Toyota announces second security breach in the last five weeks

By Written by Catalin Cimpanu, ContributorContributor March 29, 2019 at 5:37 a.m. PT

Archived: 2026-04-05 14:59:54 UTC

Japanese car maker Toyota announced its second data breach today, making it the second cyber-security incident the company acknowledged in the past five weeks.

Security

-
-
-
-

While the first incident took place at its Australian subsidiary, today's breach was announced by the company's main offices in Japan.

Toyota and Lexus car owners data at risk

The company said hackers breached its IT systems and accessed data belonging to several sales subsidiaries.

The list includes Toyota Tokyo Sales Holdings, Tokyo Tokyo Motor, Tokyo Toyopet, Toyota Tokyo Corolla, Nets Toyota Tokyo, Lexus Koishikawa Sales, Jamil Shoji (Lexus Nerima), and Toyota West Tokyo Corolla.

Toyota said the servers that hackers accessed stored sales information on up to 3.1 million customers. The carmaker said there's an ongoing investigation to find out if hackers exfiltrated any of the data they had access to.

Customer financial details were not stored on the hacked servers, Toyota said. However, the company didn't say what type of info hackers might have accessed either.

"We apologize to everyone who has been using Toyota and Lexus vehicles for the great concern," a Toyota spokesperson said today in a message to the press.

"We take this situation seriously, and will thoroughly implement information security measures at dealers and the entire Toyota Group."

APT32?

This is the second cyber-security the company has announced this year, after disclosing a similar incident in late February, but affecting its Australian branch.

The attack on its Australian office was more disruptive in nature, bringing down Toyota Australia's ability to handle sales and deliver new cars, and has been attributed by some industry experts to APT32 (OceanLotus), a Vietnamese cyber-espionage unit with a known focus on the automotive industry.

Experts suggested that APT32 hackers might have targeted Toyota's Australia branch as a way to get into Toyota's more secure central network in Japan.

At the time, Toyota declined to confirm any of these theories and attribute the attack to APT32 hackers.

However, the company did say that it would start an internal audit of its IT systems following the attack on its Australian branch, and today's announcement only pours fuel on the APT32 theories.

> The scope and scale of #APT32's 🇻🇳 activity remains largely unchanged from: https://t.co/ktit15l0si
> "Since at least 2014, FireEye has observed APT32 targeting foreign corporations with a vested interest in Vietnam's manufacturing, consumer products, and hospitality sectors."
>
> — Nick Carr (@ItsReallyNick) March 14, 2019

Updated on March 30: On the same day that Toyota Japan announced its data breach, Toyota Vietnam and Toyota Thailand also announced cyber-security incidents, albeit without any details about the hacks and if they're connected to the Toyota Japan incident.

Top vehicle hacking examples (in pictures)

More data breach coverage:

- Companies are leaking sensitive files via Box accounts
- Nokia firmware blunder sent some user data to China
- 'Yelp for conservatives' MAGA app leaks users data
- Database leaks 250K legal documents, some marked 'not designated for publication'
- FEMA 'unnecessarily' shared data of 2.3 million disaster victims with contractor
- Cryptocurrency platforms DragonEx and CoinBene disclose hacks
- Facebook passwords by the hundreds of millions sat exposed in plain text **CNET**
- Facebook data privacy scandal: A cheat sheet **TechRepublic**

Source: https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/