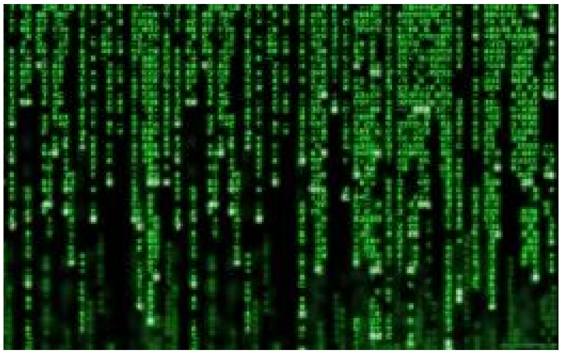
Al Qaeda suspect's porn film found to contain treasure trove of secret documents

May 4 2012, by Lin Edwards



A suspected member of the Al Qaeda terrorist group, arrested in May last year in Germany, was found with a memory stick hidden in his underwear. Police discovered the stick contained a password-protected folder with pornographic videos inside it, but suspicious computer forensic experts thought there must be more. After weeks of analysis, they determined that one of the pornographic videos contained concealed documents detailing Al Qaeda operations and plans.

The files were hidden in the video file through a process *called steganography* or concealed writing. The term steganography includes methods used for centuries, such as invisible ink, but now also includes techniques such as concealing (often unencrypted) content inside a digital image, video or audio file. Steganography conceals data within "plain sight," which makes it difficult to detect.

Digital steganography can be done on audio files by manipulating the waveform to hide data, but such changes produce noise that is more obvious than changes visible to the eye. Data can be hidden in image files opened in a text editor simply by inserting text at the end of the file, but more sophisticated and effective methods use special software to manipulate individual bytes or pixels of the media file.

For example, readily available software can be used to manipulate the properties of individual pixels within an image. The color of pixels is determined by vector values representing the intensity of each color (red, green and blue in RGB systems, for example), and these values can be manipulated to hide data.

Other steganographic software tools convert bytes of data to be concealed into individual binary bits (0 and 1) that are then substituted for the least significant bits in the media file. The substitutions are spread throughout the media file following a sequence or algorithm, to make detection more difficult and distortion of the media file less noticeable.

Another, even more sophisticated method is to manipulate the discrete cosine transform coefficients (DCTs) used to compress JPEG files to hide data into parts of an image. This method enables the hidden data to survive even if the image is later cropped, resized or compressed.

The forensic task of revealing data hidden within files is complicated because the area is rapidly developing and becoming ever more sophisticated, but security programs are available that can help researchers detect manipulations within images and other digital files.

The researchers from the German Federal Criminal Police (BKA), spent many weeks examining the hidden pornographic video found on suspected Al Qaeda member, the Austrian Maqsood Lodin, when he was arrested in Berlin after returning from Pakistan. The video, called “Kick Ass,” was stored in a password-protected folder and within the video they found a file called “Sexy Tanja.” Further analysis of this file eventually revealed that it contained more than 100 concealed unencrypted documents describing Al Qaeda plans and operations.

A video file has ample room for concealing documents, and would be relatively easy to distribute. In Maqsood Lodin’s memory stick, the porn video contained hidden terrorist training manuals in pdf form in English, German and Arabic, along with numerous documents detailing planned future Al Qaeda attacks, and lessons learned from previous operations.

Lodin is currently on trial in Berlin, and has pleaded not guilty to charges of terrorism.

Citation: Al Qaeda suspect's porn film found to contain treasure trove of secret documents (2012, May 4) retrieved 26 April 2024 from https://phys.org/news/2012-05-al-qaeda-porn-treasure-trove.html