Dear Customer

Further to the initial notification we sent you on 20 August 2022, we are writing to provide an update on the ransomware (AlphV Blackcat) attack which has affected our service provider Accelya.

**Further details of the incident**

In our notification, dated 20 August 2022, we mentioned that there were clear indications that certain BSP systems data has being leaked into the public domain and we were currently analyzing this to determine the potential extent of this exfiltration and publication. From reviewing a sample from that data, IATA has identified that personal data is included in the data made public by the purported perpetrators of the security incident.

We can confirm that the following categories of personal data are contained in the sample of data we have reviewed:

Agent:

- First and Family name
- Contact details

As matter of urgency, we have requested Accelya to confirm, in accordance with their legal obligations as a data processor, whether or not, the ultimate source of the data is the data which is processed by Accelya for the purpose of performing BSPLink Data processing and reporting and/or the related BSP Data files.

We will continue to press Accelya for further information, evidence and supporting documents relating to the data security incident in compliance with their legal obligations under data protection regulations. We will update you as further information becomes available.

In the meantime, please contact our Customer Services team if you have any questions relating to your use of BSPLink or this security incident.

## Attachment A

Dear Customer,

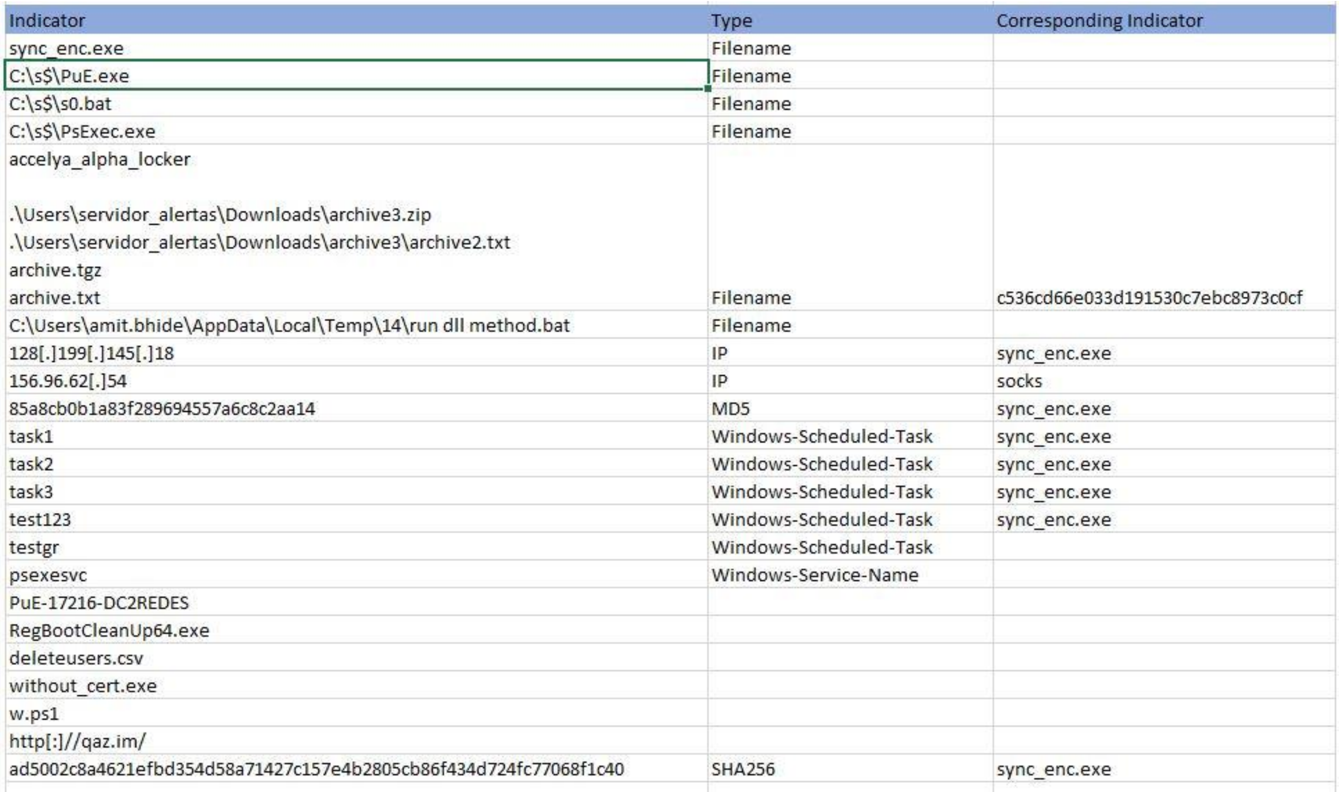
25 August 2022

Following our communication on 20 August 2022, Accelya has authorized IATA to release the following Indicators of Compromise (IOC) information to you relating to the ransomware attack on Accelya. This is the current set of IOC information available to IATA at this time.

