CASE STUDY

MARTIN ENGINEERING

IMPLEMENTING AUTOMATED SPEAR PHISHING PROTECTION WORLDWIDE

ATTACKS ESCALATE OVER THREE YEARS

Martin Engineering has over 800 employees in nine countries with about 25% of those in the US. The company provides bulk material handling services for mining, oil, pulp and paper and other industries. IT Manager Mike Komnick says, “We make moving bulk material, cleaner, safer and more effective.”

Komnick has spent 14 years with the company and six in the IT department. The company focus on business email compromise attacks such as spear phishing and social engineering started in 2014. “We used to get hit hard from emails CEO@ whatever domain. Send $600 to this account. Those emails were hitting us hard 2-3 years ago. We even had a wire transfer in process, but it was stopped in time, thankfully.” This led to the implementation of DMARC which helped but didn’t stop the attacks.

The company had another wake-up call just a year later. “We had a ransomware issue about two years ago. It was a remote user coming in through the VPN. We caught it in about three hours so the impact was limited. But, that led us into looking at the email problem more deeply,” said Komnick. “We have always tried to secure the perimeter to prevent intrusion from the outside first.” However, the company shifted its focus to a user based approach when more threats started coming in through email.

Komnick added, “We see attacks in waves. The phishing stuff is the biggest of our concerns. We were seeing more phishing emails coming in and I figured it was only a matter of time before users started to interact with them.”

PREVIOUS EFFORTS HELPED, BUT WEREN’T ENOUGH

The company had deployed DMARC as a first step, but that clearly was not enough because it didn’t stop the ransomware attack or the other frequent phishing attacks. So the company next tried employee training. “We partnered with a phishing training company in 2016. The initial phishing campaign showed about 20% of employees were phishing prone. After training that fell to 10%. We saw a significant decrease right away,” says Komnick.

But, that 10% figure still concerned Komnick who then initiated a trial with Graphus to test out an automated solution that didn’t rely solely on employee acumen to spot phishing attacks. What did he find? “Spear phishing attacks were three times higher than we thought we were seeing. I had no idea there was that much hitting our users.”

> “Spear phishing attacks were three times higher than we thought we were seeing. I had no idea there was that much hitting our users. Eye opening is a good way to word it. Shocking might be another way. We thought we had a better handle on it than we did.”
>
> \- Mike Komnick, IT Manager

> “Graphus gives you an additional layer of security that requires very little interaction so we can keep our work day moving along.” - Mike Komnick

GRAPHUS CLOSES THE SECURITY GAP

Komnick said, “The simplicity of the interface and the real-time email notifications are what drew me to the Graphus product initially. I was set-up and ready to go in minutes. The directions were concise and laid out perfectly.”

The Dashboard immediately drew Komnick’s attention. He logs in first thing in the morning and checks the threats. That offers him time to investigate issues before users see them. Throughout the day he relies on email alerts. Graphus is an automated system that enables phishing attack identification and the ability to investigate threats. Users can opt to automatically block suspected spear phishing emails or allow all emails through but alert an administrator to review suspicious communications. Users can see flagged emails in the dashboard and from automated email alerts.

Graphus founder and CEO Manoj Srivastava commented, “We caught over 25 spear phishing attacks in just the first month after Martin Engineering activated the Graphus software. These could have caused loss of login credentials or money through wire fraud. Graphus also stopped a malware campaign that included eight attacks using spoofed employee emails over 36 hours. A previous malware attack caused Martin Engineering three hours of downtime and even more hassle. We were happy that Graphus could help Mike Komnick’s team avoid those problems on this attack.”

When asked if he would recommend Graphus to his industry peers, Komnick responded, “I would definitely recommend the product. This gives you an additional layer of security that requires very little interaction so we can keep our work day moving along.”

martin® engineering

NO SECURITY ENGINEER NEEDED

“It’s always good to have another layer of protection. Especially with Graphus with the email alerts. We don’t have a dedicated security person on staff. Having that email alert and real-time response has been fantastic,” said Mike Komnick.

BY THE NUMBERS

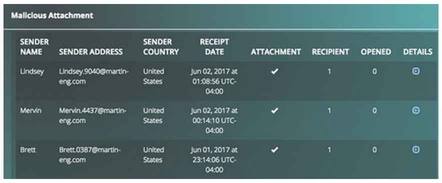
800
EMPLOYEES

500,000
EMAILS PER MONTH

25
PHISHING ATTACKS STOPPED IN A MONTH

8
MALICIOUS LINKS & ATTACHMENTS

SCREENSHOT



Malicious Attachment

SENDER NAME	SENDER ADDRESS	SENDER COUNTRY	RECEIPT DATE	ATTACHMENT	RECIPIENT	OPENED	DETAILS
Lindsey	Lindsey.9040@martin-eng.com	United States	Jun 02, 2017 at 01:08:56 UTC-04:00	✓	1	0	⊡
Mervin	Mervin.4437@martin-eng.com	United States	Jun 02, 2017 at 00:14:10 UTC-04:00	✓	1	0	⊡
Brett	Brett.0387@martin-eng.com	United States	Jun 01, 2017 at 23:14:06 UTC-04:00	✓	1	0	⊡

Three of the Malware Campaign Spoofed Emails Caught by Graphus

GRAPHUS

Graphus provides immediate protection and peace of mind by automatically identifying 99% of social engineering, spear phishing, and malware attacks. Graphus employs patented AI technology to establish a Trust Graph™ between people, devices, and networks to reveal untrusted communication and detect threats. Companies can activate Graphus in less than a minute. Graphus was founded in 2015 and is headquartered in Reston, Virginia.

o. 877-568-8875 e. sales@graphus.ai **graphus.ai**