Level 0x03

Hacker Stories

Topics

- Phreakers
- Hats
- Profiles
- Careers

Upcoming CTFs

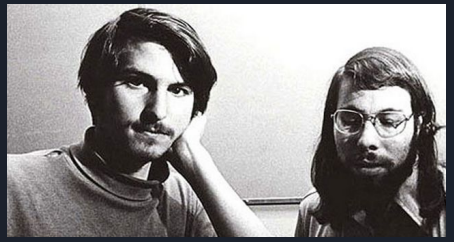
- Cyber Security Rumble CTF (Germany)
  - Open to students and beginners
  - Sat Oct 8th, 1PM - Sun Oct 9th 1PM
  - https://cybersecurityrumble.de
- REPLY Cyber Security Challenge (Italy)
  - Students and Professionals
  - Fri Oct 14th, 1:30PM - Sat Oct 15th 1:30PM
  - https://challenges.reply.com/tamtamy/challenges/category/cybersecurity

Phone Phreakers

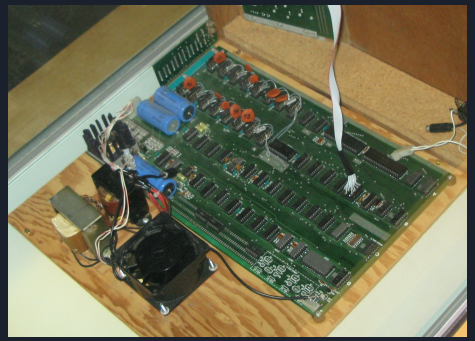
- Discover 2600 Hz tone triggers phone call termination, but leaves the line up
  - Discovered in 1957. Allows for free long distance calling
  - Joe Engressia (Joybubbles) - blind 7yr old boy. Discovers whistling in phone ends calls.
  - John Draper (Capt. Crunch) - discovers cereal toy makes a great 2600 Hz tone
- Gets featured in Esquire magazine “Secrets of the Blue Box”
  - 1954 Bell System Technical Journal publishes complete list of methods and freqs for call signaling
  - AT&T captures first blue box in 1962

Phone Phreaking Demo

The 2 Steves



- Steve Wozniak reads Esquire article, finds Capt Crunch
  - Builds more blue boxes with his other prankster friend Steve Jobs
  - Gets Draper busted (4 months federal prison, 5 yrs probation for wire fraud)
- Homebrew Computer Club
  - Woz builds Apple I computer to show off to the club (no display, no keyboard)
  - Steve Jobs helps him market / sell it as Apple I in 1976 (they sell ~200)
  - In 1977, they create and sell Apple II (the series sells 5-6 million till 1993)



1 MHz
$25

6502 Club

Atari VCS (77)
30 million sold

Commodore 64 (82)
17 million sold

Atari 400/800 (79)
4 million sold

Apple II Series (77)
6 million sold

Atari Lynx (89)
2 million sold

BBC Micro (81)
2 million sold

Nintendo NES (85)
61 million sold

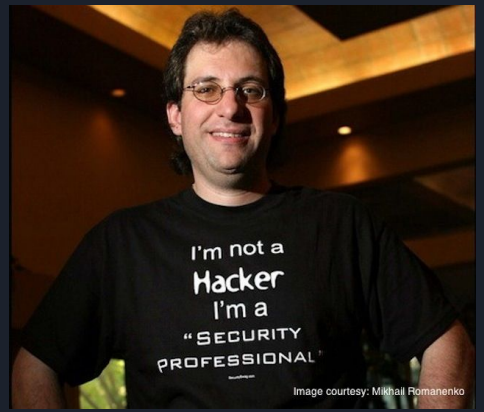
Super Nintendo (90)
49 million sold

Types of Hackers / Security Researchers

- White Hat - Ethical Hackers
  - Hired by companies / bug bounties
  - Have explicit permission to access computer systems
  - Find and secure weaknesses before others find them
- Grey Hat
  - Gain access to systems without permission
  - Motivated for fun, LOLZ, cred, or financial
  - May even report and disclose vulnerabilities to owners
  - Generally not stealing or damaging systems
- Black Hat
  - Use vulnerabilities / social engineering to gain access to system without permission
  - Steal data, financial info, and passwords
  - Destroy, encrypt, or ransom information systems
  - Botnets / DDOS

