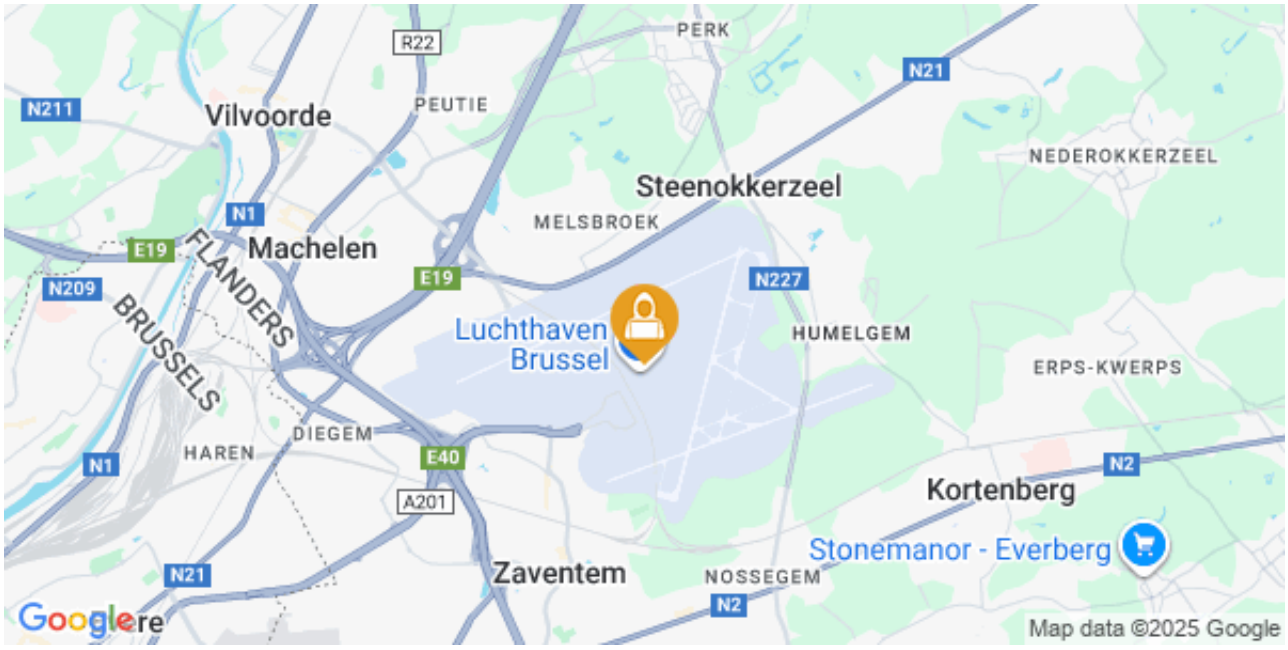
Cyber



21
SEP
9:20 UTC

Europe Alert (UPDATE): Flight disruptions ongoing at BRU, BER, LHR airports following cyberattack as of September 21; involvement of state-backed actors likely

CLICK HERE TO VIEW PREVIOUS REPORT

Current Situation

- As of September 21, flight disruptions are ongoing at several major international airports in Europe following a cyberattack on a prominent third-party service provider for check-in and boarding systems, which took place during the night hours (local time) of September 19. Details on affected airports are as follows:
- At Brussels Airport (BRU) in Brussels, **Belgium**, check-in operations remain heavily disrupted as of September 21. Consequently, airport authorities requested that airlines cancel a percentage of their flights through 04:00 on September 22. In total, 44 out of 257 flights have been canceled.
- At Berlin Brandenburg Airport (BER) in Berlin, **Germany,** disruptions to check-in services are persisting, with airport authorities warning of longer waiting times as of September 21.
- At London Heathrow Airport (LHR) in London, **UK,** flight disruptions are also ongoing as of September 21. Airport authorities have issued an advisory encouraging passengers to check the status of their flight before arriving at the airport.
- Investigations into the cyberattack are ongoing. Initial reports indicate that this was a Distributed Denial-of-Service (DDoS) attack, carried out by exploiting weaknesses in the service provider's

cloud services. No group has claimed responsibility for the attack as of writing.
- A spokesperson for the European Commission said there were no indications of a “widespread or severe attack,” with the origin of the attack still under investigation.
- Separately, Irish authorities confirmed that a suspicious object found in Terminal 2 of Dublin Airport (DUB) on September 20 was deemed harmless. The discovery of the object triggered the evacuation of the terminal and initially raised concerns over a link to the cyberattack.

