WikiLeaks Dump Shows CIA Could Turn Smart TVs into Listening Devices

Sam Biddle ⋮ 5-6 minutes ⋮ 3/7/2017

It's difficult to buy a new TV that doesn't come with a suite of (generally mediocre) "smart" software, giving your home theater some of the functions typically found in phones and tablets. But bringing these extra features into your living room means bringing a microphone, too — a fact the CIA is exploiting, according to a new trove of documents released today by WikiLeaks.

According to documents inside the cache, a CIA program named "Weeping Angel" provided the agency's hackers with access to Samsung Smart TVs, allowing a television's built-in voice control microphone to be remotely enabled while keeping the appearance that the TV itself was switched off, called "Fake-Off mode." Although the display would be switched off, and LED indicator lights would be suppressed, the hardware inside the television would continue to operate, unbeknownst to the owner. The method, co-developed with British intelligence, required implanting a given TV with malware—it's unclear if this attack could be executed remotely, but the documentation includes reference to in-person infection via a tainted USB drive. Once the malware was inside the TV, it could relay recorded audio data to a third party (presumably a server controlled by the CIA) through the included network connection.

WikiLeaks said its cache included more than 8,000 documents originating from within the CIA and came via a source, who the group did not identify, who was concerned that the agency's "hacking capabilities exceed its mandated powers," and who wanted to "initiate a public debate" about the proliferation of cyberweapons. WikiLeaks said the documents also showed extensive hacking of smartphones, including Apple's iPhones; a large library of allegedly serious computer attacks that were not reported to tech companies like Apple, Google, and Microsoft; malware from hacker groups and other nation-states, including, WikiLeaks said, Russia, that could be used to hide the agency's involvement in cyberattacks; and the growth of a substantial hacking division within the CIA, known as the Center for Cyber Intelligence, bringing the agency further into the sort of cyberwarfare traditionally practiced by its rival the National Security Agency.

The smart TV breach is just the latest example of a security problem emerging from the so-called "Internet of Things," the increasingly large catalog of consumer products that include (or require) an internet connection for contrived "smart" functionality. Last year, the Guardian reported that Director of National Intelligence James Clapper told the Senate that breaching smart devices was a priority for American spies: "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."

Security and cryptography researcher Kenneth White told The Intercept that smart TVs are "historically a pretty easy target" and "a pretty great attack platform," given that TVs are typically located in a living room or bedroom." White added that "there is zero chance the [CIA has] only targeted Samsung. It's just too easy to mod other embedded OSes" found in the smart TVs sold by every other manufacturer.

This new WikiLeaks dump contains no apparent information about who exactly was targeted by Weeping Angel, or when. It's also unclear how many models of Samsung TVs were vulnerable to Weeping Angel — the CIA documents published by WikiLeaks only mention one model, the F8000 (albeit a very popular and well-reviewed model: Engadget described it as "the best smart TV system you'll find anywhere.") After privacy concerns about Samsung's TV voice recognition feature spread in 2015, the company released an FAQ meant to soothe worried consumers. Addressing the question of "How do I know it's listening or not?," Samsung assured users that "If the TV's voice recognition feature is turned on for a command, an icon of a microphone will appear on the screen," but "if no icon appears on the screen, the voice recognition feature is off."

This assurance about displayed icons is of course worth nothing if the CIA has hijacked the TV. What Samsung seems to have taken for granted was that the company, and its customers, could fully control the operation of its televisions. As the CIA's Fake-Off exploit shows, the company's assurances to consumers that a TV's voice recognition controls would operate in a transparent manner do not hold true once spies and (potentially other hackers) get involved.

Samsung did not immediately return a request for comment. A CIA spokesperson replied "We do not comment on the authenticity or content of purported intelligence documents."

Top photo: On Thursday, Jan. 8, 2015, attendees watch a presentation at the Samsung booth at the International CES, in Las Vegas.