Exfiltrating an isolated (Air-Gapped) Computer System

#2722, Cybersecurity (CYB) , Systems Software, Senior Division

PROBLEM STATEMENT

- Third year into COVID-19 pandemic, our dependence on network connectivity, data and systems only continue to increase exponentially!
- Also on the rise is the CYBER ATTACKS and RANSOMWARE threats.
  || COLONIAL PIPELINE ATTACK || NASA SYSTEMS ATTACK ||
  10X increase in cyber attacks!
- Gold standard in protection is to isolate the computer from any network connection, called AIR-GAP.
- **Just by removing connectivity are we safe?**
- **Can one break into such an air-tight system?**
- How to fix those gaps and better protect ourselves?

Ref: Mission Impossible - lylesmoviefiles.com

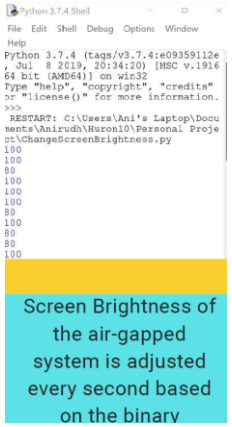
METHODOLOGY

1. Removed network and connectivity from a computer (simulated an airgap)
2. Without a connectivity, used the other means to get into the computer
   a. Sound (from speaker, mouse clicks)
   b. Magnetic waves (from Hard drive)
   c. **Light (from Monitor Screen brightness) - *Effective since it is vendor independent. Cameras can capture this easily.***
3. Wrote a Python program to convert a sample datafile from the hard drive of the air-gapped computer to binary.
4. Transmitted that binary file as fluctuations of the screen brightness.
5. Captured the fluctuations in monitor brightness remotely as a luminosity time-series data.
6. Wrote code to decode the data to binary and then into normal text.

RESULTS

Successfully exfiltrated data from the Air-gapped computer system, using the fluctuations in the brightness of the monitor.

The secured file in the air gapped computer contains "SecretKey", which is promptly converted to binary



Screen Brightness of the air-gapped system is adjusted every second based on the binary

Phyphox Sensor Captures the modulations

The data is intepreted back as binary and converted to "SecretKey" on the hacker's own computer

PREVENTION, PROTECTION and FUTURE OPPORTUNITIES

PREVENTION: This specific gap in security can be prevented by:

a. Encrypt data/ files even in a secure environment.
b. Multi-Factor Authentication for secure files not just the computer system or network.

PROTECTION: SECURITY has to be BUILT-IN and cannot be an after thought through BOLT-ON applications.

FUTURE research: Due to higher transmission range, **magnetic waves** from disk drives and RAM's of the computers can be used to transmit data.
With **Quantum** computing and **magnetic spintronic** devices on the rise, using magnetic wave as a transmitter can be leveraged as a competitive advantage!