PRESS
For immediate distribution

American Companies Being Targeted By CryptoWall Spyware

Montreal, Quebec, Canada - October 21, 2014 - Cryptowall, a malware used by hackers to lock down files and then demand ransom from their owners is causing problems for many businesses and organizations in the United States.

According to SecureWorks Counter Threat Unit, since its inception in March, CryptoWall has managed to infect 625,000 systems and 5.25 billion files worldwide. Canada ranks fourth in the list of most infected countries.

“CryptoWall is the most destructive virus in the history of the internet,” affirmed Jacques Mathieu, president and founder of Team Microfix, a company specializing in IT infrastructure. “Over the course of the last few weeks, we have worked to clean up servers in multiple municipalities. Law firms, pharmaceutical companies, and even a police station have had to pay the price for access to their own data.”

This malware scans files, encrypting some and making them unreadable. When the infected file is double-clicked, the user is informed that their computer has been infected. To regain access to the files, the user has no choice but to pay a ransom within a given period. This ransom must be paid in Bitcoins, which represents a major technical barrier for victims of the virus.

"The victims usually have a period of 48 hours to pay the ransom, while the purchase of Bitcoins may take up to 72 hours and there’s the risk of getting ripped off when buying,” says Mathieu Jacques. “If the victim is not able to get the Bitcoins in time, the files are lost forever."

The virus can get into a system in several ways, mainly via spam and corrupt hidden links on sites supported by advertising. However, the virus only targets Windows operating systems. Mac or Linux are not affected.

About Team Microfix

Team Microfix specializes in IT infrastructure. Since 2001, the company has developed solutions in the control of information in order to maximize the profitability of operations. In recent years, Microfix has specialized in decryption. Team Microfix, among others, participated in many data recovery operations following the proliferation of the CryptoLocker virus, which occurred on the web in 2013 and was neutralized in May 2014.

http://www.equipemicrofix.com/en/cryptowall-virus-new-york/