AIR HOPPER-HACKING USING FM RADIO SIGNAL

In order to secure sensitive information such as Finance, many companies and government agencies generally use totally secure computer systems by making sure it aren't connected to any network at all. But the most secure systems aren't safe anymore.

Security researchers at the Cyber Security Labs at Ben Gurion University in Israel have found a way to snoop on a personal computer even with no network connection.

STEALING DATA USING RADIO SIGNALS

Researchers have developed a proof-of-concept malware that can infiltrate a closed network to lift data from a machine that has been kept completely isolated from the internet or any Wi-Fi connection by using little more than a mobile phone's FM radio signals.

Researcher Mordechai Guri, along with Professor Yuval Elovici of Ben Gurion University, presented the research on Thursday in the 9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014) held at Denver.

This new technology is known as 'AirHopper' — basically a keylogger app to track what is being typed on the computer or the mobile phone.

AirHopper is a special type of keylogger because it uses radio frequencies to transmit data from a computer, all by exploiting the computer's monitor display, in order to evade air-gap security measures.

"This is the first time that a mobile phone is considered in an attack model as the intended receiver of maliciously crafted radio signals emitted from the screen of the isolated computer," according to a release by Ben Gurion University.

HOW DOES AIRHOPPER WORK ?

The technology works by using the FM radio receiver included in some mobile phones. AirHopper is able to capture keystrokes by intercepting certain radio emissions from the monitor or display unit of the isolated computer.

The researchers can then pick up the FM signals on a nearby smartphone and translate the FM signals into the typed text.

LIMITATIONS

The technique is completely new, although it has some limitations. The team claims that textual and binary information can be gathered from a distance of up to 7 meters with an effective FM-bandwidth of 13-60 bps (bytes per second).

"AirHopper demonstrates how textual and binary data can be exfiltrated from physically a (sic) isolated computer to mobile phones at a distance of 1-7 meters, with effective bandwidth of 13-60 (bytes per second). Enough to steal a secret password."

This, according to researchers, is enough to steal a secret password. Therefore, in an effort to obtain secret data an attacker can infect a mobile phone of someone from the staff using AirHopper method worked in stealth mode, and then transmit the data.

VIDEO DEMONSTRATION AND POTENTIAL DANGER

Researchers have also provide the Proof-of-concept video, so you can Watch the demonstration video and find out if you should be worried or not.

According to the researchers, the Airhopper technique of data theft was developed by the University in order to protect against potential intrusions of its kind in the future.

"Such technique can be used potentially by people and organizations with malicious intentions and we want to start a discussion on how to mitigate this newly presented risk." said Dudu Mimran, chief technology officer of the Ben Gurion University’s cyber security labs.