

A nighttime cityscape with illuminated buildings, partially obscured by a large red abstract shape that resembles a keyhole. The background is dark with many small lights from the buildings.

**2021-2022
UK FINANCIAL SECTOR
DARK WEB THREAT
LANDSCAPE REPORT**

2021-2022 UK FINANCIAL SECTOR DARK WEB THREAT LANDSCAPE REPORT

Elena Koldobsky, Threat Intelligence Analyst

UK firms have been recently [warned](#) over possible Russia-related cyber-attacks against western countries, the UK included, placing a scrutinizing spotlight on the UK's cyber security. Eastern European geopolitics is far from being the UK's only cyber threat. Various threat actors often target the UK for multiple reasons, including its wealth and importance to the world's economy.

This research aims to shed light on the cyber threats targeting the UK's financial sector which is following the [trend](#) of transporting banking and financial services online, putting itself at risk of being cyber-attacked. With the financial sector in the UK being the most likely sector to [hold personal data of customers](#), the question of this sector's state of cyber security is of utmost importance. In addition, the research describes threats that UK companies in general have faced during 2021 and early 2022 and provides information on advanced persistent threat groups (APTs) that have recently targeted the UK.

Exposed information

Different kinds of leaked data allow malicious actors to perform various multiple-stage attacks on companies, for example, either through social engineering attacks or simply by accessing the company's systems using the exposed information found online. Although this may not be a comprehensive list, said information often includes source codes, personal information, telephone numbers, emails, credentials to various services (such as internal services that are otherwise accessible only to company employees), and more.

UK data seems to be in demand among cybercriminals: for instance, on January 19, 2021, the user 'newagechop' posted a message on the Russian-speaking cybercrime forum ExploitIn, asking for "UK database leaks".

N uk leads Follow 1
By newagechop, January 19 in [Spam] - mailings, databases, responses, mail-dumps, software

Start new topic Reply to this topic

newagechop Posted January 19 Report post

byte

im searching for uk leads name,surname,dob an mobile number

+ Quote

N

Paid registration
0
4 posts
Joined
01/05/21 (ID: 112540)
Activity
spam / spam

Similarly, on January 9, 2022, a user named 'tovenaar777' posted on the same forum that he is "searching for UK targeted bank leads with DOB, full name, bank name/sort code, address and postal code. DOB has to be between 1935 and 1955".

RIPPER **I NEED UK TARGETED BANK LEADS** Follow 1
By tovenaar777, January 9 in [Spam] - mailings, databases, responses, mail-dumps, software

Start new topic Reply to this topic

tovenaar777 Posted January 9 Report post

byte

I'm searching for uk targeted bank leads with DOB, full name, bank name/sort code, address and postal code. DOB has to be between 1935 and 1955.

