CERT-EU

Memo
26/07/2019 - TLP:WHITE

Cloud hosting firm iNSYNQ hit by ransomware attack

Reference: Memo [190726-1] – Version: 1.0
Keywords: Cloud, ransomware, disruption
Sources: Publicly available information

Key Points

- Cloud hosting provider iNSYNQ experienced a ransomware attack that has left customers unable to access their data.
- One week after the infection, restoration was not yet completed and iNSYNQ encouraged its customers to rely on local backups.

Summary

On July 18, cloud hosting provider iNSYNQ announced[1] [2]that it is trying to recover from a ransomware attack that shut down its network and has left customers unable to access their data. According to iNSYNQ, the attack took place on July 16. On July 23, iNSYNQ CEO[3] stated that the company had started restoring access to a significant number of customers on July 22. Then on July 24, he announced that the company is "continuing accelerate the speed in which customers are restored". This means that the restoration will need more than one week.

According to Brian Krebs[4], "iNSYNQ's customers — many of them accountants who manage financial data for a number of their own clients — have taken to Twitter to vent their frustration over a lack of updates since that initial message to users. In response, the company appears to have simply deleted or deactivated its Twitter account (a cached copy from June 2019 is available here). Several customers venting about the outage on Twitter also accused the company of unpublishing negative comments about the incident from its Facebook page."

iNSYNQ claimed that they are making progress and prevented the ransomware from spreading throughout its entire network. However, the company has conceded that the effects on customers have been nontrivial and customers are being asked to rely on local backups.

The ransomware used in this attack is MegaCortex, a ransomware that surfaced online in May this year. In May, Sophos[5] explained that MegaCortex was affecting a number of organisations around the world, including in Italy, the United States, Canada, the Netherlands, and other countries. Vitali Kremez, an IT security researcher, has tweeted[6] an in-depth analysis of MegaCortex ransomware revealing that its prime target is online businesses.

Comments

Ransomware attacks have become commonplace. Cloud services providers are not immune (see for example Memo [190103-1]), especially because their customers create pressure points to incite the victim to pay the ransom.

It is important to remember that, in service level agreements (SLA) with cloud service providers, backup responsibility usually lies on the customer side. Therefore, like for protecting against ransomware effect on their own networks, organisations migrating to the cloud need to have a backup strategy to keep preventing ransomware damages.

As part of its cyber threat intelligence service, CERT-EU is collecting and sharing indicators of compromise (IOCs) to help its constituents to detect ransomware attacks, including MegaCortex.

CERT-EU however recommends its constituents that are migrating to the cloud to pay special attention to the SLA and especially the security controls in place protecting both data at rest and data in transit.

[1] https://krebsonsecurity.com/2019/07/quickbooks-cloud-hosting-firm-insynq-hit-in-ransomware-attack/
[2] https://blog.insynq.com/blog/an-update-from-the-ceo
[3] https://blog.insynq.com/blog/update-ongoing-desktop-restoration
[4] https://krebsonsecurity.com/2019/07/quickbooks-cloud-hosting-firm-insynq-hit-in-ransomware-attack/
[5] https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/
[6] https://twitter.com/VK_Intel/status/1151978975025139712