IRONSCALES
STOPS POLYMORPHIC PHISHING ATTACK

Targeted phishing attacks continue to bypass gateway security controls to arrive into employees' mailboxes in every organisation around the globe. While an external email address may arouse suspicion, when the message appears to come from a colleague it's easier for others to fall for the attacker's scam. That was the experience of one organisation earlier this year.

WHAT IS POLYMORPHIC EMAIL PHISHING?

Polymorphic email phishing is a phishing email sent to multiple users where at least one of the following is being changed either randomly or manually/intentionally depending on the attack.

- Sender name
- Sender address
- Subject
- Greeting
- Email body or signature

BACKGROUND

An international construction business, employing thousands of people within the UK, was targeted by a polymorphic phishing attack in January 2018.

Sent to just a handful of employees, the phishing message with the benign subject header 'contract' evaded the organisations existing security controls to be delivered into the users' mailboxes.

Eyal Benishti, CEO and founder of IRONSCALES, explains, "Criminals are continuously evolving their phishing strategy to circumvent controls introduced to stop them. In this instance, by targeting only a few employees, the scammer could be confident that the volume of emails being received were unlikely to trigger any spam filters or other defences employed by the e-mail server. In tandem, the subject header used was deliberately vague, but likely to be relevant to the majority of recipients, so was likely to encourage users to at least open the message to find out what the communication was about. Morphing the email message is yet another advanced tactic to avoid detection and make the response process much more challenging"

<u>One employee that opened the message fell for the scam and the attack was triggered.</u>

IRONSCALES
STOPS POLYMORPHIC PHISHING ATTACK

THE ATTACK

Attached to the message was what appeared to be a pdf file, however opening the attachment triggered two elements to the attack:

Part 1 - Credential Theft: the user was presented with a pop-up claiming that an update was needed to read the attachment. Clicking the link redirected the user to a web portal where they were asked to enter their Microsoft Office credentials.

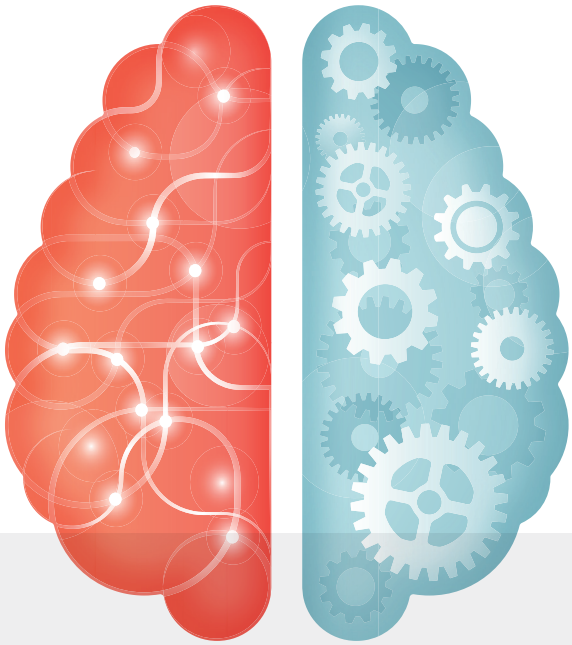
Part 2 - Further Messages: in the background, so concealed from the victim, the message was immediately replicated and sent to all users within the organisation, with moderate changes to the email body, attachment file name, sender and subject. As the sender was now a colleague, other employees were inclined to trust the message so were tricked into opening the attachment, giving away their credentials, and causing further messages to be sent. To avoid detection, with each subsequent infestation, the attachment employed polymorphic techniques – in this case changing the file-size with each iteration to avoid detection and eradication.

Eyal adds context to these events, "This type of polymorphic phishing attack is increasingly common and, once started, is almost impossible to stop.

Polymorphic phishing emails were designed to fool signature-based detection solutions and to make it harder to search and remove such emails from employee's mailboxes. Polymorphic emails perform slight changes to evade standard signature-based email security systems. The vast majority of email security are all essentially signature-based email security systems. That's problematic, because signature-based systems rely on email signatures to block the phishing email but with the constant evolution of email variants, these systems can't defend against new variants until some victims have already been infected and the new variant is identified and added to the black list or the specific signature already exists.

As the organisation found employees continued to fall victim to the scam, both entering their details on the phishing site and further spreading the malicious message. The IT team were unable to blacklist the sender given it was now being sent by internal employees. As the email was continuously changing this also couldn't be used. Although the IT team were sending messages to employees warning them not to open the messages not everyone adhered to the warning and so the attack was continuing to be spread."

