Trustwave®

DATA SHEET

Trustwave SpiderLabs® Phishing Service

ADVANCED PERSISTENT THREATS START WITH SPEAR-PHISHING BASED ATTACKS

Phishing is an attempt to trick a targeted user or a group of users into opening a crafted e-mail with the goal of eliciting sensitive information or, through the executing of an attachment, gaining unauthorized remote access to the targeted environment. Attackers love phishing and rely on spear-phishing to get into organizations' trusted networks.

Trustwave Phishing service methodically, iteratively, and quantitatively assesses the human factor of security by determining the susceptibility of the target workforce to social engineering and phishing attacks. Due to the nature of phishing and its high success rate, Advanced Persistent Threat (APT) attacks are almost entirely dependent upon phishing techniques to gain a foothold into the organization.

Trustwave SpiderLabs Phishing Service

The Trustwave SpiderLabs Phishing Service is a practical testing exercise to determine the organization's resiliency to the emergent attack vector of social engineering and phishing attacks. As organizations harden their perimeter to keep intruders out, direct attacks against the external network are becoming increasingly difficult and impractical.

It is easier for an attacker to use attacks targeting an organization's users to gain access to internal systems. Through phishing techniques an attacker can either execute code on the victim's local system, or trick the victim into divulging sensitive information such as credentials or payment information.

Our Phishing Service exercises actively help validate the users' adherence to acceptable use policy and security awareness in addition to validating the performance of key security infrastructure systems.

The Trustwave SpiderLabs Phishing Service results in an in-depth test of targeted users and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target workforce.

At a high level, our unique methodology incorporates the following:

1. **Organizational Intelligence:** Trustwave can be provided with email targets, or to simulate a real attack, Trustwave can do research on the Internet (open-source intelligence or OSINT) and in various public databases about the organization and compile a list of targets.
2. **Pretext and Campaign Design:** The pretext is designed by Trustwave, based on the OSINT, with input by the client to remove as many suspicions, inhibitors, and natural reluctances as possible on the part of the victim while simultaneously providing motivation to take an action.
3. **Attack Delivery:** The attacks may consist of client-side attacks, or collection harvesting through a phishing, or spoofed website. All communications between the target and the tester are secure.
4. **Data Extraction and Credential Testing:** The focus of this portion of testing will be on unauthorized access to sensitive systems, or data such as PII or CHD. This will allow the company to gauge the actual business impact and risk it faces as a result of this attack vector.
5. **Deliverables:** The deliverables will be both strategic and tactical in nature, presented in a format that is highly accessible to both management and operational staff.

Trustwave®

For more information: www.trustwave.com