HealthManagement
Promoting Management and Leadership

Locky Ramps Up Attack Methods via Facebook

Locky, the deadly ransomware that has been wreaking havoc on healthcare networks has ramped up its methods of attack making decryption even tougher.

A report in Healthcare IT News says there has been a drop in the frequency of ransomware attacks in recent months owing to a rise in decryption tools for ransomware strains like Crysis but Locky is slipping through the net.

How Locky hackers manage this is by using the AESIR-file extension. This disguises the virus as an email from a legitimate company with a subject line devised to encourage the reader to open the email and attached zip file.

Specifically, hackers mask the virus as a complaint query from an Internet provider saying that the user's computer is generating SPAM.

See Also: **Phishing Emails: 97 Percent Contain Ransomware**

This is not all. Locky attacks are now coming via Facebook Messenger. A recent report in CSO detailed exactly how the malware slips past the whitelisting mechanism on Facebook through imitating an image.

Locky is then spread with a Nemucod downloader which arrives in Facebook Messenger as an .svg file.

There is still no method of decrypting Locky ransomware and recovery is only possible via a viable backup.

Healthcare data breaches are potentially costly and, in a worst-case scenario, life-threatening. To mitigate the threat, organisations should:

- Keep systems as up to date as possible;
- Train users about risks;
- Undertake routine security assessments to pinpoint vulnerabilities;
- Keep up to speed on industry trends in cyber issues.

The rise in malware attacks is largely down to employees accidentally installing malicious software onto the company network. More worrying is this happens at a rate of every four seconds claims a recent Check Point report on security. Proper training of staff to be vigilant about the ransomware threats that come via email is recommended by IT security firms.

Source: Healthcare IT News, HealthManagement.org

Image Credit: Avira Blog

Published on : Wed, 23 Nov 2016