Case Study: Cheated by the Chairman

Retruster Stops Well-Disguised Phishing Email Designed To Deliver Malware (BEC attack)

The Unfolding Of Events

A senior member of the finance department of a well-known financial services company received an email from the Chairman of the Board, containing certain urgent yet confidential information. This email, which looked completely legitimate in every way, was in fact a cleverly disguised phishing email, created and sent by malicious actors based abroad. The email contained a form of malware such that if a file in the email was opened, the entire company would be infected by ransomware, its data compromised and exfiltrated, with the concomitant costs and embarrassing headlines.

Potential Impact

It has been estimated that a successful phishing attack such as this would have cost the organisation around £2.9m. This does not include the impact on the goodwill of the company, the reduction in confidence from its customers, the reputation of being associated as a victim of such an attack, and how future business would be affected. Sensitive user data would be compromised, and this personal information would likely be sold on the Dark Web to the highest bidder. The company would not be able to render its full services for hours if not days. Necessary investigations and remediation would ensue, regulatory bodies would be involved, and there would be investigations into potential breaches of legislation such as the General Data Protection Regulation (GDPR) as well as contraventions of local laws and regulations.

The Email

The phishing email itself was well-researched and constructed. It appears the attackers researched both the sender and the recipient, undertaking deep analysis of such elements as their relationship, writing styles and pressing issues that the company was dealing with. This resulted in a compelling, natural and authentic-looking email, complete with personalised content. The email was kept short so as to minimise opportunities to spot errors. The email also contained sophisticated subterfuge aimed at evading common security tools, and indeed succeeded in getting through such products' checks before being stopped by Retruster. The security checks that were evaded include those of both the native email client and 3rd-party software.

Case Study: Cheated by the Chairman

Retruster's response

Retruster's proprietary algorithms immediately identified this fraudulent email. The recipient was warned that this email was a fake. Disaster was thus averted, and subsequently an email went out to all employees to alert them to the tactics used. Another, rival company was not so lucky. A well-known competitor to our financial services company, who did not have Retruster installed, were fooled by an email sent by the same malicious actors. The attack was successful. The ransomware was deployed, and the company's files were inaccessible for several hours after data was encrypted. A ransom was demanded for the decryption key (amount currently unknown), and despite a ransom payment, company data began to show up for sale a few days later on the Dark Web. What followed was frantic activity involving forensic investigators, legal teams, reports to stakeholders, emails to customers informing them of the breach and requesting they change all passwords, legal action brought against the company, and not a small amount of very bad press.

