Exposing the UAE's Underground Digital Dangers: The Attack Surface of One of the Most Digitally Advanced Countries in the Arab World

ke-la.com/exposing-the-uaes-underground-digital-dangers-the-attack-surface-of-one-of-the-most-digitally-advanced-countries-in-the-arab-world/

May 30, 2021

The **UAE has gained global attention for the incredible improvements the country has gone through over the last few decades. While the UAE's economy continues to flourish, cybercriminals will carry on with their efforts of trying to identify where their next worthy targets may be.** With the growing success of advancing their economy and technological capabilities, UAE-related entities must continue to push their cybersecurity efforts as well to ensure that their wealth will not be harmed by lucrative cybercriminals operating in the cybercrime underground ecosystem. This research lays out the major underground digital dangers that KELA's researchers have identified posing a threat to UAE-related entities.
The research's highlights include:

- During the last six months (December 2020-May 2021), **KELA observed numerous compromised network access listings to UAE-related private and public entities offered for sale on cybercrime forums, including one that was possibly used in an attack by the Avaddon ransomware gang**.
- Among these, **KELA detected several threat actors specifically targeting UAE entities**, by selling data and network access related to UAE companies.
- KELA discovered that **UAE-related email addresses were exposed more than 1.2 million times**, with more than 200,000 of them being related to employees of government, educational, academic, and nonprofit entities.
- KELA also identified **more than 68,000 compromised accounts related to UAE users** on corporate portals, social media, e-commerce stores, and government websites.

Exposure of the Humans: Diving into UAE Organizations' Compromised Credentials and Accounts

Controlling every move made by employees is never simple, especially in organizations where employees are connecting from all different locations and may be registered to all types of services with their corporate email addresses. To kick off this research, KELA looked into the possible leaked credentials or compromised accounts pertaining to UAE-related entities, which could provide cybercriminals with what they need to compromise an organization. Let's first put the terms upfront:

Leaked Credentials refer to credentials from various breached databases constantly traded and circulating in the underground. For the most part, these databases include private and corporate email addresses and associated passwords, including plaintext ones. This data can enable attackers to access the company's resources and provide further malicious activity, such as account takeover attacks, social engineering, phishing, and malware spreading campaigns.

Compromised Accounts refer to credentials, cookie sessions and additional technical fingerprints which are offered for sale on automated underground marketplaces such as Genesis and more. These accounts are breached and stolen from victims' computers generally via infections by banking trojans or other stealers. Such accounts can grant access to tools and software used in a targeted environment, such as RDP, VPN solutions, and more. They could be leveraged by a sophisticated actor to gain initial network access to the relevant corporate network.

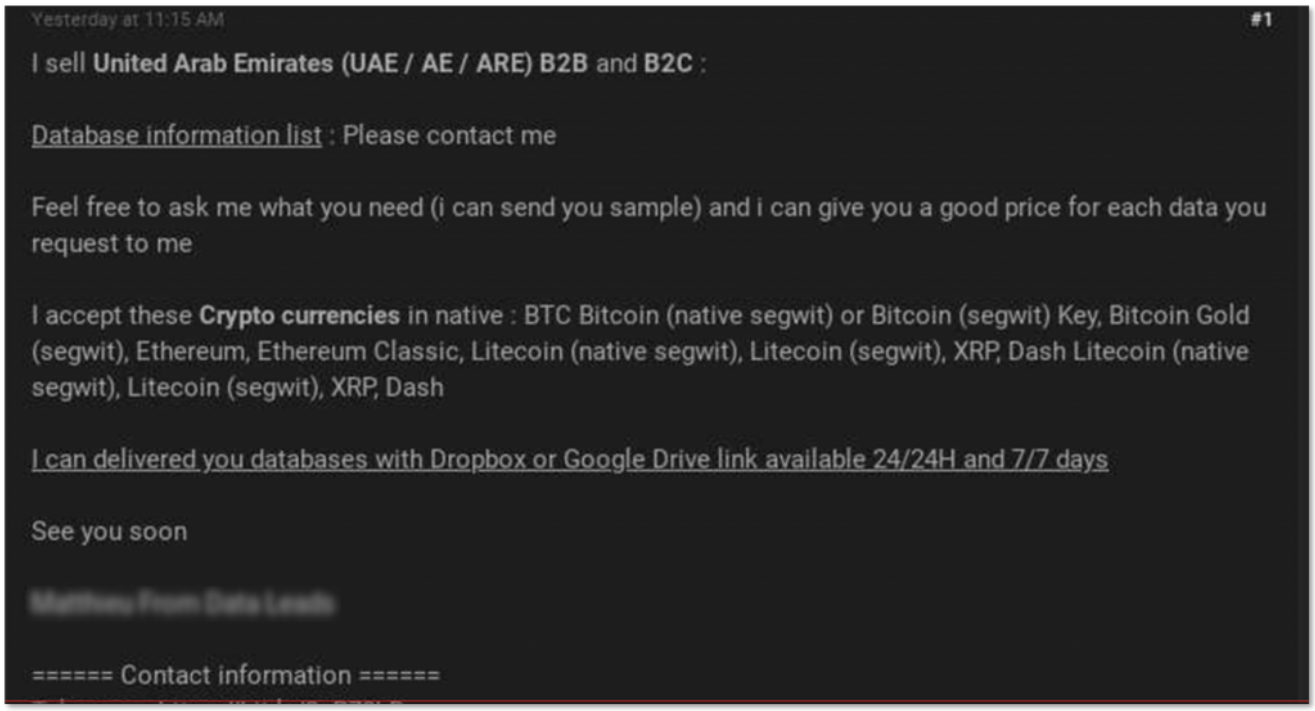
Upon analyzing this data, we identified that compromised UAE data is generally seen due to third-party breaches and leaks – such as in the recent Facebook dump, however, we also identified the Middle East- or UAE-specific offers being offered by criminal actors in underground forums. These databases can contain personal and corporate email addresses, passwords, phone numbers, corporate documents, internal information of companies, and more.

