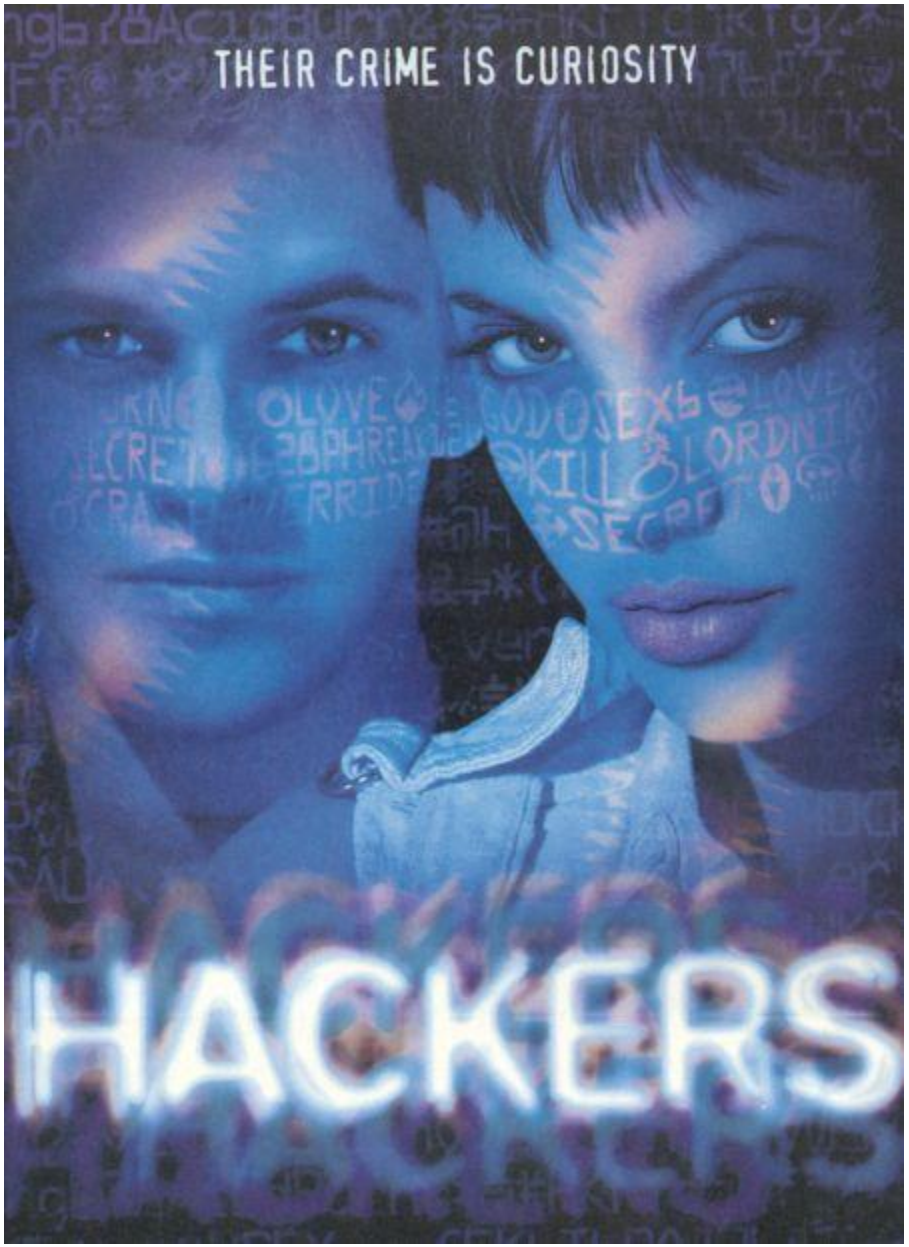
Historie hackingu ve světovém kontextu

Tomáš Vobruba, AEC



AEC
DATA SECURITY
COMPANY

Slavní hackeři

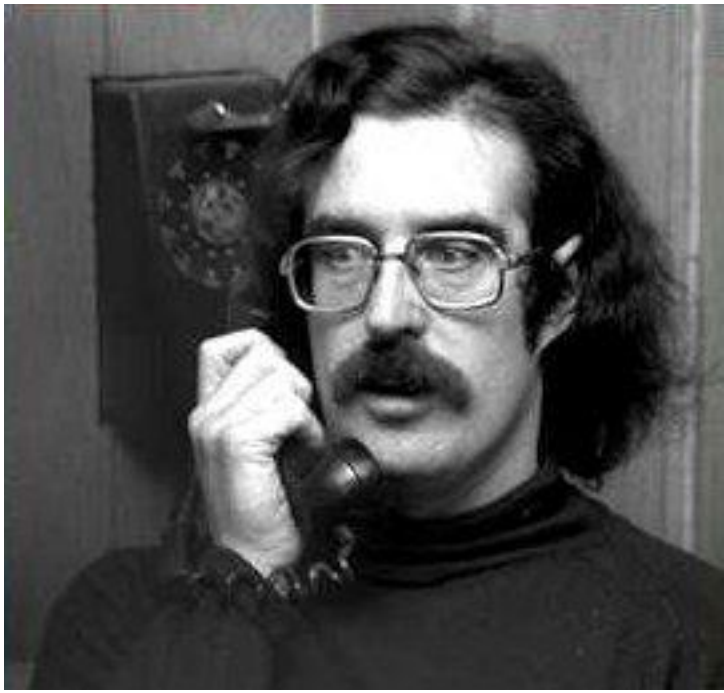
Kevin Mitnick

Nepochybně nejznámější a nejvíce nadaný hacker historie vůbec. Vybudoval si svoji pověst v roce 1981 kdy v pouhých 17letech vlámáním se do telefonní ústředny, která mu umožnila přesměrovat jakýkoliv telefonní hovor kamkoliv chtěl.

