Telegram Now Being Used in Ransomware Attacks

April 30, 2021 - Since January, the messaging application Telegram has gone through exponential growth. The application now has more than 500 million daily users and it is continuing to expand. And that expansion has made it quite attractive to cybercriminals. The app is now being used to distribute a piece of malware known as Toxic Eye.

Toxic Eye is an insidious little program. It can steal passwords, encrypt files and make them useless, look at browsing history, log key strokes and completely take over a computer system. The file is delivered to victims in a phishing-like attack; either arriving as an email attachment or sent through the messaging app itself. If a potential victim opens the attachment, the malware goes to work.

Cyber criminals are using Telegram to control Toxic Eye's behavior. Because Telegram is heavily encrypted, it offers users valuable privacy protection. But it also has the ability to shield criminals from the prying eyes of law enforcement. That makes it an attractive platform for cybercrime.

Fortunately there are simple things people can do to protect themselves from victimization. The most important thing is not clicking on links or file attachments from unknown sources. Secondly, even if you do receive a file attachment or link from a known source, check with that source before clicking the link or opening the file to make sure the message is legitimate.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.