+ Quote

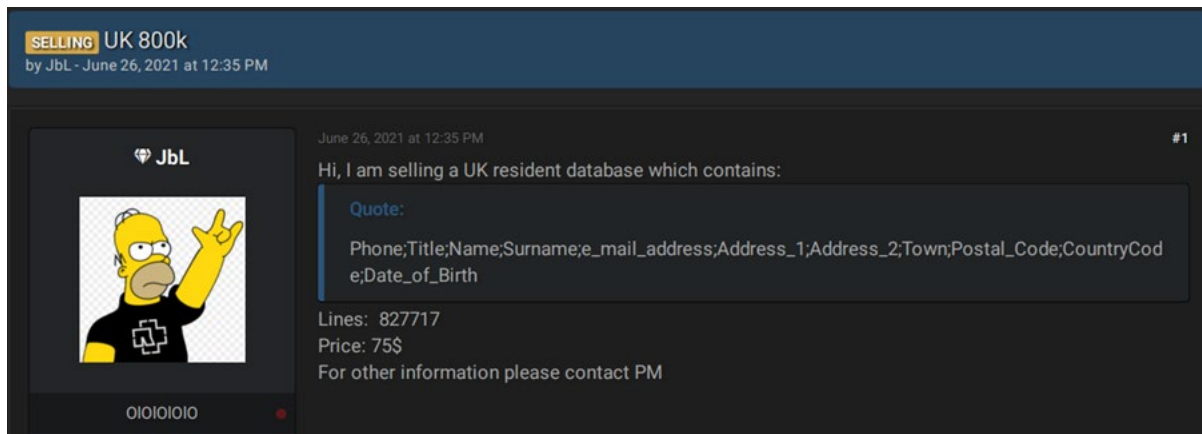
RIPPER

Причина бана: <https://forum.exploit.in/topic/200016/>

С уважением,
Администрация Exploit.In

RIPPER
0
4 posts
Joined
12/21/21 (ID: 123499)
Activity
spam / spam

Such messages are seen often on dark web forums, with similar offers emerging either as a reply or as a separate post – like the post by the user 'JbL' on the English-speaking cybercrime forum RaidForums (now defunct), offering a database of UK based individuals for sale, containing their names, phone numbers, dates of birth and more.



One of the most dangerous types of information that can be extracted and offered for sale or leaked on the dark web is credentials to the company's platforms – as threat actors use it to compromise the company by accessing its internal systems and software. KELA divides exposed credentials into two types:

Leaked credentials: Email logins to different third-party platforms (with or without passwords). These logins are usually being leaked or sold by threat actors on underground forums in the form of databases.

Compromised accounts: Logins and passwords used to access tools and softwares accounts in a compromised environment. Credentials to these compromised accounts originate from devices infected by info-stealing malware, referred to as "bots," and are offered for sale on automated markets.

To determine the level of the UK's financial sector exposure on the dark web in terms of these two threats, KELA composed a list of the UK's top financial businesses and monitored their mentions in multiple dark web sources that KELA tracks. As indicated before, the analysis was performed on data obtained throughout 2021 and early 2022.

Leaked credentials

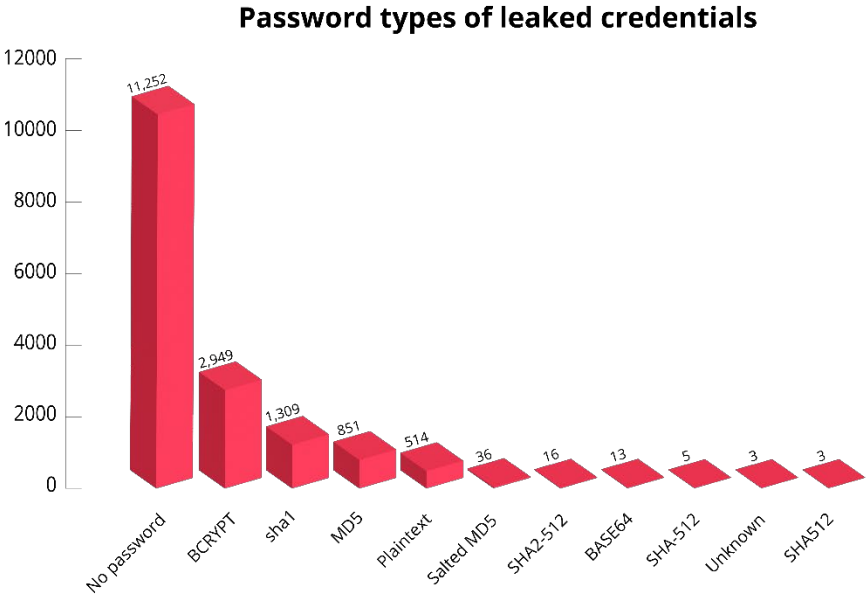
From January 17, 2021, to February 17, 2022, almost 17,000 credentials pertaining to UK's top financial businesses were leaked. Among these credentials, more than 1000 email addresses were listed more than once, meaning around 16,000 values were unique. The majority of the leaked credentials (66%) did not have passwords, while 33% had various types of passwords, such as BCRYPT (17% of the passwords), SHA1 (7%), MD5 (5%), and Plaintext (3%) - as can be seen in the graph below.

The majority of the credentials (27%) were leaked in the **RedCappi** breach, which occurred on December 6, 2021. RedCappi, an email marketing service headquartered in the US, left a private user directory unsecured, allowing a threat actor to obtain and share over 177 million records including names, emails, phone numbers, physical addresses, occupations, etc. This breach illustrates the importance of careful vendor selection, as an unsecured database belonging to a US company led to multiple UK financial institutions being open to compromise.

