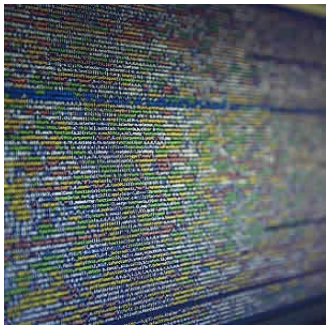
HealthManagement
Promoting Management and Leadership

New Variants of WannaCry Virus Found



The WannaCry virus continues to spread with new variants being spotted in the wild in infected computers, and experts urge organisations and individual users to "patch your system" now.

"WannaCry is widely touted as the world's first ransomworm: i.e., a type of ransomware with the ability to self-propagate without user intervention or interaction," Director of Privacy and Security for HIMSS North America Lee Kim said in a blog post. "The success of the WannaCry ransomware is based upon one tried and true fact: Many individuals and organisations don't patch their systems in a timely manner."

Security firm Recorded Future first saw the WannaCry virus in the wild on 31 March. However, the new version responsible for the recent global cyberattack that crippled operations of businesses and government offices has been modified with “worm-like” capabilities that allow the virus to spread through any networked system not patched via NetBIOS.

Matt Suiche, founder of cybersecurity firm Comae Technologies, revealed that he was able to stop another variant when he registered the new kill-switch domain name, but said industries must expect that there is still more to come. Suiche is working with MalwareTechBlog and security firm Kryptos Logic to map the domain and sinkhole servers.

It’s these group efforts that will help prevent the spread of the virus.

“Ransomware is just a large puzzle,” said Fabian Woser, chief technology officer for Emsisoft, an anti-malware vendor. “The more intelligent people are working on these puzzles, they more likely they can find a solution for its victims.”

Security companies and law enforcement scour ransomware to find mistakes, which “allows them to crack the code,” Woser added. “This works for small actors looking for a quick buck, but not for major ransomware strains, created by smarter entities, who take the time to create flawless programs.”

There are now three definitive variants of the WannaCry virus. And as the worm is already in the wild, the need to patch IT systems becomes more urgent.

"The bottom line for the consumer is to patch your system, make sure automatic updates are turned on and make sure your IT team is patching your system," according to U.S. Homeland Security Adviser Tom Bossert.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 16 May 2017