IRONSCALES Remediates Targeted Phishing Email Attack on Financial Services Company Through Automation and Awareness

The financial services industry is a prime target for cybercrime, with hackers targeting financial services firms 300 percent more than any other sector. A common and, frankly, simple method cyber criminals use to access an enterprise's confidential and personal information is through phishing attacks. In fact, phishing attacks surged by 250 percent in the first quarter of 2016 - the highest ever since 2004, according to the Anti-Phishing Working Group (APWG).

A financial services company requesting to remain anonymous, located in the United Kingdom, services both small and medium-sized businesses (SMB) and enterprises across Europe, the Middle East and Africa. As such, the company must comply with industry standards to ensure its company and its customers' data is secure. However, regulations are often far behind today's motivated and agile cyber criminals determined to hack into organizations' networks for financial gain.

IronTraps™ is a patent-pending, automatic phishing email incident response module, built to empower skilled and vigilant employees to report ongoing attacks, followed by an enterprise-wide remediation response.

While the company had traditional defenses in place, such as anti-virus, SandBox, Firewalls, IPS and spam filters, it recognized that these phishing remediation solutions were ineffective. Therefore, in early 2016, the company selected IRONSCALES as a means to proactively defend against phishing attacks and lead the company's anti-phishing awareness and immediate response effort. Employees underwent IronTrain – IRONSCALES' employee awareness program – in which its simulation program contains a comparable scenario in order to train employees to successfully navigate similar phishing, attacks. In addition, IronTraps, the automated phishing email response solution, was immediately deployed on all company endpoints.

The Attack

On July 11, 2016 at 10:58am, a malicious and sophisticated email phishing campaign targeted the financial services company, with the potential to spread to all of its employees, customers, third-party vendors and partners across the globe. The email's subject line was titled "**BAN009/0002 Bank of Ireland**" and contained an HTML file named '**Report_Template.html.**' In addition, the deceptive HTML file contained a perfect mockup page of a Microsoft Outlook Web Access (OWA) login page in an attempt to steal user credentials.

Once the email was opened and the file was downloaded, the attacker then had the opportunity to steal users' information. To do so, the attacker manipulated the email to cause some versions of Microsoft Outlook (2013) to crash. To reduce suspicions from currently logged-in users, a pop-up window appeared with the text "Due to version update logout was enforced" and the user were redirected to a fake OWA login page, created by the attacker, to submit his/her credentials.

The Response

Within five minutes of the first emails arrival, an employee reported the attack as suspicious through IRONSCALES active protection Microsoft Outlook button, a one-click process to the IRONSCALES system. At this point, 46 mailboxes were affected.

Immediately, IRONSCALES automatic remediation process was triggered and **IronTraps** automatically deleted the suspicious email from the 46 affected mailboxes and prevented spread of the phishing attack to any other mailboxes. During the seven minutes between detection and completion of remediation, IronTraps secured ALL mailboxes and protected ALL of the company's employees from unintentionally sharing credentials with the hackers. Ultimately, IRONSCALES completely removed the threat from all mailboxes in 12 minutes and prevented significant financial and reputational damages to the company.

IRONSCALES Automation and Awareness

Globally, phishing attacks have evolved from an occasional annoyance into a persistent epidemic. In fact, increasingly sophisticated and highly targeted phishing schemes have essentially transformed every enterprise employee into a primary threat vector. Most enterprises today are cognizant of the financial, reputational and even physical risks of phishing, however, few have modified their defenses to meet the complexity of the modern threat landscape.

IRONSCALES is the first and only multi-layered phishing mitigation & remediation solution to combine human intelligence with machine learning for enterprise cybersecurity. Its technology automatically protects enterprises in real-time from the financial, reputational and physical damages of targeted phishing attacks.

IRONSCALES ensures that employees are prepared to take an active role in protecting the integrity of their organizations, while reinforcing their efforts with technology that can automatically defend enterprises from attacks in real-time.