CUSTOMER STORY

proofpoint.

HOSPITAL STOPS EMAIL-BASED ATTACKS FROM UNEXPECTED SOURCE

PROOFPOINT DELIVERS VISIBILITY, AUTOMATION AND BETTER PROTECTION IN ONE SOLUTION

THE CHALLENGE

- Prevent disruption caused by phishing and malware attacks delivered via the Zix Federation Network
- Gain ability to identify and stop thousands of advanced email-based threats
- Protect users against spoofing schemes

THE SOLUTION

- Proofpoint Email Security and Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull
- Proofpoint Email Data Loss Prevention
- Proofpoint Email Encryption

THE RESULTS

- Identified sources of chronic encrypted malware attacks and stopped them
- Reduced spam emails in users' mailboxes to near zero
- Automated incident response steps to quarantine and remove malicious messages
- Simplified users' abilities to encrypt sensitive data
- Dramatically improved IT team peace of mind

THE COMPANY

This non-profit health organization began as a single, community-founded hospital in Newport News, Virginia. Since then, it has evolved into a flagship medical center with affiliates throughout the region. The medical center's commitment is to the health and wellness of all patients during every stage of life. From pediatrics to geriatrics, from birthing centers to retirement communities—it provides local, affordable access to more than 340 physician specialists and 130 care locations.

THE CHALLENGE

In spite of next-generation firewalls, email filtering, Zix encryption, and scrupulous updates, the IT team was seeing a disturbing number of threats continue to get through. These included well-crafted phishing emails, spam, spoofing emails and malware. Early in 2018, a user clicked on a phishing email and was persuaded to disclose his credentials. What followed was an organization's nightmare. The attacker accessed the user's Microsoft Outlook web email account, and using the same credentials, moved to the hospital's intranet and then the employee self-service portal. From there, the attacker obtained the user's banking information. Other users had received the same phishing emails, so the IT team worked nonstop over several days to change passwords and pull email messages from thousands of mailboxes.

"We didn't understand why we were continually seeing high volumes of phishing emails in spite of having Zix encryption and following best practices," said the senior systems administrator. "That was the catalyst that started our search for advanced threat protection."

THE SOLUTION

Finding the Right Combination

The hospital's IT team evaluated multiple vendors' solutions. They considered Barracuda, Cisco and Fortinet. None of the offerings met all of the organization's requirements for effectiveness, ease of management and cost-effectiveness. As they conducted multiple proof of concept trials, they realized that none of the solutions were keeping up with the volume of email attachments and suspicious URLs that they received. When a trusted partner suggested that they look at Proofpoint, they did.

The hospital's IT team set up a trial of Proofpoint and quickly made some eye-opening discoveries. Campaigns carrying malicious payloads were being delivered as encrypted emails from multiple Zix partners through the Zix federated network. Incoming encrypted email messages arrived at the email filter, which couldn't scan them, and then were sent to the Zix gateway appliance. There, they were decrypted and delivered directly to users' mailboxes. The mystery of ongoing malware attacks was solved. The hospital replaced its Zix encryption solution with Proofpoint Email Encryption and Email Data Loss Prevention, Proofpoint Email Security and Protection and Proofpoint Targeted Attack Protection (TAP).

"Proofpoint provided a complete solution that addressed all of the threats we had been experiencing. It gave us the visibility we needed, the automation to handle threats effectively, and the ability to respond quickly."

Senior systems administrator

Seamless, Solid Defense

In addition to stopping malicious email and attachments, TAP gave the hospital immediate insight into primary spoofing targets. This included executives, the legal team and supply management staff. Proofpoint Threat Response Auto-Pull (TRAP) orchestrates steps of incident response. This enables the team to automatically collect, analyze, quarantine and remove threats that get through. TRAP also follows forwarded mail and distribution lists, creating an auditable activity trail. The hospital replaced Zix encryption with Proofpoint Email Encryption and Email Data Loss Prevention. Proofpoint Email Security and Protection is also a valuable tool for helping the team reduce bulk email and give users more control over their mailboxes.

THE RESULTS

"With Proofpoint, the difference in spam, spoofing, and malware attacks was night and day," said the senior systems administrator. "Everyone noticed. Our executives told us 'whatever you're doing, keep it up.' They are very happy."

Hospital employees are now better protected against targeted attacks. The transition to Proofpoint Email Encryption was seamless, enabling users to encrypt email with the same keywords they already knew. And the IT team can reset a password in just seconds if necessary, without having to involve a third party.

Proofpoint is invaluable in helping the IT team identify the most attacked people within the hospital. They easily engage users and show them how to recognize spoofed emails. The hospital is rolling out their user digest to employees, giving them greater control over bulk mail. The IT team can now be more people-focused while still repelling attackers.

"Few people think email is a critical application until they can't send or receive one," said the senior systems administrator. "Proofpoint and its enhanced capabilities are a huge leap forward. I hadn't realized how much stress I felt about email threats until Proofpoint took that worry off my shoulders. It's gone."

For more information, visit proofpoint.com