Are air gaps entirely impermeable? Then you don't know Ben-Gurion team's research

February 11 2018, by Nancy Owano

We read many stories about security sleuths who discover how thieves and mischief-makers break into accounts and networks to plant bad stuff and steal personal data.

Here is an important twist: Mordechai Guri, director of the Cybersecurity Research Center at Ben-Gurion University, focuses on

what *Wired* called exfiltration: How information is pulled out once attackers got in.

Boing Boing: "Guri's research began after he observed that while there was a lot of security research devoted to theoretical ways to get data into a computer that has been airgapped, no one was thinking about exfiltration (getting the data out)."

But wait. What is all this about air gaps? *Boing Boing*'s Cory Doctorow: "Computers that are isolated from the internet and local networks are said to be 'airgapped,' and it's considered a best practice for securing extremely sensitive systems.

Guri and his team have important wake-up calls.

"Guri has uniquely fixated his career on defeating air gaps by using so-called 'covert channels,' stealthy methods of transmitting data in ways that most security models don't account for," Andy Greenberg wrote in *Wired*.

His work is a challenge to the assumption that there is what he referred to as "a hermetic seal around air-gapped networks." *Wired* said, "Guri's research, in fact, has focused almost exclusively on siphoning data out of those supposedly sealed environments." His approach involves "the accidental and little-noticed emissions of a computer's components—everything from light to sound to heat."

As shown in videos and discussed in two papers, the team pulled data off a computer protected by an air gap and a Faraday cage designed to block all radio signals.

Guri's technique communicates with strong magnetic forces that can penetrate even those Faraday barriers, said Greenberg.

A Faraday room is a metal shielded room that blocks radio signals. Their ODINI video showed the message jumped the air-gap and escaped the Faraday room.

That jump and escape appeared to be a core bit of news for Catalin Cimpanu, security news editor for *Bleeping Computer*, that the research revealed "that an attacker can steal data from air-gapped devices protected by Faraday cages."

Cimpanu described the cages as "metallic enclosures meant to block electromagnetic fields coming in or going out." He noted they are often used "to isolate sensitive devices from outside networks."

Technique? There are MAGNETO and ODINI techniques. A magnetic field passes through walls, humans, other objects, and Faraday cages, said *Bleeping Computer*.

The title of one paper they wrote to discuss their work is "MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields."

The authors discussed how attackers can leak data from isolated, air-gapped computers to nearby smartphones via covert magnetic signals.

Greenberg said it was about "coordinating operations on a computer's processor cores to create certain frequencies of electrical signals." The result is malware that can "electrically generate a pattern of magnetic forces powerful enough to carry a small stream of information to nearby devices."

Meanwhile, the authors said three different approaches can be put to use if one wants to prevent attackers from establishing the magnetic covert channel: shielding, jamming, and zoning.

The team built an Android app, ODINI, to catch signals using a phone's magnetometer, said Greenberg, the magnetic sensor that enables its compass and remains active even when the phone is in airplane mode.

The title of their paper is "ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields."

This is where the authors discussed how attackers, if seeking to leak data from secure computers, can bypass Faraday cages and air-gaps. "Our method is based on an exploitation of the magnetic field generated by the computer's CPU."

To detect and prevent this threat, the authors proposes types of defensive countermeasures.

Greenberg said Guri's focus makes him "something like an information escape artist."

Eran Tromer, a research scientist at Columbia, was quoted in *Wired*, about "answering this question of whether you can form an effective air gap to prevent intentional exfiltration, they've made a resounding case for the negative."

Cimpanu weighed in: Both attacks can be thwarted in their early phases. He said they can be thwarted by proper network hygiene and good security practices.

More information: — Air-Gap Research Page: cyber.bgu.ac.il/advanced-cyber/airgap

— ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields: cyber.bgu.ac.il/advanced-cyber … em/files/ODINI_1.pdf

— MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPUGenerated Magnetic Fields: cyber.bgu.ac.il/advanced-cyber … /files/MAGNETO_0.pdf

© 2018 Tech Xplore

Citation: Are air gaps entirely impermeable? Then you don't know Ben-Gurion team's research (2018, February 11) retrieved 2 May 2024 from https://techxplore.com/news/2018-02-air-gaps-impermeable-dont-ben-gurion.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.