Malware that turns PCs into eavesdropping devices demonstrated

November 22 2016

Credit: George Hodan/Public Domain

Researchers at Ben-Gurion University of the Negev (BGU) have demonstrated malware that can turn computers into perpetual eavesdropping devices, even without a microphone.

In the new paper, "SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit," the researchers explain and demonstrate how most PCs and laptops today are susceptible to this type of attack. Using SPEAKE(a)R, malware that can covertly transform headphones into a pair of microphones, they show how commonly used technology can be exploited.

"The fact that headphones, earphones and speakers are physically built like microphones and that an audio port's role in the PC can be reprogrammed from output to input creates a vulnerability that can be abused by hackers," says Prof. Yuval Elovici, director of the BGU Cyber Security Research Center (CSRC) and member of BGU's Department of Information Systems Engineering.

"This is the reason people like Facebook Chairman and Chief Executive Officer Mark Zuckerberg tape up their mic and webcam," says Mordechai Guri, lead researcher and head of Research and Development at the CSRC. "You might tape the mic, but would be unlikely to tape the headphones or speakers."

A typical computer chassis contains a number of audio jacks, either in the front panel, rear panel or both. Each jack is used either for input (line-in), or for output (line-out). The audio chipsets in modern motherboards and sound cards include an option for changing the function of an audio port with software -a type of audio port programming referred to as jack retasking or jack remapping.

Malware can stealthily reconfigure the headphone jack from a line-out jack to a microphone jack, making the connected headphones function as a pair of recording microphones and turning the computer into an eavesdropping device. This works even when the computer doesn't have a connected microphone, as demonstrated in the SPEAKE(a)R video.

The BGU researchers studied several attack scenarios to evaluate the signal quality of simple off-the-shelf headphones. "We demonstrated is possible to acquire intelligible audio through earphones up to several meters away," said Dr. Yosef Solewicz, an acoustic researcher at the BGU CSRC.

Potential software countermeasures include completely disabling audio hardware, using an HD audio driver to alert users when microphones are being accessed, and developing and enforcing a strict rejacking policy within the industry. Anti-malware and intrusion detection systems could also be developed to monitor and detect unauthorized speaker-to-mic retasking operations and block them.

Provided by American Associates, Ben-Gurion University of the Negev

Citation: Malware that turns PCs into eavesdropping devices demonstrated (2016, November 22) retrieved 18 April 2024 from
https://phys.org/news/2016-11-malware-pcs-eavesdropping-devices.html