DATA SHEET

ЯL ЯEVERSINGLABS

Curated Ransomware Intelligence

Detect and prevent ransomware before it strikes

ReversingLabs Ransomware Feed

Detecting emergent ransomware attacks in their early stages is critical to prevent catastrophic loss of data and business interruptions. Unfortunately, many security teams have insufficient visibility into the progression of a potential attack against their organization.

ReversingLabs designed this feed to help security teams discover the initial forays of a ransomware attack into the network and identify attempts at lateral movement. Spotting these precursor activities allows organizations to short circuit attacks that are in progress and avoid costly damage to the business.

Timely. Relevant. Context-Rich. Vetted.

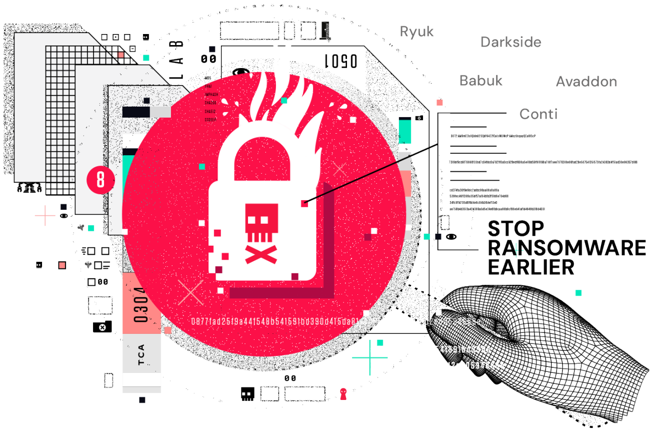
The starting point of all the indicators in our Ransomware Feed is ReversingLabs' global data corpus of more than 40 billion malware and goodware samples, giving customers access to one of the largest file sets available on the market.

Millions of unique malware files are identified every day to produce a wealth of ransomware-related datasets. This deep knowledge base of good, bad, and suspicious files means organizations that leverage our threat intelligence feed can count on always having the latest insights on new and emerging threats.

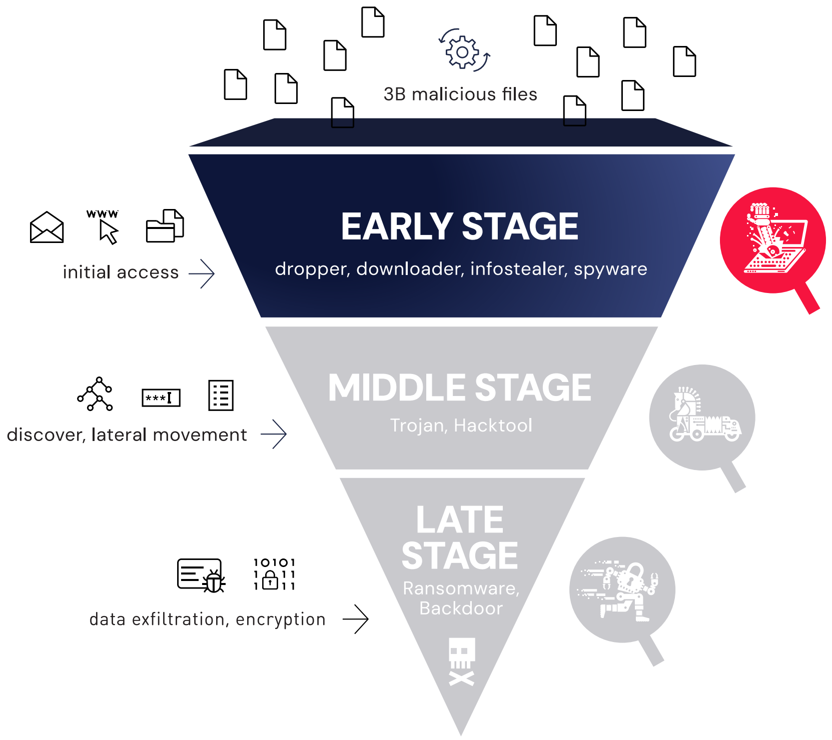
Very importantly, our strict vetting process for new intelligence and robust curation by ReversingLabs' in-house malware analysis research team ensures our ransomware indicators are of the highest quality, with the lowest number of false positives.

Key Solution Highlights

- Wider coverage and distinct IOCs compared to other feeds due to ReversingLabs massive data corpus with billions of malware samples
- Hash, IP, Domain, and URI indicators tagged with contextual data such as malware family, network parameters, MITRE ATT&CK and attack progression stage
- Aggressive aging of indicators and active filtering of obsolete threats ensures only relevant indicators are active in the list
- Strict vetting and rigorous curation of ransomware indicators means very low false positive rate
- Easy to consume via REST API, STIX/TAXII collections, and built-in integrations with leading TI/SOAR platforms



Closing the Visibility Gap



ЯL ЯEVERSINGLABS

Early stage malware is typically basic and less resource-intensive, using fewer MITRE ATT&CK techniques. ReversingLabs' Ransomware Feed provides indicators on malspam, payload links, and other early IOCs.

ReversingLabs tracks billions of malicious files and can detect middle stage malware used for lateral movement and network discovery.

Entrenchment, encryption, and exfiltration happen in late-stage ransomware attacks. ReversingLabs gives SOC teams validated, active context to the IoC so they can focus on rapid mitigation rather than wasting valuable time researching malware or dealing with false positives.

Available in these Marketplaces

ANOMALI™ | Azure Sentinel | CORTEX XSOAR BY PALO ALTO NETWORKS | ThreatConnect.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide a modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily 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.

Get Started!

Experience the ReversingLabs Difference

REQUEST A DEMO

www.reversinglabs.com

ЯL ЯEVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com