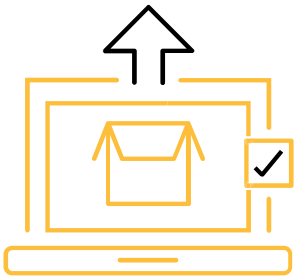
Lodestone

SERVICE BRIEF FOR

BEC INVESTIGATION



Lodestone's experts have extensive experience in business email compromise (BEC) cases for myriad types of mail environments, including on-premises Exchange and cloud-hosted email configurations. We will collect evidence, perform a thorough analysis, and provide regular updates and findings throughout the investigative process.

In addition, the bespoke tools and experience at our disposal enable us to provide some analyses for specific email environments at fixed-fee rates.

BENEFITS

- Gain an overall understanding of the incident, including the initial threat vector and what data a threat actor may have accessed or stolen from your environment.
- Consult with security experts with years of experience on how to audit and harden your email tenant and prevent future BECs.

OVERVIEW

Lodestone's BEC Investigation focuses on any threats or breaches within your organization's email platform, whether a custom, on-site solution or a popular commercial tenant such as Outlook or Gmail. Our experts provide you with a detailed understanding of how a threat actor may have accessed one or more accounts and the actions performed using those accounts.

Lodestone analysts have deep experience handling countless cases of fraud, spam, and payment redirections, and bring you knowledge, clarity, and solutions in the face of a disruptive compromise.

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

A BEC Investigation is comprised of these primary phases:

- Initial Response – Lodestone works with you to determine the scope of the BEC, including accounts compromised. We gain an understanding of your environment, the breadth of its potential impact on your company, your business objectives, and the steps that have been taken prior to our arrival.
- Incident Containment and Mitigation – Lodestone experts advise you on the fastest path to stopping the threat actors from performing more malicious activity and doing additional damage to your environment, including spreading outside of the email tenant if they have not already done so. We support you with the deployment of tooling and configurations with our expert insights and put controls in place to prevent further disruption during response and restoration.
- Evidence Collection – Our experts work with you to gain access to your email solution, collect evidence, and complete analysis that gives you the answers you need. We provide several methods for this to minimize the time your team must divert from the important work of getting your company back up and running. We use industry-standard tools and software and perform all necessary handling steps to address any legal considerations.
- Investigation – Lodestone analyzes the evidence collected to identify available indicators of compromise. We provide contextualization to the security incident, including determining, if possible, how the threat actor initiated the BEC, how many accounts were compromised, the malicious activity performed, and what data may have been accessed or exfiltrated.
- 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.
- Conclusion and Recovery – Lodestone answers your lingering questions and provides general industry best practices for cybersecurity to move your company forward. Throughout the engagement, we also work with your personnel to advise on a plan of action that can restore your email tenant to not just its pre-incident state, but a safer one.

DURATION AND DELIVERABLES

BEC Investigations vary based on the size of the tenant and the accounts potentially involved. However, this typically takes a period of one to two weeks.

As part of a BEC Investigation, 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 BEC, including key findings identified during the investigative process.
	**Digital Forensics and Incident Response (DFIR) Report –** A detailed, technical breakdown of how the threat actor operated within your email tenant, including a granular list of affected systems 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 attack.

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