Toyota alleges stolen customer data published on hacking site came from outside supplier - SiliconANGLE

By by Duncan Riley

Published: 2024-08-21 · Archived: 2026-04-05 14:45:31 UTC

Toyota alleges stolen customer data published on hacking site came from outside supplier

Data relating to customers of Toyota Motor Co. has been shared online in yet another case involving the Japanese car maker and a data breach, but Toyota is claiming that the data came from a third-party supplier and that it was not directly breached.

The latest breach involving Toyota came to light after a threat actor called ZeroSevenGroup shared 240 gigabytes of data claimed to have been stolen from Toyota on the infamous hacking site BreachForums. The threat actor claimed to have breached Toyota's U.S. branch to steal employee and customer data, contract and financial information and network infrastructure information, including credentials.

"We have hacked a branch in United States to one of the biggest automotive manufacturer in the world (TOYOTA). We are really glad to share the files with you here for free. The data size: 240 GB," ZeroSevenGroup wrote. "Contents: Everything like Contacts, Finance, Customers, Schemes, Employees, Photos, DBs, Network infrastructure, Emails, and a lot of perfect data. We also offer you AD-Recon for all the target network with passwords."

Bleeping Computer reported Monday that the files were stolen or at least created on Dec. 25, 2022, indicating the date the threat actor may have gained access to a backup server where the data was stored.

Though some reports are taking the word of ZeroSevenGroup that it hacked Toyota, the company claims it was not hacked. "Toyota Motor North America was not the subject of this activity," the spokesperson from Toyota told several media outlets. "Contrary to what has been reported, our systems were not breached or compromised," adding that the hacked data "appears related to a third-party entity that is misrepresented as Toyota."

Who the third-party entity is was not disclosed by Toyota and Toyota did not deny that the data related to its customers.

Though it's fair to give Toyota the benefit of the doubt here, jumping to the conclusion that Toyota may have been hacked directly is perhaps understandable, given the company's extensive history of data breaches.

Along with the German arm of Toyota's financial services branch being hacked late last year, previous Toyota-related breaches include a security researcher revealing that he had gained access to Toyota's Global Supplier Preparation Information Management System in February 2023. Some 300,000 customers potentially had their data stolen it Toyota left access key on GitHub in October 2022. The same month, data was also stolen from Denso Corp., a global automotive manufacturer based in Japan that's 25% owned by Toyota.

In March 2022, Toyota was forced to halt manufacturing operations at all of its plants in Japan after a cyberattack struck Kojima Industries Corp. And 3.1 million customers were affected when Toyota Motor North America was hacked in 2019.

Dr. Howard Goodman, technical director at enterprise cybersecurity solutions provider Skybox Security Inc., told SiliconANGLE that this latest breach underscores the growing sophistication of threat actors that exploit vulnerabilities within critical infrastructures.

"This breach serves as a stark reminder that traditional cybersecurity measures are no longer sufficient in isolation," Goodman said. "Organizations must adopt a comprehensive, multilayered cybersecurity strategy that incorporates cyberthreat exposure management and attack path analysis to proactively identify and mitigate potential threats before they can be exploited."

Image: SiliconANGLE/Ideogram