We hope at least with this information your security team can review your systems to improve their integrity and robustness. As further IOC information is made available we will seek to share this with you as soon as we can.

If you have any questions about the IOC information, please do not contact IATA but rather contact Accelya (at info@accelya.com), who are in a better position to assist with specific questions around the IOC information.

Many thanks



| Indicator | Type | Corresponding Indicator |
|---|---|---|
| sync_enc.exe | Filename | |
| C:\s$\PuE.exe | Filename | |
| C:\s$\s0.bat | Filename | |
| C:\s$\PsExec.exe | Filename | |
| accelya_alpha_locker<br><br>.\Users\servidor_alertas\Downloads\archive3.zip<br>.\Users\servidor_alertas\Downloads\archive3\archive2.txt<br>archive.tgz<br>archive.txt | Filename | c536cd66e033d191530c7ebc8973c0cf |
| C:\Users\amit.bhide\AppData\Local\Temp\14\run dll method.bat | Filename | |
| 128[.]199[.]145[.]18 | IP | sync_enc.exe |
| 156.96.62[.]54 | IP | socks |
| 85a8cb0b1a83f289694557a6c8c2aa14 | MD5 | sync_enc.exe |
| task1 | Windows-Scheduled-Task | sync_enc.exe |
| task2 | Windows-Scheduled-Task | sync_enc.exe |
| task3 | Windows-Scheduled-Task | sync_enc.exe |
| test123 | Windows-Scheduled-Task | sync_enc.exe |
| testgr | Windows-Scheduled-Task | |
| psexesvc | Windows-Service-Name | |
| PuE-17216-DC2REDES | | |
| RegBootCleanUp64.exe | | |
| deleteusers.csv | | |
| without_cert.exe | | |
| w.ps1 | | |
| http[:]//qaz.im/ | | |
| ad5002c8a4621efbd354d58a71427c157e4b2805cb86f434d724fc77068f1c40 | SHA256 | sync_enc.exe |

**Attachment B**

Dear Customer

20 August 2022

We are writing to inform you that we have become aware of a ransomware (AlphV Blackcat) attack which has affected our service provider Accelya (data processing centre based in Madrid) (https://w3.accelya.com/about-us/). The attack on Accelya has affected the operation of our new BSPLink  and as such Accelya have reverted to the classic BSPLink to ensure continued operations of the system. To facilitate continuity of service for our customers traffic, we will continue to reroute through classic BSPLink, until further notice.

At this point in time, it's unclear exactly what BSP data or if any replicated data used by Accelya in its own solution(s) has been compromised or leaked because of the security incident. We are therefore currently unable to confirm what (if any) categories of personal data and approximate number and records of data have been affected.

**Further details of the incident**

Regrettably the information we have been provided by Accelya has been extremely limited, but we understand that on 3 August 2022 Accelya identified that they were the subject of a ransomware attack. Accelya informed us on 5 August of service delivery difficulties, and that these were due to the ransomware attack that had occurred on the 3 August 2022 and advised us on the 16 August 2022 the nature and identity of the ransomware. We understand that the attack has affected the primary and separate backup for NFE that Accelya operates.

At this time Accelya have said they cannot confirm whether personal data processed within the BSP systems has been directly impacted within the attack, and they are estimating it will take them at least 2-3 weeks to confirm the position.  They have engaged a third-party forensic investigation firm to assist them.

**Why are you notifying us now?**

We are taking the decision to notify you now because we have separately become aware that some data from the attack has been released into the public domain. In addition, we have independent sources that have provided us with a clear indication that certain BSP systems data has being leaked into the public domain and we are currently analyzing this to determine the potential extent of this exfiltration and publication. We will update you if we become aware of any BSP system data being exfiltrated, compromised or released into the public domain, including any personal data.

There is no evidence of the attacker group having used access gained at Accelya to access IATA systems, but we continue to undertake due diligence to check this. It would be prudent for you to undertake appropriate security checks in the light of this incident. We have requested from Accelya precise IOCs (Indicators of Compromise) in order to give to your security team to allow you to detect and block any similar attack from the hackers. Once we have received this information, we will pass this on to you.

In the meantime, please contact our Customer Services team if you have any questions relating to your use of BSPLink or this security incident.