Cyber Insight

Fatemiyoun Electronic Team

aka: Fariq Fatemiyoun al-Electronic (FFE), Fatemiyoun Electronic Squad (FES)

Cyber Intelligence Bureau

a division of Laboratoire d'Epidémiologie OCD

Credits Orange Cyberdefense

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

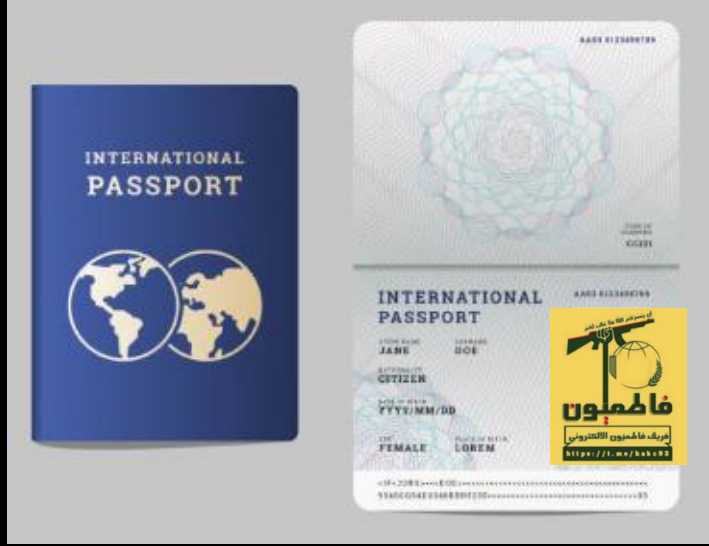
The sources have been correlated, validated and qualified as trusted sources. This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

Fatemiyoun Electronic Team

aka: Fariq Fatemiyoun al-Electronic (FFE), Fatemiyoun Electronic Squad (FES)

- Creation date: January 2020
- Strategies : DDoS, Spyware, Leaks, Smishing, Phishing
- Motivation: pro-Shiite hacktivist group linked to Iran, motivated by the defense of its religion and the promotion of Iranian interest
- Geopolitics: FES is considered a front for Kataib Hezbollah, an Iraqi Shiite militia backed by Iran
- Characteristics: supported by Iran, engaging in cyberattacks and online propaganda to defend Shia Islam
- Sectors: government organizations, computer systems and potentially critical infrastructure



Identification

Credits Orange Cyberdefense

Key Points

1
2
3
4
5
6

Structure

Hierarchical operational structure, under the control of Kataib Hezbollah (unconfirmed)

Plateform

Telegram: recruitment, coordination, communication and propaganda

Financing

Direct funding by Iranian government agencies, Provision of IT equipment and infrastructure Training and technical expertise

Associated project

Leaks sales, ransomwares

Motivations

disinformation, motivated by the defense of its religion and the promotion of Iranian interest

Targets

Targets and seeks to discredit the Iraqi government, considered too close to the United States, but also other governments of countries

Credits Orange Cyberdefense

Vectors of Influence

1

Identity and Loyalty

The Fatemiyoun Electronic Team uses Telegram to spread propaganda, coordinate attacks, and recruit new members, including young technical talent, to increase its hacking capabilities. The group works closely with other pro-Iranian groups, such as Unit 10,000, and manipulates a sense of identity and belonging to build loyalty and mobilize its supporters.

2

Propaganda

The group exploits social media to conduct smear campaigns, disinformation, and incite violence against its targets.

3

Discredit

The group spreads false information to discredit its adversaries, manipulate public opinion, and sow discord.

4

Strategies

The group participates in online vigilantism by harassing, intimidating, and threatening individuals and organizations deemed hostile. It exploits collective fears and anxieties to create a sense of urgency and danger, pushing people to take action.

5

Sophistication

A sophisticated strategy that skillfully blends geopolitical and religious elements. The group exploits religious fervor and the sense of belonging to the Shiite community to advance Iran's interests and justify its actions. By combining cyberattacks, disinformation, and emotional manipulation, the group seeks to weaken its adversaries, influence public opinion, and strengthen Iran's geopolitical influence in the Middle East.

Credits Orange Cyberdefense

Emotional Intelligence

1 The group exploits fear and anxiety by spreading threats and manipulating information to create a sense of imminent danger

2 The group uses emotional narratives and poignant imagery to elicit compassion and manipulate empathy in its audience.

3 It stirs up anger and outrage by amplifying real or perceived grievances against its adversaries, channeling frustration into cyberattacks.

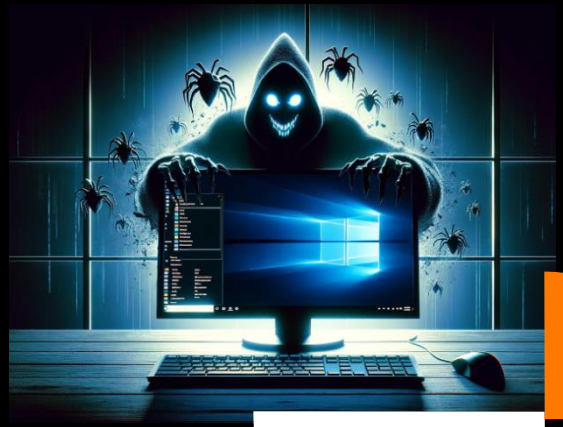
4 The group exploits a sense of belonging to a community or cause, reinforcing collective identity to build loyalty and mobilize its supporters

5 It uses partial or sensationalized information to arouse curiosity and create a sense of privilege or exclusivity, inciting engagement

6 The group uses empathy in a manipulative manner to gain the trust of potential recruits and influence them

Credits Orange Cyberdefense

Methods, Tools and services used



- Hacking websites,
- Defacing pages,
- Stealing and disclosing sensitive information,
- Spreading false information,
- Manipulating content,
- Creating fake accounts,
- Using bots to amplify propaganda,
- The group uses the reporting mechanisms of platforms like Twitter and Facebook to suspend the accounts of its opponents
- Smishing (SMS), Phishing
- Ransomwares

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government
- Diplomats
- Healthcare
- Transportation
- Technology
- Energy
- Media & Press & TV

Note

Fatemiyoun Electronic Team (FET), as an Iranian-backed group, likely targets these critical sectors to disrupt critical infrastructure, obtain sensitive information, and influence public opinion in favor of Iranian interests in the region and beyond.

Targeted Countries

United-States

Saudi-Arabia

Kuwait

Bahrain

Oman

Qatar

United-Arab-Emirates

European-Countries

Credits Orange Cyberdefense

The most dangerous hypotheses

- Sending highly targeted malicious emails or SMS messages to influential figures

Potential targets: diplomats, journalists, European politicians.

Danger: Theft of sensitive data and compromise of government systems.

- Ransomware attacks on critical infrastructures

Danger: Targeting key sectors such as energy, healthcare or transport.

- Exploitation of zero-day vulnerabilities

Using unknown security holes in widely used software.

Possible collaboration with other hacker groups to obtain these exploits.

Danger: Large-scale unauthorized access before patches are available.

- SUPPLY CHAIN attacks on software supply chains

Compromising software or updates widely distributed in Europe.

Inserting backdoors or malware into legitimate applications.

Danger: Massive and discreet infection of many European organizations.

orange Cyberdefense

Credits Orange Cyberdefense

Cyber Intelligence Bureau
a division of Laboratoire d'Epidémiologie OCD

Build a safer digital society

orange™ Cyberdefense

Credits Orange Cyberdefense