Global pharmaceutical stalwart treats chronic phishing disease with more accurate detection and faster response

GreatHorn protects pharmaceutical giant from the executive and brand impersonations missed by both Microsoft and legacy gateway

AT-A-GLANCE INFO

Organization:

Global pharmaceutical organization

Industry:

Biopharmaceutical

Challenge:

Protect employees against executive and brand impersonations

Environment:

- Publicly traded pharmaceutical
- Employees at personal risk from ADP impersonations
- Increased risk due to lengthy remediation process
- Email platform: Office 365 E5

Why GreatHorn?

- Easy cloud-based set up and management
- Eliminated day-to-day administration
- Constant monitoring and expertise
- Reduced the burden on internal team

Strong customer focus

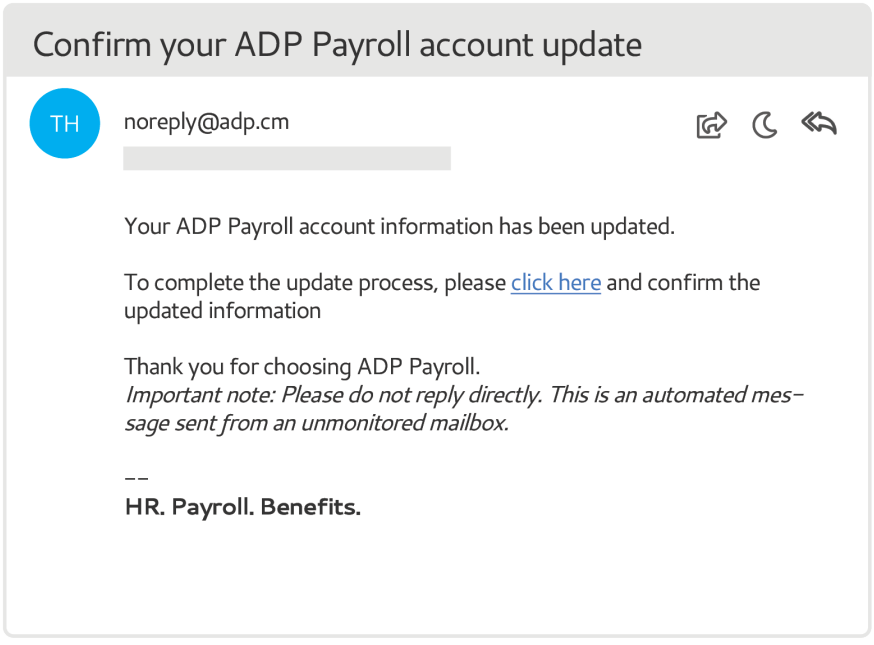
- Fast, transparent remediation

Executive attacks and ADP spoofs drive search for a new solution

Global, publicly traded companies provide a rich environment for cybercriminals for three key reasons: 1) The large employee base provides more potential targets for account compromise; 2) Many business processes occur via email; and 3) Quite a lot of information about the organization is publicly available, ready to be used in targeted attacks.

This pharmaceutical giant was no different. With more than 20,000 employees spread around the world, the company received approximately 10,000 phishing attacks a month, many of which made it past their secure email gateway and into user mailboxes.

Particularly troublesome was a wave of brand impersonations masquerading as the company's payroll provider, ADP. Such attacks used a domain lookalike of ADP, passed typical email authentication such as SPF, and requested that the user confirm or update direct deposit information.



In addition, the company's senior executives were regularly under attack, which raised the visibility and urgency of finding a solution to the problem. The problem was exacerbated by the lack of robust search and remediation tools within Microsoft Office 365. The team estimated it spent several hours a week – hours that should have been spent addressing other security needs – reviewing and remediating emails via PowerShell scripts.

A layered approach to email security

While the team was frustrated with the effectiveness of their legacy email security solution, they needed to keep the gateway for archival purposes. They began to look for a tool that could help address the business email compromise issue without adding further complexity to their mail flow.

