Jihadism & cryptography
From Internet to softwares

SecTor.ca

October, 2016
JULIE GOMMES
Agenda

1. Starting point of the study
2. Let’s talk about crypto!
3. Crypto tools they use and why
4. What can we learn about that?

Q & A
Who I am 1/2

Julie GOMMES

• Information Security Consultant
  • Iso 27001 compliance Lead Auditor certified
  • Risks analysis
  • Crisis management

• Lived/Worked in Egypt, Syria, Tunisia, Sudan...

• Researching on jihadist networks from years

• Find me there
  • @Jujusete on twitter
  • https://fr.linkedin.com/in/juliegommes
Who I am 2/2

Previous talks and trainings

• **Jihadism and cryptography**
  • HackFest Quebec, nov. 2015
  • BSides & DeepSec, Vienna, nov. 2015

• **How NGOs can encrypt their communications**
  • Ritimo (workshop), Paris, sept. 2015

• **Information security for journalists**
  • DefCamp, Bucarest, oct. 2014
  • MRMCD, Daarmstadt, sept. 2014
  • NDH2k14 (workshop), Paris, jun. 2014
  • HITBSecConf, Amsterdam, may 2014

• **Social Engineering, best practices for journalists**
  • NDH2k13, Paris, jun. 2013
  • Ubuntu Party, Paris, may 2013
Starting point
Terms and definitions 1/2

Djihad

“My Jihad is to break stereotypes with humor.”

What's yours?

#MyJihad billboard sample

SADAF SYED.COM
PHOTOGRAPHER
Terms and definitions 2/2

- **Cryptodjihad**
  - Using encryption / cryptography in order to perform jihad

- **Terrorism** (not used here)
  - Using fear to put political, religious, ideological pressure.
  - So many definitions (109 different according to Wikipedia) they vary on: the use of violence, the technics used, the nature of the subject, the level of organization, etc. In many definitions also involved the criterion of the number of victims.

- **Wikiterrorism**
  - Term created by the geopolitical researcher Marc Hecker, working on terrorism and social networks at IFRI. (wich is include in The Three Ages of terrorism)
    - Using/creating decentralized networks (online, humans, etc.), based on communication and where everyone contributes.
    - This helps to cover their tracks while extending an "ideal" but the other side is that those contributions are very inequal.
Evolution of pro-jihad websites

http://www.lemonde.fr/proche-orient/article/2015/06/01/l-etat-islamique-compte-2-8-millions-de-francophones-sur-twitter_4645047_3218.html
Websites and forums in french language

• Ansar Al Haqq, most famous forum (from december 2006)
  • From 2006 to 2011, 50,000 messages
  • 2010 Some members and the admin where arrested

• Assabyle => ribaat.org

• Le jardin des croyantes (Only for women)

• Nida Al Tawhid

**Most famous platforms are the one wich are supported by ground organizations**
Solid tools for communication

Al Farg Media Center and Global Islamic Media Forum (GIMF)

- The GIMF is known by the U.S. Federal Bureau of Investigation (FBI) as an "underground media" organization.

- The GIMF specializes in production of jihadist material for distribution. [1] It is one of several organizations that jihadists use to spread information via the Internet.

- This media organisation was born from the Global Islamic Media Group (GIMG) and Global Islamic Media Centre (GIMC).
Tools I used

Datas
- NodeXL
- GEPHI

Mapping
- Twitwheel (en 2014)
- GEPHI

Analysis
- Brandstweet
- Tweetstats
Evolution of twitter accounts

- First geolocalisation is **Saoudi Arabia**, before Syria, Iraq, USA, Egypt and Koweït

- **Arabic** is the most used language on pro-jihad accounts on Twitter (73 %), before english (18 %) and french (6 %)

- Every account is followed by **a thousand accounts**

- From march 15, « Anonymous » published on @CtrlSec0 account a list of pro-ISIS accounts to help to close them
  - They’ve annonced 9200 accounts
  - but new messages are already published
  - I used those accounts and the informations they published to renew my study

<table>
<thead>
<tr>
<th>Twitter accounts were used to broadcast ISIS propaganda*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 14</td>
</tr>
<tr>
<td>46.000</td>
</tr>
</tbody>
</table>

*Booking.edu
Let’s talk About Crypto !
Once upon a time...

