDPOINTS

Intel i3, i5, i7 processors, 4 GB RAM, Windows 7 64-bit and 32-bit, Apple OSX

SERVERS

Microsoft Windows Server 2008, SQL Server 2008 R2

About Bromium

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

Visualizing the kill chain

LAVA delivers a clear and concise summary of the complete "kill chain," enabling security operators to quickly evaluate the threat to the organization and respond instantly.

Full malware capture

Similar to a black box flight recorder, LAVA records complete samples of all malware within a Bromium micro-VM, even malware that is deleted or that never leaves volatile memory. Armed with these samples, the analyst can replay or reverse engineer the malware to uncover the complete methods and goals of the attack.

Automatic attack categorization

LAVA instantly displays a high-level, color-coded, plain language characterization of the intent of the attack elements. This enables the security analyst to quickly identify the organizational risks of each attack and prioritize the appropriate response.

How it works

Bromium LAVA leverages Bromium vSentry® to do post exploit analysis. Bromium vSentry uses micro-virtualization to isolate user tasks and automatically and safely allows malware to fully execute within a micro-VM.

LAVA observes all activity from the vantage point of the hardware "below" the operating system. This vantage point provides unique capabilities.

- **Bootkit/rootkit detection.** One of the most hard-to-detect components of malware is bootkits/rootkits. LAVA clearly identifies their installation and actions.
- **Anti-forensics detection.** Malware can evade detection by removing components used early in its infection cycle. Typical forensic tools cannot detect these.
- **Zero-day malware signature generation.** LAVA provides MD5 checksums for use in other security tools for malware identification.
- **Defense bypass detection.** Privilege escalation is used to disable resident security tools. LAVA detects and stores these actions for later study.
- **Command-and-control detection.** LAVA identifies command-and-control (C&C) channels details enabling tuning of perimeter defenses to block communications.
- **Process injection detection.** Process injection introduces malicious code into running processes on the victim. This technique is extremely difficult to detect with conventional analytic tools.
- **Malware persistence detection.** Malware often modifies the victim system to ensure the attacker has access in the future. LAVA monitors and identifies this behavior.
- **Command shell detection.** Remote command shells enable attackers to take control of a compromised system and are an unambiguous indicator of compromise.

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

DS.LAVA.US-EN.1510