The most typical offers that our research identified include:

Databases containing companies' information

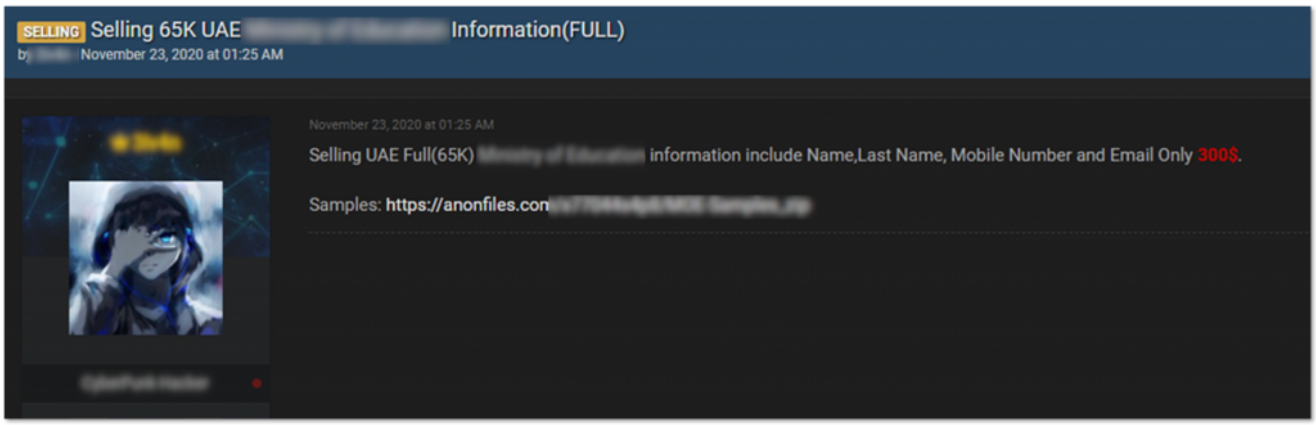
Among several, KELA's researchers have handpicked just a couple of examples to showcase the severity of compromised company information being traded between criminal actors. One recent offer we identified was a threat actor offering a database for sale most likely containing leads' contact information of various B2B and B2C businesses in the UAE. Another interesting listing contained data of a major UAE telecommunications company, including its users' usernames and passwords, employees' information, contract files, and payment details.

These exposed details can be abused by cybercriminals in many different ways. For instance, cybercriminals can leverage the victims' contact details to execute phishing or social engineering attacks, allowing them to possibly steal further information from these users or lure them into transferring money. The contract files and other sensitive data, on the other hand, can be used for even further damage, such as demanding ransom or trading it with unscrupulous competitors. Finally, when corporate credentials are leaked in these databases, cybercriminals can leverage these to perform business email compromise (BEC) attacks and, in some cases, to gain an initial foothold in a network in order to perform lateral movement and plant malware.

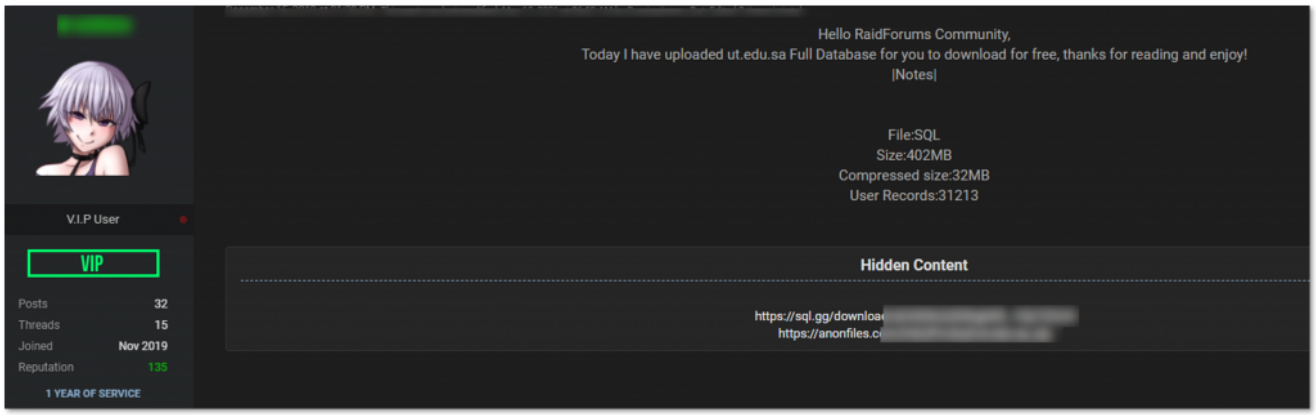


Users selling UAE databases.