Source: BBC

Assessments & Forecast

1. If the attack is confirmed to be a DDoS attack, this would indicate an intent to cause severe disruptions to Europe’s aviation sector. While DDoS attacks in Europe are often associated with state-backed actors or hacktivists, it is still possible that the attack was carried out for criminal financial gain. Indeed, cyber criminals are known to carry out DDoS attacks to extort companies for financial payment. This could be financial payments in return for stopping the attack or avoiding future disruptions. Alternatively, the attacks can be used to distract the victim from other attacks, such as data theft, which can then be held ransom for financial gain or sold on the dark web.
2. That said, the involvement of state-backed actors as opposed to cyber criminals remains high. This is especially true given the scale of the attack, which, while not described as “severe” by the EC, still resulted in widespread disruptions to Europe’s aviation sector. The fact that the attackers were able to carry out the attack on the third-party service provider, which is a subsidiary of a prominent US multinational aerospace and defense conglomerate, indicates they were highly sophisticated. This, in turn, adds credence to the involvement of state-backed actors, who have the resources needed to conduct such attacks.
3. The fact that major airports of countries viewed as key allies to Ukraine were targeted, especially Germany and the UK, also raises the possibility of Russia’s involvement. Indeed, Russia-backed actors have been accused of carrying an increasing number of politically motivated cyberattacks on European countries Moscow deems “unfriendly.” For example, recent reports indicate that Poland, one of Ukraine’s key supporters, faces 300 Russia-backed cyberattacks daily. In August, Polish authorities reported a foiled cyberattack targeting an unnamed “major city’s” water supply.
4. With regard to September 19, in addition to flight disruptions, the attack is likely to have resulted in supply-chain disruptions. This includes humanitarian and military aid destined for Ukraine, which is largely transported from donor countries to Poland’s Rzeszow–Jasionka Airport (RZE), where it is shipped to Ukraine. As such, the fact that BER and LHR were targeted also indicates intent to disrupt aid to Ukraine, given that Germany and the UK are two of the largest European donor countries.
5. **FORECAST:** Additionally, the attack itself could be aimed at testing cyber vulnerabilities in key sectors in Europe, which could be used for more severe sabotage attacks going forward. This is especially true for attacks on critical infrastructure, including aviation, transportation, energy, and water supply.
6. **FORECAST:** Considering escalating tensions between NATO and Russia, Moscow is expected to continue its hybrid warfare tactics targeting European NATO members. A key tactic remains cyberwarfare, with attacks likely to continue in the near term. Such attacks will continue to be aimed at maximizing operational disruptions rather than attempting kinetic cyberattacks that are intended to cause physical damage or loss of life.
7. **FORECAST:** Despite ongoing work to recover from the September 19 cyberattack, disruptions at the affected airport will persist in the immediate term. This includes flight cancellations and delays on September 21, as well as longer waiting times at airports through the coming days due to the associated backlog. Supply-chain disruptions affecting various sectors in Europe should be anticipated in the coming days as well, given delays to transport and delivery services.

Recommendations

1. Those intending to travel via Brussels Airport (BRU), Berlin Brandenburg Airport (BER), and London Heathrow Airport (LHR) on September 21 are advised to reconfirm itineraries due to ongoing disruptions linked to the September 19 cyberattack.
2. Allot for disruptions to travel to the ongoing check-in and boarding delays at the airports.
3. Remain cognizant of updates regarding cyberattacks targeting government and civilian services.
4. Organizations should take precautions to protect against cyber threats at all times, especially during periods of known cyber activity.
5. If any internal systems appear to be compromised, disconnect affected devices from all networks immediately and seek assistance from IT professionals.
6. For more information on the security situation and assistance, please contact intel@max-security.com.