HealthManagement.org
Promoting Management and Leadership

Meet Latest Ransomware: Crysis

A recent and advanced strain of Ransomware has suggested that security-dominated headlines will not be a thing of the past any time soon.

Crysis, first discovered in February this year, is multi-platform with the ability to penetrate both Mac and Windows systems.

Security experts also say that it is more dangerous than other forms of virus seen to date. Stu Sjouwerman, founder and CEO of KnowBe4, a security awareness platform, says one of the most alarming characteristics of Crysis is a highly-advanced code that gains administrative control of target systems.

“Once a cybercriminal has that kind of access they can do more damage," said Sjouwerman.

More concerning is Crysis' ability to encrypt files and usernames, which are then directed to a command server. The strain copies files and pulls them from the network, placing organisations into a data breach,

“It can be hard to keep tabs on these types of ransomware strains”, Sjouwerman said. "They compete; they come and go. We were expecting with the sudden demise of TeslaCrypt (a ransomware Trojan) that Locky would take over. If you look at the majority of ransomware attacks, Crysis, at the moment, is the number one prevalent attack."

Crysis attacks began at financial institutions then migrated to healthcare. Sjouwerman anticipates that manufacturing will be the next target but healthcare is still in cybercriminals’ crosshairs.

"There are no groups immune to ransomware attacks," said Lysa Myers, security researcher for ESET, a security company. "Hospitals can be lucrative targets, and many are still poorly protected. My hope, with all the coverage about hospitals being hit, is that this serves as a wakeup call and motivates hospitals to start performing thorough risk assessments and moving quickly to mitigate those risks."

Myers says that creating offsite and offline backups is the most important action hospitals can take to protect data, according to Myers.

Sjouwerman adds that it is essential that backups are kept up-to-date otherwise, if an attack strikes, they will be obsolete.

"The human is a weak link of cybersecurity and bad guys are counting on that," Sjouwerman said. "On a board level, it needs to be clear that cybersecurity cannot take the backseat. And they have to open up resources to improve their cybersecurity posture."

Source: Healthcare IT News

Image Credit: Pixabay

Published on : Mon, 13 Jun 2016