Case Study: UK Aerospace
Egress Intelligence anti-phishing solution

Security before Egress Intelligence anti-phishing solution

The customer works in the growing UK Aerospace industry. The company is experiencing rapid growth and liaises with a wide range of partners due to the nature of its mission. As a member of the aerospace community, the company is very concerned with both the physical and digital security of its hardware, operational sites, network infrastructure and staff. To strengthen its overall security posture, the company aimed to find a solution that would work seamlessly with Microsoft Office 365, protecting against all types of phishing attacks and also improving email hygiene. This was important, as some phishing attacks had already got through to users' email inboxes because employees had no consistent mechanism to identify deceptive emails.

Before deploying the Egress Intelligence solution, the customer had implemented spam and malware filtering and was conducting extensive phishing awareness training. Despite these efforts, the phishing attacks continued to arrive in users' email inboxes with the potential for an account or network compromise just a short step away.

Cloud email solutions like Office 365 are increasingly replacing a wide range of traditional email solutions, and provide a wide range of business-essential services such as email, chat, document management and project management.

While these solutions have many business benefits, the downside is that they give cyber criminals and ilicit state actors a greater attack surface to compromise users and steal company confidential information.

Recognising this increased risk, our customer started researching the email security market for a solution to specifically detect advanced phishing attacks. A tweet from the UK National Cyber Security Centre (NCSC) highlighted this advanced capability from Aquilai, a Cheltenham-based UK company with links to GCHQ. Aquilai's participation in the NCSC's Cyber Accelerator program resulted in a highly effective solution for mitigating email phishing: Egress Intelligence.

The Egress Intelligence demo

The customer's IT team found that the effectiveness of Egress Intelligence was due to its unique detection technology combined with the ability to alert and inform staff in real time. The customer was also impressed by the ease of deployment, which took around 30 minutes and offered immediate protection for all staff.

The technical team was particularly drawn to the solution's machine learning capabilities, and to its ability to inform users in real time with coloured banners when deceptive emails are detected. Egress coloured banners are "clickable", and open up to a threat display page where the user can see a more detailed breakdown of the reasons for the classification. Thus, users receive real time awareness training of phishing threats which were targeting them, making learning more relevant and enhancing company's cyber defence culture.

Implementing Egress Intelligence

Our customer shared with us that the deployment of Egress Intelligence was entirely seamless and completed in under 30 minutes in a single install session. Initially just the technical team was placed in the Egress Intelligence user group. However, after technical stress tests and performance evaluations, the remainder of the users were added into system with a single click.

Egress Intelligence employs a colour-coded banner system to alert users to threats. Following the latest academic research on psychological best practices, the solution helps users stay alert while avoiding "banner fatigue". The banners are coded red for dangerous, amber for caution and blue for advisory. This capability enables users to make informed decisions before acting on an email, thereby providing staff with real-time awareness, irrespective of the device or client used, whilst being able to report deceptive emails for further analysis.

Users commented positively on the accuracy and the detail available on the threat display page. Users felt they had a good understanding as to why certain emails might be dangerous. Even advisory banners provide useful information such as first time sender alerts, and if the email came from an external domain. Many users felt that they became more productive as mobile emails were trusted, such that mobile working became safer with Egress Intelligence deployed.

Customers can tailor the solution to provide a best fit for their particular organisation with regards to banners displayed, email delivery or quarantine, in line with compliance processes for their organisation.

Initial observations of Egress Intelligence

An unexpected bonus for this particular customer was that the Egress deployment process identified poor email hygiene with automated emails still being sent to third parties from systems that were supposedly decommissioned.

Secondly, Egress Intelligence detected those employees using their own personal emails in the workplace, which was prohibited, thereby enabling the security team to remind users and enforce the correct workplace policy. The advisory blue banners can be turned on or off at an admin level, but our customer took the view that user awareness was key in regard to the threats which may target this organisation, and a higher level of awareness would improve its defensive posture.

Living with Egress Intelligence

The users report that they appreciate and feel secure due to the colour-coded banners that Egress Intelligence inserts into external emails. They noted the solution is very accurate, with very few false positives. The consistent user experience across mobile and desktop email applications is particularly appreciated, as staff are also protected from phishing attacks when using their mobile, tablet, laptop or desktop.

Additionally, links in all external emails are re-written and a warning page is displayed for those users who click onto a link. Another tangible benefit for the IT team is that since the install has been active, email related call volumes and tickets to IT have dropped substantially. Within the first week, Egress Intelligence caught a phishing campaign specifically targeting the customer's organisation, including a zero-day Office 365 credential phish. The ability of Egress Intelligence to detect novel phishing attacks is a unique capability now present within the UK market.

The customer stated Office 365 credential phishing is one of the biggest threats, in addition to spear phishing against the executive team. Egress Intelligence has been able to negate the success of these attacks.

If you haven't already done so, Northdoor urges you to take the first step in fully securing your organisation's cloud-based email now. Whether it be Office 365 or G-Suite, schedule a demo today.

For more information contact, Northdoor:
www.northdoor.co.uk
info@northdoor.co.uk
Telephone: 0207 448 8500