Kevin Poulsen

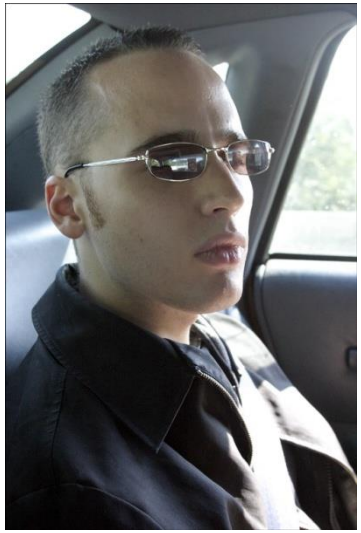
Současný vedoucí časopisu Wired, který je spíše známý přes své úplně jiné aktivity. V roce 1983, ve svých pouhých 17letech, provedl své první vlámání do cizích sítí, které měli za výsledek, problémy se systémem US.. Pokračoval v ilegálních aktivitách až do doby, než byl zatčen FBI v roce 1991. V roce 1994 byl odsouzen k pobytu ve vězení.

Slavní Hackeři



John Draper

Lépe známý jako „Cap'n Crunch". Byl to vůbec jeden z prvních hackerů v historii. Tato přezdívka vzešla z cereálií se stejným názvem uvnitř kterých jednou objevil hračku – píšťalku.



Adrian Lamo

Lamo se zcela jistě stal největší noční můrou síťových administrátorů. Od Microsoftu přes Sun, MacDonald's, Cingular, AOL, New York Times až po Yahoo. Provedl snad všechny možné a známe typy průniků do korporátních sítí. Obešel veškeré bezpečnostní procesy a ochrany s jednoduchostí a grácií.

Phreaking, První krůčky

John Draper

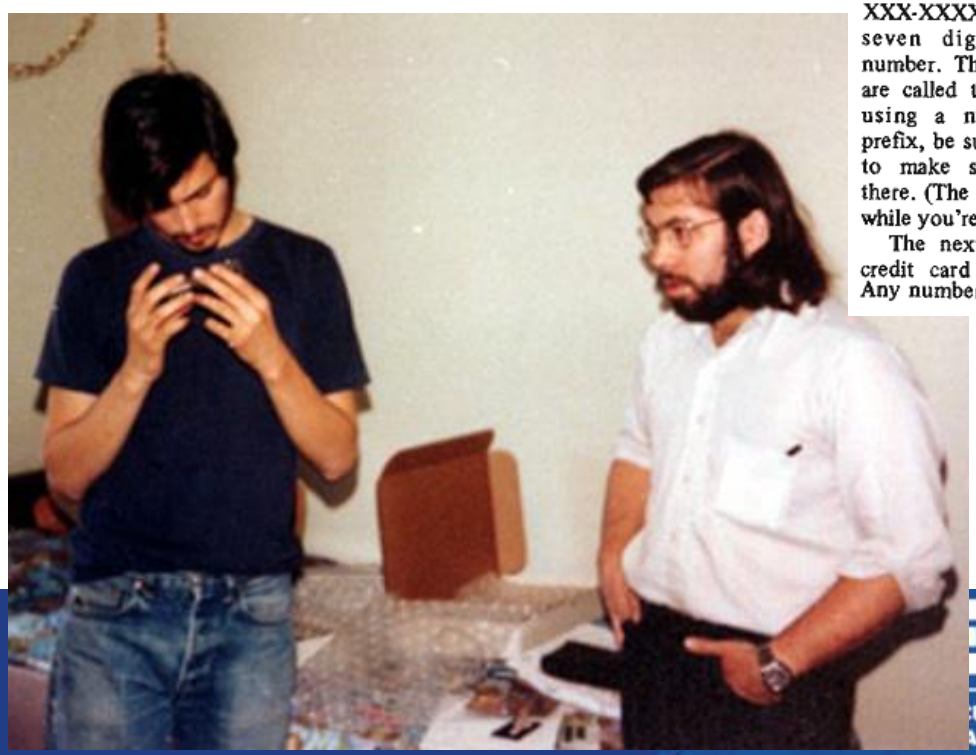
Jak již bylo řečeno. Draper získal svoji slávu a stal se jedním z prvních hackerů tím, že využil dětské hračky. To se stalo mnohem dříve, než existoval hacking ve smyslu hackování sítí nebo počítačových systémů.

Magická píšťalka

Ke konci 60. let 20. století, po objevení píšťalky uvnitř krabice s cereáliemi Cap'n Crunch začal provádět první pokusy s exploitováním telefonních sítí. Uvědomil si totiž, že píšťalka je schopná vydávat tón o 2600 Hz.

Blue Box, Phreaking pro každého

Steve Wozniak a **Steve Jobs** (zakladatelé Apple) dotáhli Draperovu techniku do konce a vytvořili přístroj zvaný BlueBox. Zařízení bylo schopno vytvářet zvuky na frekvencích nutných ke zmatení telefonních systémů.



