STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Ransomware Red Team

Simulate an Attack by a Ransomware Threat Actor

Ransomware attacks continue to cause significant financial losses for organizations, disrupt operations, and compromise sensitive data.

Additionally, attackers often threaten to leak stolen data, increasing pressure on businesses to pay ransoms and intensifying the threat risk.

Stroz Friedberg's Ransomware Red Team testing uses ransomware scenarios to help organizations find and fix vulnerabilities before threat actors can exploit them. By simulating real ransomware attacks, Red Teams can identify specific weaknesses in defenses and assess the organization's response capabilities. This proactive approach supports your efforts to improve security, enhance incident response, and reduce the overall risk of a successful ransomware attack.

Why Ransomware Red Team?

Simulate the tactics, techniques, and procedures used by a ransomware threat actor (after initial access) to compromise sensitive data, critical infrastructure, and other information backups.

Tabletop Discussions with Real-World Testing

Tabletop discussions help facilitate planning by identifying gaps in response strategies. Ransomware Red Teams then test those plans in real-world scenarios to uncover both technical and process vulnerabilities.

Real-World Attack Paths

Understand real-world attack paths that a ransomware threat actor could use to compromise sensitive data and critical production or backup infrastructure.

Enhance Security Configurations

By simulating advanced attack techniques, a Ransomware Red Team can assist Blue Teams in refining and optimizing their EDR, IDS, IPS, Firewalls, SIEM, and other security tools to ensure they operate at maximum effectiveness.

Strengthen Incident Response

The Ransomware Red Team evaluates the client's incident response processes, offering practical feedback that enhances the organization's capacity to identify, react to, and recover from real-world cyber threats.

Top Concerns for Organizations

Backup Infrastructure Compromise

Many successful ransomware attacks involve hackers targeting backup systems first, making traditional recovery methods useless. Organizations often find out too late that their "air-gapped" backups aren't really isolated from the network access.

Detection Blind Spots

Attackers often spend weeks mapping networks, escalating privileges, and positioning themselves for maximum damage before deploying ransomware. Security teams commonly lack visibility into lateral movement across hybrid cloud environments.

Incident Response Gaps

When ransomware strikes, organizations often encounter communication failures that hinder containment efforts. Teams manage fragmented response procedures that haven't been tested in real attack scenarios.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 537SVB 07-2025

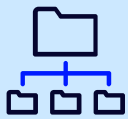
Business Continuity Failures

Critical systems interdependencies are often not understood until an attack causes cascading failures. Manufacturing, supply chain, and customer-facing operations can remain offline for an extended period due to insufficient prioritization of recovery measures.

Regulatory and Legal Exposure

Data exfiltration is increasingly associated with ransomware attacks, prompting complex compliance requirements across multiple jurisdictions. Organizations face rising legal costs and regulatory fines that often surpass the original ransom demands.

Ransomware Red Team Goals and Scenarios



Data Storage

Goal 1

Goal: Move undetected across the network to obtain access to sensitive data stores (e.g., file shares, databases, data lakes, cloud storage, etc.)

Scenario: A threat actor gains access to sensitive data stores and starts the encryption process before being detected

Critical Production Infrastructure

Goal 2

Goal: Move undetected across the network to obtain access to critical production infrastructure (e.g., web/application servers deployed to production)

Scenario: A threat actor accesses critical business infrastructure and takes business operations offline

Backup Infrastructure

Goal 3

Goal: Move undetected across the network to obtain access to backups

Scenario: A threat actor compromises backups, hindering the recovery or efficient resuming of operations

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 537SVB 07-2025

Ransomware Red Team Life Cycle

Stroz Friedberg can emulate persistent, motivated, and well-funded attackers by applying our expertise and understanding to use advanced tactics, techniques, and procedures (TTPs) to infiltrate the organization and meet realistic scenario goals. This type of testing is designed for clients with a mature and highly developed security posture. It represents the highest level of testing capability from both attacker and defense perspectives, identifying technical, procedural, and behavioral security control weaknesses.

Stroz Friedberg's Ransomware Red Team testing elevates an already mature security-aware organization by exercising all aspects of their prevention, detection, and response capabilities and demonstrates the return on their investment in security:

1

Realistically emulate the actions and activities of a team of skilled attackers attempting to gain access to internal infrastructure and carry out further actions against critical systems once a successful foothold is established.

2

Assist in identifying and evaluating ways to improve an organization's existing compromise detection controls, incident response and management, and breach reporting processes.

3

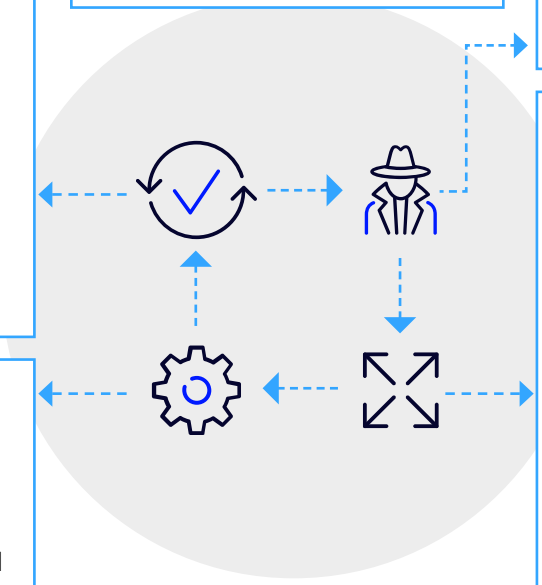
Assist in identifying vulnerable systems, missing security controls, and potential detection blind spots.

Persistence and Egress
Mimicking the activities of an advanced attacker, persistent access to the target is secured and simulated exfiltration of staged data is performed.

Staged data is created in line with the risk assessment and approved by the target organization before any action is taken.

Actions on Target
Gaining further access to compromised systems and reaching targets previously agreed upon. This phase is carried out within the scope and scenario / objectives approved by the organization.

Ransomware Red Team Life Cycle



Target Compromise
Targets are compromised using predetermined scenarios and attack paths.

Control and Movement
After successfully compromising an initial system within the environment, attempts are made to escalate the initial attack by moving laterally across the network. This process involves probing the compromised system(s) and the surrounding network environment for other vulnerable points or high-value targets, such as servers containing sensitive data, critical business applications, or systems with elevated privileges.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 537SVB 07-2025

STROZ FRIEDBERG
A LevelBlue Company

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 537SVB 07-2025