REVERSINGLABS

Bromium®

Detailed Threat Intelligence Powers Instant Preventive Security

Rich malware results for rapid action on threats isolated by Bromium

Joint ReversingLabs & Bromium Solution Value

According to Verizon's 2018 Data Breach Investigations Report "This year we saw, yet again, that cybercriminals are still finding success with the same tried and tested techniques, and their victims are still making the same mistakes." For example, even with all of the security spend and employee phishing training, "...4% of people will click on any given phishing email."

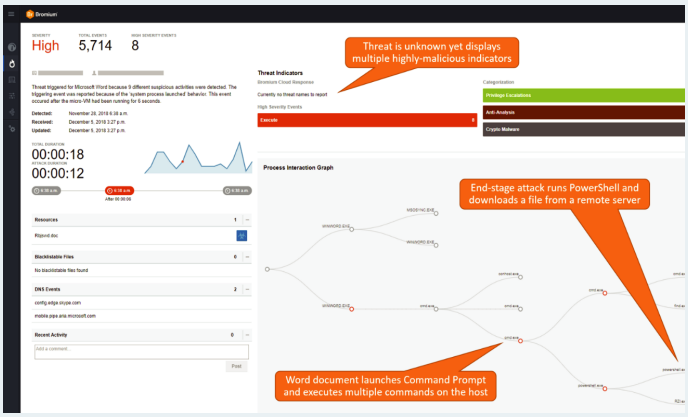
The Bromium Secure Platform allows any file or document to be opened on an endpoint in isolation without risk of infection - whether downloaded from the web, received in email, or saved via portable USB drives using application isolation. Bromium creates single-use micro-VMs for each untrusted document or web page. These are disposable containers that completely isolate all activity from the host PC. If malware does execute, it has nowhere to go, has no impact, and Bromium captures the full kill-chain of malicious indicators.

Using the ReversingLabs Advanced Malware Analysis solution, analysts can upload file samples that they've captured for detailed threat information, from a link in the Bromium UI.

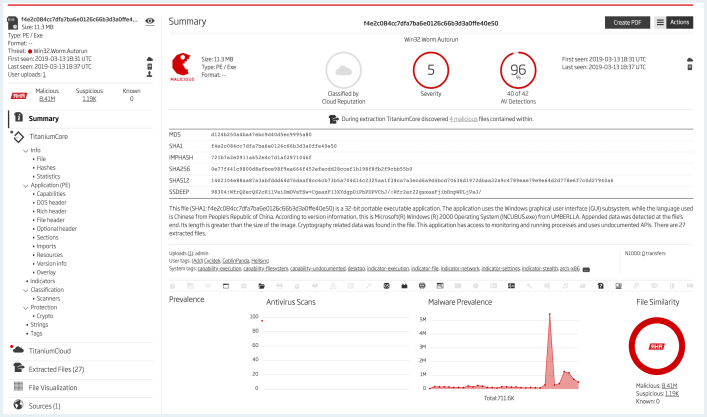
This detailed threat intelligence on malicious and unknown files helps analysts understand: what the malware does, classification (ex: malicious), threat level, malware type and many more details, accelerating threat triage. Endpoint defenses can also be updated to be on the look-out for malware indicators, reducing the overall attack surface.

Key Solution Highlights

- ReversingLabs provides second-level insights into malware such as threat levels and indicators triggered and displays them in the Bromium UI to identify threats that entered through non-Bromium managed devices like servers, Macs, Linux and mobile devices.
- ReversingLabs enriches Bromium's Breachless Threat Intelligence with contextual file data to accelerate analysts' malware detection and response processes and enable proactive defenses.
- One-click to the ReversingLabs Advanced Malware Analysis solution for analysts to upload unknown samples for detailed malware results to rapidly triage threats.
- One-click back to the Bromium UI from the ReversingLabs Advanced Malware Analysis solution for rapid threat response.
- ReversingLabs enriches actionable Bromium Threat and CISO/CIO executive summary reports with detailed malware metadata.



Bromium isolates an unknown threat exhibiting multiple highly-malicious indicators, and forwards the sample to the ReversingLabs Advanced Malware Analysis Platform for additional threat intelligence correlation and detail.



ReversingLabs Advanced Malware Analysis Platform displays detailed malware analysis results that analysts can drill into for further investigation.

This powerful integration allows sophisticated security defenders to identify novel threats and targeted attacks unknown to the anti-malware industry in isolation without a breach, then deeply analyze them in an automated fashion to determine necessary steps for remediation and proactive attack surface reduction across the enterprise.

James Wright,
Vice President Engineering, Bromium

How It Works

- The ReversingLabs Advanced Malware Analysis Platform can be deployed in the cloud or locally on premises.
- Analysts can forward threats to ReversingLabs through a link in the Bromium UI.
- ReversingLabs displays detailed malware analysis results like threat severity levels and recent activity that analysts can drill into for further investigation.
- From the ReversingLabs dashboard, analysts can quickly return to the Bromium Analysis UI with a single click to triage threats.

About ReversingLabs

Malware routinely evades detection and lurks within corporate infrastructures causing damage and loss. Unique automated static analysis technology and authoritative file intelligence services power our innovative solutions that enable security teams to combat unknown malware. TitaniumScale high volume analysis and classification creates local threat intelligence across all internal objects, and empowers security teams to identify and neutralize malware that evades detection.

About Bromium

Bromium protects organizations brands, data and people using virtualization-based security via application isolation. They convert an enterprise's largest liability – endpoints – into its best defense. By combining patented hardware-enforced containerization to deliver application isolation and control, with a distributed Sensor Network to protect across all major threat vectors and attack types, stopping malware in its tracks. Unlike traditional security technologies, Bromium automatically isolates threats and adapts to new attacks using behavioral analysis and instantly shares threat intelligence to eliminate the impact of malware. Bromium offers defense-grade security and counts a rapidly growing set of Fortune 500 companies and government agencies as customers.Visit Bromium at https://www.bromium.com to learn more.