Ransomware no cause for New Year celebration: Sophos

16 December 2013, by Nancy Owano

Cryptolocker encrypts a victim’s files and demands a ransom.

(Phys.org) —From operating systems on desktops to software and peripherals on smartphones, information thieves have been clever, inventive and successfully stealthy in finding pathways for stealing personal information. Malicious software is alive and well; one only has to glance at the daily headlines reporting on security exploits in government and the private sectors. A new report from the security firm Sophos, "Security Threat Report 2014," calls attention to the latest types of security headaches. They include ransomware, the type of malicious software that locks you out of your computer or your data and demands money to let you back in. Ransomware itself is nothing new, as a ploy to make files inaccessible, and then demanding money from the victim before the attackers hand back control of the system to the victim.

But this year Sophos security experts saw a newer ransomware version, called Cryptolocker. In a blog posting about the report, company CTO Gerhard Eschelbeck called Cryptolocker an exceptionally nasty strain, locking users out of their files with the use of "extremely strong" encryption. The Cryptolocker thieves have thus far been successful in getting their victims to pay large sums, in electronic payments. The report said that Cryptolocker is ransomware that "adds itself to the list of Windows programs that run at startup, tracks down an infected server, uploads a small ID file from your computer, retrieves a public key from that server (which stores a matching private key), and then encrypts all the data and image files it can find on your computer."

Attack points may be via e-mail spam but Cryptolocker often arrives through botnets. Generally, said the BBC, in reporting on the Sophos findings, cybercrime kits have helped many people with only light technical skills enter the world of high-tech crime for the first time; with some kits even offering technical support for those who need advice on how to roll their own malicious programs, and have been a contributing factor to the rise in malicious programs circulating online. The BBC said that one study of some servers run by the criminals behind Cryptolocker indicated 12,000 victims a week were being hit.

The Sophos report said ransomware targeted against Android devices has been noticed. In June, Sophos researcher Rowland Yu discovered the first ransomware attack against Android devices. Posing as an antivirus solution the ransomware app asked for a $99.99 payment to restore access to Android devices.

The new Sophos security threat report was released on December 10. Later that week, the Sophos blog issued a specific warning about ransomware, predicting its rise. "Ransomware, including the infamous file-encrypting Cryptolocker, posed a major threat in 2013. But this cyber-crimewave could get much worse in 2014." According to the blog posting, cybercriminals are

plotting to create new ransomware using automated malware kits.

James Lyne, global head of security research at Sophos, told BBC News that "Cryptolocker is very much a deviation from the norm, and I actually think it is a sign of things to come."

More information: Report: www.sophos.com/en-us/medialibr … reat-report-2014.pdf

APA citation: Ransomware no cause for New Year celebration: Sophos (2013, December 16) retrieved 2 December 2021 from https://phys.org/news/2013-12-cryptolocker-ransomware-year-celebration-sophos.html