CORPS RELAY

Prepared by: Mike Bluestone CSyP & Neil Shanks CSyP
James Henderson MSyl

Date: December 2022

CORPS
Est. 1859
SECURITY

The Conflict between Ukraine and Russia

Recent developments, linked to the war in Ukraine, include the continuing impact on the energy market, international food provision, and an alleged link to recent letter bomb attacks in Spain. The latter of these is the most immediate concern to the safety and security of businesses as the targets for the attacks ranged from high profile individuals to an EU satellite company. Due to this threat, letter bombs (IEDs) are the Corps Relay Focus of the Month. More information on the recent attacks and steps businesses can take to protect themselves/their employees can be found at the end of this report.

National Security Officer Shortage

The trade body for the UK professional security industry, the British Security Industry Association (BSIA), has stated that there is a requirement to recruit and train in excess of 62,000 new security officers to meet the demand for services in 2023. Their research suggests that there is a requirement for over 450,000 security officers next year, 42,000 more than currently operating in the UK. Based on current trends, the BSIA also predict losing approximately 20,000 currently active security officers through a combination of factors including retirements, leaving the sector for better paid jobs in other areas (including picking and delivery jobs), and leaving the country. The increase is linked to the current perceived requirement, however, the Protect Duty may also increase the requirement for security officers where the security assessments it mandates is likely to highlight the need for additional security personnel to secure relevant locations and the public.

Security and Border Force Staff Strike

Travel in and out of the UK may be affected by planned strikes by UK Border Force staff and the Security Staff of the Eurostar. The PCS union, representing members of the Border Force, have voted for strike action that will begin in mid-December and last one month. The Government have announced plans to use uniformed soldiers to cover key positions during this period. Eurostar security staff that are members of the Rail, Maritime and Transport (RMT) union and plan to walk out on the 16th, 18th, 22nd, and 23rd of December.

A Series of Data Breaches

WhatsApp
Following the security vulnerabilities highlighted in the November Corps Relay, WhatsApp are again in the spotlight due to a data leak that resulted in just under 500 million user records being placed for sale online. There was an advert posted within a well-known hacking community forum on 16th November that claimed to have a database of 487 million WhatsApp users' mobile numbers. Significantly, this is a current database from 2022.

The data set is said to include users from 84 countries, most notably: 32 million from the U.S., 11 million from the UK, 20 million from France, 35 million from Italy, 6 million from Germany, and 10 million from Russia. The data set is being partitioned and sold via region, with the UK database being sold for $2,500, the German database for $2,000, and the U.S. database being sold for $7,000. The seller claimed to have used their "strategy" to obtain these numbers and provided a sample to prove the validity of the breach that included 1097 UK user numbers and 817 US user numbers.

These databases are often used by criminals to conduct 'smishing' and 'vishing' attacks (variations of phishing attacks using voice and video calls and text messages as the attack medium) against uses, whereby different forms or messages are sent to their mobile devices that attempt to get the recipient to click on a dangerous link or to divulge personal information. The guidance provided in the Corps Relay Special Bulletin relating to the threat of Cybercrime linked to the Ukraine and Russia conflict, includes guidance on protecting yourself from these types of attack.

Dropbox Breach
Many individuals and businesses use Dropbox as a file sharing platform. Dropbox confirmed that they suffered a data breach on 1st November 2022 that allowed a malicious actor to access to the site's credentials, data, and various information inside the Dropbox internal GitHub code repositories. GitHub is an internet hosting service for software development and includes the codes used for the sites it services. The breach occurred when a Dropbox developer was successfully targeted by a phishing attack, providing the attacker with access to the developers Dropbox GitHub account.