Bell phone formula cracked

NEW YORK (LNS) – Self-styled "people's operators have leaked the alleged credit card formulas for 1972. They claim that the following numbers and letters correspond with each other:

1–Z 2–J 3–Q 4–S 5–D 6–H 7–U 8–M 9–A 0–X. These code numbers are now matched with the fourth digit of the telephone number, not with the sixth digit. Other than that the procedure is the same as last year.

A credit card consists of eleven digits and looks like this: XXX-XXXX YYY A. The first seven digits are a telephone number. The first three numbers are called the prefix. If you are using a number with a local prefix, be sure to call the number to make sure no one answers there. (The operator may check it while you're calling).

The next three digits of the credit card are called the RAO. Any number from 001-599 can be used. These RAO's stand for cities, so if you are using a number with a local prefix you have the correct RAO. IF an operator says, "What city are you calling from?" and looks up the RAO, hang up and try again from another phone. (Some RAO's are: 157–Berkeley-Oakland, 158–San Francisco, 072-074-021–New York, 035–Atlanta, 032–Washington D.C., 105–New Mexico.)

The last digit of the credit card is the letter that matches the fourth number of the phone number. 834-1656 087 Z is an example of a 1972 credit card formula.

The operators handle real credit card calls all day, and can tell if you are nervous. Don't hesitate, read your number like it's memorized and have all information handy. Say it fast. 834-1656 087 Z w... In the daytime op... busy to check u... night, they may. You don't have to say who the call is being billed to or the number you are calling from.

In any case, keep your phone calls brief, use a public phone and don't use the same booth twice.

Únosy linek: Mitnick na scéně

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (N3C/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex:.....MALE
Race:.....WHITE
Place of Birth:.....VAN NUYS, CALIFORNIA
Date(s) of Birth:.....08/06/63; 10/18/70
Height:.....5'11"
Weight:.....190
Eyes:.....BLUE
Hair:.....BROWN
Skintone:.....LIGHT
Scars, Marks, Tattoos:.....NONE KNOWN
Social Security Number (s):.....550-39-5695
NCIC Fingerprint Classification:...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132 (Rev. 3/2/92)

November 1992

PACIFIC BELL
A Pacific Telesis Company

Stejně jako jeho předchůdci, začal Mitnick s hackingem tím, že modifikoval telefonní linky v jeho okolí. V roce 1981, 17letý Kevin a jeho kamarád se vlámali do ústředny COSMOS (Computer System for Mainframe OperationS), která patřila společnosti Pacific Bell v Los Angeles.

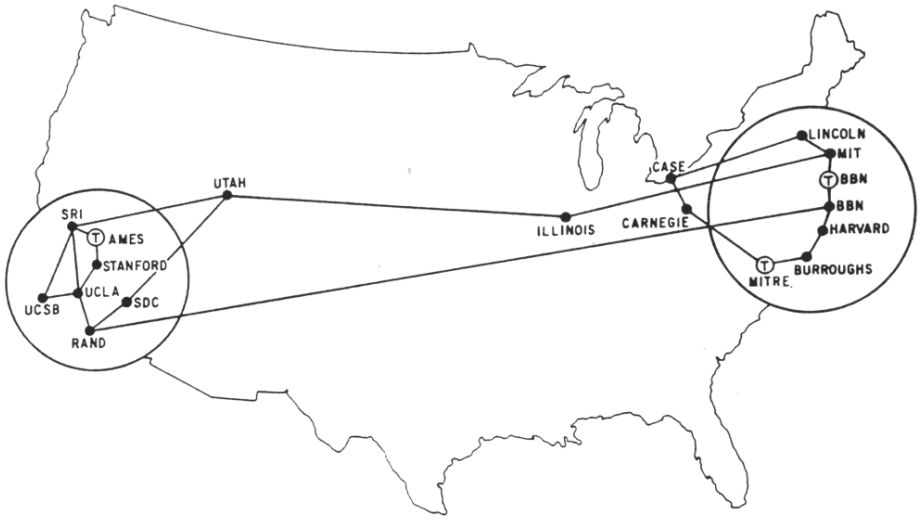
Jakmile byly uvnitř systému, přesměrovali všechny linky a zachycené hovory směrované přes tuto ústřednu.

Kevin Mitnick a Pentagon

TSR-80, Zilog 1.77MHz

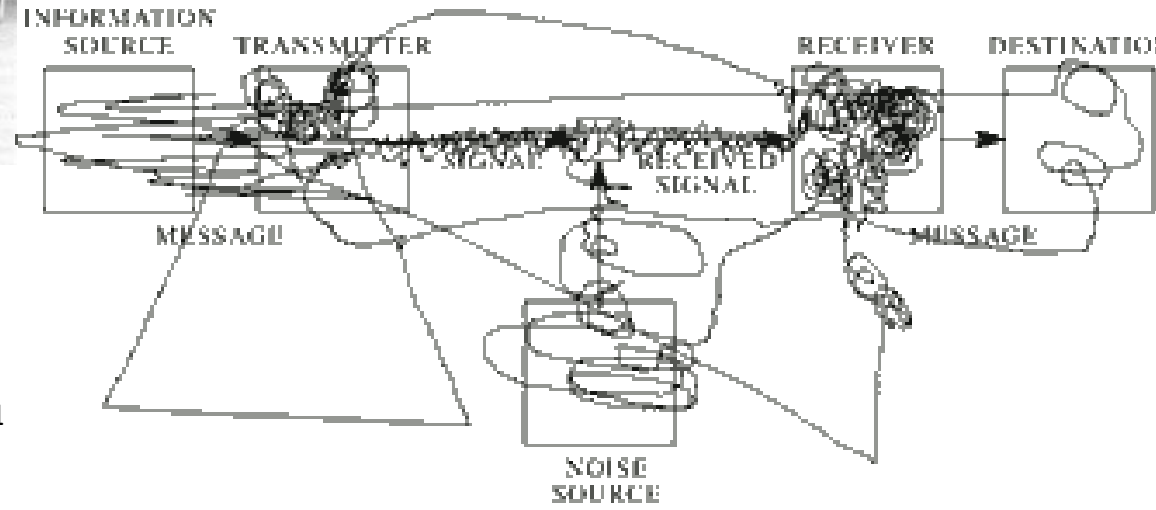
V roce 1983 Kevin Mitnick dosáhl svého největšího úspěchu.

