AQUILAI

CYBERINTELLIGENCE

CASE STUDY - UK AEROSPACE

Security before AQUILAI

The subject of this case study is a UK Aerospace company. They work with a wide range of partners due to the nature of their mission. They were growing fast, and became increasingly concerned with regards to both physical and digital security.

They had a duty to protect their hardware, operational sites, network infrastructure and staff from compromise. Their key security challenge was finding a solution which could work seamlessly with Microsoft Office 365. They'd been targeted by phishing attacks before, and needed a system that could not only protect against all types of attack, but also improve their overall email hygiene.

Stage 1: Discovery

Employee Challenge - They realised that the first step to preventing attacks was enabling their employees to consistently identify phishing threats. They'd previously implemented Spam and Malware filtering, and were conducting extensive phishing awareness training. Despite these efforts, phishing attacks continued to gain access to their employees' inboxes, and they knew that another potential account or network compromise was just a short step away.

Software Challenges - The company, like an increasing number of fast growing organisations, run primarily on Office 365. While these cloud solutions have many benefits, the downside is that they give cyber criminals and state actors a greater attack surface to work on, and make it easier to steal confidential company information. Recognising this increased risk, the company started researching the email security market for a solution to specifically detect advanced phishing attacks.

Stage 2: Research

A tweet from the UK National Cyber Security Centre (NCSC) highlighting the advanced capability solution they were looking for led them to: Aquilai. Aquilai is a Cheltenham based UK company with strong links to GCHQ through their participation in their Cyber accelerator program, resulting in a highly effective solution for mitigating email phishing called "Ajax Intelligence."

Testing - During their investigation, the company's IT team found that Aquilai's Ajax Intelligence effectiveness was due to its unique detection technology combined with its ability to alert and inform staff in real time. They felt that Aquilai's seamless blend of Machine Learning and intuitive coloured warning banners were both effective and user friendly. During the demonstration, they were particularly interested in how Ajax's clickable banners opened up a threat display page, allowing users to see a more detailed breakdown of the reasons for the classification. This worked towards the company's overall security goal, fixing the weakest link by providing employees with real-time cyber threat training.

Stage 3: Implementation

The company found deploying Ajax intelligence seamless, installing it in around 30 minutes in a single session. Initially just the technical team was placed in the Ajax Intelligence user group, however after technical stress tests and performance evaluations, the remainder of the users were added into the system with a single click. They also were able to tailor their solution to provide the best fit for their needs, with control over what banners were displayed, email delivery and quarantine, and more, in line with compliance processes for their organisation.

Ajax Intelligence employs a colour-coded banner system to alert users as to the general threat of the emails they see. The three-colour system had input from NCSC's socio technical team, based on the latest academic research on the psychological best practice to keep users alert to threats using innovative graphic representations whilst avoiding "banner fatigue". Aquilai based the banner colours on Red for dangerous, Amber for caution and Blue for advisory. This capability enabled the company's users to make informed decisions before acting on an email, providing staff with real time awareness, irrespective of device or client used whilst being able to report deceptive emails for further analysis.

The company found an unexpected bonus from the deployment of Ajax. The process identified poor email hygiene with automated emails still being sent to third parties from systems that were supposedly decommissioned.

Stage 4: Psychological Shifts

In the first few months, the company noted a few key shifts in their workforce habits. Ajax Intelligence detected that some employees were using their own personal emails in the workplace, which was prohibited. This enabled the security team to remind users and enforce the correct 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 their defensive posture.

Employees commented on the accuracy and the detail in the threat display page, feeling that they were developing a good understanding as to why certain emails might be dangerous. Even advisory banners provided useful information such as first time sender alerts, and whether or not the email came from an external domain.

Many people in the test group even felt that they became more productive, as mobile emails were now able to be trusted so mobile working became a possibility.

Stage 5: Living with Ajax

The company reported that users felt more secure with the colour-coded Ajax Intelligence banners in their emails. They noted the accuracy and seamlessness of the solution, with consistency being appreciated across mobile and desktop. All external email links were re-written and a warning page was displayed for those users who clicked onto a link. The IT team also discovered that since Ajax was installed, email related tickets to IT dropped substantially.

The real benefit came within the first week, when Ajax Intelligence caught a phishing campaign specifically targeting their organisation including a zero-day Office 365 credential phish. The ability of Ajax Intelligence to detect never before seen phishing attacks is a unique capability now present within the UK market, and the company felt the value immediately.

They stated Office 365 credential phishing as one of the key threats for them alongside spear phishing against their executive team. Ajax Intelligence was unparalleled in defending against these attacks. If you haven't already done so, Aquilai would urge you to take the first step in fully securing your organisations cloud-based email whether it be Office 365 or G-Suite. — schedule a demo today