OFFENSIVE CYBER GROUP IN DEPTH

A Macquarie University
CiLab - PACE Project
DarkMatter promotes itself as a top tier cyber defence group, and claims to offer services protection against potential threats for government agencies, enterprises and individuals. It leverages a range of protocols, products and services, such as network security, bug sweeping and a 'cyber-secure' mobile phone.

DarkMatter was founded in the United Arab Emirates (UAE) in 2014 following Project Raven, an offensive operational division of the UAE’s Signals Intelligence Agency (SIA), which monitored opposition to the Emirates government. The Project hired former intelligence operatives from the USA and other countries, including whistleblower Lori Stroud from the NSA who exposed widespread abuses. Stroud professed that fellow Americans, political rivals, human rights activists and those criticising the Emirati government were being targeted.

Allegedly a hacking service, DarkMatter utilises surveillance techniques taught by ex-NSA intelligence officers to hack and shut down threats - all being concealed under the idea of national security.

Through the analysis of the company’s background, executive team, technical means, principal targets as well as its ties with other organisations, we can conclude that DarkMatter is not a typical cybersecurity company. It can be more closely described as offensive cyber for hire. They assist the UAE and other gulf nations and their intelligence agencies to conduct offensive cyber intrusions and surveillance of individuals both at home and abroad that are critical of their actions.
FOUNDER AND CEO

FAISAL AL BANNAI
Faisal Al Bannai founded DarkMatter in 2014 before it was sold to multiple parties in late 2019. Al Bannai is the son of a retired major general of the Dubai police and was also the founder of Axiom Telecom. He has since become the CEO and Managing Director of EDGE, a conglomerate of 25 state-owned and private companies, which develop 'state-of-the-art' technologies and solutions in areas such as cyber defence, missiles, electronic warfare and intelligence.

KARIM SABBAGH
Karim Sabbagh was appointed CEO of DarkMatter in 2018. Sabbagh was once the Senior Vice President of Booz Allen Hamilton (1998-2003), the firm that employed whistleblower Edward Snowden who leaked sensitive information about US surveillance programs in 2013. Previously, he served as the President & CEO of SES (2013-2018), a Luxembourg firm that provides secure satellite and ground communications solutions. He departed in 2019 after DarkMatter was acquired.
DarkMatter is a sophisticated threat actor capable of deploying a wide range of technical and deception techniques against their targets.

DarkMatter focuses mainly on offensive strategies using social engineering tactics with malware to steal information and infiltrate their targets (Marczak & Scott-Railton 2016a).

DarkMatter’s Project Raven used many tools to carry out offensive cyber-attacks such as spear phishing, installing backdoors, exploiting zero-day vulnerabilities and installing malware (Farley 2019).

Their most well-known spyware is called Karma, which was bought from a foreign vendor whose name and location could not be determined (Bing & Schectman 2019d).

Karma provided the UAE with the ability to hack iPhones throughout 2016 and 2017 to obtain photos, emails, text messages and geolocation information from their target’s smartphones.

This also gave UAE the ability to access saved passwords, which allowed access to other personal data and information (Bing & Schectman 2019a).

Karma granted access to iPhones by uploading phone numbers or email accounts into an automated targeting system.

Although the tool does not work on Android devices and is unable to intercept phone calls, it remains potent since it did not require a target to click on the link that is sent to compromise their mobile devices.

It is believed that Karma was no longer used by late 2017, when iPhone software security updates made it less effective.

However, DarkMatter has continued its surveillance operations since then either through an improved variant or the use of other tools at their disposal.
DarkMatter’s project Stealth Falcon carried out an attack on state-run Qatar News Agency. DarkMatter used the below methods to publish fake news articles to dispute official Qatari statements (Al Jazeera 2017).

Figure 1: Example of Technical Means and Methods: Stealth Falcon.

