Forbes http://onforb.es/1XZKPro

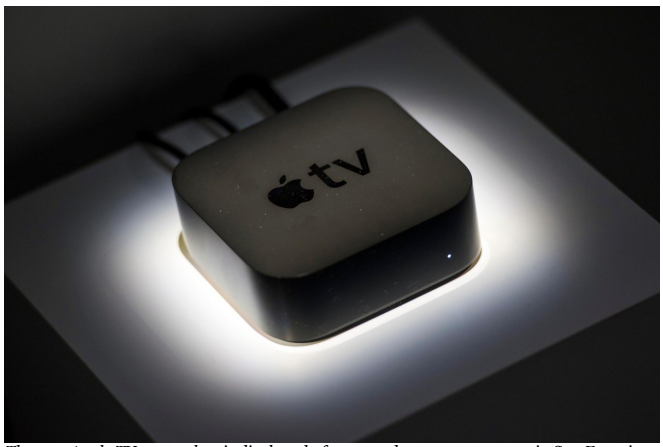


**Quora** Contributor

Opinions expressed by Forbes Contributors are their own.

TECH 12/10/2015 @ 2:27下午 | 274 views

# Can Smart TVs Be Hacked?



*The new Apple TV set-top box is displayed after a product announcement in San Francisco, California, U.S., on Wednesday, Sept. 9, 2015. (David Paul Morris/Bloomberg)*



*Can Smart TVs be attacked? originally appeared on Quora: The best answer to any question.*

**Answer by Candid Wueest, IT Security researcher at Symantec, on Quora.**

**Yes SmartTVs can be attacked.** As part of my job as a security response researcher in Symantec, I recently got a chance to experiment on a new generation smart TV to see how well it was secured against attacks. I quickly realized, that after a successful attack, I was looking at an ultimately unusable brand new TV infected with ransomware (a type of malicious software designed to block access to a computer system until a sum of money is paid). Thankfully, there's plenty to be learned from my tinkering.

**How my TV got infected with malicious software.**

The TV I purchased has a pre-installed gaming portal, where you can select and install games. Unfortunately this portal doesn't use encrypted web requests when communicating with the server. This allows an attacker to do what is called a MitM (Man-in-the-Middle) attack. The lack of encryption allows the attacker to modify all the information displayed about the app, including the location of the app, making it easy to trick the user into installing a malicious app. While the user thinks their installing a new racing game, the attacker redirects the request to an identical-looking

Trojanized version. This is just once scenario and there are a few other attack vectors for the cyber criminals to attack the different brands of smart TVs.

Using this MITM attack scenario, I hijacked the installation of a game and downloaded a ransomware malware variant that I knew was capable of infecting mobile devices and started the malicious app on the TV. As expected, the threat worked and locked the TV after a few seconds, displayed the dreaded ransom note on the screen, and made the TV unusable. This particular ransomware displays the ransom note every few seconds, which prevented me from carrying out any meaningful interaction with the TV.

**A happy ending…eventually**

So what can you do if you have ransomware on your smart TV? Sometimes the solution may be as simple as un-installing the malware through the system menu, as our friends at oxid demonstrated. In other cases, cleaning an infected smart TV can be more challenging. Unfortunately, the ransomware version I used was a bit more aggressive and the two-second interaction window that it allows was not long enough to go through the menu to uninstall it. When restarting the TV, there was a 20-second window before the threat started, but again this wasn't long enough to successfully initiate a factory reset or to access the uninstall settings.

I raised my case with the TV manufacturer's online support, but to make matters worse the malware prevented me from starting a remote-support session on the TV. Sadly, they weren't able to help me remove the ransomware from my TV and could only offer me to send my TV back to the factory. Fortunately for me, I had previously enabled the hidden Android ADB debugging option and was able to remove the ransomware through it. Without this option enabled, and if I was a less experienced user, I'd probably still be locked out of my smart TV, making it a large and expensive paper weight.

**What can smartTV owners do to protect themselves?**

Although we've yet to see any widespread malware attacks targeting smart TVs and most of the attacks to date are proof-of-concepts created by security researchers, it doesn't mean attackers won't target these devices in the future. As smart TVs continue to gain in popularity, cybercriminals will eventually start to target them. Smart TV owners should consider the following advice to reduce the risk of possible attacks:

- At purchase and during setup, review the privacy policy and understand the data you are agreeing to share. Many companies share and sell user data to third parties and users need to carefully review these policies and the implications to their privacy.
- Be careful when installing unverified applications from unknown sources
- Enable app verification in the settings when possible
- Modify the privacy and security settings of the device to your needs
- Disable features that are not used, such as the camera or microphone, and consider covering the camera sensor
- Disable or protect remote access to smart TVs when not needed
- Use a strong encryption method, such as WPA2, when setting up Wi-Fi networks

- Use wired connections instead of wireless where possible
  Set up devices on a separate home network when possible, such as a guest account to help isolate the impact of compromised devices
- Be careful when buying used smart TVs, as they could have been compromised or tampered with
- Research the vendor's device security measures and update frequency before making a purchase to see if the vendor provides timely security updates
- Install updates as soon as they become available and, if available, enable automatic updates

*This question* originally appeared on Quora. Ask a question, get a great answer. Learn from experts and access insider knowledge. You can follow Quora on Twitter, Facebook, and Google+.

*More questions:*

- Smart TVs: What is the point of getting a Smart TV if you already have a streaming box?
- Cyber Secruity: How do I hack a cell phone from another cell phone?
- Hacking: What is it like to attend a hackathon?