Získal přístup do vládní vojenské sítě Arpanet (předchůdce dnešního Internetu). Tato síť byla sdílená pouze vládou, armádou, velkými korporacemi a univerzitami.



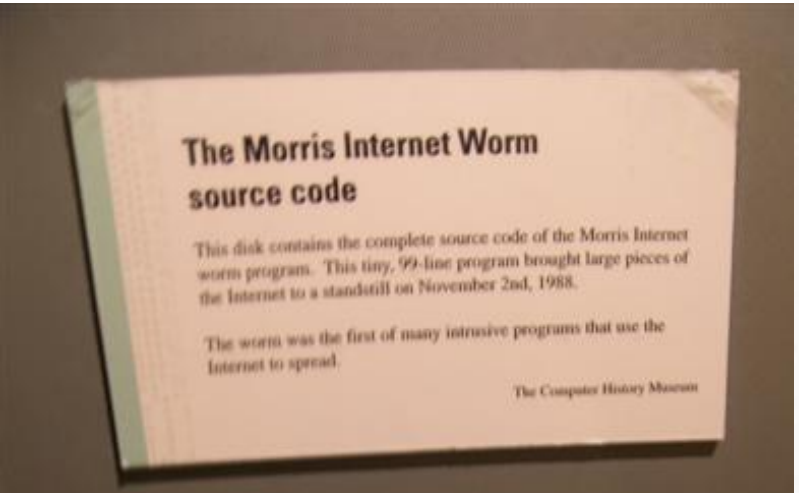
Objev zmatečné a náhodné komunikace

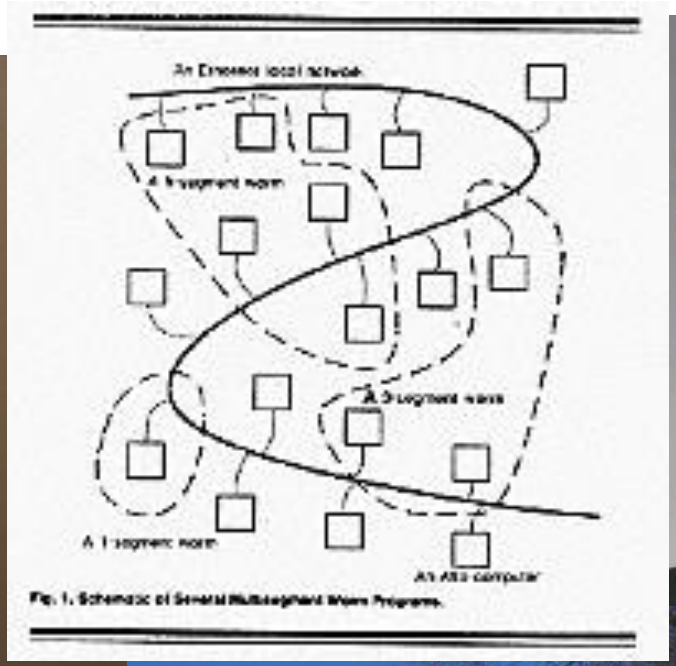
- Kamarádova zrada dostala Mitnicka do vězení