- **ZERO-DAY EXPLOITS**
  DarkMatter constantly use Zero-Day exploits in the targets software to gain access to their systems

- **SOCIAL ENGINEERING**
  DarkMatter use In-House developed exploits and social engineering to carry out attacks

- **SPYWARE**
  DarkMatter also use enterprise spyware solutions purchased from external firms

Source: Graphic made with information sourced from Marczak & Scott-Railton 2016b.
Ahmed Mansoor (pictured right), a well-known Emirati activist, has been revealed as a key target of Project Raven for a number of years.

Through evidence revealed in first-hand accounts that were published in 2019, Reuters mentioned that Mansoor was targeted by DarkMatter after publicly criticising UAE’s war in Yemen, the treatment of migrant workers and detention of political opponents.

Mansoor was also surveilled by the UAE government and DarkMatter through the cyber-espionage platform, Karma.

As a result of the covert surveillance, Mansoor was sentenced in a secret trial in 2017 for allegedly ‘damaging the country’s unity’ and sentenced to 10 years in jail.

Mansoor was not the only target. In 2017, the mobile device of his wife, Nadia, had also been monitored by Project Raven using Karma. They gave her the code name ‘Purple Egret,’ which was revealed in the program’s exposed documents.

Mansoor was also the target of another offensive cybersecurity firm (NSO Group) affiliated with the Israeli government. NSO Group made its first deal with the UAE in 2013, and were caught one year later deploying NSO spyware into Mansoor’s mobile phone.

**TARGETS**

Whilst the development of UAE cyber capabilities was associated with mitigating terror threats following 9/11, individuals that became their targets go well beyond the category of ‘terrorists’.

DarkMatter continues to act in accordance with UAE’s political agenda to preserve the status quo and targets individuals including human rights activists, journalists and dissidents who challenge or criticise the regime.

**HUMAN RIGHTS ACTIVISTS AND THEIR AFFILIATED ORGANISATIONS**

DarkMatter is suspected of targeting human rights activists that criticise the UAE government.

Ahmed Mansoor (pictured right), a well-known Emirati activist, has been revealed as a key target of Project Raven for a number of years.

Through evidence revealed in first-hand accounts that were published in 2019, Reuters mentioned that Mansoor was targeted by DarkMatter after publicly criticising UAE’s war in Yemen, the treatment of migrant workers and detention of political opponents.

Mansoor was also surveilled by the UAE government and DarkMatter through the cyber-espionage platform, Karma.

As a result of the covert surveillance, Mansoor was sentenced in a secret trial in 2017 for allegedly ‘damaging the country’s unity’ and sentenced to 10 years in jail.

Mansoor was not the only target. In 2017, the mobile device of his wife, Nadia, had also been monitored by Project Raven using Karma. They gave her the code name ‘Purple Egret,’ which was revealed in the program’s exposed documents.

Mansoor was also the target of another offensive cybersecurity firm (NSO Group) affiliated with the Israeli government. NSO Group made its first deal with the UAE in 2013, and were caught one year later deploying NSO spyware into Mansoor’s mobile phone.

Source: Human Rights Watch 2019
DarkMatter is suspected of attacking journalists and their close associates for criticising the UAE Government.

**Rori Donaghy** (pictured right) from the United Kingdom (UK) was targeted by Project Raven, which later became known as DarkMatter.

Unbeknownst to Donaghy, he was considered a top national security target of the UAE government for over five years.

He was previously a news editor with the Middle East Eye who also acted as the Director of the Emirates Centre for Human Rights from 2012 until 2014, a UK human rights organisation centred on the UAE.

Similar to Mansoor, his relatives, partner and close associates became the targets of surveillance by DarkMatter.

Posing as a human rights activist, a Raven operative initiated contact with Donaghy online and prompted him to download a piece of software.

**Image 1.** A phishing email containing a link, which requires no user interaction to install the malware received by Donaghy. Source: Marczak & Scott-Railton 2016b

From: the.right.to.fight@openmailbox.org

Subject: Current Situation of Human Rights in the Middle East

Donaghy, We are currently organizing a panel of experts on Human Rights in the Middle East.