Databases containing government and educational entities' data.
Cybercriminals often target government entities via phishing and social engineering attacks using data leaked or bought on cybercrime forums. Recently, KELA observed an instance of a user trying to sell data belonging to a UAE ministry. Such data has been in demand for quite some time already; in 2019, a user leaked a database belonging to a university in the UAE, and as other members are still interested in it, the publisher periodically updates the download link to enable everyone to access the data.

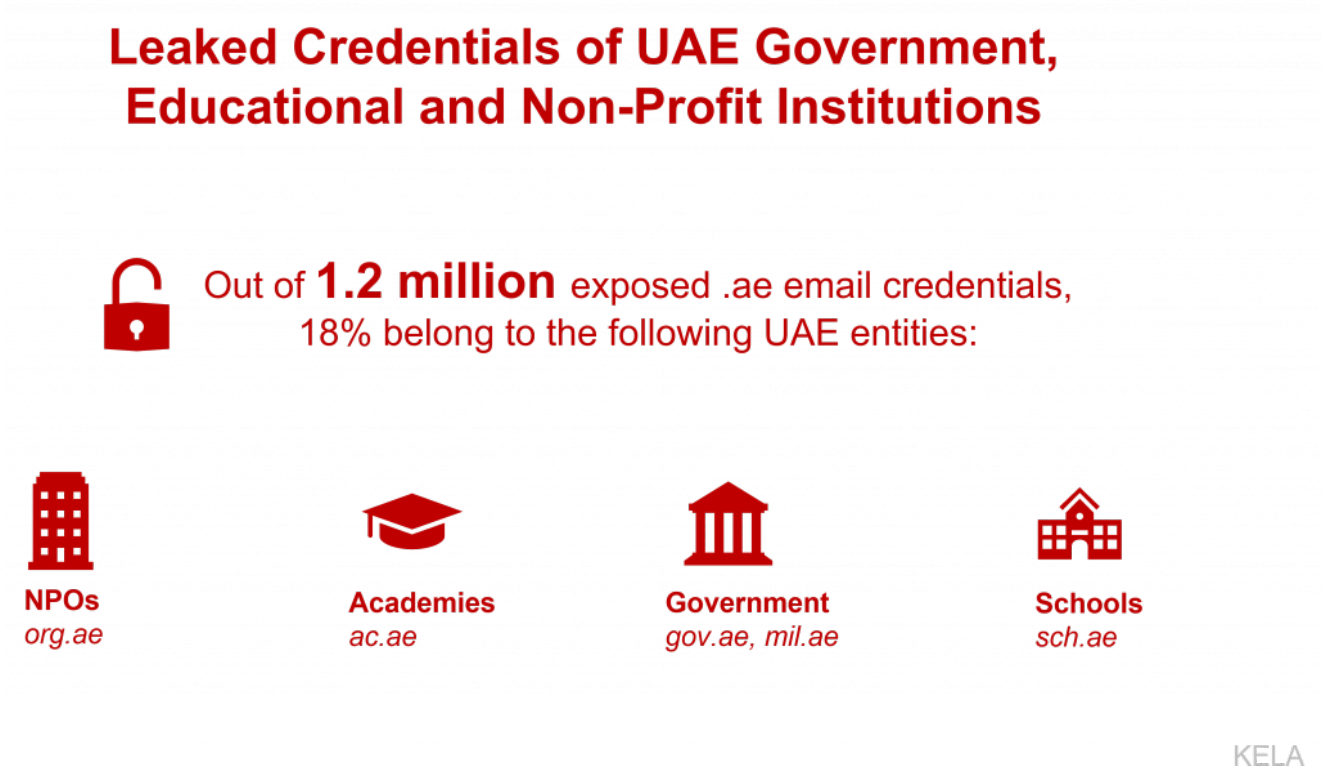


A user selling data of a UAE's ministry.



A user offering a database of a university in the UAE in 2019, which is still in demand.

Such leaks and sales result in massive amounts of leaked credentials available for cybercriminals to use in order to conduct phishing, social engineering, BEC, and other attacks. When analyzing leaked credentials pertaining to certain domains associated with government and educational institutions (gov.ae, ac.ae, mil.ae, sch.ae, org.ae), KELA discovered more than 221,000 leaked credentials of their personnel.



