Muqawama Cyber-Surge (Part 2): Attributing Attacks to Militia Platforms

by Hamdi Malik **(/experts/hamdi-malik)** , Crispin Smith **(/experts/crispin-smith)**

Apr 25, 2022
Also available in
العربية (/ar/policy-analysis/tsad-alhjmat-alalktrwnyt-llmqawmt-aljz-althany-nasb-alhjmat-alsybranyt-aly-mnswat)

ABOUT THE AUTHORS

Hamdi Malik (/experts/hamdi-malik)

Hamdi Malik is an Associate Fellow with the Washington Institute, specializing in Shia militias. He earned his doctorate at the school of social, political and global studies, Keele University. He is a co-founder of the Militia Spotlight platform, which offers in-depth analysis of developments related to the Iranian-backed militias in Iraq and Syria. He is the coauthor of the Institute's 2020 study "Honored, Not Contained: The Future of Iraq's Popular Mobilization Forces."

Crispin Smith (/experts/crispin-smith)

Crispin Smith is an associate at a Washington-based national security law group. His research focuses on Iraqi security, human rights, and law of armed conflict issues. He is a co-founder of the Militia Spotlight platform, which offers in-depth analysis of developments related to the Iranian-backed militias in Iraq and Syria.

Brief Analysis

Part of a series: Militia Spotlight (https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight)

or see Part 1: How to Use Militia Spotlight (/policy-analysis/how-use-militia-spotlight)

Sabereen News has seemingly broadened its capabilities to include simple hacking tactics like DDoS attacks, and it might quickly proceed to more complex exploits.

As noted in P**art 1 (/node/17398)** of this analysis, the principal Telegram account claiming a recent series of cyberattacks emanating from Iraq was al-Tahirah Team, which is very clearly a subsidiary of the major *muqawama* (resistance) media outlet **Sabereen News (/node/16673)** . Over the past two years, however, the Iran-backed *muqawama* have frequently used social media brands and facade channels to claim kinetic attacks without exposing the individuals and groups who perpetrated them to legal, social, or physical reprisals. The same now appears to be true for cyber operations.

The cyberattacks that began on April 19 were not reported evenly across militia information and social media networks. A core group of channels predicted and amplified al-Tahirah Team's claims, and analysis of their posts

indicates a cross-militia operation involving at least **Asaib Ahl al-Haq (/node/16715)** and **Harakat Hezbollah al-Nujaba (/node/16716)** .

Sabereen's Evolving Role and Capabilities

Sabereen's role seems to have changed recently. As Militia Spotlight has **reported (/node/17382)** , the influential channel was banned from posting in late March and early April, possibly because Iraqi militia leaders and Iran believed it was deviating from the *muqawama* mission. Since its return on April 8, Sabereen has created a number of subsidiary channels, refocused its reporting on Iraqi *muqawama* issues, and now perhaps added a cyberwarfare capability that has already been against Iran's enemies.

Previously, Sabereen had not performed many activities outside of disseminating *muqawama* news and propaganda, though at various points in its history it has enjoyed suspiciously good access to *muqawama* operations and influenced attackers. The channel has a "research team" ("Sabereen for Security Studies and Analysis"), though this side outlet has mostly engaged in reposting Sabereen's flagship content. In fact, the research team may comprise the same individuals as the main channel.

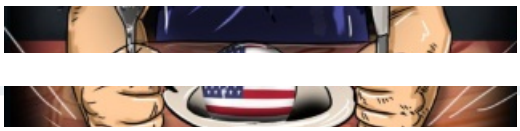
Since Sabereen never previously demonstrated any cyber capability to speak of, its apparent connection to the latest wave of attacks could mean that a new team with new skills has been absorbed into the wider Sabereen group, or perhaps contracted on a per-job or retainer basis. Such a personnel upgrade may have been necessary even for the basic attack method used so far: distributed denial of service (DDoS).

Alternatively, the Sabereen brand may have been used to propagandize the cyberattacks of a non-Sabereen entity, thus obfuscating the campaign's true origin. For instance, Iran has demonstrated significant capability to conduct cyber espionage and disruptive cyberattacks, using both as core tools of statecraft to understand and shape the regional environment and retaliate against its enemies.

What Next?

The cyber actor behind these DDoS attacks will likely continue targeting websites belonging to the enemies of Iranian security agencies and the Iraqi *muqawama*. This could include further targets in Israel, Turkey, and Saudi Arabia, as well as the United Arab Emirates, Iraqi Kurdistan, and Iraq's body politic. Al-Tahirah Team has also posted a graphic indicating an interest in targeting U.S. websites (Figure 1).

At present, the actor responsible does not appear capable of launching operations other than DDoS website attacks, though *muqawama* propaganda surrounding the recent incidents indicates an interest in more sophisticated attacks on critical infrastructure. By drawing on Russian assistance and/or the active commercial market for hacking services, the *muqawama* could quickly enhance their available attack options if they decide to escalate. ❖



PART OF A SERIES

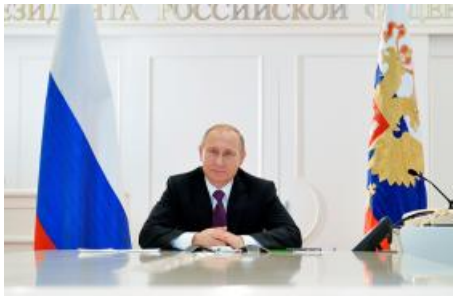
Militia Spotlight (/policy-analysis/series/militia-spotlight)

How to Use Militia Spotlight
(/policy-analysis/how-use-militia-spotlight)

Muqawama Cyber-Surge (Part 2): Attributing Attacks to Militia Platforms
(/policy-analysis/muqawama-cyber-surge-part-2-attributing-attacks-militia-platforms)

Muqawama Cyber-Surge (Part 1): Chronology of Recent Attacks
(/policy-analysis/muqawama-cyber-surge-part-1-chronology-recent-attacks)

RECOMMENDED



ARTICLES & TESTIMONY

We Can't Face Down Putin Alone

May 6, 2022
◆
Dennis Ross
(/policy-analysis/we-cant-face-down-putin-alone)

BRIEF ANALYSIS

Hezbollah-Shia Dynamics and Lebanon's Election: Challenges, Opportunities, and Policy Implications

May 12, 2020, starting at 12:00 p.m. EDT (1600 GMT)

◆

Hanin Ghaddar,
David Schenker,
Bashshar Haydar

(/policy-analysis/hezbollah-shia-dynamics-and-lebanons-election-challenges-opportunities-and-policy)

BRIEF ANALYSIS

Building an Arab-Israel Bloc: Can It Compensate for a Reluctant Washington?

May 10, 2022, starting at 3:30 p.m. EDT (1930 GMT)

◆

Nickolay Mladenov,
Ebtesam al-Ketbi,
Zohar Palti,
Karim Haggag

(/policy-analysis/building-arab-israel-bloc-can-it-compensate-reluctant-washington)

TOPICS

Military & Security (/policy-analysis/military-security)

Shia Politics (/policy-analysis/shia-politics)

Terrorism (/policy-analysis/terrorism)

REGIONS & COUNTRIES

Gulf States (/policy-analysis/gulf-states)

Iran (/policy-analysis/iran)

Iraq (/policy-analysis/iraq)

Israel (/policy-analysis/israel)