We would like to formally invite you to apply to be a member of the panel by responding to this email.

You should include your thoughts and opinions in response to the following article about what more David Cameron can be doing to help aid the Middle East.

http://aaz.me/d0ddde

Thank you.

We look forward to hearing back from you,

Human Rights: The Right to Fight

The perpetrator sent numerous emails and tweets from UAE citizens’ accounts who had previously been arrested by authorities featuring URLs embedded with their spyware.

Donaghy suggested that it was common for the UAE to take control of the accounts of arrested political activists or dissidents in an attempt to lure in other targets they would want to surveil.

**Image 2.** The link contained a document detailing a plea to uphold human rights directed to unsuspecting victims. Source: Marczak & Scott-Railton 2016b
Following the Arab Spring, there was mass instability within the region, with uprisings posing a major threat to the UAE Monarchy.

International media has reported that Qatar was a strong supporter of the uprisings and a known backer of rebel groups that attempted to overthrow the Syrian President at the time. This added to existing frictions between the UAE and Qatar.

This led DarkMatter to launch an attack on hundreds of Qatari government officials in 2014.

More recently, there was an attack launched against the United Nations offices in New York. The intention behind the act was to compromise email accounts belonging to the diplomatic representatives of governments considered rivals of the UAE.

A UN spokesperson has confirmed that there was a security incident that was identified but did not confirm whether any information was breached or acquired from the attack.

The attack also targeted FIFA executives, which was believed to be politically motivated (Bing & Schectman 2019c).

The UAE intended to access damaging information against Qatar, through the hacking of FIFA executive accounts. Collected information would then be used to embarrass Qatar, and draw into question their bid for the 2022 FIFA World Cup (Ahmed 2019).

However, it has been difficult to establish a pattern in victimisation beyond opponents of the UAE.
NETWORKS

DarkMatter has close ties to both domestic and foreign entities consisting of state-sponsored and private cybersecurity companies. These organisations, similarly to DarkMatter, also share an interest in developing offensive cyber and state surveillance capabilities.

Known to work closely with UAE's government and intelligence agencies, DarkMatter and its networks are part of a growing number of entities that are utilised by the Emirati government to carry out its national security objectives.

PAX AI

PAX AI is a subsidiary of DarkMatter, previously known as Pegasus. PAX AI is headed by CEO Peng Xiao and has become a division of Group 42 (G42), a leading artificial intelligence and cloud computing company based in the UAE. G42 is known to be the sole registered shareholder of ToTok, a messaging app that has been used by the Emirati government as a spying tool.

Through G42, PAX AI has ties with the country's intelligence apparatus and Emirati officials, such as Tahnoun bin Mohammed Al Nahyan, the country's National Security Advisor and son of the founding father. It has been under scrutiny for hiring former NSA, CIA and Israeli intelligence operatives to conduct state surveillance against journalists, human rights activists, and dissidents (Associated Press 2020).

PAX AI is also reportedly capable of monitoring any individual in the UAE with the use of surveillance devices implanted in cities, working closely with the Dubai police in big data and 'Smart-City' solutions (Benito 2020).

Although PAX AI representatives refuse to comment on DarkMatter, LinkedIn accounts reveal that G42 and PAX AI have absorbed many former DarkMatter employees into their companies over the years (Associated Press 2020).
In 2017, Huawei signed a global Memorandum of Understanding (MoU) with Pegasus (now PAX AI) on solutions for ‘Smart-City’ and big data.

The agreement solidified their partnership in developing technology and professional capabilities, such as Huawei’s Public Safety Cloud and Big Data Solution, as well as Pegasus’ Big Data Analytics applications. The MoU also aimed to increase cooperation in order to share, exchange, store and process data between the two entities (Olt News 2020). This would allow Huawei to collect actionable intelligence to provide 'Smart City' solutions.

However, Huawei has also received criticism for investing heavily in surveillance equipment, facial recognition technology and wireless access controllers, which could be used for state surveillance.