FBI Most Wanted Cyber Criminal

- Kevin Mitnick (aka Condor)
  - Gray Hat - Hacked into a lot of systems, but didn't cause much / any damage
  - Gained access to DoD computer at 16 years old
  - Social Engineering
    - Convinced bus driver to give him card punch machine / free bus rides
    - Convinced Motorola employees to give source code for new phone to him
  - Angered a fellow hacker (Tsutomu Shimomura), which led to his downfall
  - 5 ½ years in prison
  - 8 months solitary, Feds feared he could launch nuclear missiles by whistling into a phone
  - Now well regarded author and security consultant



Aaron Swartz - Hactivist

- Involved in the development of
  - Web feed format Really Simple Syndication (RSS)
  - Markdown publishing format
  - Creative Commons organization
  - Reddit
- Downloaded 2.7 million documents from PACER (Public Access to Court Electronic Records)
  - FBI doesn't charge him, because documents were public access
- JSTOR incident (2011)
  - Used his student account / credentials to download thousands of academic journals
  - JSTOR / MIT catch Aaron. He gets arrested January
  - Reach a settlement with JSTOR, and Aaron surrenders documents in June
  - Federal Grand Jury charges him with felony wire fraud and computer fraud and abuse
    - Max charges of 1 million dollars, and 35 years prison
    - Feds propose plea bargain for 6 mons in federal prison
- Takes his own life

