



When I wrote earlier on the latest from [Mujahideen Secrets](#), I had only performed a cursory review of the tool and not performed a more in depth analysis. I asked one of my colleagues, Mike Blanchard

([http://www.amazon.com/AVIEN-Malware-Defense-Guide-Enterprise/dp/1597491640/ref=sr\\_1\\_1?ie=UTF8&s=books&qid=1205709616&sr=1-1](http://www.amazon.com/AVIEN-Malware-Defense-Guide-Enterprise/dp/1597491640/ref=sr_1_1?ie=UTF8&s=books&qid=1205709616&sr=1-1))

to take a look at the tool and give it the once over. I continued to examine some older documentation associated with this line of work.

Mike noticed a couple of items that I had not noticed. One in particular was the Cyrillic spelling of MYPppp located on the splash page of the tool. The analysis we came up (right or wrong) with related to what we originally thought to be a Russian hacker.

After further examination (including additional translation of help pages), it could be said that one of the authors of this product to be either a Ukrainian or Chechnyan associated with the Islamic Emirate of the Caucasus.

<http://www.kavkaz.org.uk/eng/>

Mike also discovered the use of fish on the splash page alongside the more



visible keys. We have not as yet made a tie to the fish symbol if in fact there is any relevance. Not quite sharp enough I guess.

Analysis of older documentation (Technical Mujahid) demonstrates that an earlier release of a jihadist magazine is directly aligned with the latest release of Mujahideen Secrets. The magazine has several articles written from jihadists from across the Middle East including Egypt, Morocco, and Algeria with its own chief editor and artistic director. There are direct similarities between TEQANYMAG and Mujahideen Secrets including references to the magazine in Mujahideen Secrets using the tool to encrypt and zip the file for transmission. If you'd like an overview of the magazine, see

<http://www.jamestown.org/terrorism/news/article.php?articleid=2370293> for more detail. Much like the information security community we call home, it is small and networked in any culture or language.

Many might think that most sites have been shut down relative to Mujahideen Secrets but access is still available and has been since the release of the tool. The main site is still fully accessible and available and defined in the help files of the tool.



Many tried to get access to the tool early on and complained about sites being password secured. This is true since you must sign up for access prior to gaining access. These sites are in Arabic and they do use cookies. Once you do so, there is a great deal of information to be had.

The other interesting piece of information (other than the direct swipe at the NSA and their 'weak' encryption as described by the authors of Mujahideen Secrets) was the use of digital fingerprinting that provides a nice visual comparison.

Overall, those who believe that the tool is not effective or advanced are mistaken. Those who believe the intent of this blog is for FUD, are also mistaken. This is a 'matter of fact' description of what it is. 'Secrets' runs quite well from either flash drive or PC. It says what it does and it does it. I would imagine the next version (whether it is the 4.0 of Electronic Jihad (a DoS / DDoS / Pentesting type tool) - below or Mujahideen Secrets III) to be quite robust.

Until next time - Inshallah Bukarah...



Addendum: The Dawn Media Center -