Hackers root Google’s Nest thermostat in 15 seconds

Firm advises buying one of its security cameras

By Chris Merriman

Mon Aug 11 2014, 16:33

GOOGLE’S NEST THERMOSTAT has been rooted by hackers at the Black Hat Conference in Las Vegas.

In the demonstration that the team has replicated on Youtube, Daniel Buentello from the University of Central Florida shows how he is able to gain root access and remote control over a Nest thermostat via USB in 15 seconds.

The smart thermostat maker, which was bought by Google earlier this year for $3.2bn, has been made the focal point of the “Works with Nest” programme, an Internet of Things initiative that allows a growing number of household appliances to interact.

Speaking to the conference, Buentello pointed out, “This is a computer that the user can’t put an antivirus on. Worse yet, there’s a secret back door that a bad person could use and stay there forever. It’s a literal fly on the wall.”

While The INQUIRER does not condone Buentello’s use of the word “literal”, he made a valid point. If this is the hub device of our automated home, then a rogue...
element could leave in the realms of dystopian Sci-Fi.

To illustrate the point, Bentello’s demonstration changed the display of the Nest to an image of HAL the killer computer from 2001, with the message, “I know that you and Frank were planning to disconnect me, and I am afraid that is something I cannot allow to happen.”

A statement from Zoz Cuccias of Nest given to Venturebeat does little to quell the concern, as it turns into a sales pitch. “All hardware devices - from laptops to smartphones - are susceptible to jailbreaking; this is not a unique problem. This is a physical jailbreak requiring physical access to the Nest Learning Thermostat. If someone managed to get in your home and had their choice, chances are they would install their own devices, or take the jewelry.”

He went on to suggest, “One of your best defenses is to buy a Dropcam Pro so you can monitor your home when you’re not there.”

By sheer coincidence, Dropcam was purchased by Nest in June and is part of the “Works with Nest” programme, making it potentially susceptible to malware from a hacked Nest thermostat.

Follow the INQUIRER

Follow the INQUIRER

Follow

Like

Follow

607

Comment on this article

Flame Author

Print

Tags: IoT, Intel-IOT, Hacking, Security, Smart Working

Share this:

bel.icio.us

Digg

Facebook

Linkedin

Reddit

StumbleUpon

Twitter

Share

Related articles

Teenagers hack ATM by reading the instructions

Google admits Nexus 6 and Nexus 9 sales have been sluggish

Kim Dotcom is bankrupt and possibly doomed

PlayStation 5 could be completely cloud based, says Sony

Subscribe to INQ newsletters

Sign up for INQbot – a weekly roundup of the best from the INQ

First Name

Email Address

SUBSCRIBE

More newsletter options
Andrea Sibaldi • 9 months ago
"Bentello’s demonstration changed the display of the Nest to an image of HAL. Yeah, this isn’t exactly fresh news. The catch is that you need physical access to the Nest and plug an usb drive into it, in order to achieve the exploit. So, I sneak into your apartment and all I do is... plant a rootkit in your Nest. Yes, exactly... that makes a lot of sense.

3 ▲ | ▼ • Reply • Share ▶

HMan2828 • Andrea Sibaldi • 5 months ago
It does make sense if the Nest is on a VPN that cannot be accessed from the outside. You set it up as a proxy and have direct access to the protected network.

Everyone wants to be in the digital age and have nice gadgets and computers everywhere, but few understand what that means. Security exploits like these can serve as an entry point to a whole other level.

3 ▲ | ▼ • Reply • Share ▶

ruBaluVua • 9 months ago
and what would be the point its not like it has a camera or microphone so what nefarious things could you actually do apart from mess with the temperature??

3 ▲ | ▼ • Reply • Share ▶

ruZZ • ruBaluVua • 4 months ago
I wonder if the Wi-Fi chip could be put into "monitor" mode. This would enable the Nest to sniff all Wi-Fi traffic. Worse, if it already knows the networks password, it could be configure to sniff for an authentication process and use the key to de-crypt the data. Alternatively, it could run some attacks on the surrounding Wi-Fi networks until it gets in. hmmm

3 ▲ | ▼ • Reply • Share ▶
Hackers root Google's Nest thermostat in 15 seconds - The Inquirer

You can remove the data logging services running on the device. This way Google and their NSA friends can't monitor you.

Edward Snowden → rubbaluvva • 9 months ago

Or you buy a used Nest off of Ebay that has already been modified.......

zoobot • 9 months ago

TattooGate: Apple Watch won't work properly on inked wrists
Francois Lukawekci — Double-douche factor: an iwatch AND a wrist tattoo? Let call it douche ...

Apple Watch release pushes iOS 8 past 80 percent adoption
Steven De Bondt — And since 80% of people is subject to the "I got an iPhone zone" You can …

LG G4 hands-on review
Dave Knight — You forgot two of the biggest features. It has an SD card slot and a removable …

There's an Orwellian undertone to Microsoft's Build keynote
tman — Actually loved reading that report. Very amusing, and likely quite accurate. I can only …

Network Security Testing
No False Positives. Ensure Your Systems Security with an IT Audit.