... encryption

From Moujahdeen Secret until today

MEMRI
http://www.lefigaro.fr/international/2007/07/06/01003-20070706ARTFIG90133-secrets_de_moudjahidins_le_programme_de_cryptage_des_terroristes.php
Mojahedeen Secrets platform

- It encrypts email as well as file transfers using RSA public/private encryption systems. Sort of PGP alternative.
- Symmetric cryptography.
- Users create their own private keys.
- The application supports a file shredder feature to delete files safely.
From Moujahdeen Secret until today

MEMRI
http://www.lefigaro.fr/international/2007/07/06/01003-20070706ARTFIG90133-secrets_de_moudjahidins_le_programme_de_cryptage_des_terroristes.php
More and more smartphone tools
Sub-title

- Some people does not have Internet at home in some countries
- Easier for instant messaging
- Wikiterorism => more and more people, younger... (as WhatsApp users in Belgium last year)
- Zapping culture

New security risks for them
Geolocalisation
Lack of control (wikiterorism)
After Paris, what about now?

Telegram - 10 billion messages daily

- They could still establish private connections, Telegram admitted that it is not able to block communications that happen in private groups, which can include up to 200 users.

- “All Telegram chats and group chats are private amongst their participants,” Telegram’s spokesperson wrote. “We do not process any requests related to them.” (Telegram co-founder - Pavel Durov)

Securityaffairs.co - November 15
Paris terrorists used burner phones, not encryption, to evade detection http://arstechnica.com/tech-policy/2016/03/paris-terrorists-attacks-burner-phones-not-encryption/
Telegram and breach

Telegram. In the OS X version, text that was copied-and-pasted into the app was also written to the file /var/log/system.log

Secure messaging app Telegram leaks anything pasted in to it

Official #Telegram for MacOS logs every pasted message to syslog, even in secret chats. @durov what's going on?
Tools (finally)
Groups definition according to the tools they’re using

3 big categories

- Crazy religious
- Proof certified
- Home made tools
Crazy religious 1/2

Source: http://alfajrtaqni.net/amm.html
"Cryptography is changing, time passes and we must apply the changes in technology in this area with the command of Allah and the Sunnah of the Messenger of Allah peace be upon him"
“Proof certified” 1/2

• Using TOR, Pigdin, Cryptocat, Wickr, and Telegram encrypted chat tools, ProtonMail, RedPhone...

• Ansar-el-Dardashah, Ansar Al Ghurrabaa

• December 2015, al-Aqsa IT Team (from Al Quaeda) distributed the manual “Tor Browser Security Guidelines” for ensuring online anonymity while using Tor software.

• "Militants and extremists don't seem to find the Tor hidden services infrastructure very useful. So there are few jihadis and militants in the darknet, it's used for criminal services, fraud, extreme, illegal pornography, cyber attacks and computer crime.”*

• Want to be protected of international intelligence services

• ISIS support Tails using on his forums

• AQAP created a guide about its well using

• They download hacking tools from publicly available sources. Those program may contain custom malwares

Some extract from **guidebook**


Note: The download version (7.1) of the TrueCrypt program only and do not download new versions (7.2) for the existence of the changes and stop the encryption properties by developers for unknown reasons.

**SpiderOak service:** cloud storage service encrypted very high encryption keep confidential files where no one can not company employees see the contents of your files.

**Hushmail service:** safe and free e-mail service through which to open an account and start correspondence which ensures service encrypts messages without user intervention lies Service servers in Canada, which is one of the most secure mail services.

9/4/2015

Several cyber security to protect your network communication SOCIAL ... justpay.at

iPhone to falsify the geographical location of the image, or apply Photo GPS Editor (https://itunes.apple.com/us/app/photo-gps-editor/id471263055?mt=8) also

use an application The Serval Project for Android .7 (https://play.google.com/store/apps/details?id=org.servalproject&hl=en) devices, which makes your application is a station to communicate with other parties using the same application in the vicinity of 200 meters and the more the number of users increases, the more the vicinity of the application work, communication is done by internal numbers such as "Operator" system.
(not so) home made tools

- Twofish algorithm is in (close) every new program since 2013
- They communicate a lot
- Creating this tools means having a technical high level they don’t have
  In french language, we say “that is coded with feet
- Amn Al Mujahid par Al-Fajr Technical Committee, Tashfeer Al Jawal
So what can we learn about that?
Conclusion

- Communication: from a target to a decentralized network
- Encryption is not used just since a few days
- Increase in technical skills (creation of tools and piracy) and new recruits who are not on ground
- A different feeling according to cryptography and existing tools, creating the same separation as on the ground

Thank you!
Questions ?

https://twitter.com/jujusete

https://fr.linkedin.com/in/juliegommes
Julie GOMMES
Information Security Consultant
julie.gommes@devoteam.com