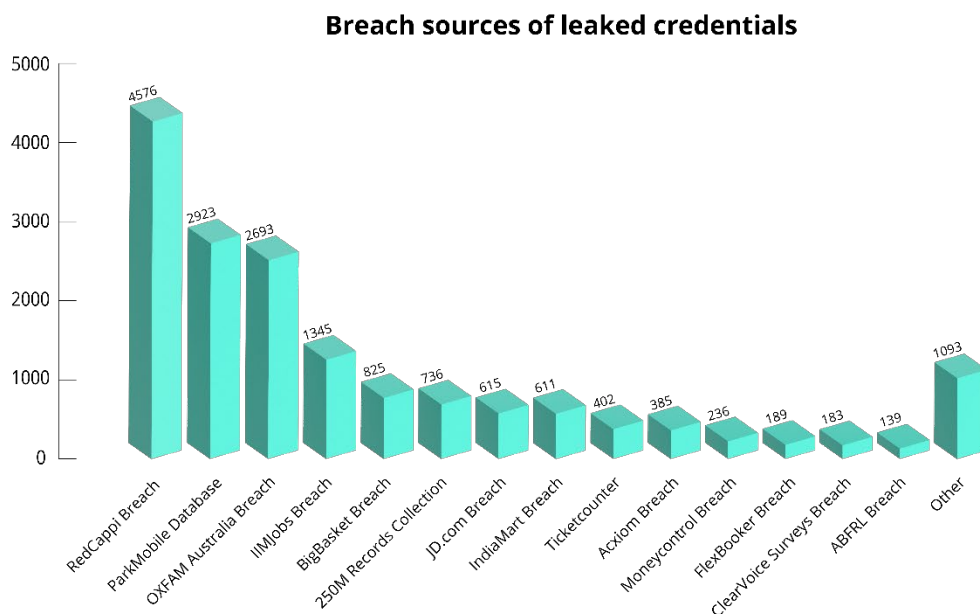
Another major breach that led to the exposure of many credentials (17%) belonging to UK financial institutions is the **ParkMobile** breach. [ParkMobile](#) is an app that allows users to "easily find and pay for parking.". The US-based company was [breached](#) in March 2021, leading to the exposure of 21 million customers' personal data, including email addresses, license plate numbers, names, passwords, and phone numbers.

The **OXFAM Australia** breach caused the leak of 16% out of all credentials. The charity organization was breached in January 2021 and resulted in the [exposure](#) of the names, addresses, dates of birth, email addresses, phone numbers, and gender of 1.7 million supporters.

Interestingly, none of the 14 top-breached companies with over 100 exposed credentials was a UK company. Most of these top breaches pertained to the Indian companies IIMJobs, BigBasket, IndiaMART, Moneycontrol, and ABFRL. As the UK plays a significant role in the global economy, often providing services to international companies and organizations, it is likely that breaches related to foreign companies would affect UK firms. The historical and economic connection between the UK and India constitutes a reasonable explanation for these results.



Number of credentials per password type. The majority of the leaked credentials did not have a password.



Number of credentials listed per breach. Most of the credentials (4,576 out of 16,951) were leaked in the RedCappi breach.

Compromised accounts

KELA performed a similar analysis of compromised accounts belonging to top UK financial companies. From January 17, 2021, to February 17, 2022, around 2000 accounts were compromised. Most of those accounts got listed on the TwoEasy and Russian Market botnet markets.

Many of the credentials were related to the internal services of the companies of interest. For instance, KELA detected credentials of a large UK-based investment bank's secured email service, granting threat actors access to the company's internal email accounts.

Other found credentials belong to the ADFS (Active Directory Federation Services) of a multinational professional services network headquartered in London. These may be used to log in to the company's Active Directory service. As the ADFS is a single sign-on (SSO) feature that provides safe access to any internal domain, system, or application, such credentials would allow a threat actor to access multiple company's applications, systems, and assets.

KELA also found credentials to a corporate VPN used by a multinational professional services network. Typically, a VPN provides employees access to a secure end-to-end encrypted connection to resources on the company network. An unauthorized VPN access would allow an attacker to compromise the company network and perform various malicious actions.