Leaked credentials found through KELA's solutions (the overall number of leaked credentials is the minimum exposed quantity since it's based on the .ae TLD, while many UAE companies have international TLDs)

Dumps of documents

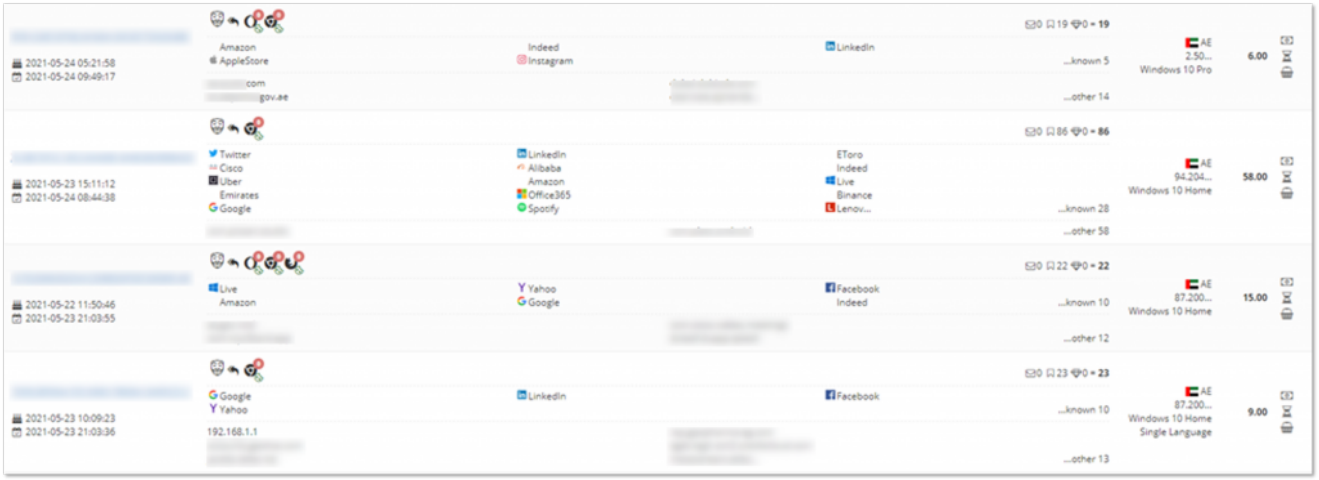
KELA has recently observed users offering scans of UAE passports and IDs. Such data can be used for various fraudulent activities, including manipulation of personal data for cybercriminals interested in taking advantage of citizens' financial aid. This phenomenon has only grown during 2020 as more and more cybercriminals were interested in taking advantage of COVID-19 aid packages offered for those in need globally.

A user offers UAE passports, IDs, CVs, and photos (auto translated from Russian)

However, leaked credentials and personal information aren't the only way that cybercriminals could take advantage of UAE users and companies. As mentioned above, another common way is through compromised accounts – logins and passwords to accounts that grant access to tools and software used on a compromised computer, such as RDP, VPN solutions, and more, which are usually being sold through underground automated shops.
If the compromised machine resides in a corporate environment, these offerings, which are for sale for just a few dollars per bot (computer), provide criminal actors with unauthorized access to systems that could allow them to perform a variety of large-scale attacks, ranging from attacks such as social engineering to malware attacks. KELA identified at least 68,000 compromised accounts to tools and software used in UAE-related entities (based on the .ae top domain).

SERVICE	USER NAME	PASSWORD	BOT IP
https:// gov.ae/ords/f			
https://www gov.ae			
https:// gov.ae			
https://www gov.ae/en/customer/my-a...			
https: gov.ae/irj/portal/anonymous			
http:// gov.ae/			
https://www. gov.ae/Ar/pages/register.a...			
https://www gov.ae/en/Pages/Default.as...			

A few examples showing compromised accounts available for UAE government services (taken from within KELA's DARKBEAST)

