volue

Update 10 May 2021 - 10:00 CEST

On 5 May 2021, Volue was subject to a cyberattack impacting Volue Technology ("Powel"). The ransomware attack was caused by Ryuk, a type of malware usually known for targeting large, public-entity Microsoft Windows systems. Following the attack, Volue immediately launched the operation 'Stop & Recover' and has increased efforts to scale the operation, both towards security partners and relevant authorities.

Volue has initiated a close cooperation with KraftCert, a Norwegian Computer Emergency Response Team. During the past two days, KraftCert has analysed and gained additional insight on the address of the attack and the malware used. This insight gives us a better understanding of the timeline for the attack, including the attackers' preparations, reconnaissance and the actual execution. All information KraftCert obtains is shared responsibly with those who need it, and as soon as the data from the internal investigation is ready. Please visit the Volue website to find the contact details for KraftCert if you want to receive their regular updates.

We have made substantial progress over the weekend, both with the forensics investigations and the recovery program, including the risk assessments for applications and towards our customers. The results strongly indicate that the incident occurred in the period from 4 May, 10 pm to 5 May, 10 am and followed a more or less "typical" RYUK ransomware attack pattern. The data we have suggests the attack was aimed at Volue infrastructure and networks and was not targeted at third parties or customers.

It's important to note that we have found no evidence to suggest that any of our customers have been compromised in this attack. We have neither received any reports to date that this is the case. So far, 70% of customer environments and applications have been deemed safe or not impacted by this attack. With respect to data exfiltration, investigations have employed various tools and methods including log trailing and network traffic analysis looking over a relevant timeframe. We cannot say with 100% certainty that no data was stolen or leaked but so far, the results have been consistent in that no evidence of such exfiltration has been found. The investigations will continue until we are fully satisfied that we have exhausted all avenues.

Once again, we urge customers not having reported the incidence to their respective Data Protection Agency and other relevant authorities to do so immediately.

We have received questions about how to communicate with Volue Technology employees in your daily work. We consider the use of email, Microsoft Teams, Teamviewer and phone as safe. Unfortunately, it is not possible for us to log on to your computers and systems, nor to share files.

Our primary focus has been to deem safe our customers' products and services and provide customers with sufficient information. In our daily webcasts, held every morning at 9.30 AM, we will inform you about the current situation. **The next webcast is scheduled on Tuesday, 11 May, 9.30 AM.**

Register for the daily webcasts here.
View today's recorded session here.

For more information, please contact Volue Support.