Network access

Initial network access can assist threat actors with ransomware operations and other malicious activity, serving as a foothold from where they can move laterally throughout the compromised network. These accesses are often sold in underground forums. KELA's automated platform continuously monitors these forums to identify potential threats to its customers, one of which is a possible ransomware attack. From January 2021 to February 2022, KELA observed around 60 instances of access to UK companies and organizations being sold on the dark web; some of these offers promised network access to UK companies in the financial sector.

For instance, on February 11, 2022, the threat actor 'brown' was observed selling access to a UK-based fintech company, with USD 5 million in revenue. The actor claimed the access is provided through RDP and enables to log in to a local admin-privileged machine. It was offered for sale for USD 300.

 **brown**
HDD-drive Пользователь

Вчера в 17:30

Новое   #8

Англия, ведущая мировая финтех-компания, которая самостоятельно разрабатывает программное обеспечение, помогающее брокерам зарабатывать больше денег, сокращать расходы и снижать риски, ревеню 5кк, права локал админ, цена 300\$

 Жалоба

 Like +  Цитата  Ответ

Access to the fintech company offered for sale

A threat actor who was seen selling access to UK companies 13 times during the past year, making him the threat actor targeting the UK more often than others, is 'barf'. The Russian-speaking initial access broker has been active on the Russian-speaking cybercrime forum ExploitIn since at least July 2020.

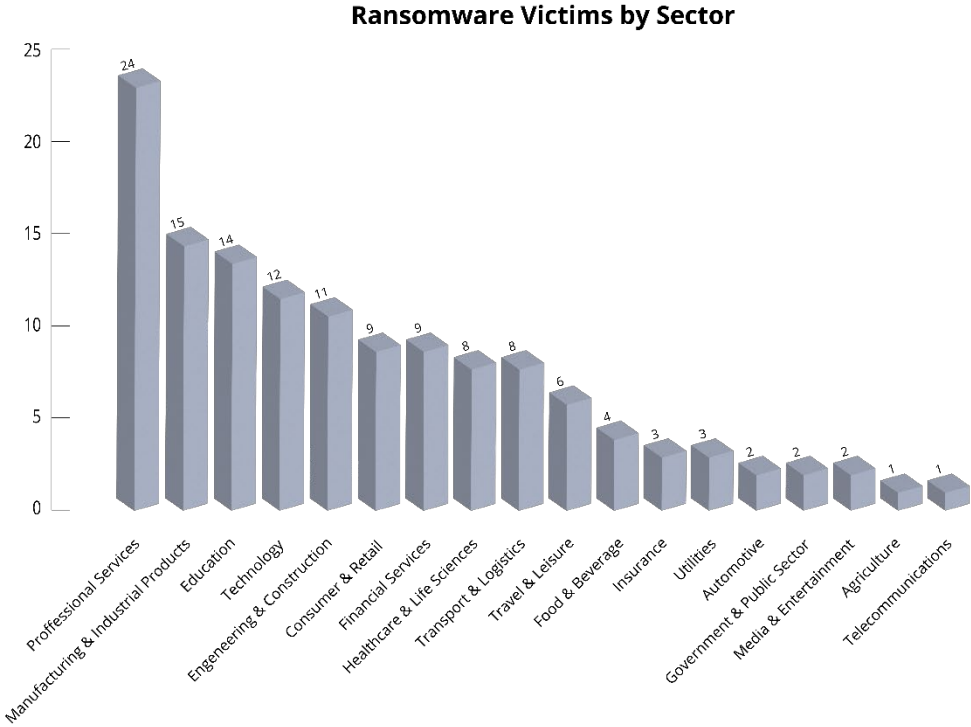
Each of those accesses can turn into millions in ransom, demanded by buyers, who can leverage them into ransomware attacks. Nevertheless, it is important to note that a ransomware attack is hardly the only outcome of using network access. Many other malicious activities can also be performed, including information theft, phishing attacks, and malware distribution.

