HealthManagement
Promoting Management and Leadership

Cybersecurity Report: New Threats

HIMSS Director of Privacy and Security Lee Kim's latest monthly report on cybersecurity features a very interesting finding, and email users – that means most of us – should take note of it. There's a new cyberattack technique, called ROPEMAKER, that allows attackers to modify or edit the content in an email after it has been sent to the recipient.

Remember this acronym, ROPEMAKER, which stands for Remotely Originated Post-delivery Email Manipulation Attacks by Keeping E-mail Risky.

"Whether this ROPEMAKER technique will be leveraged remains to be seen," Kim said. "According to the MIMECAST report, there is no known activity in the wild. No one has actually done this, but I don't see why it couldn't be done."

ROPEMAKER is perhaps the most intriguing development in Kim's monthly HIMSS Healthcare and Cross-Sector CyberSecurity Report, but health and infosec pros will also want to know about the others.

Security vendor Proofpoint, for instance, uncovered the Defray strain of ransomware and determined that the healthcare and education sectors are specific targets – though it is currently a small campaign that has yet to wreak havoc on either.

There's also this warning from the U.S. Internal Revenue Services about a new phishing scheme that impersonates both the taxman and the Federal Bureau of Investigation. Such scheme would appear to many would-be victims as a convincing request. Kim said telltale signs include grammatical mistakes as well as errors of fact about laws and regulations.

Another threat concerns the Internet of Things. Ankit Anubhav, a researcher at New Sky Security reported thousands of leaked IoT telnet credentials. "Telnet credentials and data can be 'sniffed' or otherwise stolen by using certain popular hacking tools available on a variety of platforms," Kim explained.

The report also includes the U.S. Food and Drug Administration's advisory that many medical devices can be vulnerable to both exploits and intrusions and FDA pointed specifically to St. Jude Medical's implantable cardiac pacemakers. St. Jude constructed a firmware update and the FDA approved it.

"We are hearing more and more about new vulnerabilities – but old vulnerabilities never die. There are well-known vulnerabilities that are 10-15 years old that are still pretty effective against many systems," Kim pointed out. "When you are deciding what to patch, don't just focus on what's new. Pay attention to what's old and effective as well."

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 5 Sep 2017