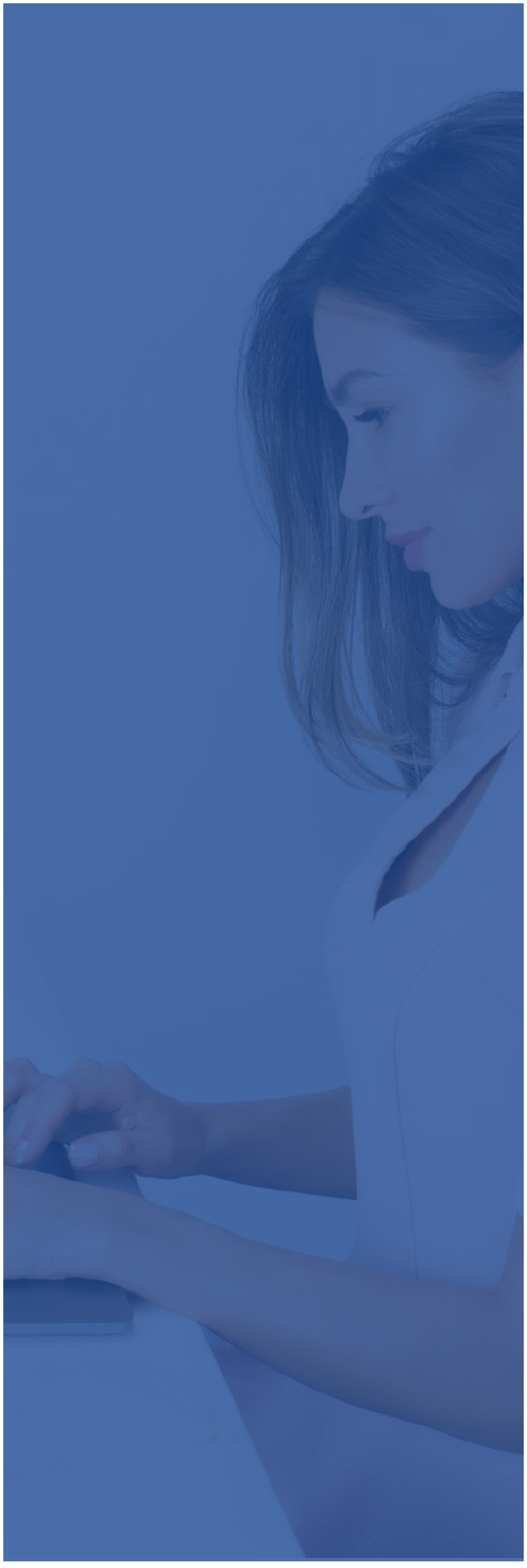
Staying Safe

Protecting individual users and the organisation in general requires a few key actions, such as ensuring the latest versions of software are used, and that services are patched and up-to-date. One of the most important areas to secure is the email function. Email is generally a company's most exposed interface with the outside world. Anybody can send any user an email, and malicious actors have the resources to take advantage of this. With over 90% of cyber attacks originating with a phishing email, it makes sense to tackle this vector first. Installing Retruster goes a long way to ensure the organisation's email function is protected.

"Installing Retruster goes a long way to ensure the organization's email function is protected."

Retruster

Next generation online protection



Security starts here

How do over 90% of cyber attacks start?

With a phishing email. Ransomware, malware, financial fraud. All from phishing emails. These emails are getting more sophisticated, and the tools available just can't keep up. These tools grew out of the anti-spam world of the 90's and are generally rule-based, slow to respond, require massive servers, and are ill-equipped to deal with modern threats. Attackers are agile: leveraging automation, artificial intelligence and machine learning.

Isn't it time those tools were used against them?

The right to know

How do you know if an email is legitimate?

Answer: you don't.

With around 15% of phishing emails getting through the well-known email security products, you're taking a chance every time you open an email. If an email is not stopped by these solutions, it's trusted by the end user. There's no last line of defense, no further information given, no safety net.

Introducing Retruster

What is Retruster?

Retruster is the next-generation in email protection. It's a product that's purpose-built to protect against phishing emails, leveraging the latest technology: including Artificial Intelligence and Machine Learning.

Crucially, it connects this proprietary advanced technology to the user in a meaningful way – resulting in a solution that is seamless, effective and intuitive.

The Retruster advantage

Your last line of defense

Retruster truly is a last line of defense. A user thinks that phishing emails that got through filtering solutions are automatically safe. Retruster keeps them aware & protected.

Previously Unseen First-time Threats

Other solutions classify emails as they go through their servers. Now malware automation means classification is becoming irrelevant as malware mutates constantly, meaning no two instances are alike. Retruster's architecture enables it to deal with Previously Unseen First-time Threats.

"Retruster truly is a last line of defense, keeping users aware & protected – constantly."

Benefits of Retruster

- Effective immediately
- No settings changes
- No changes to DNS or MX records
- Seamlessly integrates with Microsoft Office 365 and Google G Suite
- Supports cloud, on-prem, hybrid
- No disruption, ever
- Completely seamless
- No ongoing maintenance required
- No manual rules or exceptions, everything completely automated and smooth

Works with existing solutions

No need to "rip and replace". Just add Retruster to your current stack, it's as simple as that. Retruster can be deployed as a standalone product, or together with other well-known email security products to provide comprehensive – and much needed – specific advanced anti-phishing capabilities and the most robust security posture possible.

The proof is in the thousands of phishing attacks that Retruster has stopped that evaded well-known solutions when Retruster is deployed together with these products.

Retruster customers

Retruster protects organizations large and small across the globe. Financial institutions, healthcare providers, manufacturers, educational institutions and other organizations in every industry benefit from Retruster protection. With thousands of phishing attacks stopped, millions of dollars saved, and a loyal customer base, Retruster continues to add value to its clients every single email.

About Retruster

Retruster's mission is to protect those vulnerable against the threats of malicious actors. Not enough was being done by existing products, and too many innocent individuals and businesses were exposed and being taken advantage of.

Retruster leveraged its founding team's deep technical knowledge and experience to provide a solution that levels the playing field and utilizes advanced technology to provide continuous and effective protection against cyber threats.

Retruster is privately owned and operates in most countries worldwide.