volue

Update 11 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.

Almost one week has passed since the cyberattack. From the time of discovery, our emergency team and security partners have been working tirelessly to understand the nature of the attack, the impacted infrastructure and services. Through our advanced security software, we were able to provide the forensic investigators with plenty of data. This insight has given us a good understanding of the timeline for the attack, including the attackers' preparations, reconnaissance and the actual execution. All available and relevant data have been shared with KraftCert, a Norwegian Computer Emergency Response Team, that again shared this information responsibly with their customers and partners. Contact information for KraftCert can be found on our Urgent Update page.

Over the past few days, we have made significant progress and we expect to be fully operational within a few days. We have a structured process in place to deem safe our customers' products and services. We continue to see no evidence that customer environments or applications were directly impacted from this attack. We would like to emphasise that the recommendation given to customers are based on facts and evidence. However, based on what we know today, we are comfortable to deem safe customers' products and data. The forensic investigation is still ongoing, and we cannot rule out that further investigation will find indicators that might change the situation.

With regards to data, we continue of have no evidence of data exfiltration, personal as well as infrastructure data.

Some applications were taken down in the attack. These have been restored and rebuilt but with much improved security, including an improved network security infrastructure. Users for those applications will be invited to resume activities in a staged rollout of the services. We have also begun the process to collect insights and facts into documentation that will be used as part of a post-mortem process.

We believe communication with our customers and partners is key to resolve the situation and we will continue to share the most relevant information with you. The ways to contact and collaborate with Volue employees remains email, telephone, Microsoft Teams and TeamViewer, and we will inform our customers directly about additional ways of collaborating with us.

We have conducted daily webinars since last Friday. However, as we have made considerable progress and are starting to deem safe products and customers. This means, today marks the last webcast on the overall situation.Today's recorded session can be found here. For more information, please contact Volue Support.