REVERSINGLABS

DATA SHEET

Ransomware Feed

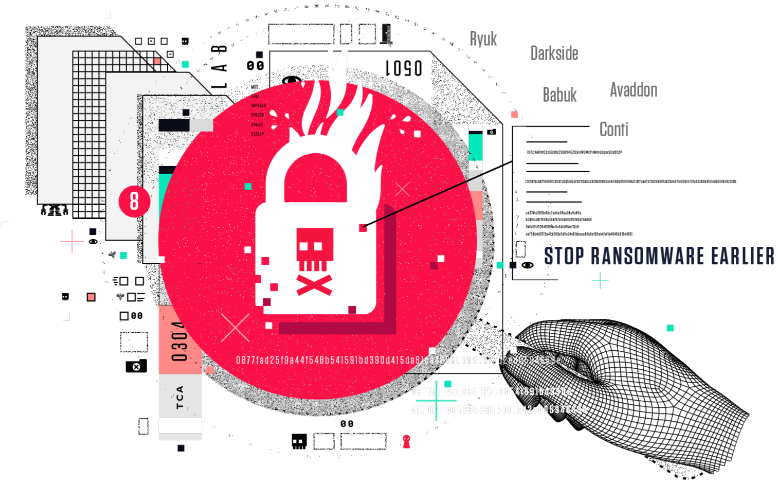
Detect and prevent Ransomware before it strikes with deeper intelligence and better Ransomware detection

Key Solution Highlights

- Indicators from multiple stages of typical attacks allow for early detection and the ability to reduce damage associated with IP theft and ransomware attacks
- Aggressive aging of the indicators ensures only relevant indicators are active in the list
- Extensive post processing of indicators eliminates or reduces confidence on indicators likely to produce false positives
- IP, Domain and Hash indicators tagged with contextual data such as malware family, network parameters, MITRE ATT&CK and attack progression stage

Ransomware Feed

Everything we do is about enabling enterprise defenders to level the playing field, putting their own attack/incident data to work. Today, many teams have insufficient visibility into the progression of a potential ransomware attack against their organization. ReversingLabs designed this feed for organizations that are searching for better ways to detect ransomware attacks in the early stages. This feed of network indicators and lateral movement patterns is based on latest commodity malware variants and solves your visibility gaps, enabling teams the opportunity to discover adversaries' initial network access and lateral movement before data is encrypted.

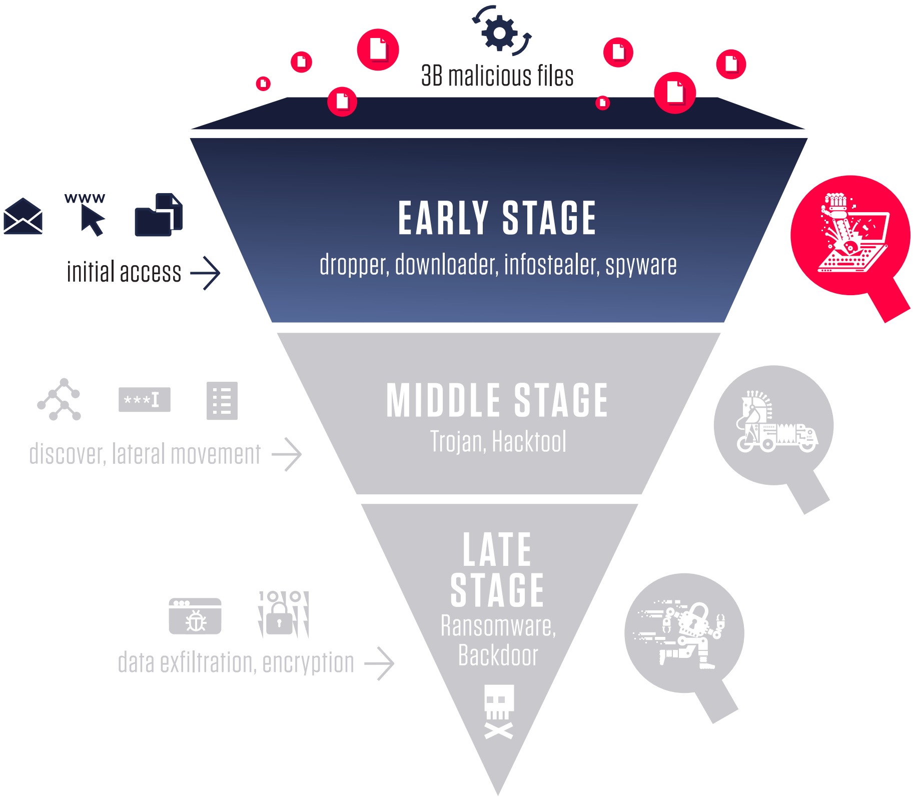


Feed Details

The starting point of all the indicators in our Ransomware Feed is ReversingLabs' file repository, one of the largest file sets available on the market. On average, 2.5 million unique malware files are analyzed every day to produce a wealth of ransomware-related datasets that encompasses more than 13 billion classified files, 3 billion of them malicious. This deep knowledge base of good, bad, and suspicious files means that organizations that leverage our threat intelligence feed can count on having the latest insights on new and emerging threats.

Closing The Visibility Gap

Detecting the early stages can head off a ransomware attack. In many cases the deploying of ransomware is delayed after the attacker gains access. The delay can be minutes, hours or days. This feed will help your team gain early visibility to the attacker's moves.



ЯEVERSINGLABS

Early stage malware is simple and lightweight, using fewer MITRE ATT&CK techniques. ReversingLabs' Ransomware Feed provides indicators on malspam, payload links, and other early IOCs.

ReversingLabs tracks 3 billion malicious files and can detect middle stage malware used for lateral movement and network discovery.

ReversingLabs maintains a comprehensive repository of known ransomware and other indicators of imminent ransomware deployment, enabling victim organizations to pre-empt ransomware attacks.

Available in these Marketplaces

ANOMALI paloalto® NETWORKS THREATCONNECT™ Azure Sentinel

Get Started!

WE'LL SHOW YOU HOW REVERSINGLABS DETECTS AND ANALYZES MORE HIDDEN THREATS

REQUEST A DEMO

About ReversingLabs

ReversingLabs is the leading provider of explainable threat intelligence solutions that dissect complex file-based threats for enterprises stretched for time and expertise. Its hybrid-cloud Titanium Platform enables digital business resiliency, protects against new modern architecture exposures, and automates manual SOC processes with a transparency that arms analysts to confidently take action and hunt threats.

ЯEVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com