SERVICE BRIEF FOR

RANSOMWARE RESPONSE

Ransomware is a type of malicious software that infects one or more systems and blocks users' access to them until a ransom is paid. The use of ransomware variants has been observed for several years by threat groups that attempt to extort money from victims by displaying an on-screen alert.

In the event of ransomware or a suspected ransomware event, we will work with you to collect evidence and perform an in-depth investigation with minimal disruption to your business flow. We will interface with any additional groups to support your best outcome against ransomware and ransomware groups.

BENEFITS

- Support for your organization with any legal reporting, litigation, or cyber insurance considerations.
- The fastest approach to achieve a return to operations while still ensuring a thorough investigation of the incident aligned with business objectives and regulatory concerns.
- Identification of malicious activity and validation that threats and threat actors have been eliminated from your environment.
- Answers surrounding the malicious activity and impact on your environment, ensuring you have the information you need to know the threat has been eliminated and how to protect yourself from future attacks with the same vector.
- Demystification of threat actor tactics, techniques, and procedures (TTPs) and responding to ransomware demands with poise and confidence.
- Weekly updates from forensics experts and a comprehensive report that includes a timeline of the events surrounding the attack. We will work closely with your team to give visibility and answer questions throughout the progression of the incident, which will inform business decisions and provide final findings to support internal and external reporting needs.

OVERVIEW

Lodestone's Ransomware Response equips organizations that have been targeted by ransomware with the knowledge and confidence to respond and recover quickly and effectively. A Case Lead supported by a team of Lodestone experts uses industry-standard forensic techniques to preserve evidence and identify the type of ransomware that has affected your organization and the modus operandi of the associated ransomware group.

We evaluate the impact of the attack on your environment and discover what data may have been accessed or exfiltrated by an unauthorized party. We help you get to the bottom of how the attack occurred, what malicious activity took place within your environment, and what recovery options are available with or without paying the ransom.

WHY LODESTONE

Lodestone is a global cybersecurity firm committed to helping clients prevent, investigate, and prepare for security incidents. It was built from the ground up to offer an innovative, behavior-based approach to proactive cybersecurity and digital forensics and incident response (DFIR). We are comprised of top investigative talent and offensive security experts from several of the world's largest cybersecurity firms, as well as military veterans and former members of national security organizations, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). We combine this expertise with our unique understanding of legal requirements through our relationship with our parent company, Beazley, which has been at the forefront of cyber insurance for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while preventing, preparing for, and responding to some of the toughest security challenges that industries face today.

Compliance
Since its founding as a subsidiary of Beazley in 2017, Lodestone has offered its customers insight into both cybersecurity and the cyber insurance industry. We help companies align and stay compliant with cyber insurance coverage requirements. In addition, we offer discounts to channel partners to form long-term relationships.

Security Focus
Lodestone's experts live and breathe cybersecurity and are committed to helping customers face some of the biggest challenges of their careers. We do not sell vendor security products – our offerings are purely service-focused, and any third-party tools we recommend are the product of genuine, vendor-agnostic, and tested endorsement, not business deals.

Expertise
Lodestone's approach to Incident Response is to have the top cybersecurity experts in the world, as the lead, and as the touchpoint, when responding to cybersecurity incidents. This is done with the backing of comprehensive, real-time threat intelligence to provide clients with protection across the life cycle of a potential security event or incident.

Tailored Approach
We understand the individual challenges of every situation and consider the human side of the equation, never taking a "one size fits all" approach. We blend design, threat intelligence, and technology with human insights to provide clients with the greatest cybersecurity advantage.

Threat Intelligence
Our deep understanding of threat actor tactics, techniques, and procedures (TTPs) is based on decades of experience in DFIR and the diligent gathering of threat intelligence from all possible sources.

Agility
Time is of the essence before, during, and after an intrusion. We stand ready to move in quickly and effectively at the first sign of an intrusion.

Team Experience

1000+
ENGAGEMENTS

200+ YEARS
COMBINED EXPERIENCE

50+
CERTIFICATIONS

Experts Unlike Anyone Else

EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

Lodestone Ransomware Response includes forensically sound evidence collection, expert analysis of evidence sources, clear communication of findings, and an understanding of the incident.

The Ransomware Response is comprised of these primary phases:

- Initial Response - We work with you to determine the scope of the environment, our initial impressions of the breadth of impact on the environment, business objectives, and steps that have been taken before we arrived to support the incident response.
- Incident Containment - We advise on the quickest path to stopping the threat actors from continuing their activity and additional damage being done to your environment. This occurs through the deployment of tooling and configurations with insight from our experts.
- Mitigation – We work with you to put controls in place to ensure the containment efforts are bolstered by actions to prevent further disruption during the response and restoration of the environment.
- Recovery – We advise you on the recommended actions necessary to restore the environment to not just a pre-incident, but a safer one.
- Evidence Collection – We work with you to collect the necessary evidence to complete the analysis and give you the answers you need. We provide several methods for this for ease and to prevent keeping your team from the important work of getting you back up and running. We use industry-standard tools and software and provide all necessary handling steps to address any legal considerations.
- Investigation
  - We analyze the evidence* collected to find all available indicators of compromise to achieve the objectives of the engagement.
  - We provide contextualization of the analysis to describe how the attack chain occurred and uncover as much information as possible about the timeline and progression of the incident.
  - We communicate with you to inform you not only of our progress, but also of any significant findings that can either help with intermediate actions or posture for future actions that may be necessary.
  - We provide the most thorough answers possible based on evidence as to how the incident was executed, what the total impact and scope of the incident were, and how to take steps to prevent future recurrence of similar attacks.
- Reporting – We provide a written final summary of the investigation with a concise description of the findings and details of the investigation for any historical preservation and reporting requirements you may have.
- Case Conclusion and the Way Forward – At the end of the investigation, we provide you with industry general cybersecurity best practices to aid you in moving forward. We remain available to deliver other services to further harden your environment

*Evidence Examples

While the total list of ransomware evidence items is ever-expanding with new technologies, these are the most common examples of evidence we collect during our investigation phase:

- Physical drives from workstations or servers
- Logical forensic images of workstations or servers
- Copies of security appliance logs (e.g., firewalls, network device management suites, VPN devices, copies of server logs)
- Alert histories from antivirus and endpoint detection solutions
- Threat actors lists of any claims surrounding data exfiltration
- Other sources of evidence as applicable that provide context or support of the investigation

DURATION AND DELIVERABLES

The Ransomware Response varies in duration based on the size of your environment, the number of affected systems, and evidence delivery times, but typically takes four to six weeks. It can be delivered on-premises or remotely.

As part of the engagement, Lodestone will provide any or all of the following upon request:

	**Executive Summary Report** – A high-level summary report that provides an overview of the ransomware attack, including key findings identified during the investigative process.
	**DFIR Report** – A detailed, technical breakdown of how the threat actor operated within your environment, including a granular list of affected systems, locations, and user accounts, in addition to the information provided in an Executive Summary Report.
	**Executive Debrief** – An overview of the investigation and key findings presented in person or via video conference with our Case Lead.
	**Best Practices Overview** – A generalized list of best practices that can help you strengthen your security posture against future attacks.

Learn more at www.lodestone.com

Connect with us:

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com