Bromium Threat Analysis

Instant Attack Visualization and Threat Intelligence

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. Bromium Threat Analysis 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

POWERFUL SEARCH CAPABILITIES

Quickly identify indicators of attack (IOAs) and indicators of compromise (IOCs) on your endpoints

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

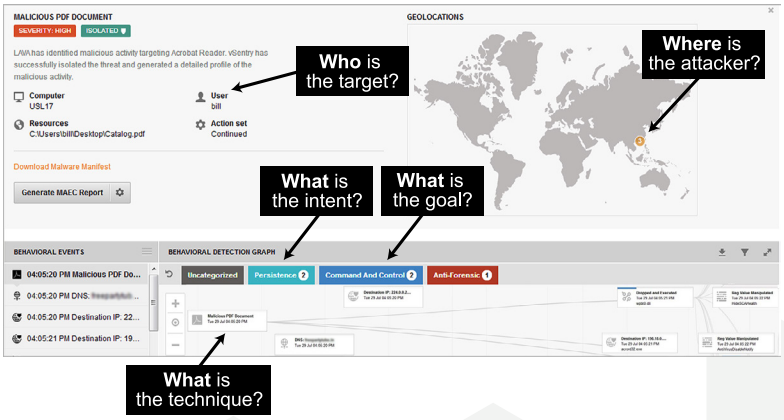
Security teams spend valuable time reacting to hundreds of routine events every day. These can be minor or a truly serious attack—and sometimes it is difficult to tell the difference.

Bromium® Threat Analysis,™ a component of Bromium Advanced Endpoint Security, 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 with unmatched threat intelligence

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

Bromium Threat Analysis 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.



Bromium®

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 pioneered the next generation of endpoint protection that eliminates breaches. Just as virtualization transformed IT, Bromium is transforming security with its unique micro-virtualization technology. Bromium provides the world's most advanced endpoint security, even against the most sophisticated zero-day malware. Unlike traditional security technologies, such as antivirus or virtual containers, which rely on ineffective detection techniques, Bromium's solution automatically isolates each user-task in a lightweight, CPU-enforced micro-VM. This enables users to click on anything without risk of compromise, protecting the enterprise. Bromium's technological innovations have earned the company numerous industry awards. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers. Visit us at www.bromium.com.

Visualizing the kill chain

Bromium Threat Analysis delivers a clear and concise summary of the complete kill chain, enabling security operators to quickly evaluate the threat and respond instantly.

Full malware capture

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

Automatic attack categorization

Bromium Threat Analysis instantly displays a high-level, color-coded, plain language characterization of the intent of the attack elements. This enables quick identification of the organizational risks of each attack and the prioritization of appropriate responses.

How it works

Bromium Threat Analysis leverages a key capability in Bromium's architecture—the real-time detection of malicious activity on enterprise endpoints, using introspection to observe execution within each micro-VM and the endpoint host operating system.

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

- **Bootkit/rootkit detection.** Bromium clearly identifies rootkit/bootkit installation and actions.
- **Anti-forensics detection.** Bromium detects malware removing components used early in the infection cycle which typical forensic tools cannot detect.
- **Zero-day malware signature generation.** Bromium provides MD5 checksums for use in other security tools for malware identification.
- **Defense bypass detection.** Bromium detects and stores for later study privilege escalation actions used to disable resident security tools.
- **Command-and-control detection.** Bromium identifies command-and-control channels details enabling tuning of perimeter defenses to block communications.
- **IOA/IOC generation.** Bromium assembles and correlates across endpoints IOAs from host monitoring and IOCs from micro-virtual machines.
- **Process injection detection.** Bromium detects malware injecting malicious code into running processes on the victim.
- **Malware persistence detection.** Bromium identifies and monitors malware modifying the victim system to ensure future access.
- **Command shell detection.** Bromium detects remote command shells that enable attackers to take control of a compromised system and are an unambiguous IOC.

Bromium®

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.BromiumThreatAnalysis.US-EN.1602