SOLUTION BRIEF

REVERSINGLABS

Threat Intelligence Browser Extension

Up-to-the-Second Threat Intelligence Where It Counts

The Browser is the Desktop

With the shift to web-based Software-as-a-Service (SaaS) applications and cloud infrastructure, the browser has become the focal point for today's enterprise. From office productivity to sales forecasting to infrastructure administration, the tasks that keep your enterprise running are increasingly performed in a web browser.

For the modern Security Operations Center (SOC), browser-based security tools have become the primary mechanism leveraged by security analysts to perform incident investigation and triage. Having the latest threat intel on adversary tools and infrastructure is crucial for assessing impact and criticality of endpoint and network-based security alerts.

The Need for Speed

With the spread of ransomware and other destructive malware, Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR) to new incoming attacks is crucial. SOC teams have seconds, not hours or days, to validate and respond to each alert they're tasked with investigating. Is this a real incident or a false positive? What's the potential impact of a true positive? What does this malware sample do? Is this URL malicious or benign?

Solution Highlights

ReversingLabs Browser Extension provides:

- IOC highlighting and enrichment for files, hashes, URLs, domains and IP addresses displayed in the browser
- URL scan at the point of impact to prevent opening malicious sites
- Download scanning to ensure all downloads entering the perimeter are verified, with malicious downloads blocked before it gets the chance to compromise the endpoint

Key Benefits

- One-click enrichment for IOCs on screen without pivoting away from an active investigation
- Powerful threat intelligence based protection against web-based threats

How ReversingLabs' Browser Extension Boosts Enterprise Security

Use Case 1

Accelerating Incident Response

Challenge:
Job one for security analysts is to determine if the alert they're investigating is a real incident or a false positive that can be dismissed. Assuming the incident is real, the criticality, scope, and impact of the incident determines the level of response needed.

Solution:
ReversingLabs' Browser Extension provides one-click enrichment with a clear, validated verdict on each IOC on screen while using browser-based security solutions. Security analysts can see at a glance, without pivoting away from their existing workflows, the Risk Score, Classification, Threat Name and disposition of file hashes, URLs, domains, and IP addresses being displayed. This provides in-the-moment validation of security alerts, allowing SOC teams to focus on the most important issues while closing lower priority and false positive alerts. And, if analysts want deeper context or further analysis, Spectra Analyze is just a click away.

By adding the browser extension from ReversingLabs, security analysts get a powerful, fast, and simplified way to enrich IOCs, prioritize the true threats, and accelerate response actions.

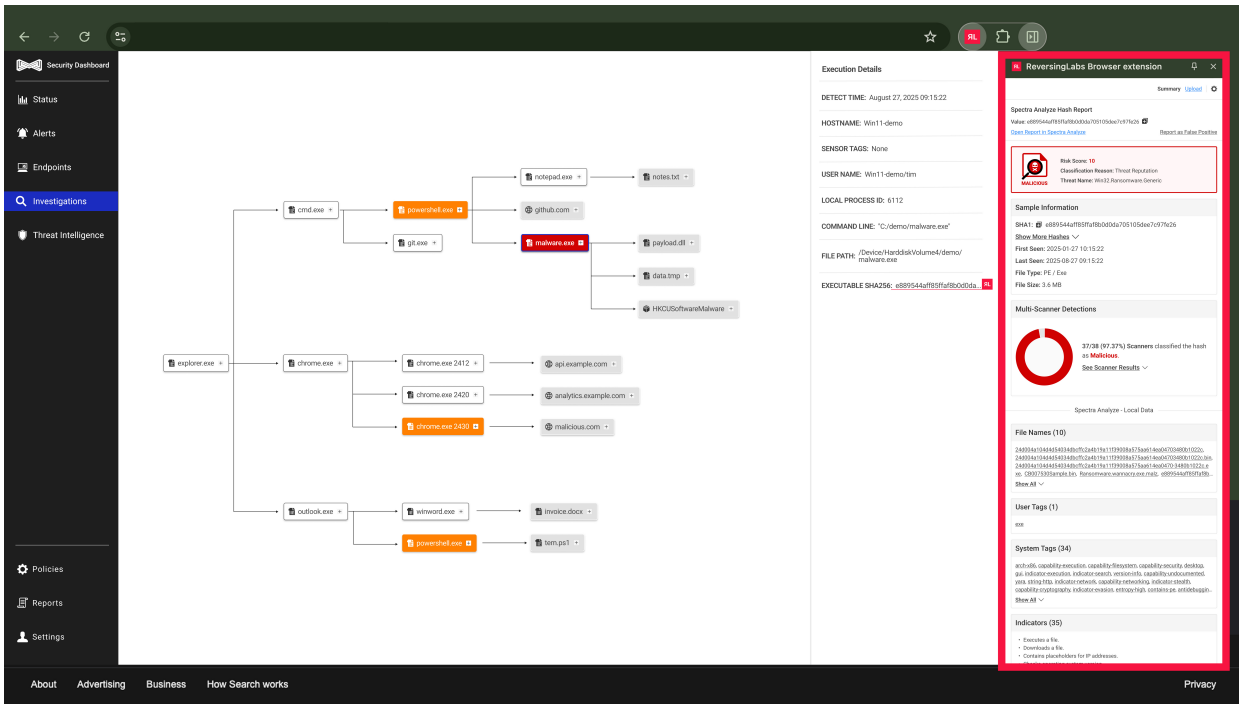

Figure 1: Example SOC workflow with IOC enrichment from the RL Browser Extension.