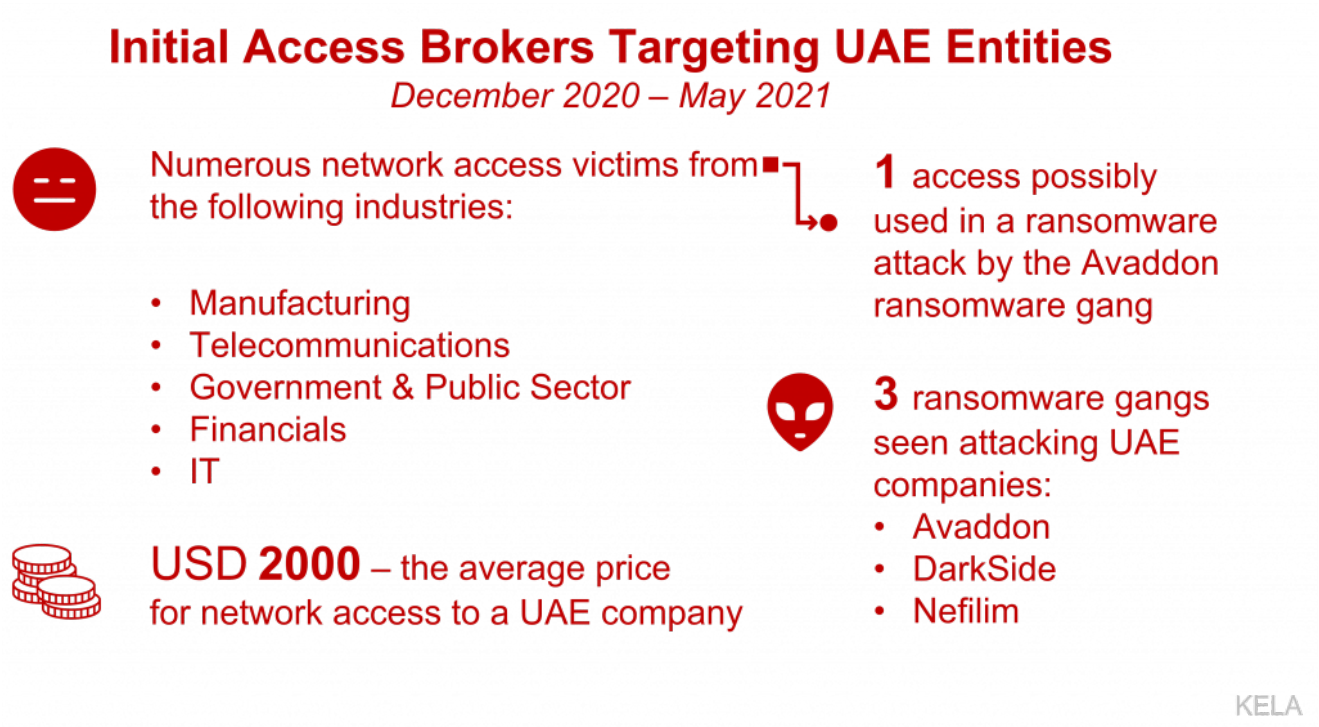


Bots offered on one popular underground market and enabling access to social media, e-commerce sites, corporate and government portals.

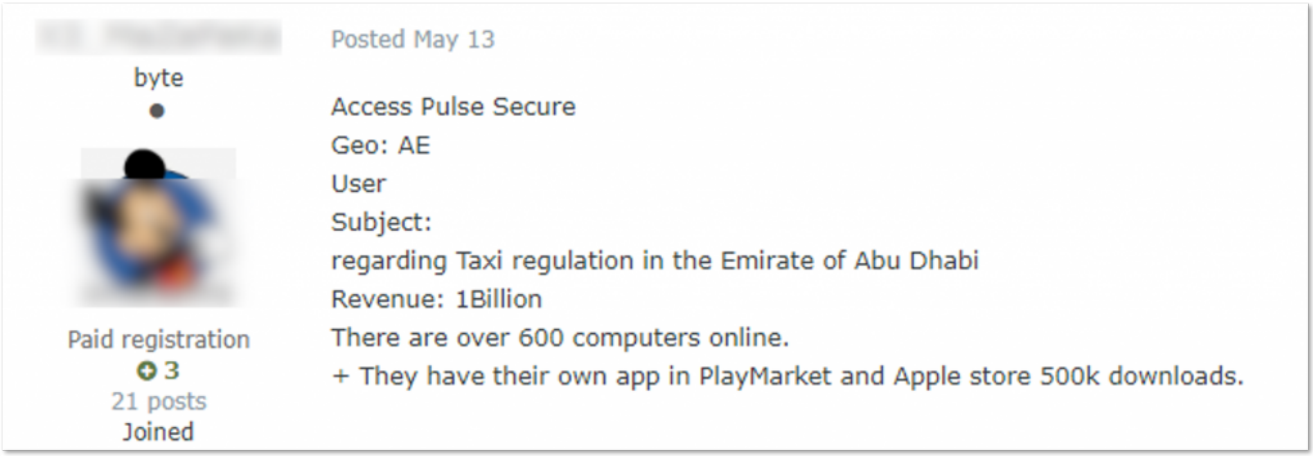
The Path to a Ransomware Attack: Initial Network Access and Ransomware in the UAE

Initial network access listings offered on underground forums can serve as entry points for ransomware operators and other malicious actors looking for a foothold into a victim's network. Initial Access Brokers – the actors selling those accesses, offer these items for sale so that buyers can purchase them to attempt to move laterally within the targeted network and to deploy ransomware or steal intellectual property. **During the last six months (December 2020-May 2021), KELA observed numerous UAE accesses offered for sale**

on underground forums. Each of these accesses can be turned into millions of dollars of ransom demanded by buyers who would manage to leverage them to infect the victims with ransomware.