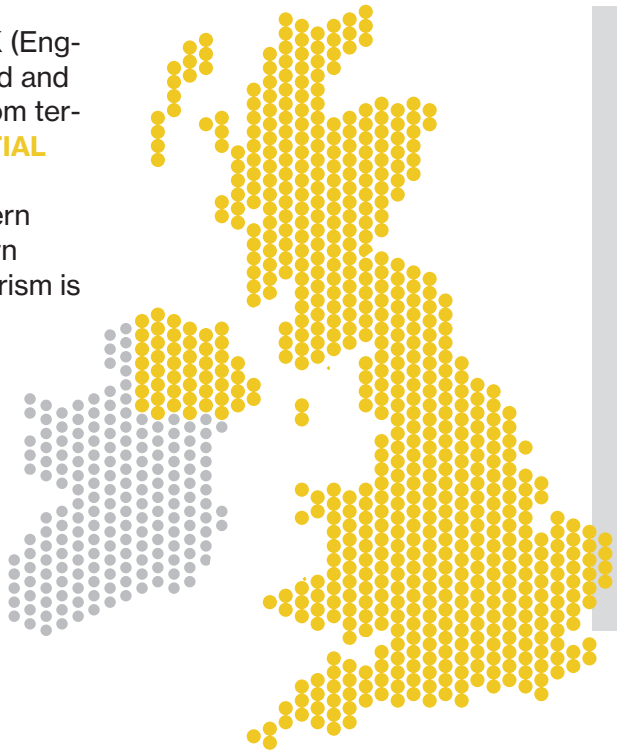
The result of this breach included the malicious actor gaining access to some application programming interfaces (API) for the platform, other credentials, and thousands of names and emails belonging to Dropbox employees. Dropbox have not been forthcoming with details as to what exactly the APIs relate to. Despite stating that they believe the risk to site users is minimal, this attack shows that the widely used hosting service is vulnerable and not secure at this time. As with the WhatsApp breach detailed above, malicious actors may attempt to use information they gained from this breach to target others or their data.

Twitter Breach
Similar to the WhatsApp breach detailed above, the user records for over 5.4 million Twitter users have been shared for free on a hacker forum. The records were stollen using a vulnerability with one of the sites API's that was fixed in January 2022. There was also another, possibly more damaging, data dump of millions of Twitter records disclosed around the same time. The data, which includes user ID's, login names, locations, phone numbers, and email addresses, is for sale for $30,000. As with WhatsApp and Dropbox, this breach creates a vulnerability for the users that could be exploited by malicious actors.

Current National Threat Level

The threat to the UK (England, Wales, Scotland and Northern Ireland) from terrorism is **SUBSTANTIAL**

The threat to Northern Ireland from Northern Ireland-related terrorism is **SUBSTANTIAL**



NOTE:

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack

LOW means an attack is highly unlikely

MODERATE means an attack is possible, but not likely

SUBSTANTIAL means an attack is likely

SEVERE means an attack is highly likely

CRITICAL means an attack is highly likely in the near future

Notable Dates/Events

Key Religious Events, National Celebrations, and Anniversaries
There are significant days for several religions and nations throughout December. It is not only important to be mindful of these dates to celebrate our diverse society, but also because several terrorist groups have been known to select these days to carry out their actions.

Notable dates in December include:

- 8th December – Bodhi Day – A Buddhist day of commemoration
- 18th-26th December – Hannukah – a Jewish festival and international event
- 24th December – Christmas Eve – an international event
- 25th December – Christmas Day – a Christian celebration and international event
- 26th December – Boxing Day – an international event
- 26th & 27th December – Bank Holidays – a national event
- 26th December-1st January – Kwanzaa – a celebration of African heritage
- 31st December – New Year's Eve (Gregorian calendar) – an international event
-

Letter Bombs (IEDs & IIDs)

Corps Focus: Security Issue of the Month

Letter and Parcel Bombs are examples of either an improvised explosive device (IED) or an improvised incendiary device (IID). These are created by malicious actors and sent through the mail or a courier service to get the device to their target location covertly, maximising the chances of success and the damage that can be caused. These devices contain several parts, including an initiator, a switch, the main charge/ explosive/incendiary material, a power source, and the container. These parts are then placed in an envelope or parcel, before being sent via mail to the target. Many of these devices are set to detonate upon opening, although some may have different trigger types such as a remotely activated detonator switch.

The Spanish Police declared that an employee of the Ukrainian embassy in Madrid required hospital treatment after opening a letter bomb on Wednesday 1st December 2022. A total of 6 letter bombs were identified having been sent to the Ukrainian Embassy, Prime Minister Pedro Sanchez, government offices, the U.S. Embassy, and a European Union satellite company. The letters are believed to have all been sent from the city of Valladolid, northern Spain, between 24th November and 2nd December 2022. The individual(s) responsible for sending the letter bombs are yet to be identified, however, it is believed the letter bombs are being sent in connection with Spain's support of Ukraine during the Russian invasion. Below is some information to help businesses protect themselves against such attacks.