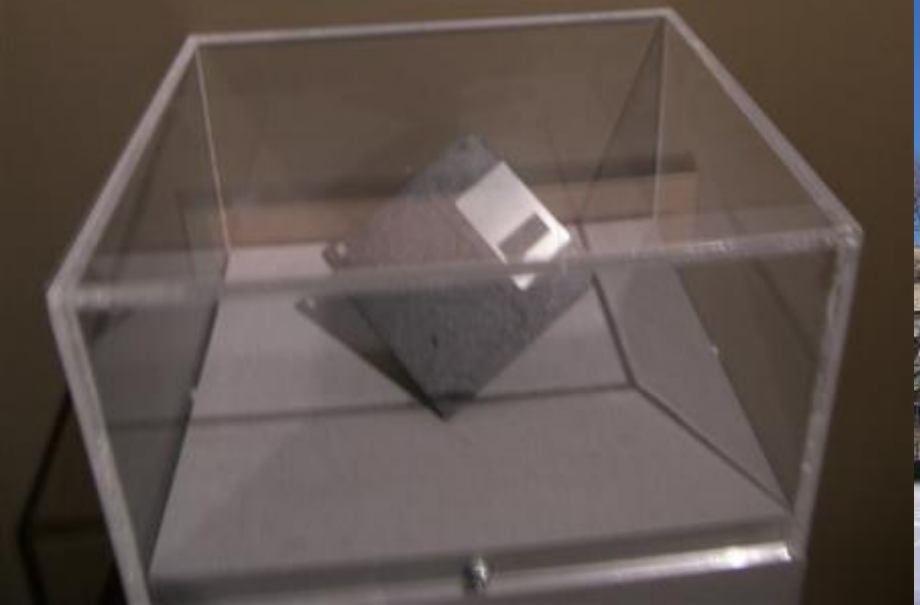


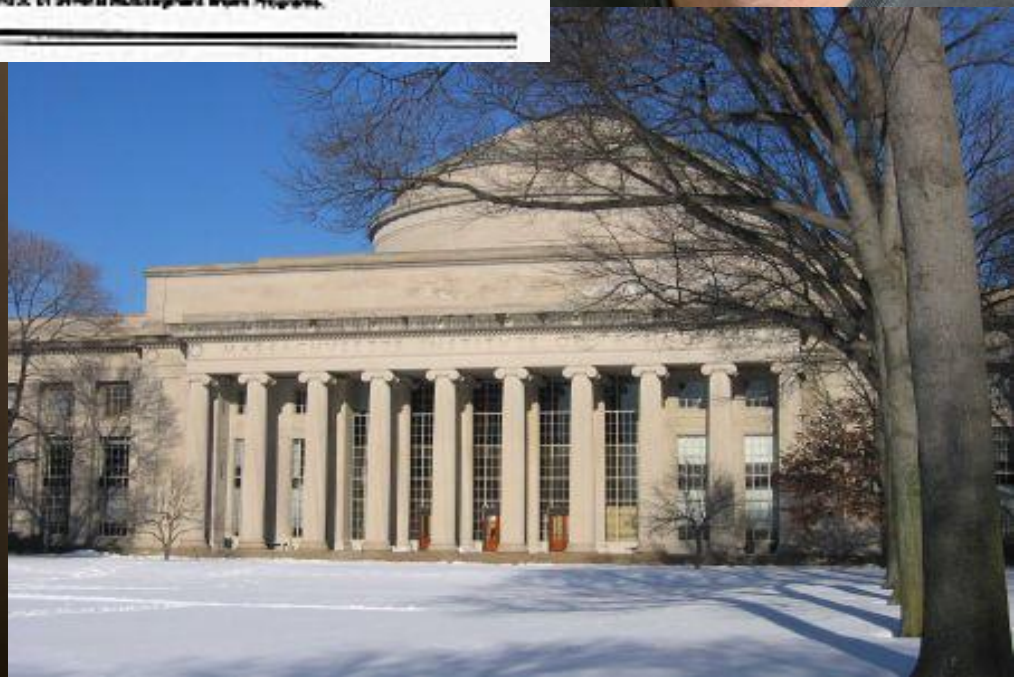
- Krádež zdrojových kódu operačního systému
- Zmatení útočníkem ke skrytí stop

