MOTHERBOARD
TECH BY VICE

The Car Thieves Using Tech Disguised Inside Old Nokia Phones and Bluetooth Speakers

Motherboard posed as an interested buyer to learn more about the wild world of car hacking.

By Joseph Cox

April 18, 2023, 4:26pm

Listen to this article

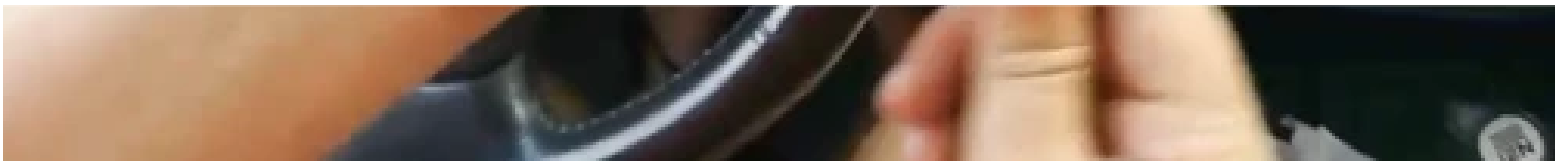


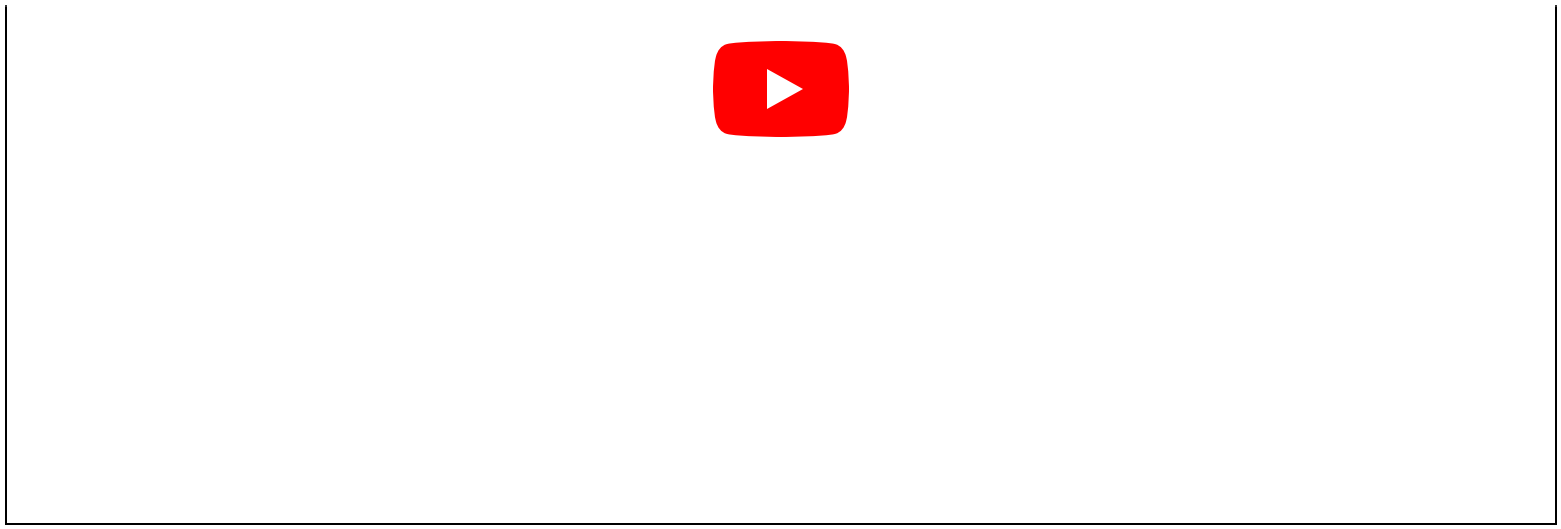
IMAGE: MOTHERBOARD

A man sitting in the driver's seat of a Toyota is repeatedly tapping a button next to the steering wheel. A red light flashes—no luck, the engine won't start. He doesn't have the key. In response, the man pulls up an usual tool: a Nokia 3310 phone.

