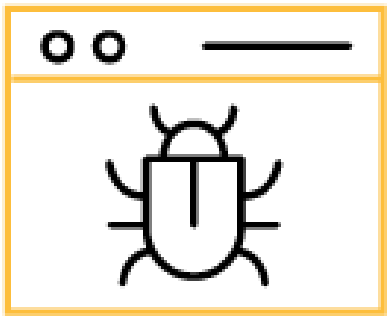
Lodestone

SERVICE BRIEF FOR

PHISHING CAMPAIGN ASSESSMENT



Lodestone's Phishing Campaign Assessment prepares your personnel to combat one of the most common initial intrusion vectors used by threat actors. Threat actors use phishing to imitate legitimate online services, other businesses, or individuals to manipulate their victims into clicking malicious links or downloading malicious files that could enable unauthorized network access or a data breach.

Our assessment measures your employees' susceptibility to email phishing lures that are commonly used to steal sensitive information or obtain initial, unauthorized access to a network. Arm yourself to understand your employees' security awareness and identify critical areas where additional training and planning can strengthen your security posture.

BENEFITS

- Decreasing security risks to your organization due to social engineering attacks involving human manipulation and deception.
- Increasing employee awareness to form a solid first line of defense against malicious emails. Fostering a strong security posture and ensuring that everyone is accountable for making policies, procedures, and tech solutions genuinely effective.
- Fulfilling your organization's regulations and standards, conducting regular training sessions for employees and monitoring the effectiveness of such training sessions.

OVERVIEW

Lodestone's Phishing Campaign Assessment measures your company's susceptibility to the phishing emails that are often used to steal sensitive information or provide an initial access point into a network via a malicious link or attachment. Our experts give you the experience of a realistic phishing campaign without the risk to your organization, gathering critical metrics at every phase of the attack, including the number of employees that opened the phishing email, clicked the malicious link, and submitted user credentials.

The information gathered during the campaign's initial phase is compiled into a report describing the number and details of each email sent, along with the statistics of how many employees opened, clicked, and submitted user credentials.

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's Email Phishing Campaign Assessment simulates a real-world phishing scenario to identify personnel security awareness gaps. The assessment aims to understand whether employees can identify a suspicious or malicious email and what action they take upon identifying it.

Lodestone employs a standard methodology that includes the assessment in multiple phases:

- Information Gathering and Open-Source Intelligence - Gathering as much information as possible about the target. Lodestone can either conduct a black box-style campaign or an open-source intelligence (OSINT) gathering to obtain employee email addresses, names, and roles to develop relevant pretexts for phishing emails. We will also work collaboratively with you to design the right phishing campaign to meet your testing needs.
- Attack Planning and Pretexting - Lodestone engineers register a phishing domain and configure the DNS zones for the SMTP provider. The planning phase also includes generating SSL certificates and creating a users list in the SMTP provider. Configuration of the phishing campaign launch instance and the development of an appropriate HTML "lure" also occur in this phase. Finally, we develop an HTML credential-stealing landing page or education page to capture user-typed credentials.
- Phishing Campaign Execution - Once the above phases are complete, Lodestone engineers execute the actual campaign and monitor the results. Phishing emails are sent out in a phased manner over a period of hours or days, depending on the number of employees in scope, and the email campaign stays open and active for typically one to two weeks to ensure the email is seen by all intended recipients.
- Reporting - Reports are a crucial step in a phishing campaign assessment as the cornerstone deliverable that provides meaningful insights regarding your organization's security posture, especially the human element. Our experts share the campaign results so you can use them to develop or enhance your security awareness training. We are also here to guide you in developing more mature security awareness training as well.
- Report Review - We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

ENGAGEMENT ARTIFACTS

This is the information that we gather based on how the engagement is scoped:

- A list of client personnel that were targeted
- Credentials gathered through the campaign

DURATION AND DELIVERABLES

The Phishing Campaign Assessment varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement:

	**Weekly Status Reporting –** Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
	**Executive Summary Report –** Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable.
	**Final Report –** After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings.

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