Vytvoření prvního síťového červa

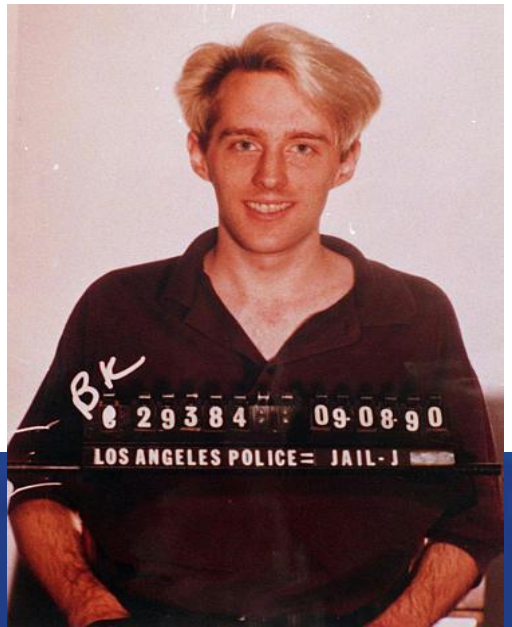






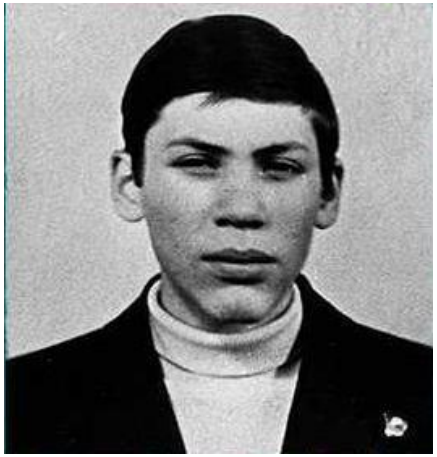


Hacking, FBI, útěk a Porsche



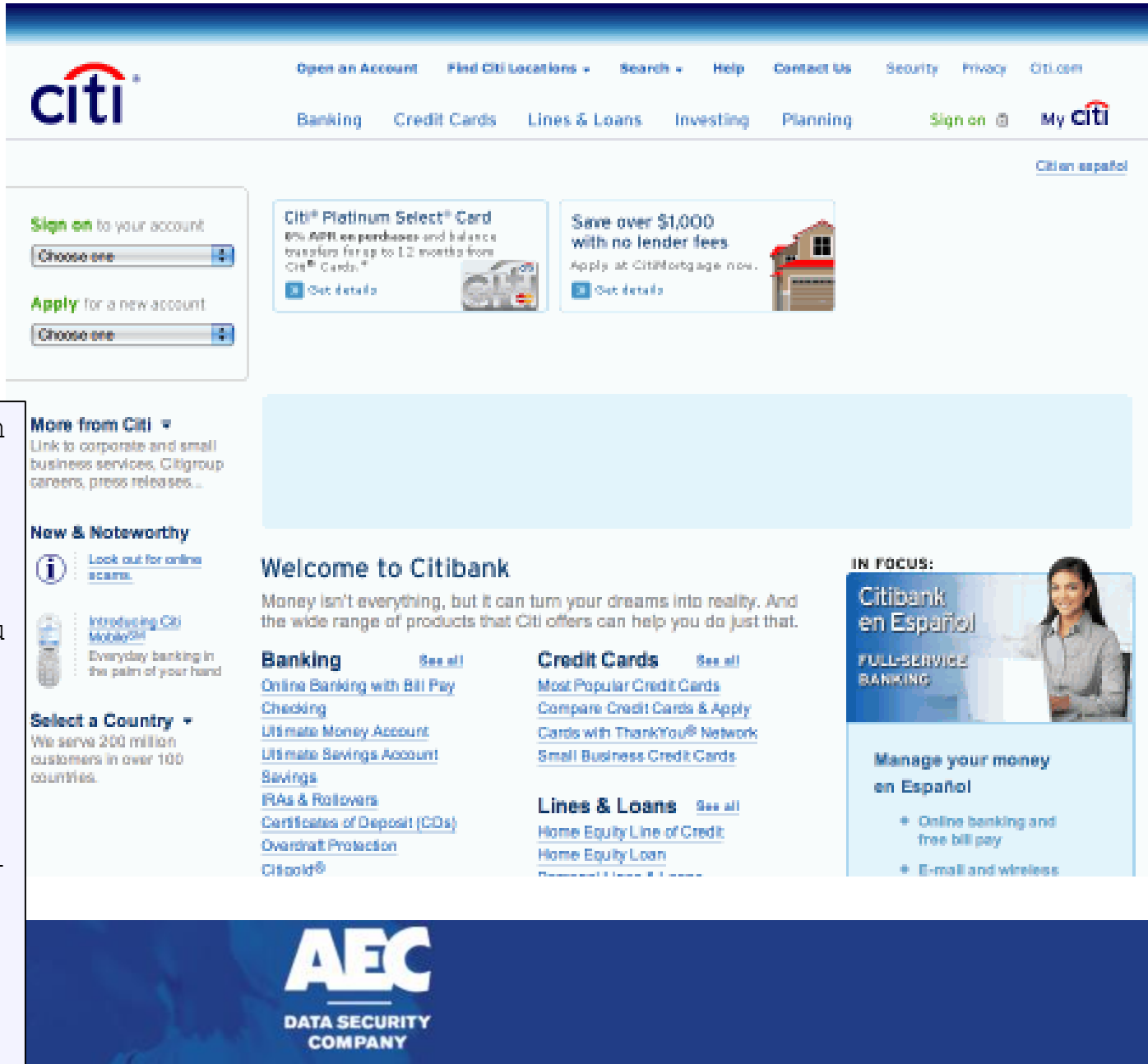
Herní soutěž odstartovaná Los Ageleským rádiem KIIS-FM. Soutěž vyzvala posluchače, že ten kdo zavolá jako 102 v pořadí vyhraje auto Porsche 944 S2. Kevin nelenil: převzal kontrolu nad všemi přepínači telefonních linek a efektivně vyblokoval všechny příchozí hovory, tak aby měl jistotu, že on bude právě 102. volající a vyhraje cenu.

Velká bankovní loupež



V roce 1994 se Levin vlámal do interní sítě americké banky CitiBank.

Jakmile byl uvnitř, převedl 10.7 milionů dolarů na účty ve Spojených státech, Finsku, Německu, Izraeli a Nizozemsku. Převody provedl s pomocí tří kolegů, kteří mu měli pomoci vrátit virtuálně ukradené peníze zpět.



Hra na kočku a myš – nové techniky přicházejí

Tsutomu Shimomura

VS.

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM -132

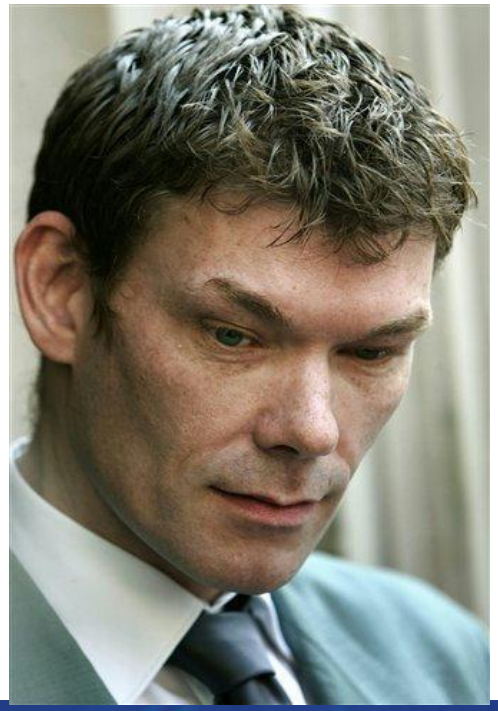
Útok na NASA

- 16letý hacker Jonathan James, známý jako c0mrade
- Zcizení zdrojových kódů ke stanici ISS
- „Kód sám o sobě je špatný… nestojí za 1.7milionu dolarů.“