Ransomware incidents

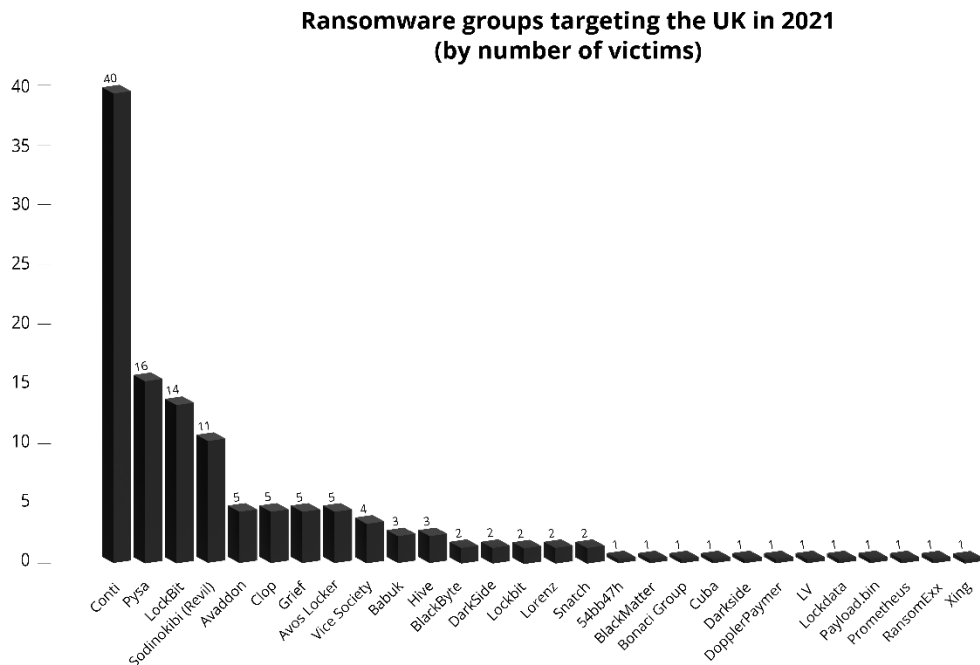
In 2021, KELA observed 135 UK companies experiencing ransomware attacks, placing the UK in fourth place on the list of known ransomware victims of 2021, as 4.83% of all ransomware victims that year were UK-based. The UK followed France, with 4.86% of all known ransomware victims, Canada, with 4.97% and the US, with 49.41%.

The information is based on data obtained from ransomware gangs’ blogs and leak sites, threat actors’ negotiation portals, and media reports. Thus, the amount of 135 victims does not demonstrate the absolute number of victims. It is important to note that some compromised companies pay the ransom and evade being publicized in ransomware blogs. Additionally, it is not always possible to identify others in ransomware negotiation portals. Therefore, the amount of ransomware victims is significantly higher, yet, the number of 135 victims is sufficient for KELA to identify patterns in targeted companies.

KELA’s previous [research](#) indicated that the “ideal” ransomware victim, based on posts of ransomware attackers from July 2021, generally has more than USD 100 million in revenue and is not from the education, healthcare, government, and the non-profit sector. UK ransomware victims often match this pattern, with the majority of the 135 ransomware victims being companies and organizations providing professional services (20%). Following are companies in the manufacturing & industrial products sector (11%) and the education sector (10%). The financial sector was ranked 7th, with 6% of known ransomware victims during the research, the same as the consumer and retail sector.

