HealthManagement.org
Promoting Management and Leadership

Hospital Ransomware Infects Visitor Computers?

Following news of ransomware attacks on two Southern California hospitals, a Canadian facility was targeted by cyber hacks and the infection may have had a knock-on effect to visitor and staff computers

Norfolk General Hospital in Simcoe, Ontario, said last week it had fallen victim to a ransomware attack. In a *CBC News* report Security firm Malwarebytes said the hospital's website has spread ransomware to staff, patients' and families' computers.

"Our honeypots visited the hospital page and got infected with ransomware via the Angler exploit kit. A closer look at the packet capture revealed that malicious code leading to the exploit kit was injected directly into the site's source code itself," wrote Malwarebytes senior security researcher Jérôme Segura in a blog.

Segura claimed that in late February, "Norfolk General Hospital's website was observed pushing ransomware called Teslacrypt to computers that visited the website".

Teslacrypt locks files and, using encryption, makes them inaccessible. It then demands a $500 ransom to restore access. Payment doubles after a week, Segura said.

Worse still, the security expert assed that the file was served in a 'drive-by download' attack meaning website visitors did not have to click on anything on the page.

Segura said that Norfolk General runs an out-of-date release of the Joomla content management system which made the website more vulnerable. He added that he had contacted the hospital several times about what he had detected.

However, Dennis Saunders, the IT lead for Norfolk General Hospital, said he didn't respond to Segura at first because Segura's initial email sounded like a sales pitch.

Saunders said the hospital got its first report of ransomware four days before Segura got in touch.

Following investigations, Saunders confirmed that the hospital website had been redirecting visitors to other sites that host malware, but there was nothing on the hospital's website itself.

Three hospital computers were infected with ransomware, but the hospital said its own website was not the source. The infected computers were restored and the hospital did not pay any ransom. The hospital is located in Simcoe, Ontario which has a population of fewer than 15, 000.

Segura recommended that hospitals protect themselves by:

- Keeping their website software up-to-date;
- Keeping staff with administrative privileges to a minimum.
- Using strong passwords.

His advice for users was:

- Using an up-to-date browser;
- Uninstalling software not in use;
- Installing anti-exploit software to detect and block suspicious behaviour from websites.

Just a week earlier, Ottawa's Hospital network was the target of a ransomware attack after hackers broke into IT systems and encrypted four computers.

The hospital said that no patient data was compromised and the IT department cleaned the infected systems and restored data through back-up material. The remaining 9, 800 computers were not affected by the hacking.

Source: CBC News

Image Credit: Pixabay

Published on : Mon, 28 Mar 2016