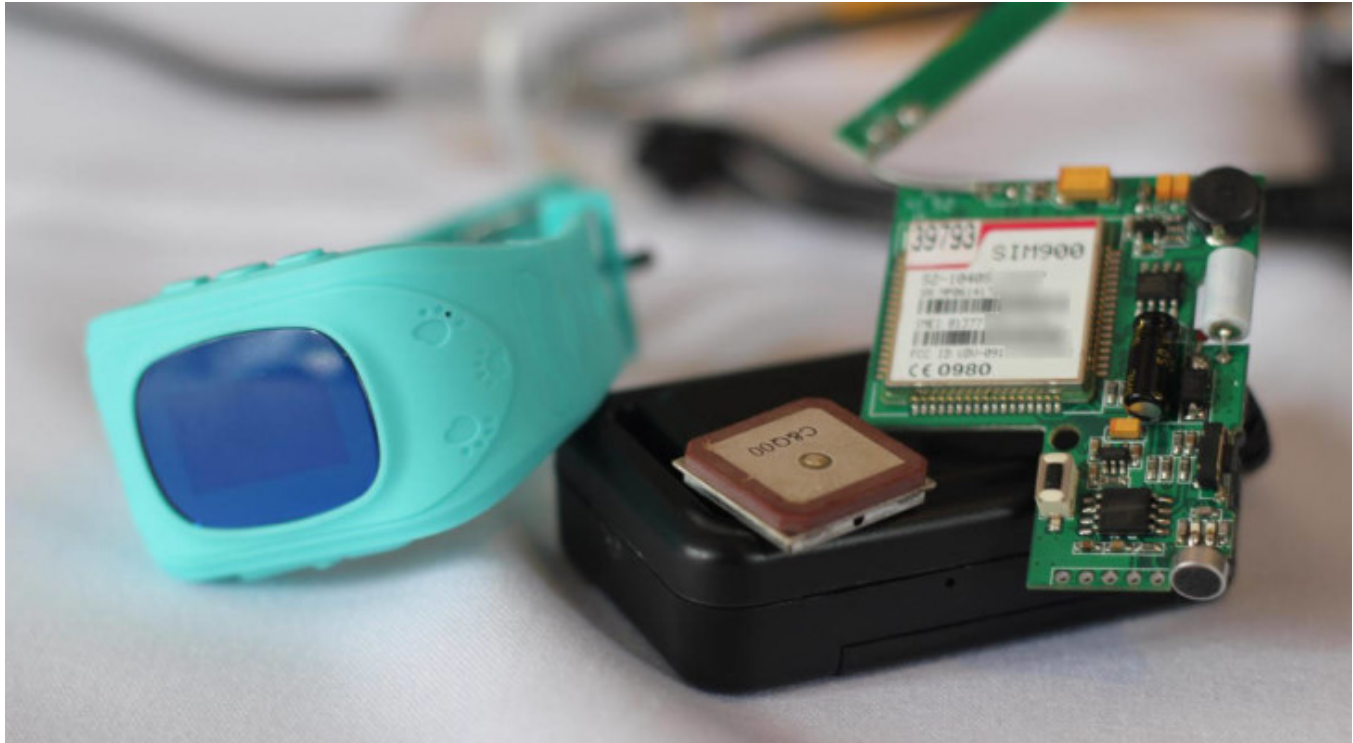


**MUST READ** The FBI continues its crusade against the encryption



## Hundreds of thousands of engine immobilizers remotely hackable

December 11, 2015 By [Pierluigi Paganini](#)



A New Zealander expert has found hundred of thousands of vulnerable engine immobilizers are remotely hackable due to a flaw.

The New Zealander Lachlan Temple ([@skoooooch](#)) has discovered hundred of thousands of

vulnerable engine immobilizers are remotely hackable. The expert discovered a flaw in a popular cheap car tracking and immobilizer gadget that can allow remote attackers to locate, eavesdrop, and in some cases interrupting the fuel supply to the engine to hundreds of thousands of vehicles, and more alarming, even while they are in motion.


Once the users have installed the engine immobilizers on their car they are able to remotely track the vehicle, block the engine, enable microphone recording, enable geo-fencing, and track the car movements.


The gadgets are rebranded by various vendors, including the Chinese ThinkRace, meanwhile in Australia the engine immobilizers are branded as “Response” and offered for sale at electronics


Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | **igence** | Laws and

Laws and regulations | Malware | Mobile | Data Breach | Security | Social Networks |





Reports | EXTENDED COOKIE POLICY | Contact me | **KIE POLICY** | Cont







whereabouts of your vehicle in real time via the Internet on a computer or Smartphone. The dev...

Share |    

[Shipping & Delivery Information](#)

Bulk Pricing:

1-3	\$139.00
4+	\$126.95

In Stock

1

ADD TO CART

Have a question about placing your order?

**Call our Techstore**


on 1800 022 888

One of the models available on the market is able to control the car fuel pumps, a feature implemented to remotely immobilize a stolen vehicle, but Temple discovered that a an attacker could exploit a flaw in the management of session cookies to enable this function.

This means that while you are driving, someone everywhere is able to stop your engine!

