HealthManagement
Promoting Management and Leadership

Healthcare Now Top Gatak Trojan Target

Security vendor, Symanetc, has said in a study that the Trojan.Gatak group behind the Trojan malware has ramped up its attacks on the healthcare sector as data is more valuable than that of other industries. The fact that healthcare providers use legacy software that is not as secure as upgraded versions make the task easier for the hackers.

Trojan.Gatak is undertaking a campaign to infiltrate organisations with focus recently turning to healthcare.

How Gatak works is it infects targets via websites that tout product licensing keys to attract pirated software. Victims are infected when they access these sites. The product key is bundled with the malware and, once downloaded, installed on the victim's computer.

Our of the top 20 organisations most affected by Gatak, Symantec said that 40 percent were in the healthcare sector.

See Also: **Cloud Security Toughest Role for HIT to Fill**

What isn't clear is just how Gatak is benefiting from making the attacks although Symantec says that the sale of personally identifiable information and additional stolen data is likely.

"This could explain the attackers' heavy focus on the healthcare sector, with healthcare records usually selling for more than other personal information," the study said. "Healthcare organisations can often be pressurised, under-resourced, and many use legacy software systems that are expensive to upgrade."

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

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.

Source: HealthcareITNews

Image Credit: TechCabal

Published on : Fri, 25 Nov 2016