UFO Hacker

Joseph Kaufman

NASA, Navy, Army, and Pentagon Security Issues

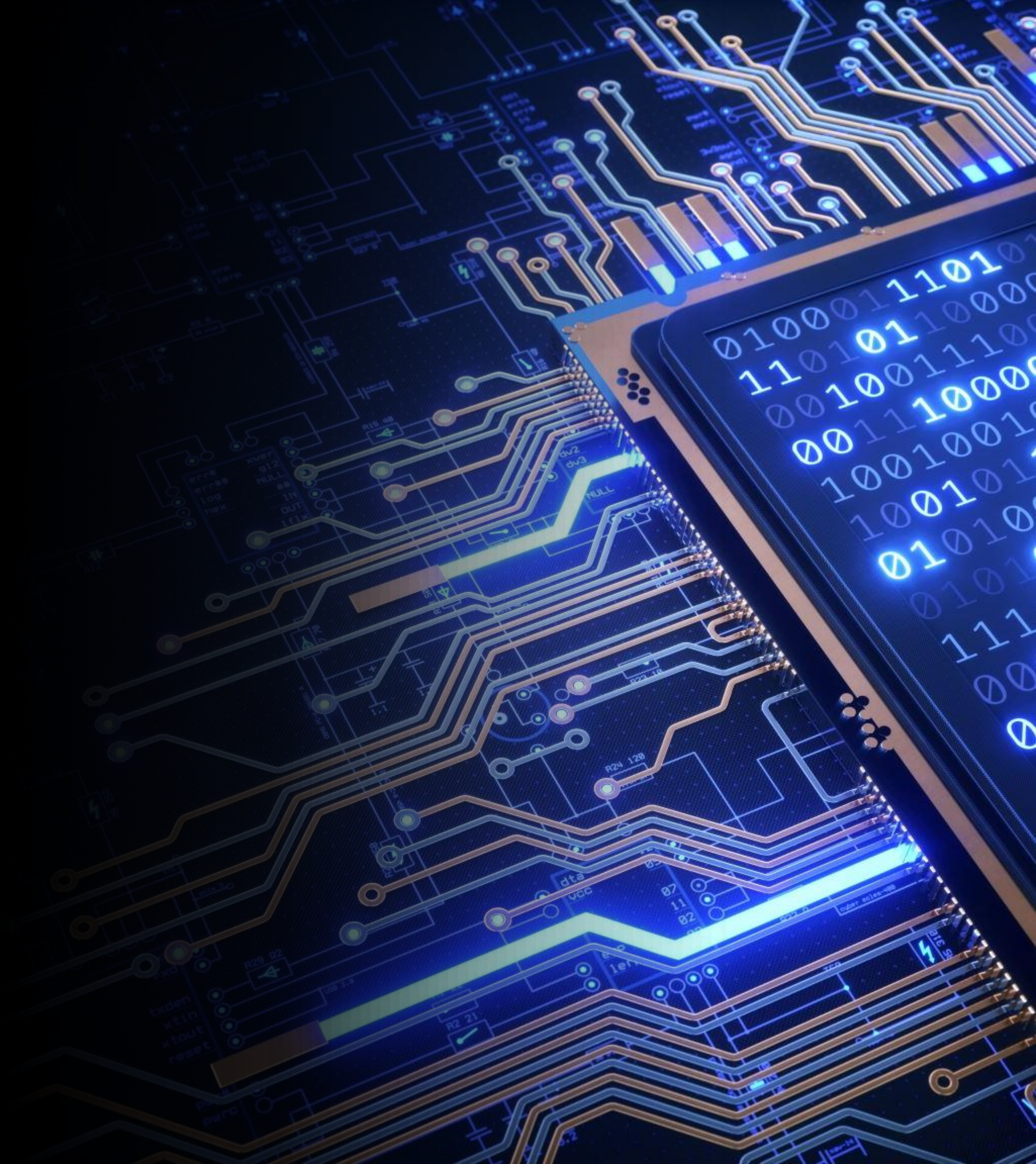
- From the late 90s to early 2000s known to Run Windows (and probably still do)
- Vulnerabilities:
  - Windows Office Protocol (Phishing) and NetBIOS (IP Scanning)
- Weak or lack of passwords on computers
- Human engineering issues
- General lack of security

McKinnon Background

- UK High School dropout and self-taught computer systems administrator
- Had an obsession with UFOs
- Hacked into various US government institutions from February 2001 to March 2002
- Later diagnosed with Autism

Technically what happened?

- February of 2001 hacks begin until 2002
- NetBIOS allows McKinnon to access government computers from UK
- Windows Office Protocol allows McKinnon to run Pearl scripts to scan for passwords
- Weak passwords
  - McKinnon is in!



Remotely Anywhere

LogMeIn RemotelyAnywhere User Guide

April 2007

ight © 2007 LogMeIn, Inc. All rights reserved

Once In

- McKinnon downloads virtual access software RemotelyAnyhwere
  - Enabled deleting and transferring files
- Searches NASA, Navy, Army, and Pentagon for UFOs
- Worker discovers him
  - Talks his way out
- McKinnon downloads various images of UFOs and confidential documents

McKinnnon Caught

- March 2002
- McKinnon left multiple messages on government websites and RemotelyAnywhere led to his discovery
- US seeks to extradite him because…

What damage did it cause?

- Damages to Naval Air Station and Earle Naval Weapons Station after 9/11 causing 300 computers to crash
  - Suspected of causing $800,000 in damages
- Resulted in a lack of trust in US government security systems
- Unknown damages to operations of military

How could it be prevented?

- Stronger firewalls
  - Prevent installation of suspicious software
  - Security against Windows NetBIOS and Office Protocol
  - Very limited access or no access for remote users
- Increased cybersecurity funding
  - Education against human engineering
  - Stronger passwords for users

Sources

- https://www.bbc.com/news/uk-19946902
- https://www.sciencedirect.com/topics/computer-science/vulnerability-window
- https://beyondsecurity.com/scan-pentest-network-vulnerabilities-windows-host-netbios-information-retrieval.html
- https://www.blackhatethicalhacking.com/articles/free-access/hacking-stories-gary-mckinnon-and-the-biggest-military-computer-hack-of-all-time/