SoylentNews

SoylentNews is people

A "Tamper-Proof" Currency Wallet Just Got Backdoored by a 15-Year-Old

posted by martyb on Friday March 23, @11:48AM
from the And-I-would-have-gotten-away-with-it-too,-if-it-weren't-for-you-meddling-kids^H dept.

Fnord666 writes:

Never say can't.

> For years, executives at France-based Ledger have boasted their specialized hardware for storing cryptocurrencies is so securely designed that resellers or others in the supply chain can't tamper with the devices without it being painfully obvious to end users. The reason: "cryptographic attestation" that uses unforgeable digital signatures to ensure that only authorized code runs on the hardware wallet.
>
> "There is absolutely no way that an attacker could replace the firmware and make it pass attestation without knowing the Ledger private key," officials said in 2015. Earlier this year, Ledger's CTO said attestation was so foolproof that it was safe to buy his company's devices on eBay.
>
> On Tuesday, a 15-year-old from the UK proved these claims wrong. In a post published to his personal blog, Saleem Rashid demonstrated proof-of-concept code that had allowed him to backdoor the Ledger Nano S, a $100 hardware wallet that company marketers have said has sold by the millions. The stealth backdoor Rashid developed is a minuscule 300-bytes long and causes the device to generate pre-determined wallet addresses and recovery passwords known to the attacker. The attacker could then enter those passwords into a new Ledger hardware wallet to recover the private keys the old backdoored device stores for those addresses.

Oops. To be fair, he's a very clever 15 year old.

Original Submission

(1)

- **Haxxor (Score: 2) by pkrasimirov on Friday March 23, @12:14PM (3 children)**

  by pkrasimirov (3358) on Friday March 23, @12:14PM (#657093)

  Best part is he cannot get sued because he's minor.

  - **Re:Haxxor (Score: 3, Informative) by All Your Lawn Are Belong To Us on Friday March 23, @12:30PM**

    by All Your Lawn Are Belong To Us (6553) on Friday March 23, @12:30PM (#657096)

    No. You can name anyone as a party to a lawsuit, and a minor can commit a tort. The leading theory is you name the minor and you name the parents (for negligent supervision to allow the minor to _____).

    Minors generally cannot enter into contracts.

  - **Re:Haxxor (Score: 2) by PiMuNu on Friday March 23, @12:49PM (1 child)**

    by PiMuNu (3823) on Friday March 23, @12:49PM (#657100)

    What has he done that he can be sued for?

    - **Re:Haxxor (Score: 2) by c0lo on Friday March 23, @01:16PM**

      by c0lo (156) on Friday March 23, @01:16PM (#657105)

      Breach of DMCA - it's an universal law, like the law of gravitation, didntcha know?

      (grin)

- **Proof of concept? (Score: 2) by All Your Lawn Are Belong To Us on Friday March 23, @12:27PM (2 children)**

  by All Your Lawn Are Belong To Us (6553) on Friday March 23, @12:27PM (#657095)

  > It simply requires an attacker to install a custom MCU firmware that can exfiltrate the private keys without the user’s knowledge, next time they use it.

  If you let someone get at the firmware of the device you can make it do quite a bit. It's not that this isn't legitimate, only that any device that hasn't adequately secured its firmware is likely vulnerable to something similar. (And only slightly more variable.... if you can do the firmware can you replicate the functions of the device accurately enough to fool the user into thinking it's legitimately working when it is working for you?)
  The author of the attack will go far in life, technically. I wonder about their quality of life, but hopefully it will be a happy one.

  - **Re:Proof of concept? (Score: 1, Informative) by Anonymous Coward on Friday March 23, @12:43PM**

    by Anonymous Coward on Friday March 23, @12:43PM (#657099)

    > The author of the attack will go far in life, technically.

    Indeed.

    > I wonder about their quality of life, but hopefully it will be a happy one.

    Considering the Muslim nature of his name, those chappies in Cheltenham will, no doubt, be paying *especial* attention to his career..and no doubt some plod somewhere is currently poring over the various computer misuse laws here in the UK looking for a stick to beat him with...mind you, as he's making a *French* company look a bit silly, they're probably feeling very conflicted.

  - **Re:Proof of concept? (Score: 4, Insightful) by Arik on Friday March 23, @01:33PM**

    by Arik (4543) on Friday March 23, @01:33PM (#657111)

    ```
    "If you let someone get at the firmware of the device you can make it do quite a bit. It's not that this isn't legitimate, only that any device that hasn't adequately secured its firmware is likely vulnerable to something similar."

    Well one thing that seems rather important which you don't mention is that this is a device that is *specifically* marketed as being designed and built so that physical security isn't necessary. The company makes a big deal out of the claim, so it's not like he's demonstrating this sort of attack against a typical consumer device that's not supposed to be able to withstand it.

    --
    "Unix? These savages aren't even circumcised!"
    ```

- **15? (Score: 2) by FakeBeldin on Friday March 23, @01:23PM (1 child)**

  by FakeBeldin (3360) on Friday March 23, @01:23PM (#657107) Journal

  I've seen the claim that he is 15. I poked around a bit, but couldn't find confirmation.
  I'll readily admit that I haven't looked that well into it, but still: writing style and level of explanation of the blog post do not suggest 15 years old to me.

  Has anyone seen some sort of origins for the claim this chap is 15?

  - **Re:15? (Score: 0) by Anonymous Coward on Friday March 23, @01:35PM**

    by Anonymous Coward on Friday March 23, @01:35PM (#657113)

    Based on your writing style, I believe you are 15. I've seen nothing else to believe otherwise.

(1)