

Police: Laptop used to reprogram, steal more than 100 cars

August 5 2016, by Michael Graczyk And Tom Krisher



This undated photo provided by the Houston Police Department shows Michael Armando Arce. Houston police say they've arrested Arce and Jesse Zelaya, accused of using pirated computer software to steal more than 100 vehicles that

likely ended up in Mexico. Authorities say Arce and Zelaya focused on new Jeep and Dodge vehicles, which attract big money on the black market in Mexico. The men allegedly used a laptop computer to reprogram the targeted vehicles' electronic security. (Houston Police Department via AP)

Two men jailed in Houston and accused of using pirated computer software to steal more than 100 vehicles may have exploited an electronic vulnerability to advance auto theft into high-tech crime.

Michael Arce, 24, and Jesse Zelaya, 22, focused on new Jeep and Dodge vehicles, which attract big money on the black market in Mexico, authorities said. The men allegedly used a laptop computer to reprogram the targeted vehicles' electronic security so their own key worked.

The stolen vehicles had a common software that's used by auto technicians and dealers, Houston police officer Jim Woods said.

"As you get more and more computers installed in vehicles—if somebody has that knowledge and that ability, they can turn around and figure out a way to manipulate the system," he said.

Fiat Chrysler, which makes Jeeps and Dodges, and police are investigating how the thieves got access to a computerized database of codes used by dealers, locksmiths and independent auto repair shops to replace lost key fobs, said Berj Alexanian, a spokesman at the company's U.S. headquarters in Auburn Hills, Michigan. He said the code database is national and includes vehicles in areas outside of Houston, although he wasn't aware of similar thefts elsewhere.

"We're looking at every and all solutions to make sure our customers can safely and without thinking park their vehicles," Alexanian said Friday.

With more automotive tasks becoming computerized and more cars being linked to the internet, such thefts are likely to increase across the globe, said Yoni Heilbronn, a computer security expert.



This undated photo provided by the Houston Police Department shows Jesse Irvin Zelaya. Houston police say they've arrested Zelaya and Michael Arce, accused of using pirated computer software to steal more than 100 vehicles that likely ended up in Mexico. Authorities say Zelaya and Arce focused on new Jeep and Dodge vehicles, which attract big money on the black market in Mexico. The men allegedly used a laptop computer to reprogram the targeted vehicles' electronic security. (Houston Police Department via AP)

The auto industry has worked hard in the past year to develop protections, but hackers with multiple motivations will always be looking for ways to get in, said Heilbronn, vice president of marketing for Argus Cyber Security, an Israeli company that works with automakers.

While increased computerization brings safety benefits, Heilbronn foresees more thefts, malicious software being installed that shuts down cars until a ransom is paid, and even attacks that disable many cars at a time. The industry, he said, has to install multiple layers of defense.

Automakers have been working together to develop best practices and to share information on cybersecurity threats. Companies, including Fiat Chrysler, have their own hacking teams and have offered bounties to outside hackers if they find vulnerabilities.

The Houston investigation began in late May with the theft of a Jeep Wrangler near downtown. Leads in that case had been exhausted when investigators received information from federal Homeland Security and Immigration and Customs Enforcement officers about vehicles being stolen using a laptop. Arce and Zelaya then were identified as suspects.

The two men, who each have criminal records, were arrested last weekend driving a stolen Jeep Grand Cherokee after police had been concentrating on an area of Houston that had been hit previously by auto thieves. They also recovered electronic devices, keys and other tools believed used in the thefts, along with drugs, firearms and body armor.

In the Jeep Wrangler case caught on a surveillance video, the suspect got under the hood, cut wires to the horn to disable an alarm and then got inside the SUV. Once inside, he used the database and the vehicle identification number to program a new key fob for the Jeep.

Arce remained in jail without bond on charges of unauthorized use of a vehicle, felony possession of a weapon, and possession with intent to deliver a controlled substance. He was set for a court appearance Aug. 26.

Zelaya is being held on \$500,000 bond on a charge of unauthorized use of a vehicle and was due in court Wednesday.

© 2016 The Associated Press. All rights reserved.

Citation: Police: Laptop used to reprogram, steal more than 100 cars (2016, August 5) retrieved 25 April 2024 from <https://phys.org/news/2016-08-police-laptop-reprogram-cars.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.