Threat Level
Privacy, Crime and Security Online

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen ✉ March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots.

"We initially dismissed it as mechanical failure," says Texas Auto Center manager Martin Garcia. "We started having a rash of up to a hundred customers at one time complaining. Some customers complained of the horns going off in the middle of the night. The only option they had was to remove the battery."

The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven't been paid for. Operated by Cleveland-based Pay Technologies, the system lets car dealers install a small black box under vehicle dashboards that responds to commands issued through a central website, and relayed over a wireless pager network. The dealer can disable a car's ignition system, or trigger the horn to begin honking, as a reminder that a payment is due. The system will not stop a running vehicle.

Texas Auto Center began fielding complaints from baffled customers the last week in February, many of whom wound up missing work, calling tow trucks or disconnecting their batteries to stop the honking. The troubles stopped five days later, when Texas Auto Center reset the Webtech Plus passwords for all its employee accounts, says Garcia. Then police obtained access logs from Pay Technologies, and traced the saboteur's IP address to Ramos-Lopez's AT&T internet service, according to a police affidavit filed in the case.

Ramos-Lopez's account had been closed when he was terminated from Texas Auto Center in a workforce reduction last month, but he allegedly got in through another employee's account, Garcia says. At first, the intruder targeted vehicles by searching on the names of specific customers. Then he discovered he could pull up a database of all 1,100 Auto Center customers whose cars were equipped with the device. He started going down the list in alphabetical order, vandalizing the records, disabling the cars and setting off the horns.

"Omar was pretty good with computers," says Garcia.

The incident is the first time an intruder has abused the no-start system, according to Jim Krueger, co-owner of Pay Technologies. "It was a fairly straightforward situation," says Krueger. "He had retained a password, and what happened was he went in and created a little bit of havoc."

Krueger disputes that the horns were honking in the middle of the night; he says the horn honking can only be activated between 9 a.m. and 9 p.m.

First rolled out about 10 years ago, remote immobilization systems are a controversial answer to delinquent car payments, with critics voicing concerns that debtors could suffer needless humiliation, or find themselves stranded during an emergency. Proponents say the systems let financers extend credit to consumers who might otherwise be ineligible for an auto loan.

Austin police filed computer intrusion charges against Ramos-Lopez on Tuesday.

(Image courtesy drbrain)

(Updated 15:35 to report Ramos-Lopez's arrest)

Tags: cars
Post Comment | Permalink

Also on Wired.com

- AT&T Zero Charger Switches Itself Off
- SXSW: Amps Set on 11, Bagpipes Set on Stun
- SXSauced: Sinfully Good Cocktails at Péché
- Feds Move to Break Voting-Machine Monopoly
- Robert Rodriguez Brings *Predators* 'First Look' to SXSW
- Wired's Biometric Super Bowl Ad Winner Is a Geeky Surprise

Related Topics:

- Omar Ramos-Lopez,
- Austin (Texas),
- Martin Garcia,
- Texas Auto Center,
- Jim Krueger,
- Pay Technologies

Comments (69)

Posted by: wayneo | 03/18/10 | 9:15 am |

Even the most secure computer system in the world can’t protect against user account theft. That’s why password protection and change policies are so important. This wasn’t a hack, just another form of identity theft.
If disabling the vehicle forcing the owner to catch up on the debt are the goal, then more power to them. If the buyer doesn’t like it, then they should improve their credit so they aren’t confined to shopping at those “Everyone is approved” dealerships.

Posted by: RRmike | 03/18/10 | 9:48 am |

put this kid to work in Afghanistan disabling IEDx.

Posted by: Gewburr | 03/18/10 | 9:50 am |

>”Omar was pretty good with computers,” says Garcia.<
In other words, Omar knew how to turn on reboot a PC and how to use twitter. The guy that said this probably barely knows how to open a web browser, and certainly knows nothing about how to set up an email account or use a printer.

Posted by: teton | 03/18/10 | 10:18 am |

This disabling device sounds like a lawsuit waiting to happen and is a definite invasion of privacy. What if a mother is out in the 110.. degree heat and has a baby in the car, decides to stop for a minute and turns the engine off at the time the disabling device is activated and the baby dies from the heat. There are many other scenarios that could take place also. Thanks to the hacker this invasion of privacy is out in the open now and a law should be passed to keep the dealers from doing it.

