

Ransomware Monitoring & Investigation with Recorded Future

Real-time intelligence to detect, hunt, and remediate ransomware threats

Challenge

Ransomware methods continue to evolve, with the successful delivery of different versions of ransomware threatening small, medium and large organizations globally. Ransomware actors constantly evolve their operations and shift the tactics, techniques, and procedures (TTPs) they use, only Recorded Future is constantly keeping tabs on these trends providing intelligence to identify and mitigate ransomware attacks from doing damage.

Solution

Detect

How can you be sure you aren't missing signs of an ongoing ransomware attack against your organization? Leveraging technical collection and diverse threat intelligence from Recorded Future you can detect indicators of compromise that may already be present within your network or get ahead of threats that are newly discovered or trending within your industry and peers.

Hunt

The hunt for ransomware activity is never-ending. With ransomware-specific hunting packages from Recorded Future's expert intelligence analysts, the Insikt Group, you can uncover early indicators of ransomware activity before it becomes a problem. Using their detailed threat analysis in conjunction with Sigma and YARA detection rulesets, the hunt for ransomware has never been easier.

Monitor

Continuously monitor real-time ransomware-related threats and trends. With advanced queries and dashboards in Recorded Future you can stay up to date on general ransomware trends, look specifically at ransomware threats to your industry and peers, track behaviors related to major ransomware families, and identify new ransomware infrastructure as it emerges.



Recorded Future Features to Enable Ransomware Investigation

Detailed Intelligence Cards for Comprehensive Insights on Ransomware, Threat Actors, Threat Groups, and More

Recorded Future Intelligence Cards organize all relevant insights and collection on a specific investigation topic in one place. Easily understand everything that Recorded Future knows about a certain ransomware campaign, threat actor, or indicator and pivot on the things that matter to your organization for deeper investigation.

Unmatched Dark Web and Technical Collection

Monitor open and closed dark web and criminal underground sites in any language including direct collection of boutique ransomware extortion sites operated by threat actors and large forums and marketplaces where actors sell access to stolen data or compromised machines. All of this information can be accessed in the platform without having to navigate to the sites themselves.

Dynamic Risk Scoring for Ransomware Associated Indicators Of Compromise (IOCs)

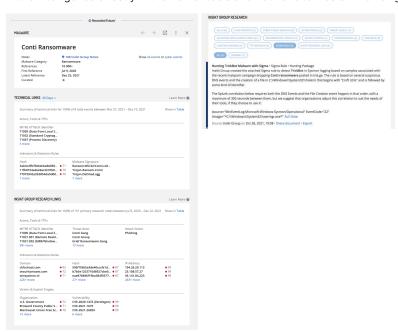
Quickly surface and prioritize IP, Domain, Hash, URL, and CVEs that could be used as infrastructure to deploy ransomware by using Recorded Future risk scoring. Derived from the collection and aggregation of intelligence and entity-specific risk rules, these scores are continually updated, rich with the context, and completely transparent so you can understand their criticality and attribution.

Tailored Ransomware Hunting Packages and Finished Intelligence Reporting

Understand the ransomware landscape from the experts. Recorded Future's research team, the Insikt Group, publishes tactical and strategic research on the ransomware landscape such as daily ransomware rollups, reporting on the extortion sites, validated breach event information on what organizations have been hit, what was compromised and by whom, and other large data analysis to help customers evaluate the business risk posed by a particular threat. In addition to the more general reporting you can leverage Insikt Group's tailored hunting packages with YARA, Snort, and Sigma detection rulesets that can be used for proactive threat hunting within your network.

Actionable Intelligence Delivered Where Your Analysts Need It

Get all of the relevant, actionable intelligence you need delivered to your analyst's favorite tools. Recorded Future has out of the box integrations with all of the leading security products across SIEMs, EDRs, SOAR platforms, TIPs, and more, that allows analysts to use Recorded Future intelligence directly in their other tools and not have to waste time navigating away from them.



Example Intelligence Card showing comprehensive intelligence on a type of ransomware with indicators, expert analysis, transparency to original sources of intelligence, and more.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

