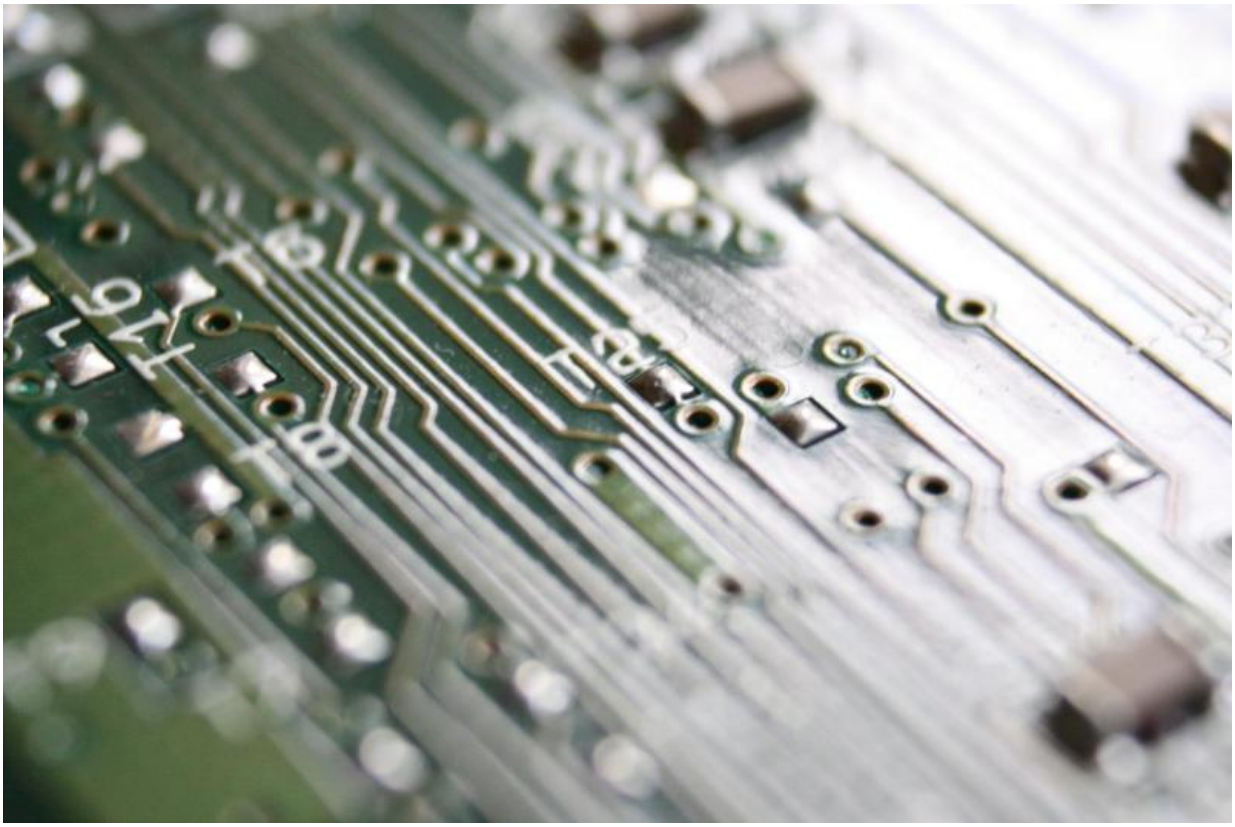
Researchers say new generation of ransomware emerging

April 11 2016, by By Tami Abdollah



Credit: Public Domain

An unusual strain of virus-like hacker software that exploits computer server vulnerabilities without requiring human interaction is a leading example of a new generation of "ransomware," according to a new report

by Cisco Systems Inc.

Hackers use such software to target large-scale networks and hold data hostage in exchange for bigger payments. Such a strain, known as Samas or samsam, hit the MedStar Health Inc. hospital chain in the U.S. last month.

In such attacks, hackers target backup files and records, encrypting them to make them unreadable. To regain access, users without additional safe backups who don't want to lose critical files often pay the ransom, typically $10,000 to $15,000 for an entire network or hundreds of dollars for a single computer.

The ability to demand payment in bitcoin, a difficult-to-trace virtual currency not controlled by any country, was "basically the birth of ransomware" and has helped drive its success since the currency's introduction in 2009, said Craig Williams, a senior technical leader at Cisco's Talos security research group.

Samas exploits vulnerabilities giving hackers a way into JBoss application servers that are frequently used by some of the largest corporations. Once inside, the hackers sometimes implant a tool that steals credentials, allowing it to spread through the system, and encrypt scores of digital files along the way.

Ransomware has become a new targeted attack, with thousands of variants emerging over the last six months, said Dmitri Alperovitch, co-founder and chief technology officer of Crowdstrike Inc.

Most ransomware still requires a human to click a link or open an infected email attachment, but Cisco's report warned that "the age of self-propagating ransomware, or cryptoworms, is right around the corner." Worms are generally virus-like infections that are programmed to spread

automatically, without human interaction.

Ransomware has become an increasing threat over the last six months. Last year's 2,453 reports of ransomware hackings to the FBI totaled a reported loss of $24.1 million, making up nearly one-third of the complaints over the past decade. They also represented 41 percent of the $57.6 million in reported losses since 2005.

Such losses are significantly higher than any paid ransoms because companies routinely include remediation costs, lost productivity, legal fees and sometimes even the price of lost data in their estimates.