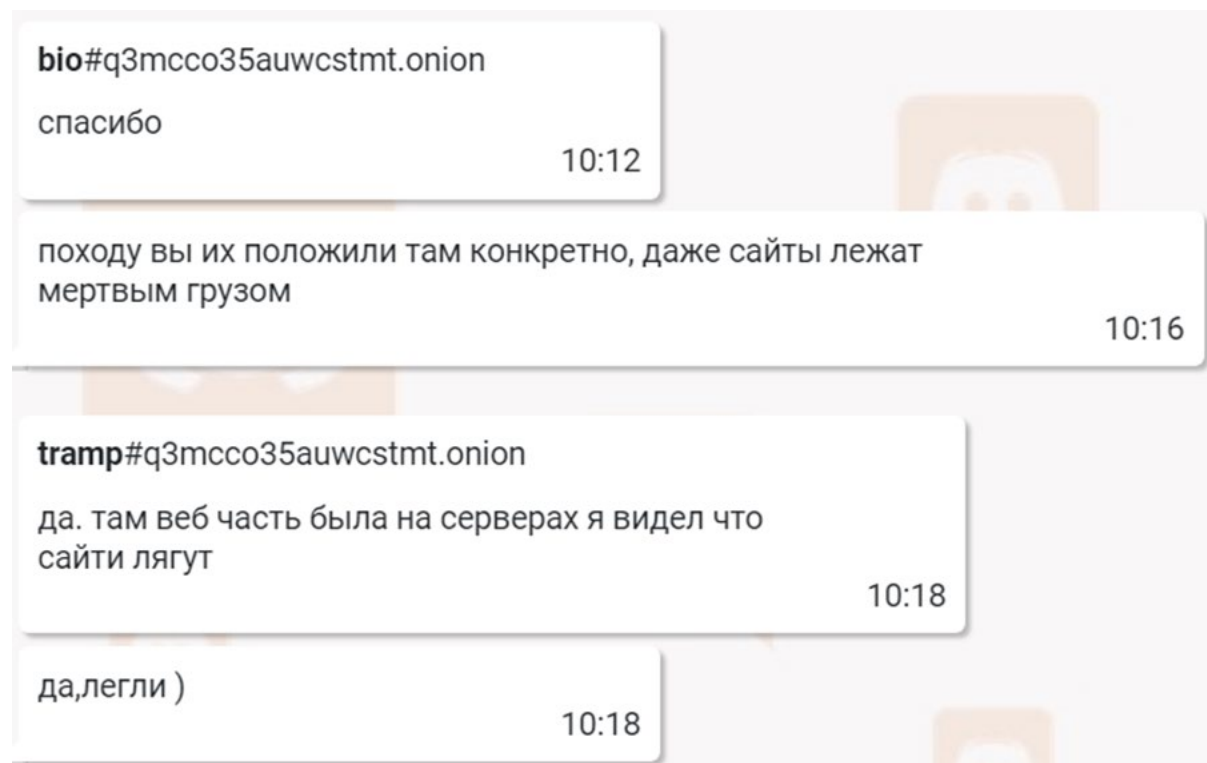


Among the observed UK victims, the most active ransomware gangs were Conti (40 ransomware instances), PYSA (16), LockBit (14) and Sodinokibi (10).



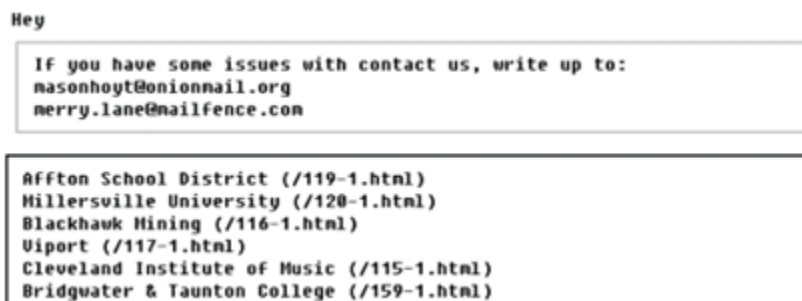
Conti is a Russian-speaking Ransomware-as-a-Service (RaaS) operation that is believed to be a successor of the Ryuk ransomware operation. Ransom payments received from Conti's attacks are [divided between](#) the affiliate directing the attack and the Conti managers. The group's affiliates often breach the target's networks after infecting corporate devices with BazarLoader or Trickbot malware – which provides them with remote access to the compromised system. After successfully stealing files and compromising the network, Conti sets ransom depending on the company's revenue and threatens the victim to pay ransom, as KELA observed when [analyzing](#) internal conversations of Conti ransomware group members that were leaked in February 2022, as a result of the group's support of the Russian invasion of Ukraine.

For example, KELA found that a UK-based provider of supply chain solutions that Conti ransomware claimed to have compromised on December 25, 2021, was previously discussed by Conti members on December 10, 2021. An actor named 'tramp' sent the details of several attacked companies, including those of the aforementioned UK-based supply chain solutions provider, to an actor named 'bio', who appears to be responsible for creating the blog posts on the victims. bio, who could not access the websites of the attacked companies, asked tramp whether it's the result of their work. tramp confirmed, saying the sites were hosted on the compromised servers, he expected them to go down. Apparently, two weeks later, the company still did not agree to pay the ransom, its name was disclosed on Conti's blog.