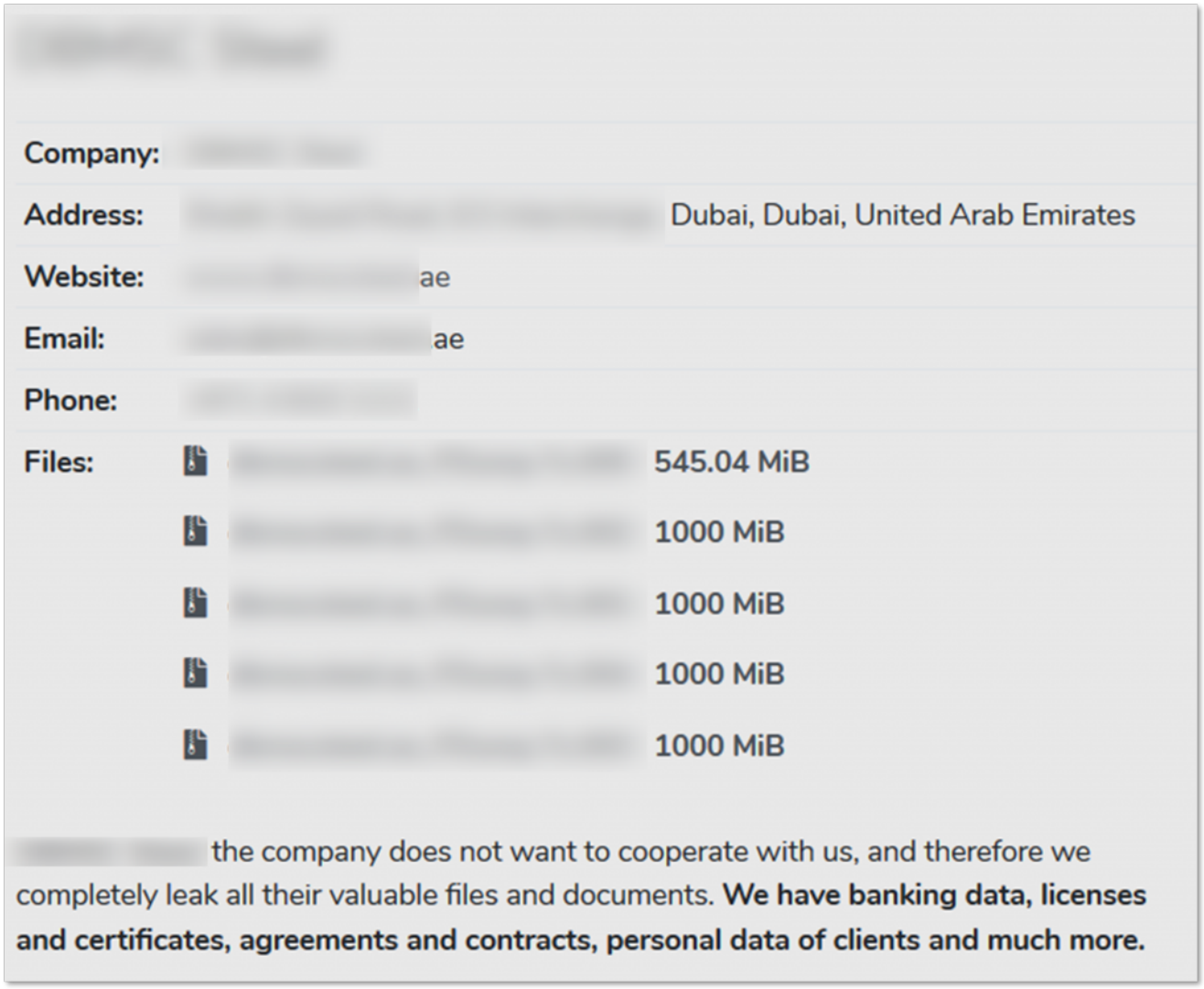


KELA regularly tracks initial access brokers and the network accesses that they are selling on a daily basis. The image below shows a typical example of a network access listing published for sale on an underground forum.

