Cyber thugs taking data hostage

February 26 2015, by Glenn Chapman

Like other forms of malicious code, ransomware can get into computers, smartphones or tablets when people click on dubious links or open infected email attachments

Marriage therapist Valerie Goss turned on her computer one day and found that all of her data was being held hostage.

Malicious code referred to as "ransomware" had encrypted her files and locked them away. Cyber criminals demanded $500 in hard-to-trace virtual currency Bitcoin to give her the key. The ransom would jump to

$1,000 in Bitcoin if Goss took more than a day to pay.

"I felt shocked; like I had been robbed," the Northern California therapist said. "And, I felt pressed for time to make a rational decision. It felt so surreal."

After online research by her son revealed that in a quarter of more of ransomware cases victims never see their files again even if they pay, Goss refused to pay.

Instead, she bought a new computer and fortified it with security software. She also started backing up data off the machine.

As painful as it was, Goss did the right thing, according to cyber security specialists interviewed by AFP.

"Unfortunately, it is the right thing to do," said Malwarebytes chief executive Marcin Kleczynski.

"If you do pay the ransom, that money is gone and there is no guarantee you will get your data back."

Data kidnappers are taking aim at smartphones and tablets

Kidnapping smartphone files

Ransomware has been around a while, but has been making a big comeback, according to Kleczynski and mobile security researchers at Lookout. Gross fell prey to the hacker tactic last year on the computer she used in her home office.

Data kidnappers are also taking aim at smartphones and tablets, particularly models powered by Google-backed Android software, said Lookout consumer safety advocate Meghan Kelly.

Lookout saw mobile malware "encounters" in the United States jump 75 percent in 2014 as compared with the prior year. Ransomware accounted for a big part of the jump, according to Kelly.

The United States seems to be a preferred target zone, perhaps because people here keep a lot of cherished, personal data on mobile devices and computers, or because they are seen as having the money to pay to get it back.

A US study released last year by Lookout revealed that one-in-three people considered pictures, contacts, and other digital files on mobile devices so precious they would pay to get them back.

Goss said that she was willing to pay the ransom, but had no assurance she would actually see her files again even if she did pony up the Bitcoin.

Like other forms of malicious code, ransomware can get into computers, smartphones or tablets when people click on dubious links or open infected email attachments.

Drive-by attacks

People can also be hit with ransomware at legitimate websites that have been unknowingly booby-trapped by hackers to infect visitors in what are referred to as "drive-by" attacks.

"Sometimes you don't have to do anything wrong, just visit a website that has been infiltrated and then all of a sudden you have a piece of malware on your computer," Kleczynski said.

Ransomware locks and encrypts all files on infected devices. Kleczynski said that ransom demanded typically ranges from $100 to $1,000.

Ransomware targeting mobile devices can lock phones, email and more, essentially stripping control from owners, according to Kelly.

"Ransomware is a pretty loud piece of malware," Kelly said. "It is going to be in your face saying you can't navigate away and we want money from you."

People can protect themselves by being wary of what links they click on or files they open, and by keeping operating software up to date so the latest security patches are in place.

It is also recommended to have security software running to intervene before malware takes root, and to keep back-up copies of files in the cloud or elsewhere in case defenses are breached.

"One day ransomware can hit you and you have to prepare for the worst," Kleczynski said.

"The threat is very serious, users are infected all of the time, and the encryption keys are so strong you can't get those files back."

Malwarebytes and Lookout offer free versions of their security applications.