CASE STUDY

proofpoint.

COLLEGE OF MEDICINE IMPLEMENTS PREVENTIVE MEDICINE AGAINST ADVANCED EMAIL THREATS

TEAM GAINS PROACTIVE INCIDENT RESPONSE WITH PROOFPOINT

CHALLENGE

- Gain visibility into advanced threats and user interaction
- Move from reactive to proactive incident response
- Monitor email across Office 365 and other email environments

RESULTS

- Defended against advanced threats with no impact to users
- Reduced email compromises by 75%
- Identified malicious email interactions immediately, instead of taking days or weeks
- Began automating incident response

The college of medicine is a renowned private health sciences university with activities spanning the full range of healthcare. Protecting academic, personal health, and proprietary research information is integral to the college's operations and reputation. The college chose Proofpoint to help it identify and block email threats before they can cause lasting harm.

As a college, healthcare provider, and leading research facility, the college is a triple target for cyber attackers. Personal Health Information (PHI) sells for a premium on the dark web. Intellectual property—the school's medical research data—is essential for securing patents and valuable partnerships.

"Email delivery has become the primary vector for delivering malware, phishing attempts, and social engineering threats," said the IT Manager for the college. "We knew that the volume of malicious email we saw was only the tip of the iceberg. That just wasn't good enough."

Unless a user called the team to report an issue, they had no visibility into compromises. Often, time passed between when a user clicked on a malicious URL or attachment and when the threat became active. When credentials or machines displayed symptoms of a compromise, the team had to backtrack and painstakingly investigate to understand what happened and the extent of the damage.

"We needed deeper visibility and a better understanding of specific threats that target us," the IT Manager said. "We knew who received emails, but we needed to know who clicked, when they clicked, and what happened so we can prevent reoccurrences."

A HOLISTIC APPROACH

The college considered Microsoft anti-malware features in its Office 365 environment. But those features didn't cover other email environments that the college supports. The team wanted one solution to handle inbound and outbound email traffic for its entire network. The team chose Proofpoint as its email gateway and to stop advanced threats that use tactics such as malicious attachments and URLs.

"Proofpoint sandboxes attachments and rewrites URLs with zero impact to our users," said the Messaging Architect at the college. "That's what we wanted. Deploying it was simple—a couple of clicks and we were done."

The college also uses Proofpoint to encrypt confidential data ranging from Protected Health Information (PHI) to Personally Identifiable Information (PII). Users can add a secure tag to any email, which triggers its encryption. If the college's data-loss prevention (DLP) application flags the email as containing confidential information, then the email is automatically encrypted—even if users haven't tagged it. Proofpoint helps the college minimize regulatory, legal, public relations, and financial risks.

"Proofpoint plays a critical role in enabling proactive incident response. That's essential to protecting the college's users, research, and reputation."

Messaging Architect, College of Medicine

UNDER THE MICROSCOPE

With Proofpoint, the team has detailed insight into how users interact with malicious emails. When a user clicks on a malicious link, the team is notified at once. Even if a user clicks on a valid link that later becomes malicious, Proofpoint notifies the team and tells them which users clicked. Instead of threats going undetected for days or weeks, the team now knows what happened right away. Not only can the team remedy the situation, any potential damage is contained. The team estimates that they see at least 75% fewer compromised accounts and can act much faster to remediate the few that still occur.

"We see what Proofpoint blocks and can use that information to update other security tools," the IT Manager said. "In case something does get in, the rest of our security architecture is better positioned to protect us."

VACCINATING AGAINST SPAM

Many physicians and medical staff that work at the college also work at other hospitals and clinics. They have mailboxes on the college's email system, but they might also have mailboxes on other facilities' systems and open email at home. Proofpoint has been a valuable asset to the team for these users.

"The ability to block and rewrite malicious URLs is absolutely a key benefit to us," the IT Manager said. "Our users' college emails are protected no matter where they open them, and we know that we won't be the cause of a campaign getting into another hospital's network."

AUTOMATING RECOVERY

The college has begun automating the response process. Until now, the team has manually recovered malicious email from users' mailboxes. Proofpoint will automate that step and accelerate incident response with additional containment, alert enrichment, and forensics features.

"Proofpoint plays a critical role in enabling proactive incident response," the Messaging Architect said. "That's essential to protecting the college's users, research, and reputation."

For more information, visit www.proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.