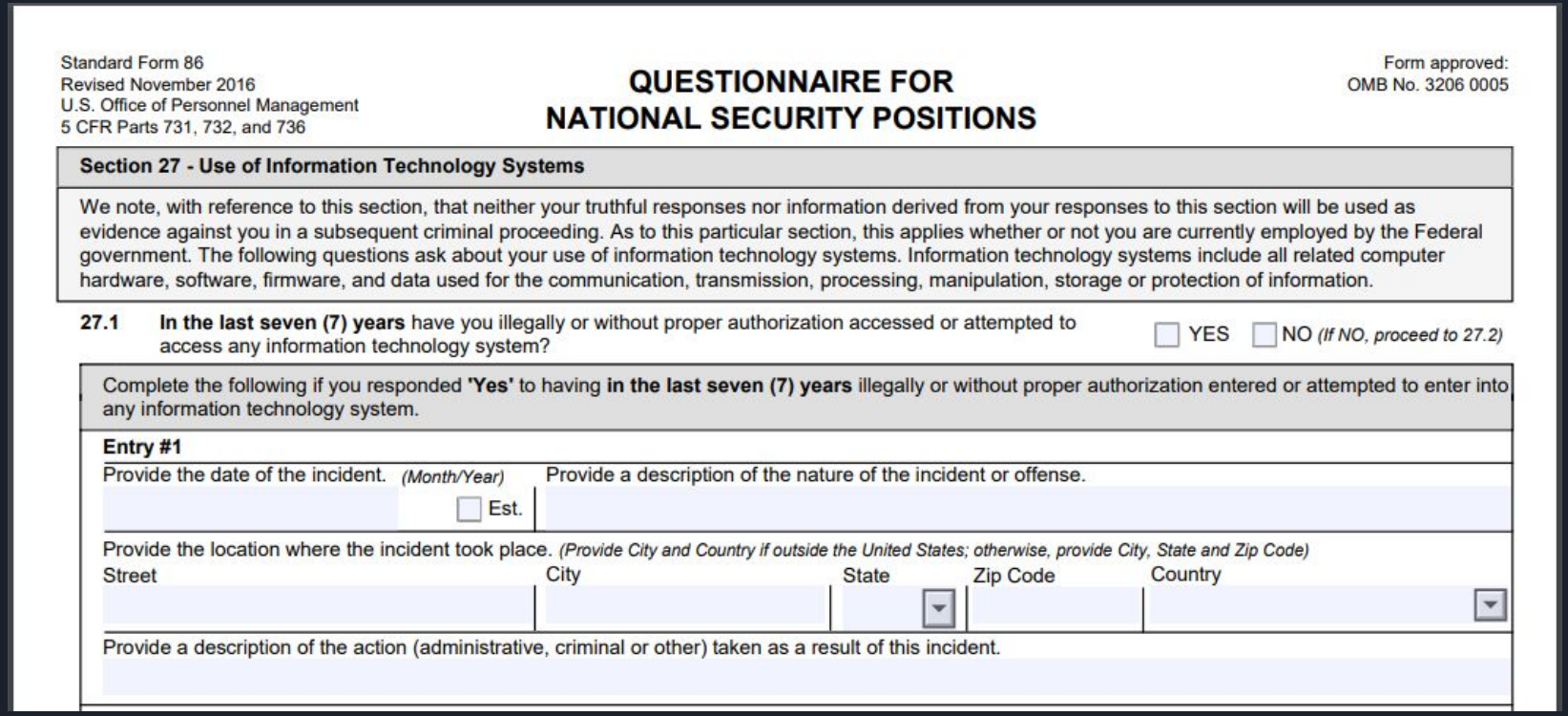
Marcus Hutchins
a.k.a. MalwareTech

- Malware security researcher in England
- At age 21, creates a blog about his security research of Malware / botnets: malwaretech.com (2015)
- Gets noticed by company Kryptos Logic in LA, they hire him for over $100K salary
  - Writing custom tools to track malware infections
  - Research botnets (Necurs, Dridex, Emotet - millions of infected computers)
  - Tracked down Mirai DDOS botnet controller, and convinced him to stop
  - Activates WannaCry killswitch domain (infected 300,000+ PCs, damage est $100+ billion)
- Attends DEFCON in Las Vegas, gets arrested at airport on way home (2017)
  - From age 15-20, Marcus had been writing botnets, keyloggers, and other malicious tools for cyber criminals and selling them on hacker forums to pay for drugs
  - Faced $250K fine and 5 years in prison for 2 charges of wire fraud
- Sentenced to time served and 1 year probation in 2019

Hack the Planet! sorta...

- Hack for the government
  - Intelligence communities
  - Join Cyber units of any military branch
  - DoD research labs
- Gov't contractors
- Pentesters
  - Software / networking
  - Physical security
- Bug Bounties
- Any Large companies with hacking risks (ALL)
  - Defenders
  - Internal attackers / auditors

SF-86 Easy Mode



Standard Form 86
Revised November 2016
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

Section 27 - Use of Information Technology Systems

We note, with reference to this section, that neither your truthful responses nor information derived from your responses to this section will be used as evidence against you in a subsequent criminal proceeding. As to this particular section, this applies whether or not you are currently employed by the Federal government. The following questions ask about your use of information technology systems. Information technology systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage or protection of information.

27.1 **In the last seven (7) years** have you illegally or without proper authorization accessed or attempted to access any information technology system? ☐ YES ☐ NO *(If NO, proceed to 27.2)*

Complete the following if you responded **'Yes'** to having **in the last seven (7) years** illegally or without proper authorization entered or attempted to enter into any information technology system.

Entry #1

Provide the date of the incident. *(Month/Year)* ☐ Est.

Provide a description of the nature of the incident or offense.

Provide the location where the incident took place. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)*

Street | City | State | Zip Code | Country

Provide a description of the action (administrative, criminal or other) taken as a result of this incident.

Links

- https://en.wikipedia.org/wiki/Phreaking
- https://en.wikipedia.org/wiki/John_Draper
- https://www.dailydot.com/layer8/john-draper-captain-crunch/
- https://cyberexperts.com/kevin-mitnick-the-most-infamous-hacker-of-all-time/
- www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet
- https://www.vice.com/en/article/ywp8k5/researcher-who-stopped-wannacry-ransomware-detained-in-us-after-def-con