From the leaked Conti conversations: bio states that the websites are down and tramp confirms, stating that the sites were hosted on compromised servers

[Pysa ransomware](#) was first observed in 2019, targeting large corporate networks. Throughout the years, and unlike other ransomware operations' patterns which tend to [exclude the education sector](#), the ransomware operators have specifically targeted higher education, K-12 schools, and seminaries. Although the official reason for Pysa to choose this path is unknown, it is possible that it is related to the education sector's lack of resources to defend their systems, making their networks [vulnerable to various cyber-attacks](#). Among Pysa's 16 victims in the UK, 10 were education institutions, with the victims ranging from primary schools to colleges. One of the compromised institutions was Bridgwater & Taunton College, a college in the UK, which was claimed to have originally been compromised on January 12, 2020, and was officially announced on the Pysa leak site on March 29, 2021.



Pysa's leak site claiming to have compromised Bridgwater & Taunton College

LockBit, the next ransomware group targeting the UK with 14 victims through 2021, is a Russian-speaking group that operates using a RaaS model. LockBit's victims include companies from various sectors, including major financial companies.

Last but not least is [REvil/Sodinokibi](#), a now-defunct highly evasive Russia-based or Russian-speaking ransomware-as-a-service (RaaS). Some of its members have [recently been arrested](#) in Russia. In 2021, the group attacked 10 UK companies from various sectors. Among the compromised companies was MBA Group LTD, a provider of multi-channel communication solutions for enterprise and marketing, based in London, which was [claimed](#) to have been compromised on March 30, 2021.



MBA Group LTD claimed as victim of Sodinokibi ransomware

APTs targeting the UK

Another danger threatening the UK is [Advanced Persistent Threat \(APT\)](#) groups. The term refers to the coordinated cyber activities of sophisticated criminals and state-level entities. APTs often target large organizations and foreign governments to steal information from the target system, mainly for espionage. As APTs are state-sponsored, their motivations are typically political or economic, according to the state's interests. In order to conduct an attack on the target of interest, APT groups can use data shared on cybercrime forums, including compromised accounts, exploits and tools. In addition, these groups often use unique methods designed to infiltrate the target, gather additional intelligence, or engage in further malicious activity. These methods often include social engineering campaigns, spear-phishing campaigns tailored for specific targets and active search for vulnerabilities within the target's network.

In general, APTs may target the financial sector to commit fraud, burglarize ATMs, execute transactions, and penetrate organizations' internal financial systems. Although specific threats to the UK financial sector have not been identified, there is no doubt that the UK has occasionally been a target of APT groups during 2021.

In July 2021, for instance, the UK [confirmed](#) that in early 2021, Chinese state-backed actors APT40 and APT31 were responsible for gaining access to computer networks

worldwide via Microsoft Exchange servers. The attacks enabled large-scale espionage, including acquiring personally identifiable information and intellectual property.

In November 2021, the UK, US, and Australia issued a joint [cybersecurity alert](#) over Iranian APT actors exploiting Fortinet and Microsoft Exchange ProxyShell flaws to compromise critical infrastructure entities in these countries. After the exploitation, the groups exfiltrated data and sometimes deployed ransomware to extort the victims.

The most recent warning regarding APT cyber-attacks was [published](#) on January 2022, with the UK urging British companies to strengthen their cyber security over concerns of possible cyber-attacks conducted by Russia due to the UK's stance regarding the political crisis in Ukraine.

Conclusions and mitigation solutions

This report sheds light on the multiple, varying cyber-threats posed to UK companies and organizations in general, and the UK financial sector in particular. Through 2021, both financial and other UK companies have been subject to multiple ransomware attacks, and credentials and compromised accounts belonging to British entities were often offered for sale on cybercrime forums.

Monitoring such sources, as KELA's technology does in real-time, could provide UK-based defenders with significant intelligence value. It can allow a more proactive approach to threats by learning and understanding new tactics used by threat actors and taking measures to protect against them.