

## **New Ransomware Attack Using Spam Is Underway**

A new surge in ransomware attacks is underway, posing a threat to businesses and consumers, Symantec Corporation says.

The computer security company said attackers are encrypting files and demanding ransom by using an updated version of the ransomware program TeslaCrypt. Over the past two weeks, attackers have sent “out massive volumes of spam emails seeded with the malware.”

“TeslaCrypt uses strong encryption to encrypt a wide range of files on the victim’s computer,” Symantec warns. “Its creators have continually refined the malware and the tactics used to distribute it, making it one of the most dangerous threats currently in circulation.”

The fake emails use subject lines including, “Would you be so kind as to tell me if the items listed in the invoice are correct?” “Please accept our congratulations on a successful purchase and best wishes,” and “Would you be nice enough to provide us with a wire transfer confirmation?” The emails contain an attachment with the word “invoice,” “doc,” or “info.” Opening the attachment launches the encryption program, which requires a private key to unlock. To obtain the encryption key, victims must pay a ransom.

When the files are encrypted, the programs become inaccessible. The ransomware displaces a message explaining that the files were encrypted “and you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.” The attackers tell the victims that if they do not act quickly, then the private key will be changed. “If you really want your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

Symantec observes that the TeslaCrypt malware can be purchased on the underground black market.

The resurgence of the TeslaCrypt underscores the importance for businesses to keep all antivirus and malware software up to date and to remind their employees not to open attachments to emails from unknown sources, which is also good advice for consumers.

*Balough Law Offices, LLC, is a Chicago-based law firm which focuses on cyberspace, business, and intellectual property law. Our homepage is [balough.com](http://balough.com).*