THE PHISHING LANDSCAPE

Today, regardless of the maturity and periodicity of a company’s security awareness plans, social engineering remains the number one threat in breaching security defences. In some cases, threats originate from unintentional negligence of employees, giving access to or choosing to divulge sensitive information. The evolution and combination of various techniques requires even non-technical employees to stay vigilant and improve detecting attacks. To respond to this, companies need to change their security awareness and email culture.

KEY FACTS

- **$3B** The cost to businesses of phishing scams in the last 3 years [1]
- **45%** The percentage increase in phishing scams for Q4 of 2017 alone [2]
- **400** No. of businesses targeted by e-mail compromise scams every day [3]

OUR CAPABILITIES

To combat the growing threat of social engineering, Accenture provides Phishing as a Service: an Accenture run service that can be leveraged in an ad-hoc manner or integrated in wider security awareness and security testing projects. The service is built on top of an extensible, computational, power-aware and light-weight platform, that may be hosted without constraints depending on client operational and security requirements. The open-source and low-cost platform allows the execution of state-of-the-art social engineering campaigns with an easy-to-deploy solution, skilled resources and interactive drag and drop style reporting.

With Accenture’s expertise, it is possible to run tailored campaigns with different levels of credibility depending on past training performances and employee job roles. Phishing as a service can involve email-based campaign targeting, consisting of malicious attachments and links with fake login pages, but can also involve a phone or VoIP & IM based campaigns involving sophisticated scenarios and impersonation tactics. Ultimately doing so facilitates recommendations being provided to improve a clients’ security awareness and training program.