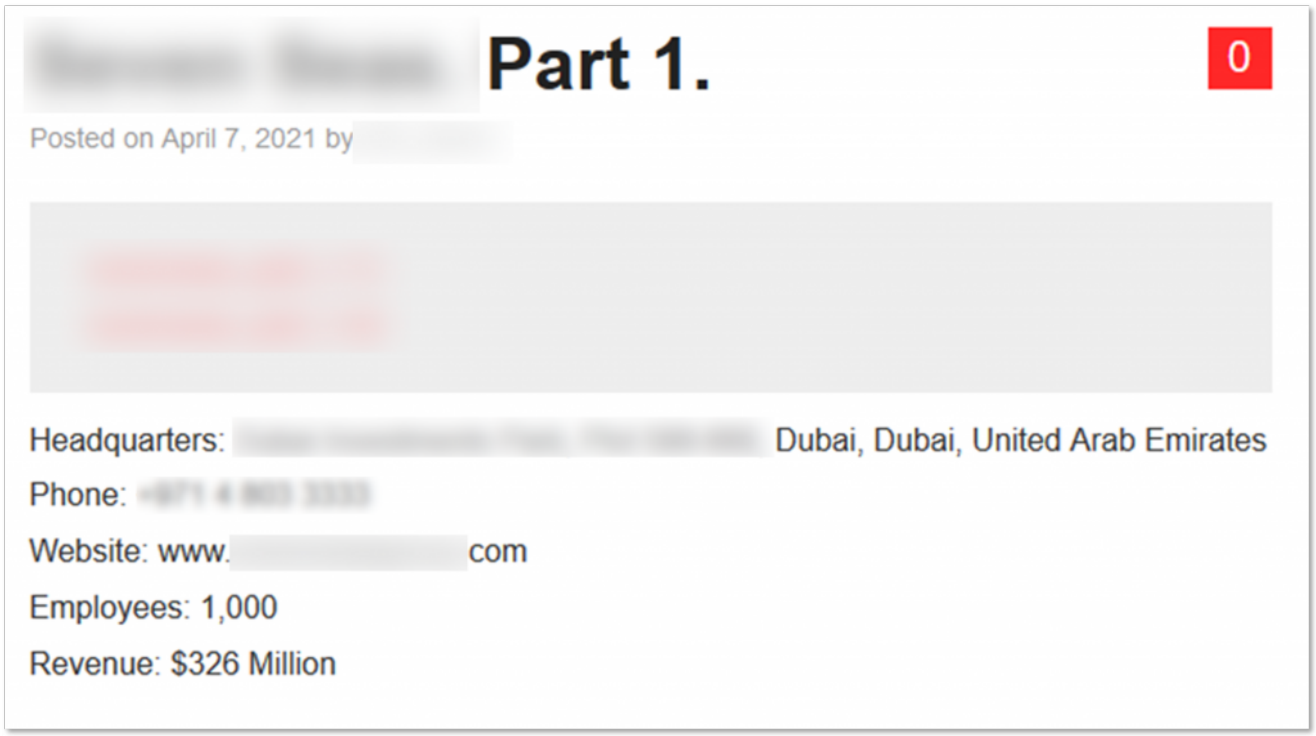


A user selling Pulse Secure VPN access to a UAE government body.

Though identifying the direct connection between the network access sale and a ransomware attack is not always possible, we observed an instance in which a recently sold network access seems to have possibly resulted in a ransomware attack on a manufacturing company based in Dubai. On March 31, 2021, Avaddon ransomware operators published a blog post claiming they hit the company and published “proof-of-breach” documents pertaining to the company. Prior to this event, on March 8, 2021, a threat actor offered for sale access to a UAE-based manufacturing company in a private conversation with KELA. Since the offer was made about a month prior to Avaddon disclosing the victim, it is possible that the actor sold the access to one of Avaddon’s affiliates who then exploited it to get into the system and infiltrate the network with the Avaddon ransomware. The data of the victim was leaked in full after the victim apparently refused to pay the ransom.