Posted by: gadkarisid | 03/18/10 | 10:24 am |

I totally agree with Gewburr — the guy can’t be considered a hacker.

Posted by: catbeller | 03/18/10 | 10:32 am |

All cars will be become black boxes. The circuitry will be integrated into the motor controllers, and then the frame itself, where you will not be able to cut it out without destroying the driveabilty of the car.

It’s happening because Americans will accept anything, as long as a private businessman does it. Anything.

Posted by: saris | 03/18/10 | 10:40 am |

catbeller, There will never be a time when some clever gear-head will not be able to remove something like this from a car.

Posted by: bbjohn | 03/18/10 | 10:47 am |

Is It also possible that the braking systems on Toyota’s has been hacked since it is primarily computer controlled? you take you car in for service they diagnose it with a computer which could have been infected. I don’t know just spit-wadding here……..

Posted by: jweller | 03/18/10 | 10:49 am |

Please explain to me why I would buy a car that let the dealership disable it remotely.

Posted by: rootytooty | 03/18/10 | 10:52 am |

HERE’S A GREAT IDEA, CAN SOMEONE WORK ON THIS? Please invent a device that’ll disable sound systems in the cars of morons who play rap music at concert-volume level in their cars. Everytime I’m at a stop light one of these idiots pulls up beside me, windows down, with the volume turned all the way up — they even leave the volume turned up when they stop to pump gas. I want a button in my car I can push to immediately mute/disable their car’s music system. Could this work?

Posted by: will564 | 03/18/10 | 11:09 am |

The guy couldn’t have been too bright. — He was “hacking” (read: using somebody’s password gotten while he work there)…from his own ISP account.

Posted by: qudduz | 03/18/10 | 11:25 am |

Next step will be of an actual hacker (unlike the guy in this story), hack into the “onStar” computer and start messing with peoples cars and or at least giving them wrong gps directions!
It’s a good point about the computer system on the toyota cars too!

Posted by: mrplow911 | 03/18/10 | 11:55 am |

i do beleive in afgahn they actualy have devices to remotley shut down a running care it has to do with destorying electrical components with certain waves

Posted by: nclined | 03/18/10 | 12:00 pm |

I agree… not a hack. Just because I used my wifes Amazon.com account to buy a book bc i knew the password doesn't mean i hacked her account.

Posted by: beta447 | 03/18/10 | 12:08 pm |

If I found out a dealer was putting a black box in my car I'd brick the car my own special way and leave it on the little shit's doorstep.

Posted by: HipCat | 03/18/10 | 12:43 pm |

@quidduz:
Hacking onstar could be a new hacker toy. See how many cars you could direct to one spot at the same time or in a 24 hour period.

for the story:
If i found out a dealer had a black box on my vehicle i'd definatly NOT be happy. Whats to say a computer glitch or a fat finger doesn't shut the vehicle down on accident. If it wasn't the vehicle they intended and it happened without someone knowing then i could have a 4 wheel paper weight until i figured out what happened.

Posted by: pendal | 03/18/10 | 1:01 pm |

This is just stoopid!!

This guy was not a hacker.. he used an existing account. Unless someone hacked his computer and used it to frame him. Now that would've been a good hacker story.

This is just a guy who wanted to get someone else in trouble probably.

The only way to stop this at all is to have mandatory password change polices. Why you wouldn't in a scenario where peoples lives are a stake it beyond me.

We do it here at work, and these people only read their own email.

Posted by: PhoobarID | 03/18/10 | 1:32 pm |

While I chuckled when I read this…just goes to show how American business will use any type of system or do anything as long as the hype/BS is right. With this attitude & bad economic times…should be common sense & the first thing you do whenever you fire someone or lay people off…reset passwords no matter what. Some companies deserve this to happen to them to MAYBE wake them up.

This was just an event just waiting to happen. When you take the livelihood of someone…what do you expect them to do? While I hope the companies might learn something from this incident…it won't happen & will happen again.

Posted by: djwaffles | 03/18/10 | 1:39 pm |

I heard from a very credible source that Omar's account was never deactivated after he was fired. Calling him a hacker is innacurate and misleading. There was no security flaw with the software and it wasn't "hacked". If that's considered hacking then I'm a hacker for logging in and posting this comment!

« Previous 1 2