The man plugs the phone into the car using a black cable. He then flicks through some options on the 3310's tiny LCD screen. "CONNECT. GET DATA," the screen says.

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

SEE MORE →



This under 30 second clip shows a new breed of car theft that is spreading across the U.S. Criminals use tiny devices, sometimes hidden inside innocuous looking bluetooth speakers or mobile phones, to interface with the vehicle's control system. This allows thieves with very little technical experience to steal cars without needing the key, sometimes in just 15 seconds or so. With the devices available to buy online for a few thousand dollars, the barrier of entry for stealing even high-end luxury cars is dramatically reduced.

"JBL Unlock + Start," one ad for a device hidden inside a JBL-branded bluetooth speaker states. "No key needed!" The ad states that this specific device works on a variety of Toyota and Lexus cars: "Our device has a cool stealthy style and look," it says.

"The device does all the work for them," Ken Tindell, CTO at vehicle cybersecurity firm Canis Labs, told Motherboard in an email. "All they have to do is take two wires from the

Earlier this month Tindell published his and Ian Tabor's, a friend in automotive cybersecurity, research into these devices. Tabor bought a device to reverse engineer after car thieves appear to have used one to steal his own Toyota RAV4 last year, the write-up says. After some digging, Tabor came across devices for sale that target Jeeps, Maseratis, and other vehicle brands, the post reads.

The video showing the man using a Nokia 3310 to start a Toyota is just one of many YouTube videos Motherboard found demonstrating the technique. Others show devices used on Maserati, Land Cruiser, and Lexus-branded vehicles. Multiple websites and Telegram channels advertise the tech for between 2,500 Euro and 18,000 Euro ($2,700 and $19,600). One seller is offering the Nokia 3310 device for 3,500 Euro ($3,800); another advertises it for 4000 Euro ($4,300). Often sellers euphemistically refer to the tech as "emergency start" devices nominally intended for locksmiths. Some of the sites offer tools that may be of use to locksmiths, but legitimate businesses likely have no use for a tool that is hidden inside a phone or other casing.

Motherboard posed as an interested customer to one person offering to sell engine starters online. That person said they would ship a device to the U.S. via DHL.

“Yes, Nokia works with USA cars,” they wrote, referring to the engine starter hidden inside a Nokia phone. The seller said they take Western Union, MoneyGram, or bank transfers,

removing the headlights, they can use their device to send these messages, it adds.

Despite the devices' high prices, the one Tabor bought contained just $10 worth of components, the write-up says. These include a chip with CAN hardware and firmware, and another CAN-related chip.

Once a device manufacturer has reverse engineered a particular vehicle's messaging, creating each device would only take around a few minutes, Tindell told Motherboard. "It's not a lot of work: solder some wires down, encase everything in a blob of resin," he wrote.

At the moment, impacted vehicles are generally wide open to these sorts of attacks. The only proper fix would be to introduce cryptographic protections to CAN messages, Tindell

ways to circumvent existing anti-theft systems. We are committed to continuing to work on this issue with theft prevention experts, law enforcement, and other key stakeholders."

Subscribe to our cybersecurity podcast, CYBER. Subscribe to our Twitch channel.

TAGGED: CYBER, WORLDNEWS, HACKING, HACKERS, CRIME, CAR THIEVES

MORE FROM VICE

Tech

Tech

LastPass Shouldn't Be Trusted With Your Passwords

JOSEPH COX

02.28.23

Tech

Ransomware Group Claims Hack of Amazon's Ring

JOSEPH COX, JASON KOEBLER

03.14.23

Tech

Inside the DEA Tool Hackers Allegedly Used to Extort Targets

JOSEPH COX

03.17.23