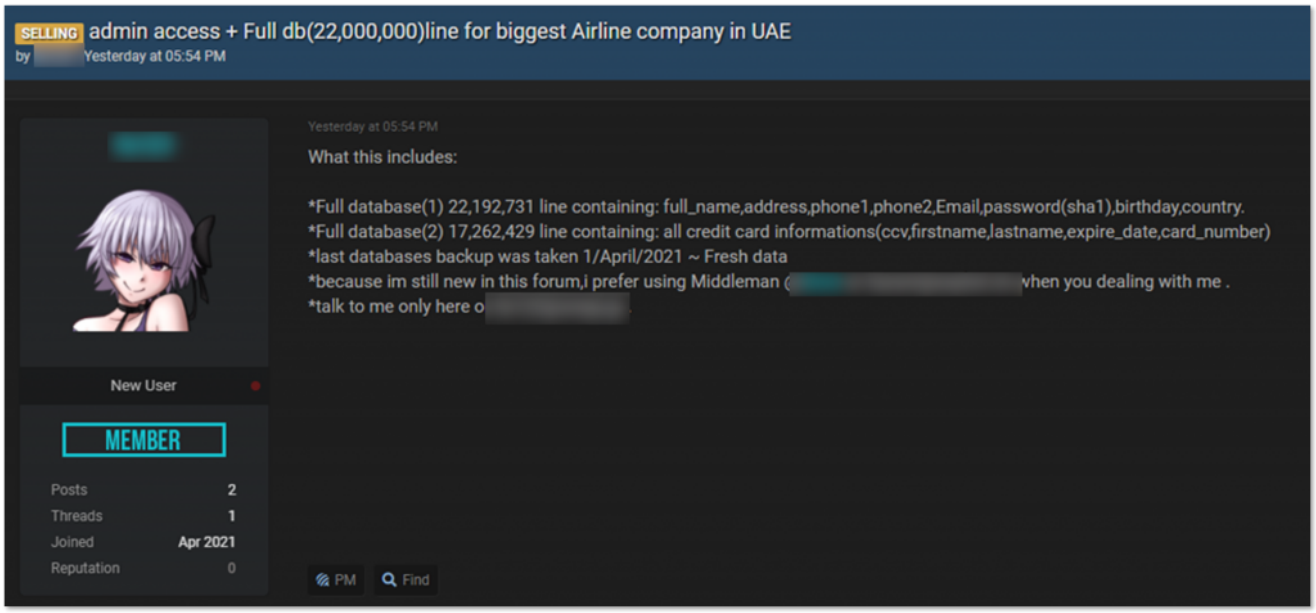


UAE victim in the Avaddon ransomware blog



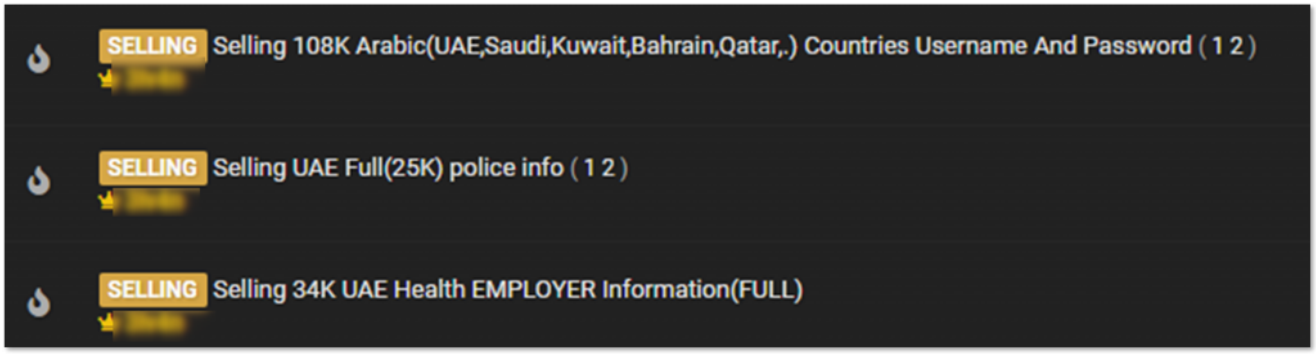
UAE victim in Nefilim ransomware gang's blog

The other listings of compromised network access were related to various companies, including government organizations as well as organizations in the telecommunications, healthcare, and financial services sectors. In some cases, such as the one below, initial access brokers sell not only the access to the victim's network, but also the data that they managed to extract from the victim's systems.



A user selling both access and database related to the "biggest airline company in UAE."

While analyzing these different initial access brokers, we observed that there are certain ones who specialize in targeting victims in the Middle East. For example, in 2020, one of the actors who claimed to be a “Turkish Hacker” mostly offered access to companies located in the UAE, Jordan, Saudi Arabia, Egypt, and a few additional countries in the region. The actor mentioned that they bought and used the Thanos ransomware, illustrating that initial access brokers earn their money in many ways. Here, the actor also offered various databases pertaining to the UAE police and private companies.



A user known for selling initial access to UAE companies sells databases belonging to UAE companies.

It’s crucial to note that the majority of listings were offered by a number of different initial access brokers, and not all offered by the same one. This indicates that there are multiple cybercriminals attempting to target UAE companies and they use different approaches to monetize the compromised networks.

Conclusions and Mitigation Efforts

As the UAE stands as one of the most digitally advanced countries in the Arab world, underground cybercriminals will continue to view it as a lucrative target. With leaked credentials, compromised accounts, and network access listings for sale, the UAE-related entities must take major steps to avoid potential significant damage due to cyberattacks. Cyber readiness applies not only to organizations in the UAE but to organizations around the world. If anything was made clear for businesses in 2020, it was the need for proper cybersecurity measures to be put in place. Though many companies have adapted to the forced work-from-home trend, many still are facing numerous threats from criminal actors operating in the cybercrime underground ecosystem. Organizations in the UAE, and globally, should ensure to continually:

1. **Train all employees and key individuals on how to safely use their credentials and personal information online**. This cyber training should include specifying how to identify suspicious activities, such as possible scam emails, or unusual requests from unauthorized individuals or email addresses. The human factor plays a significant role in an organizations' cybersecurity, and the larger the organization, the bigger chance of threats – therefore creating this mandatory cybersecurity training across all these organizations would significantly reduce the chances that they would be compromised due to an unknown mistake of an employee of theirs.
2. **Invest in regular vulnerability monitoring and patching.** Due to the increased use of digital systems, and ongoing updates of technologies, vulnerabilities in an organization's network are constantly going to rise. These organizations must invest in regular monitoring of their entire network infrastructure to ensure that any possible entry points for initial access brokers or other network intruders are immediately blocked.
3. **Targeted monitoring of your assets to automatically detect your most relevant threats emerging from the cybercrime underground ecosystem.** Nowadays, every organization – private or government, small, medium, or large, is constantly at risk due to the ever-growing cybercrime ecosystem. Cybercriminals continually search for new opportunities to achieve one simple goal: monetize the data they obtain. They are active in the hardest-to-reach corners of the cybercrime underground and organizations are constantly in need of defeating these cybercriminals. Therefore, constant automated and scalable monitoring of an organizations' assets could significantly improve maintaining a reduced attack surface, ultimately helping organizations thwart possible attempts of cyberattacks against them.