advanced
Software Powered Possibility

Advanced Cybersecurity Incident Summary

Below please find information summarising Advanced's current understanding of the recent cybersecurity incident and the actions the Company has taken and continues to take in response.

Attack Path

The earliest evidence of threat actor activity identified on the Advanced network was on 2 August 2022 and the most recent date of activity is 4 August 2022.The threat actor initially accessed the Advanced network using legitimate third-party credentials to establish a remote desktop (RDP) session to the Staffplan Citrix server. During the initial logon session, the attacker moved laterally in Advanced's Health and Care environment and escalated privileges, enabling them to conduct reconnaissance, and deploy encryption malware. Immediately prior to encrypting systems, the threat actor copied and exfiltrated a limited amount of data.

Our threat intelligence and forensic firms have confirmed that the malware strain used in this attack was LockBit 3.0. We are happy to share additional Indicators of Compromise (IOCs) with Advanced customers upon request.

The forensics are very nearly completed and at this stage, it is highly unlikely there will be additional findings. We expect to have a formal forensic report completed in the coming weeks, which will be available upon request to our customers.

Containment

Upon first detecting suspicious activity, our security team promptly disconnected the entire Health and Care environment to contain the threat and limit encryption to a small number of systems. This action also prevented any further threat actor activity within the environment. However, by taking this action, our customers lost access to Health and Care platforms, as well as a limited number of non-health and care environments and services, such as eFinancials.

Remediation

Once our teams were able to contain the threat, we promptly began rebuilding and restoring impacted products and systems in a separate, secure, and new environment. We also implemented the below immediate measures to the Health & Care environment:

- Scanned for identified Indicators of Compromise (IOCs)
- Installed real-time monitoring, detection, and response agents
- Reset passwords
- Rebuilt and hardened compromised systems, including Domain Controllers
- Enhanced network segmentation
- Strengthened firewall rules

These are only some of the efforts we've made to enhance our cybersecurity defenses and we are continuing to evaluate additional steps we can take to further secure our environment.

Recovery

Our teams have worked around the clock to recover from this attack as quickly and safely as possible.

Although we were equipped and able to completely rebuild certain health and care products by the Monday following the incident, we were required to satisfy an assurance process set forth by our partners at the NCSC, NHS, and NHS Digital. This assurance process helped to provide confidence that once our rebuilt products were ready to go live, they were fully remediated and safe for our customers to use. As we learned more about this assurance process and adjusted in real time to meet certain requirements, it took longer than expected, which has impacted our overall recovery timeline. We have prioritized safety and security during every step of our recovery process.

Our Health and Care and environments beyond Adastra and 111 will also require additional compliance checks, scanning, and going through the same assurance processes. This is time consuming and resource intensive and it continues to contribute to our recovery timeline. As we work through scanning and clearing systems, we are in parallel continuing to assess and/or develop recovery plans for remaining impacted products.

We are working diligently and bringing all resources to bear, including outside recovery specialists, to help us restore services to our customers as quickly as possible, and in the interim, providing data extracts and assisting with contingency planning as appropriate.

Data Review

We can confirm that the perpetrators of the attack, who were financially motivated in nature, were able to temporarily obtain a limited amount of information from our environment pertaining to approximately 16 of our Staffplan and Caresys customers. We have now notified each of those affected customers as the controllers of the exfiltrated data.

Importantly, no data was taken from other products.

Additionally, we were able to recover the limited amount of data obtained from our systems and we believe the likelihood of harm to individuals is low. This is based on our expert threat intelligence vendor's considerable experience with cases of this nature and the fact that there is no evidence to suggest that the data in question exists elsewhere outside our control. We are, however, monitoring the dark web as a belt and braces measure and will let you know immediately in the unlikely event that this position changes.

We have been and continue to be in contact with the ICO, the NHS, the National Cybersecurity Centre (NCSC), and the National Crime Agency to provide regular status updates on this incident.

Again, Advanced has now given required notice to all affected data controllers. If you were not contacted, your data was not copied out of the environment.