IRONSCALES
STOPS POLYMORPHIC PHISHING ATTACK



NEUTRALISING THE ATTACK

The construction company had anti-virus and other security solutions in place, including email security modules from Symantec and Trend Micro, that it hoped would eventually detect and stop the attack. However, having struggled unsuccessfully to regain control for two days, the company was introduced to IRONSCALES [by Proact IT].

Eyal recalls, "For the company there was a significant risk of further elements to the attack from those users that had disclosed their credentials to the scammers. In addition, each time someone interacted with the message it was flooding the email system. With the email security tools unable to stop the attack, the internal messages warning employees not to interact with the message failing, and the IT team unable to remove the messages from the mail servers, IRONSCALES was approached and asked if it could help. Once we gained connectivity to the organisation, as unfortunately the company was not previously a customer, we deployed IronTraps and in just a few hours it stopped the attack completely."

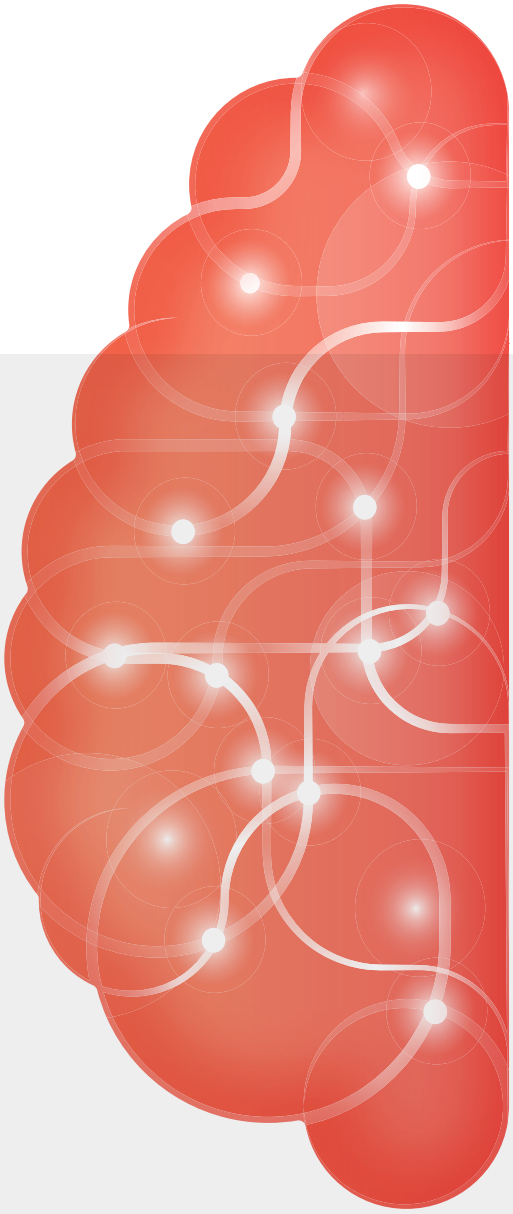
To defend against polymorphic phishing emails, your organization needs predictive email defence that protects against both known and unknown email phishing variants. Signature-based can only defend against known emails, leaving you vulnerable to all polymorphic email variants.

IronTraps provides advanced comprehensive email security that utilizes email phishing forensics, mitigation and remediation automatically or at the click of a button, while incorporating human intelligence with machine learning to increase detection of such evasive attacks by clustering similarities in the emails in real time, allowing smart detection and aggregation of polymorphic emails which can be remediated in seconds.

We use multiple layers of analysis to determine the safety of emails before and after they end up in your employees' inboxes. This allows us to defend against all email threats, including polymorphic email variations from these families.

IronTraps' email server-side remediation enables organisations to automatically detect and remove polymorphic emails before it can be engaged with by unaware employees. Available as both an on-premise and cloud-based email app, IronTraps facilitates enterprise-wide remediation, even for users not connected or logged in, providing real-time coverage to eliminate a threat in seconds.

IRONSCALES **STOPS POLYMORPHIC PHISHING ATTACK**



NEUTRALISING THE ATTACK

Eyal concludes, "In this instance, the message was imported and proprietary analytics performed. Having verified the message as malicious, IronTraps then connected to all mailboxes and automatically removed the malicious message enterprise-wide. This prevented anyone from opening further messages so stopping the attack in its tracks."

With the attack resolved the IT team were then able to work on limiting further damage. This included asking all affected employees to change their Microsoft Office credentials to prevent the scammers abusing these details.

As IRONSCALES was not installed prior to the first message arriving, it was unable to identify who was behind this attack nor what they were trying to achieve.