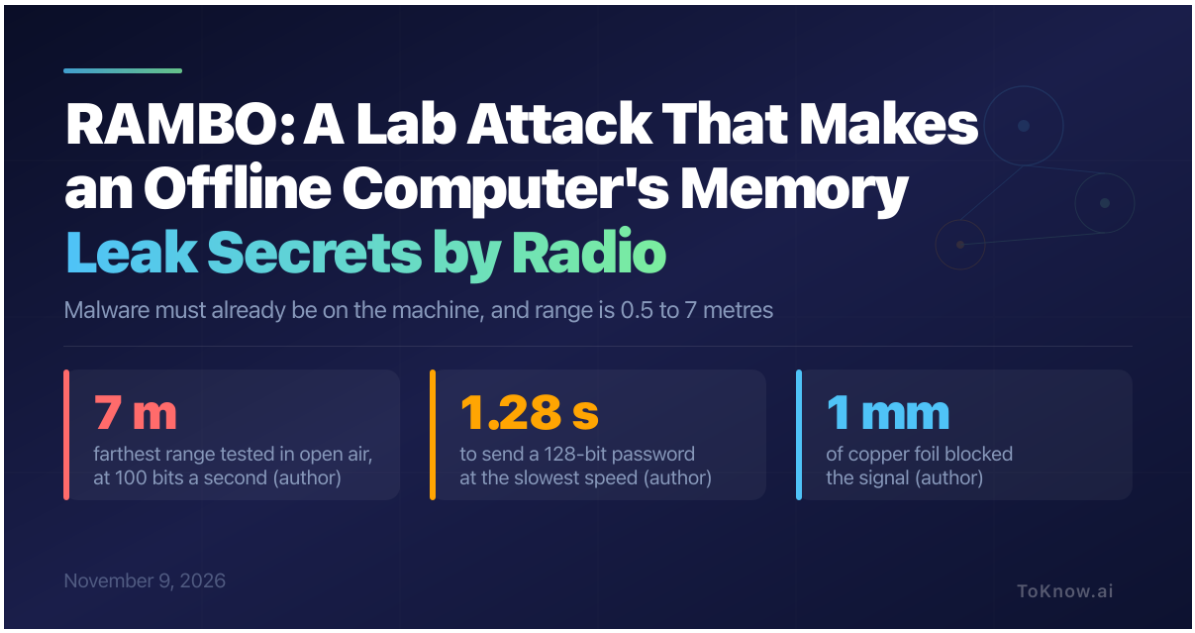
RAMBO: A Lab Attack That Makes an Offline Computer's Memory Leak Secrets by Radio

Kabui, Charles

2026-11-09

Read at ToKnow.ai



RAMBO is a lab attack on air-gapped computers, the machines that organisations keep off every network to protect sensitive data. If malware is already on such a machine, it can make the memory chips give off radio signals that carry data, and a radio receiver nearby decodes them. Mordechai Guri of Ben-Gurion University in Israel published it at the NordSec security conference in 2023, and it reached the free arXiv archive in September 2024. In the paper, a

128-bit password (about 16 characters) takes 1.28 seconds to send at the slowest setting and 0.128 seconds at the fastest, 1,000 bits a second.

The tests used open air, 0.5 to 7 metres from the computer. Range falls as speed rises: 7 metres at 100 bits a second, 3 metres at 1,000. Malware must already be on the machine, for example from an infected USB drive. At the top speed a 1 MB file would take about 2.2 hours, BleepingComputer reports, so the channel suits keystrokes, passwords, encryption keys and small images.

The paper's defences include a metal shield around the computer (it says 1 mm of copper foil blocked the signal) and keeping radio receivers several metres away. In October 2026 a different research team posted SPECTER, which sends bits by changing a USB port's power settings once malware has administrator rights. A phone's charging state or a USB mouse's behaviour shows the pattern, at 0.2 to 1 bit a second.

Read More: A browser tool that moves files between two devices with no network, using flashing QR codes and SPECTER, a lab attack that leaks secrets from an offline computer by flipping USB power settings

Sources:

- RAMBO: Leaking Secrets from Air-Gap Computers by Spelling Covert Radio Signals from Computer RAM (arXiv)
- RAMBO, NordSec 2023 conference paper (Springer)
- New RAMBO attack steals data using RAM in air-gapped computers (BleepingComputer)
- Researchers snoop data from air-gapped PC's RAM sticks by monitoring EM radiation from 23 feet away (Tom's Hardware)
- SPECTER: Covert Data Exfiltration from Air-Gapped Systems via USB Power Modulation (arXiv)

Disclaimer: *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*