Huawei and Pegasus signed a MoU agreement in 2017.
Source: TRT/Huawei

CyberPoint was founded in Baltimore, Maryland, by Karl Gumtow in 2009. The company was responsible for recruiting as well as facilitating the transition of retired NSA operatives, including DarkMatter’s whistleblower Lori Stroud, to be involved in Project Raven (Malicious Life n.d.).

Reports have revealed that the Emirati government requested CyberPoint to train members of its Signals Intelligence Agency (SIA) and sell surveillance equipment that would later be used to monitor US citizens (Sarmin n.d.). American staff however were not willing or able to perform those operations.

As a result, DarkMatter replaced CyberPoint in 2015 as the UAE grew increasingly uncomfortable with their core state intelligence program being controlled by foreigners. Consequently, UAE defense officials provided CyberPoint staff the option to join DarkMatter or leave, to which many chose the former (Rahman Sarmin n.d.).
NSO Group was founded in Israel, and is a DarkMatter competitor. Although improved bilateral relations between the UAE and Israel could witness increased cooperation, governments and cybersecurity firms in the Middle East compete fiercely in luring top hacking talents from countries such as Israel and the United States (Ganon and Ravet 2020).

According to a New York Times report (2019), DarkMatter and other cybersecurity firms in the region recruit operatives from Unit 8200 - Israel’s elite signals intelligence group - with promises of extravagant salaries and lavish properties. In 2017, NSO Group was reported to have lost a considerable portion of its Unit 8200 graduates to a research and development facility owned by DarkMatter in Cyprus (Ziv 2019).

NSO Group developed its own surveillance tool named Pegasus (not to be confused with the DarkMatter subsidiary) capable of intercepting phone calls, texts, emails, contacts, location and any data transmitted over apps like Facebook, WhatsApp and Skype.

Additionally, NSO Group assisted countries such as the UAE and Saudi Arabia using Pegasus to surveil renowned slain Saudi critic Jamal Khashoggi.

Image 4. Pegasus, a spying tool that is capable of hacking Android and iOS devices.

Source: Khandelwal 2018.
CONCLUSION

DarkMatter was founded by Faisal Al Bannai in the UAE in 2014, and has been mired in controversy for working with the country’s intelligence apparatus to conduct cyber intrusions and state surveillance.

DarkMatter relies on offensive strategies and techniques taught by former intelligence operatives from countries such as the US and Israel, sending spear-phishing emails with malware to infiltrate their target’s mobile devices to steal information.

The Group portrays itself as a provider of cyber protection solutions. However, it has been exposed for committing a number of high-profile intrusions against prominent human rights activists, journalists, governments including their own officials and citizens who are critical of the UAE such as Emirati activist Ahmed Mansoor and British journalist Rori Donaghy.

The main spyware tool used is known as Karma, which was able to exploit specific iPhone security vulnerabilities to grant access to data stored on their target’s smartphone, including photos, emails, text messages and geolocation information.

Moreover, DarkMatter has ties with other state-sponsored cybersecurity and defense entities in the UAE. This includes Pax AI and Group 42, sharing personnel, techniques and technologies.

In conclusion, DarkMatter is not the image it portrays to the general public. The group undertakes illegal operations and pose a large threat to individuals and organisations, though it remains difficult to establish a pattern of victimisation beyond opponents of the UAE.
AUTHORS

This report was prepared in collaboration with:

**CiLab Master Interns:**
Amanta Cotan
Andreane Laurin
Priandhini Triana Asih (Leader)

**PACE Team Members:**
Omar Moussa
Michela Mueller
Ellen Munns (Leader)
Hannah Power
Emily Rich
Sydney Smith
Chloe Summersson
Rachael Tuilaselase
Emilia Turnbull (Leader)
Sam Vasic
Olivia Zibara

**Academic Mentors:**
Stephen McCombie
Fred Smith
Allon J Uhlmann


BIBLIOGRAPHY


BIBLIOGRAPHY


