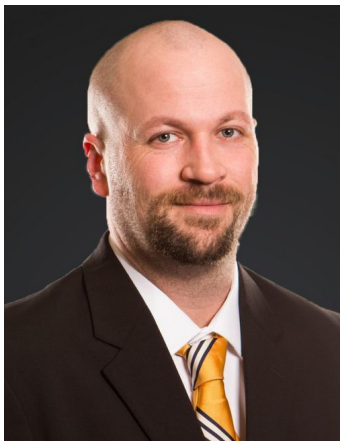
CASE STUDY

NEWK'S EATERY

AUTOMATED SPEAR PHISHING & MALWARE PROTECTION ACROSS 115 LOCATIONS

IMPLEMENTING DMARC, DKIM, SPF & TRAINING STILL WASN'T ENOUGH



Newk's Eatery is a leading next generation restaurant chain of fast casual with it's culinary-driven menu prepared in Newk's open kitchens. Newk's is based in Jackson, Mississippi and currently operates and franchises more than 115 units in 15 states. The award-winning brand is consistently named among Fast Casual's Top "Movers and Shakers" and was named to Franchise Times' "Fast and Serious" list for 3 consecutive years.

Adam Karveller, Newk's Eatery Vice President of Information Technology has been with the company for over 9 years. Karveller states, "Historically our focus on cybersecurity has been based around educating our business users on how to avoid potential virus/malware/rogue access points or other threats. We also focused on DKIM and SPF records however, when these solutions weren't able to fully protect us, we began to utilize the cumbersome DMARC framework to further secure our company's digital communications."

Unfortunately they found out that no amount of phishing awareness training and education in combination with DMARC, DKIM and SPF could fully protect their organization from the number of cyber criminals and scammers as the number of spear phishing techniques seemed to be increasing daily.

"We needed a tool that would provide another layer of automated security on top of all the other policies, practices, and security measures that were already in place. The tool would need to automate the prevention of a message reaching our business users or, in the event that it required human review, would allow any member of the IT team to easily monitor and quickly act on threats that may bypass other solutions," said Karveller. "We needed a platform that could be trained to recognize false positives and identify fringe and borderline scams that traditionally aren't detected by existing checks and security protocols."

ATTACKS INCREASED EXPONENTIALLY

Over the last two years, the frequency and sophistication of phishing attacks targeting Newk's Eatery has increased exponentially. Karveller states, "It can range from hundreds to thousands of attacks. Google's built-in policies and security tools do a decent job of isolating most to the spam folder however a large percentage still make it through." One of the more common types of attacks Newk's has received are spear phishing attacks against their Corporate Officers. Attackers review their 'About Us' section of their website and attempt to social engineer a wire transfer or money order by spoofing their CEO or CFO.

Prior to Graphus, Newk's Eatery had an instance where a spear phishing attack was successful and one of their business users provided their email login credentials via a form skinned to mirror a popular cloud software that Newk's Eatery uses. Within minutes, the attackers gained access to the users email account and their contact list and began automating phishing emails of a similar nature from this trusted account within their domain. Newk's security protocols caught the issue and were quickly able to isolate and remediate the threat however in a matter of five minutes, seven other users had clicked through on this phishing attack. "We managed to isolate the affected users but had our IT Team been completely occupied with other tasks at that exact moment, it could have been much worse. This was a clear indication that we needed an additional, automated security solution and support to help us catch potential threats in real-time," says Karveller.

> "Graphus meets that need for an additional layer of security and requires a minimal investment in terms of time from your existing manpower."
>
> - Adam Karveller, VP of IT

> “We needed a tool that would provide another layer of automated security on top of all the other policies and practices.” - Adam Karveller

GRAPHUS PROVIDES AUTOMATED PROTECTION

The ease of implementation allowed Karveller to get started with Graphus, with minimal effort from his part. He said the activation process was “quick, painless, and easy.” But it wasn’t just the easy implementation that eventually sold him. Karveller said, “The tight integration with our chosen mail and collaboration platform - G Suite for Business - was the major driving factor in choosing Graphus.”

This tight integration provides Newk’s with automated yet powerful protection. Graphus is part of their daily checklist. They typically check the system about three times a day, not including when alerts come through. Most of the alerts they’ve received recently have been drive-by malware attacks which are handled automatically so by the time they get the alert, no action is required on their part. According to Karveller, this is the most critical feature. The “automated removal of threats without any human interaction whatsoever.”

When human interaction is required, the IT Team members are able to investigate threats and then delete messages, quickly and in a single click.

The warning banner is another important features for Newk’s. This warns end users of messages that Graphus has flagged as a potential threat but doesn’t meet the auto-deletion or quarantine standards. This causes their business users to pause and a call to action to have IT review any questionable messages before proceeding. The one-click deletion capability for “IT Team members to delete messages that have been investigated via the Graphus Dashboard and identified as threats – quickly, and in a single click – without providing additional permissions to the users security class, or direct access to a sensitive inbox is by far the most valuable tool,” says Karveller.

When asked if he would recommend Graphus, Karveller responded, “Yes. I think in today’s climate where spear phishing attacks are so much more prevalent, sophisticated and specifically targeted at/or disguised as key cloud softwares that exist in almost every business ecosystem an additional layer of security is absolutely necessary. Leveraging machine learning and AI to review your communications are powerful tools in helping mitigate the risk for our business users in being exposed to risk. I think Graphus meets that need for an additional layer, and requires a minimal investment in terms of time from your existing manpower to do so.”

Newk’s EATERY

NO SECURITY ENGINEER NEEDED

According to Karveller, this is the most critical feature. The “automated removal of threats without any human interaction whatsoever.”

BY THE NUMBERS

5,000
FULL & PART-TIME EMPLOYEES

140,000
EMAILS PER MONTH

16
PHISHING ATTACKS STOPPED IN A MONTH

6
MALICIOUS LINKS & ATTACHMENTS

SCREENSHOT

CREATED	CATEGORY	SEVERITY	STATE	SENDER
Dec 12, 2017 at 19:46:33 UTC-05:00	Drive By Download Malware	CRITICAL	CLOSED	pjohn@emirates.net.ae
Dec 04, 2017 at 12:05:48 UTC-05:00	Drive By Download Malware	CRITICAL	CLOSED	efren.salazar@meyersgrp.com
Nov 16, 2017 at 15:30:32 UTC-05:00	Drive By Download Malware	CRITICAL	CLOSED	purchasing@sarongbail.com
Nov 07, 2017 at 15:35:10 UTC-05:00	Drive By Download Malware	CRITICAL	CLOSED	gsuite-alerts-noreply@google.com
Nov 07, 2017 at 11:06:44 UTC-05:00	Phishing	HIGH	CLOSED	notifications@bettercloud.com

Five of the Malware Campaign Spoofed Emails Caught by Graphus

GRAPHUS

Graphus provides immediate protection and peace of mind for cloud application users by automatically eliminating social engineering - phishing, email scams, and malware attacks. The simple, powerful, and automated Graphus solution employs artificial intelligence 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**