Use Case 2

Safeguarding Endpoints

Challenge:
Browser-based threats have exploded, making the browser the point of impact for security incidents in today's enterprise. For the first time, browser-based attacks have overtaken email as the main attack vector, comprising 70% of malware cases versus 15% for email[1].

Solution:
ReversingLabs' Browser Extension blocks malicious URLs and downloads, stopping browser-based threats before they have the chance to compromise your enterprise. Traditional AV or even Next Gen AV / Endpoint Protection (EPP) solutions attempt to identify malware and malicious network connections *after* these threats have been downloaded or accessed. The threat is now inside your enterprise where it may or may not be stopped using traditional security solutions.

By utilizing the ReversingLabs Browser Extension, organizations get an additional layer of security at the endpoint to protect against browser-based threats *before* they can be downloaded or accessed. The result is fewer security incidents and a stronger security posture.

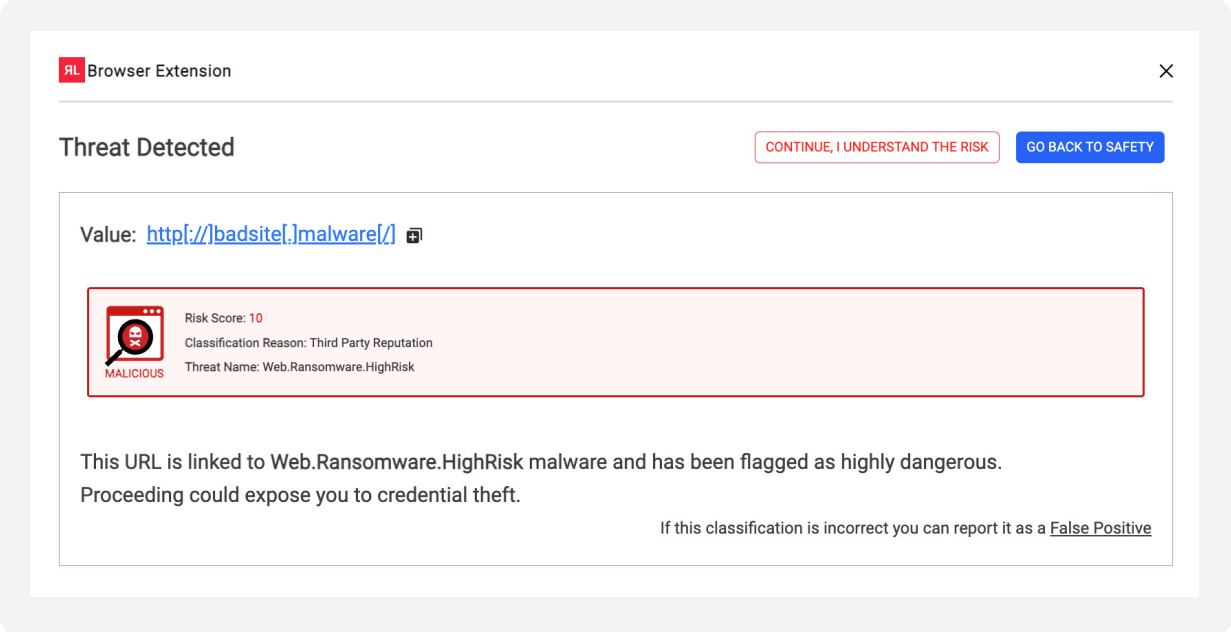

Figure 2: Protection in real time from the RL Browser Extension.

[1] eSentire "The Modern Threat Actors' Playbook: How Initial Access and Ransomware Deployment Trends are Shifting in 2025"

Conclusion

The ReversingLabs Browser Extension is a multi-faceted, easy-to-use tool that provides immediate threat visibility and intelligence to boost enterprise security and protect against threats before they gain a foothold in the organization.

It empowers SOC analysts with instant insights into IOCs – with a single click – to significantly streamline and speed investigative workflows, and in turn, dramatically improve detection and response times. At the same time, it enhances endpoint security by automatically scanning and blocking malicious URLs and downloads to proactively stop threats at their source and point of impact.

Get Started!

REQUEST A DEMO

reversinglabs.com

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 billion searchable files with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

SB-Rev-09.12.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com