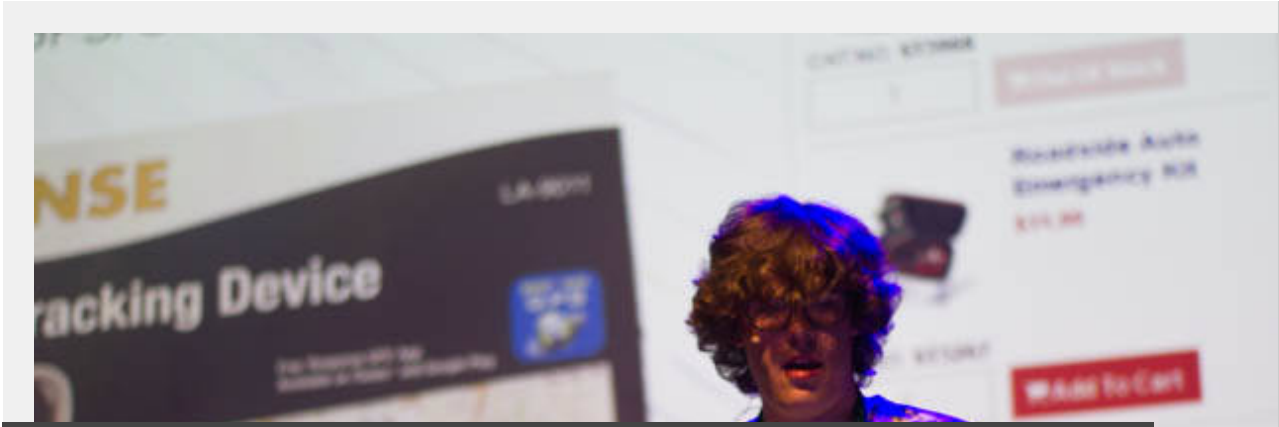
Temple presented his findings at the Kiwicon security confab in Wellington, he added that today flaws allow attackers who log into any account, including a demo account, to log into any of the 360,000 units ThinkRace that are sold without need of a password.

DISTRIBUTION



http://securityaffairs.co/wordpress/42714/hacking/vulnerable-engine-immobilizers.html

2/6



This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Accept](#) [Read More](#)



Lachlan Temple. Photo by Darren Pauli / The Register

*“You just brute force everyone account, you can increment each one,” Temple told Vulture South. “You could disable someone’s car if they have wired the relay, so if that happened on a freeway that is pretty dangerous.” “Most people would wire it this way, that’s the main point of it and the reason why mechanics sell it.”*

Temple suggests users to wire the relay to the starter motor, in this way a remote hacker cannot stop the engine while in motion and instead would prevent it starting up once turned off.

The flaws could be also exploited by attackers to access user personal details, including phone numbers, or eavesdrop on cars through the a microphone installed in the set of the engine immobilizers.

Temple discovered that the same tracker is used by ThinkRace in the watches sold to track children, in this case, an attacker can eavesdrop on kids and track them.

Temple announced that he will focus next test on more expensive tracking solution available on the market, including engine immobilizers used by commercial fleets of vehicles.

Stay Tuned ...

**Pierluigi Paganini**

A BITLINK 1

THOUS  
,259 clicks

New Sp  
exploits  
Security  
malicious  
strain of  
malware

5

6

7

8

Pl  
it

**(Security Affairs – engine immobilizers, car hacking)**

Share it please ...



## Cyber Security Solution

Protect Data Across The Kill Chain. Leading Cyber Security. Free

[Hacking](#)[privacy](#)[automotive](#)[Car hacking](#)[engine immobilizers](#)[Breaking News](#)[Hacking](#)[Security](#)

### SHARE ON



#### Pierluigi Paganini

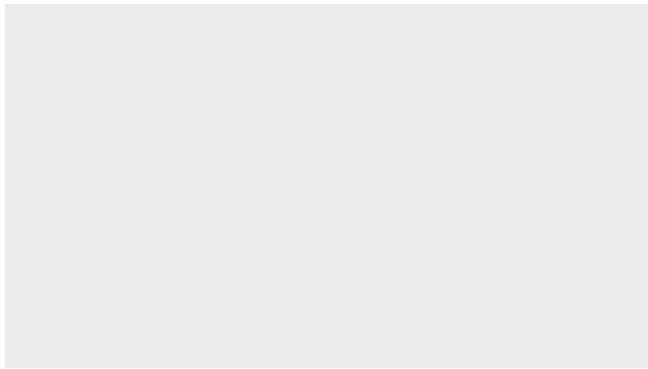
Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".



#### PREVIOUS ARTICLE

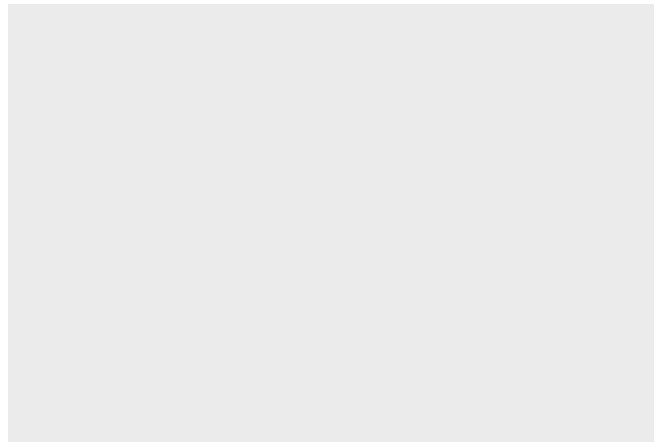
**New Spy Banker Trojan Telax exploits  
Google Cloud Servers**

## YOU MIGHT ALSO LIKE



[AVG, McAfee, and Kaspersky antivirus were vulnerable to critical flaw](#)

December 10, 2015 By [Pierluigi Paganini](#)



[Internet root servers flooded with 5 million queries a second](#)

December 10, 2015 By [Pierluigi Paganini](#)

Promote your solution on Security Affairs

Promote your  
solutions on  
Security  
Affairs...  
contact us!



Copyright Security Affairs by Pierluigi Paganini - All Right Reserved.

