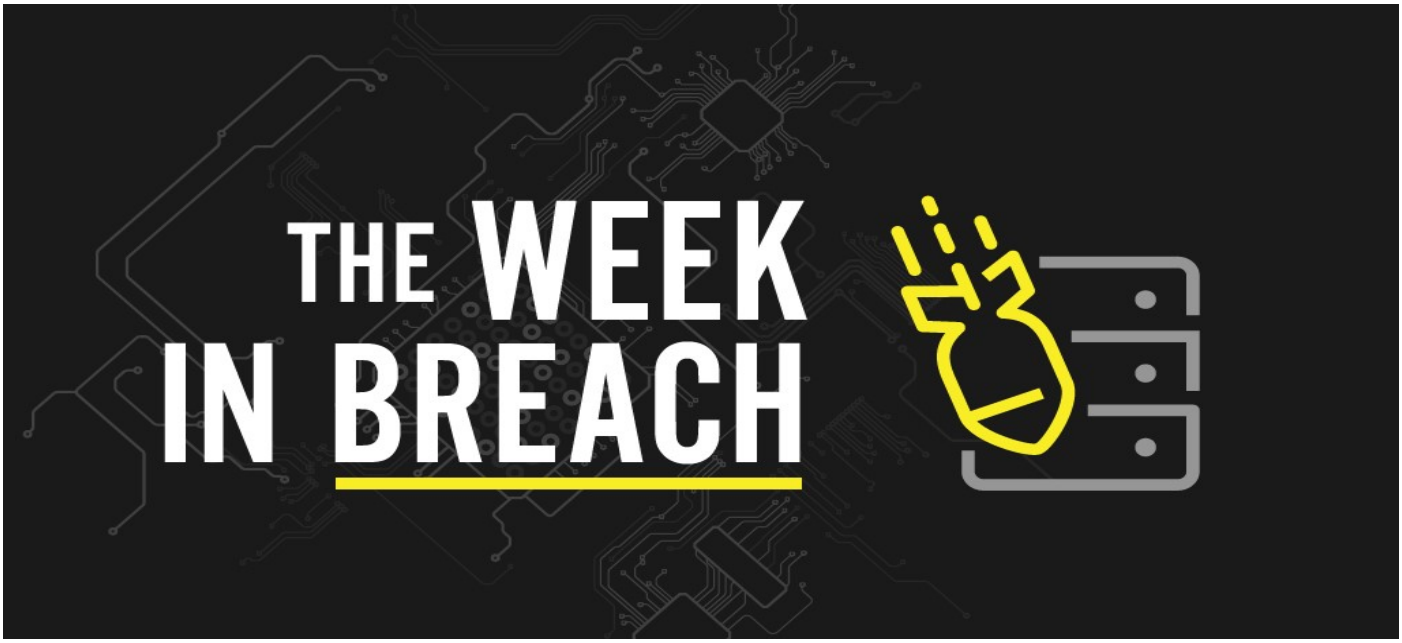
THE WEEK IN BREACH NEWS: 04/14/21 – 04/20/21

DenBe Computer Consulting
Connecting Business

April 21, 2021 by Dennis Jock

This Week in Breach News:

Codecov discloses a doozy of a breach.



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

LogicGate

https://techcrunch.com/2021/04/13/logicgate-risk-cloud-data-breach/

Exploit: Hacking

LogicGate: Software Company

Risk to Business: 1.631 = Severe

LogicGate notified customers that an unauthorized third party obtained credentials to its Amazon Web Services-hosted cloud storage servers storing customer backup files for its flagship platform Risk Cloud in 02/21. The risk and compliance specialty firm noted that only data uploaded on or prior to 02/23/21 would have been included in that backup file. The company said that an unauthorized third party was able to use filched credentials to decrypt files stored in AWS S3 buckets in the LogicGate Risk Cloud backup environment.

Customers Impacted: No sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

How it Could Affect Your Business: Hacking into databases is a profitable enterprise for cybercriminals. Ebsuring that you're using strong security for information storage is a modern essential.

Codecov

https://therecord.media/codecov-discloses-2-5-month-long-supply-chain-attack/

Exploit: Third Party Data Breach

Codecov: Software and Cloud Developer

Risk to Business: 1.337 = Extreme

Codecov is facing a mess after a threat actor managed to breach its platform and add a credentials harvester to one of its tools, Bash Uploader Codecov said the breach occurred "because of an error in Codecov's Docker image creation process that allowed the actor to extract the credential required to modify our Bash Uploader script." The attacker gained access to the Bash Uploader script sometime in 01/21 and made periodic changes to add malicious code that would intercept uploads and scan and collect any sensitive information like credentials, tokens, or keys. Unfortunately, the bad guys had 2.5 months to run wild – the breach wasn't discovered until 04/01. The damage isn't limited to only to clients who used the Bash Uploader script, either. Because the script is also embedded in other products, a large chunk of the company's customers may be affected.

Customers Impacted: No sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

How it Could Affect Your Business: Not only did Codecov fall victim to a cyberattack that adulterated its product, it didn't find out for 2.5 months. Not a good look.