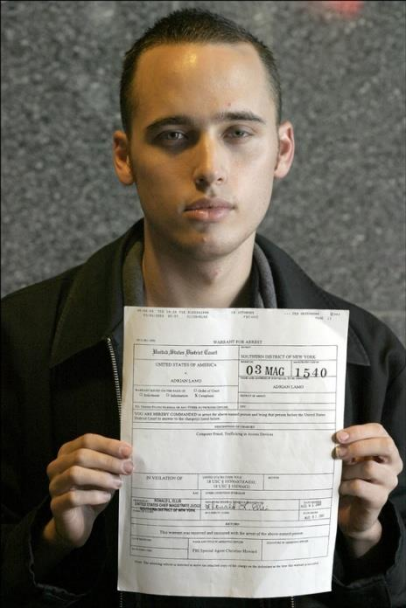
AEC
DATA SECURITY COMPANY

Zvědavost, UFO a Gary McKinnon

Stopy jeho činu byly objeveny v počítačích patřících armádě, námořnictvu, Ministerstvu obrany, letectvu a Pentagonu. Celkem získal přístup k 97 serverům. Pokaždé hledal informace o létajících talířích.



Sheffield, England, 4 March 1962



Útočí se i na média,

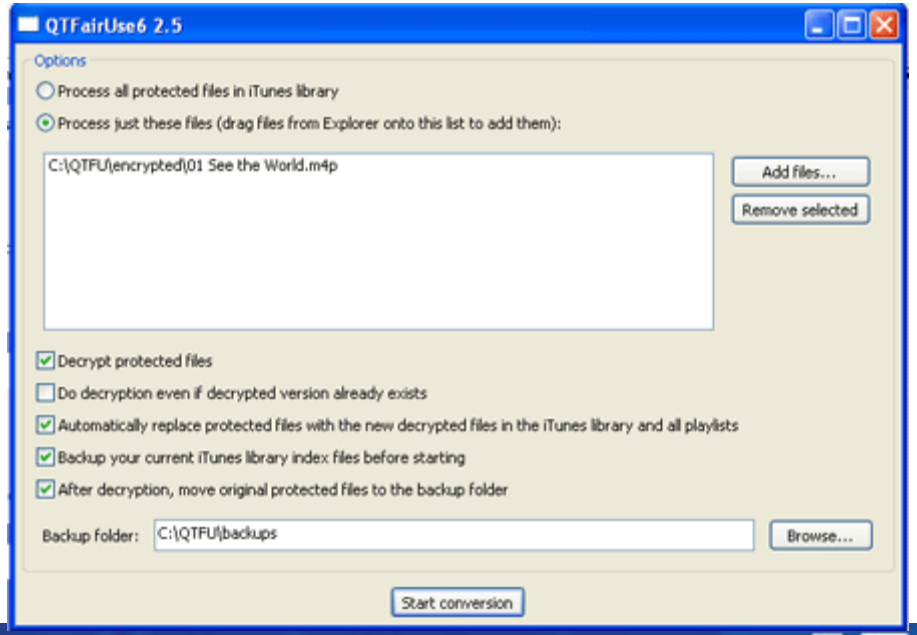
modifikují se databáze

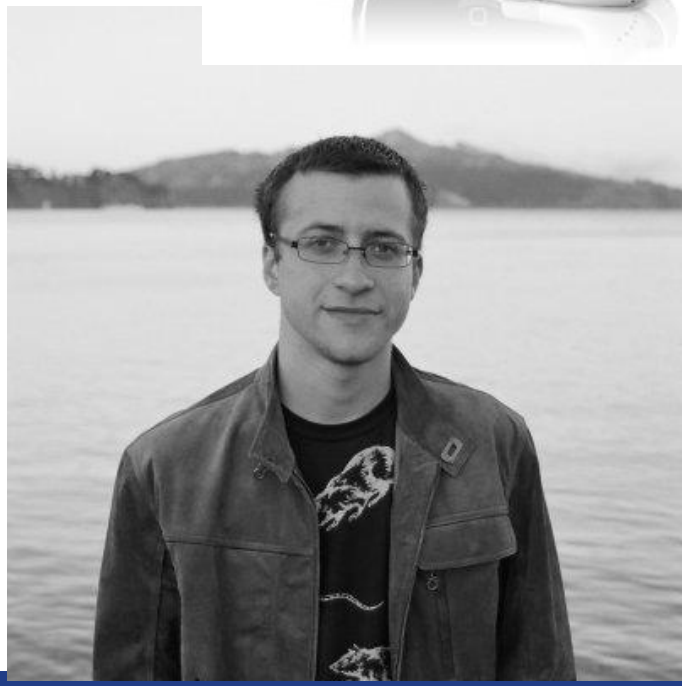
Všechny myslitelné odvětví již padli za oběť hackerům. Včetně médií a novin. Nejvíc známý příklad je útok na noviny New York Times, který byl proveden jedním z nejznámějších hackerů - **Adrianem Lamem.**

AEC
DATA SECURITY COMPANY

Celý svět proti DRM, DVD Joe na koni

QTFairUse program byl schopen získat RAW data ze souboru koupeném na iTunes extrahovat je a obejít tak ochranou metodu DRM.





