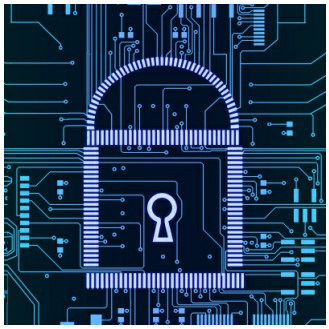
HealthManagement
Promoting Management and Leadership

Common Healthcare Cyber Threats



A new Proofpoint study, carried out between 2Q 2018 and 1Q 2019, provides more evidence that tactics employed by cybercriminals to attack healthcare organisations are changing frequently. While ransomware was used in many cyberattacks in 2Q 2018, ransomware incidents then took a sudden drop as cybercriminals gravitated to banking Trojans.

Proofpoint's "2019 Healthcare Threat Report" shows banking Trojans comprised the biggest malware threat to healthcare organisations for the period of the study. Of all malicious payloads delivered via email between 2Q 2018 and 1Q 2019, more than two-fifths (41%) were attributed to banking Trojans. Of note, Emotet banking Trojan accounted for 60% of all malicious payloads in the first quarter of 2019 alone.

Although there were more malware attacks reported during the study period compared to phishing attacks, researchers found a significant increase in the number of phishing incidents in 2019. On average, targeted healthcare organisations received 43 imposter emails in 1Q 2019, a hefty increase of 300% from 1Q 2018. Those attacks saw an average of 65 members of staff attacked at each healthcare organisation.

When email attacks at several healthcare organisations were further analysed, Proofpoint found that some individuals are more targeted than others. Among the “Very Attacked Persons” or VAPs are doctors/physicians, researchers, and admin staff at healthcare providers; customer support/sales staff, admin staff, and IT teams at health insurers; and executives, marketing employees, and logistics/sourcing and supply chain staff at pharmaceutical companies.

Proofpoint researchers also shared another interesting finding: cybercriminals are using new tactics, not just email attachments, to spread malware. Attackers have begun using URLs (embedded hyperlinks) that direct users to phishing websites where credentials are stolen. Moreover, such hyperlinks can also send healthcare employees to websites where malware is silently downloaded. As noted by the researchers, 77% of email-based attacks during the period of study used malicious URLs.

Other notable findings of the study include:

- Malicious emails are most commonly sent during business hours, usually between 7am and 1pm, Monday to Friday
- Malicious emails are more likely to be opened if the sender of the email is known to the recipient
- 95% of targeted healthcare organisations received emails that spoofed their own trusted domain
- 55% of malicious emails had subject lines containing the words “urgent”, “payment”, or “request”

In addition, shared email aliases used to request patient information or for patient portals received the most malicious emails. These email addresses have the potential to result in multiple malware infections and several responses to phishing emails, according to the researchers.

The report recommends the use of layered defences to block these cyber threats. For example, anti-phishing and anti-malware solutions can help protect the email system. Also, filtering controls are needed to block web-based threats, whereas anti-malware controls are required on endpoints.

It is also important that employees receive regular training to help them identify threats and condition them to take appropriate action when a suspicious email is received, the report says.

Source: HIPAA Journal

Image: iStock

Published on : Wed, 23 Oct 2019