Postal Threats

- Terrorists and others wishing to cause harm or disruption have long used postal and courier services to deliver hazardous items to target recipients
- Delivered items can include letters, packets and parcels and may contain:
  - Explosive or incendiary devices
  - Sharps or blades
  - Offensive materials
  - Chemical, biological, radiological or nuclear (CBRN) materials (either bulk or small / discrete quantities) or devices. Hazardous chemical can include explosives or narcotics, as well as benign materials.
  - Please Note: materials vary in colour and texture, including powders, crystalline (e.g. sugar), oily or waxy residues, or liquids.
- Anyone receiving a suspicious delivery is unlikely to know exactly which type it is, so procedures should cater for every eventuality
- A delivered item will probably have received fairly rough handling in the post and so any device is unlikely to function through being moved, but any attempt at opening it may set it off.
- In contrast, even gentle handling or movement of an item containing CBRN material could lead to the release of contamination
- Delivered items come in a variety of shapes and sizes; a well-made one will look innocuous but there are many possible indicators that a delivered item may be of concern
- Bulky deliveries (e.g. office equipment, stationery and catering supplies) are also a potential vulnerability
- This risk can be reduced through measures such as:
  - Matching deliveries against orders
  - Only accepting those which are expected
  - Using trusted suppliers wherever possible
  - Maintaining vigilance; inspecting deliveries

Letter Bombs (IEDs & IIDs)

General protective measures

- Although any suspect item should be treated seriously, remember that the great majority will be false alarms and a few may be hoaxes
- Try to ensure that your procedures, while effective, are not needlessly disruptive
- A properly conducted risk assessment should give you a good idea of the likely threat to your organisation and indicate precautions you need to take
- While this advice applies particularly to staff in post rooms, it is also relevant to all staff who may be the recipients of such items, as well as staff at entrances who may receive hand and courier delivered items
- Encouraging regular correspondents to put their return address on each item, and in particular to provide advance warning of unusual items can help reduce false alarms
- Sorting and processing mail in areas away from the main site, reducing the chances of an explosion or contamination impacting on heavily occupied buildings, is advantageous and should be considered during any new site builds or re-designs

Tools/Standards/Equipment

- PAS 97:2015 provides a specification for mail screening and security within an organisation. PAS stands for Publicly Available Specification, a tool for formalising speciation's for key processes or technologies.
- Use of X-ray systems to screen mail:
  - X-ray machines can be used to screen mail for the presence of hazardous items such as blades and explosive, incendiary or CBRN devices
  - They will not, however, reliably enable detection of small amounts of loose CBRN materials or "white powders", especially if multiple items are X-rayed simultaneously (any container should, however, show up)
  - X-ray machines are available in a wide range of models offering different detection capabilities and throughput
- Handheld metal detectors can indicate if there are any metal elements within the package (such as those required as part of the detonation/trigger system)

What to look for:

- It is oddly shaped or lopsided
- The envelope flap is stuck down completely (a normal letter usually has an ungummed gap of 35mm at the corners)
- There is a pin-sized hole in the envelope or package wrapping
- There is any unusual smell, including but not restricted to almonds or marzipan
- It has greasy or oily stains on the envelope
- There is an additional inner envelope which is tightly taped or tied

In addition to the checks for Post & Parcels, look out for:

- Deliveries from an unknown / unreliable source
- Deliveries by an unknown carrier
- Deliveries not made to a normal receiving point
- Items left in a suspicious location
- Where there is any doubt - the delivery must be inspected for any 'tell-tale' signs of an explosive device or other material of risk to security

If you require any assistance with training for your staff or your planning an preparedness to protect against letter/parcel bombs, please contact Corps Consult.

Mike Bluestone CSyP FSyI
Executive Director
+44 (0)7773 320 234

Neil Shanks CSyP FSyI
Director of Corps Consult
+44 (0) 7890 590352

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

intel@corpssecurity.co.uk
www.corpssecurity.co.uk