AEC
DATA SECURITY COMPANY

Krádež zdrojových kódů Windows

Statement from Microsoft Regarding Illegal Posting of Windows 2000 Source Code

Last updated: Feb. 20, 2004, 12:00 p.m. PST

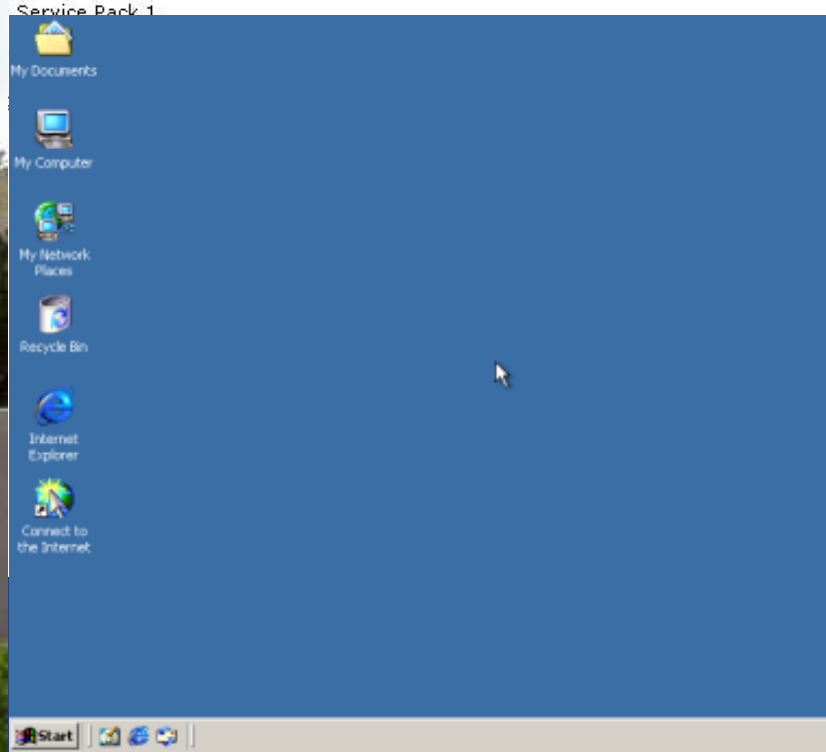
REDMOND, Wash., Updated, Feb. 20, 2004 — On Thursday, February 12, Microsoft became aware that portions of the Microsoft Windows 2000 and Windows NT 4.0 source code were illegally made Internet. Subsequent investigation has shown this was not the result of any breach of Microsofts corporate network or internal security, nor is it related to Microsofts Shared Source Initiative or its Gov Program, which enable our customers and partners, as well as governments, to legally access Microsoft source code. Microsoft reaffirms its support for both the Shared Source Initiative and the Gover Program.

Microsoft continues to work closely with the U.S. Federal Bureau of Investigation and other law enforcement authorities on this matter. Microsoft source code is both copyrighted and protected as a trac is illegal to post it, make it available to others, download it or use it. Microsoft will take all appropriate legal actions to protect its intellectual property. These actions include communicating both directly those who possess or seek to possess, post, download or share the illegally disclosed source code.

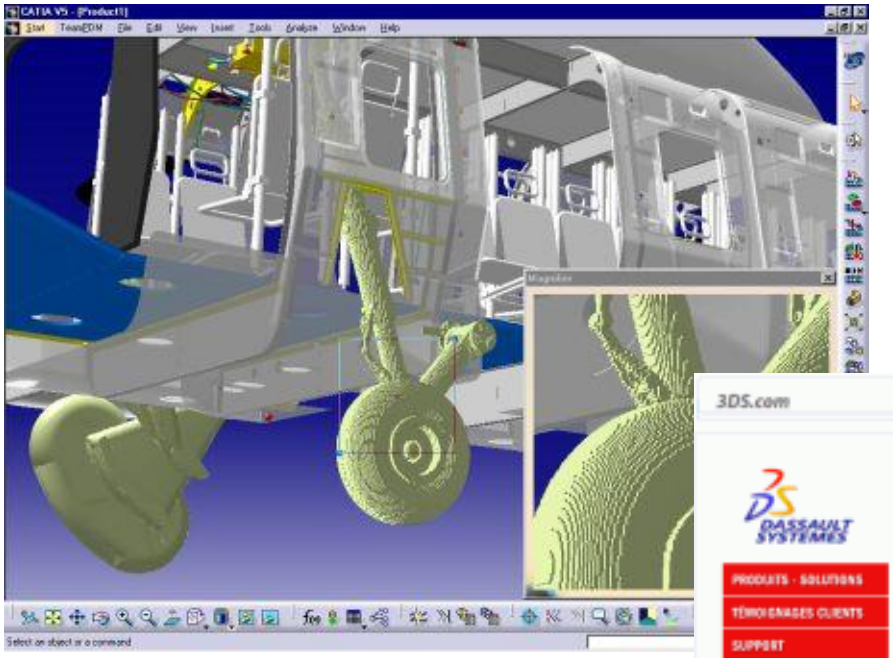
Specifically, Microsoft is sending letters explaining to individuals who have already downloaded the source code that such actions are in violation of the law. Additionally, Microsoft has instituted the use such illegal sharing of the source code has taken place. These alerts are designed to inform any user who conducts specific searches on these networks to locate and download the source code that su

Questions about the ongoing investigation should be referred to the FBI.

ly discovered by an individual studying the leaked source code. This exploit is a known Windows 98, Windows Millennium, Windows NT 4.0, Windows 2000, and Windows XP s rs running Windows XP Service Pack 1 or Windows Server 2003 who have installed all Service Pack 1.



Poslední velký útok



Krádež v hodnotě $245.000.000 proti firmě Dassault

Hacking dnes

Fenomén evoluce

Děkuji za pozornost

www.aec.cz