That's when they came across GreatHorn. GreatHorn's API-based integration with Office 365 meant that it could be used in conjunction with the existing infrastructure without redirecting MX records or changing existing mail flow. The five-minute implementation was so easy, the team assumed something had gone wrong and that the implementation would need to be rescheduled.

Designed from inception to address the issues of executive and brand impersonations, GreatHorn combines a wide range of threat detection techniques, including patented domain lookalike technology, sophisticated relationship analysis, executive impersonation identification, and threat intelligence. During the three-week pilot, GreatHorn identified 6,800 impersonation attacks passing through the legacy Secure Email Gateway, making the decision to move forward an easy one.

Reducing time to response

While threat detection was one critical area for improvement, the operations team had two other equally important goals: reducing both the exposure time from email threats and the manpower it took to review and remove such threats.

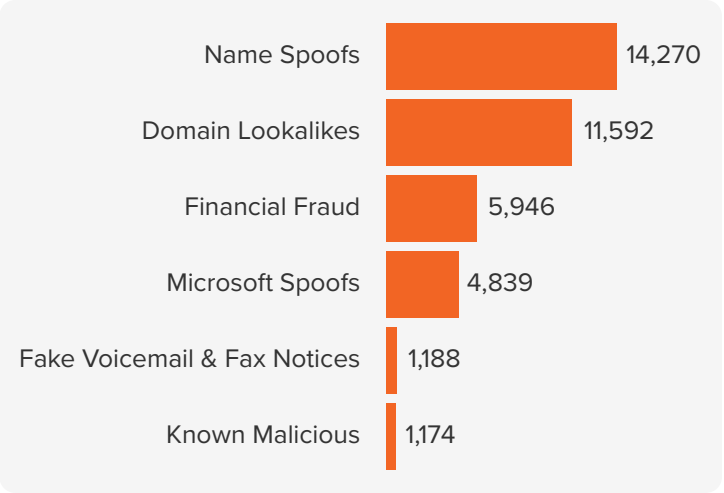
In one attack just prior to the evaluation, an internal email account was compromised and in turn sent out a highly sophisticated phishing campaign to more than 500 users, each with different links, subject lines, sender domain, and email address. Since it was an internal attack, the pre-existing gateway didn't even see the messages, let alone flag them. The team spent hours identifying the full scope of the attack – difficult to do particularly due to a lack of robust controls in the Office 365 administrative interface – and remediating it. However, the combination of lengthy response time with a lack of visibility into user engagement rates meant that the team had to resort to resetting passwords en masse for all 500 affected users. In contrast, a more recent attack (after GreatHorn had been implemented) involving nearly 200 emails took less than four minutes for GreatHorn to remove.

An indispensable tool for email security

Since its initial investment in GreatHorn, the company has grown both organically and via acquisitions, increasing its threat surface. As part of a separate initiative, the company decided to purchase Microsoft's top tier offering, Office 365 E5, prompting a reevaluation of their email security strategy due to Microsoft's recent investments in security and bold claims of phishing protection.

After extensive testing however, the team not only concluded that detection of sophisticated phishing attacks remained insufficient compared to GreatHorn, but that the lack of robust controls, particularly with regard to remediation, would put the company at risk.

Over the course of a recent month for example:



GreatHorn identified **more than 30,000 phishing attacks** that had bypassed both the gateway and Office 365 E5's detection.

With the core functionality implemented successfully, the company deployed an additional layer of security against payloads delivered via hyperlinks. GreatHorn's Link Protection performs on-click analysis of every url, ensuring interception of malicious links, even those weaponized post-delivery. A built-in credential theft check on suspicious links further protects from the potential havoc wreaked by resolving to compromised websites.

Says the company's vice president of IT operations, "GreatHorn is one of the best vendors we work with. They have an ongoing commitment to providing a leading- edge product."