

History of Computer Crime

CSH6 Chapter 2
 "History of Computer Crime"
 M. E. Kabay
 With supplemental updates

Topics

- Why study historical records?
- Trends
- 1960s / 70s – Sabotage
- Impersonation
- Phone Phreaking
- Data Diddling
- Logic Bombs
- Trojan Horses
- Notorious Worms and Viruses
- Spam
- Denial of Service
- Hacker Underground
- Recent Developments

CSH6
Chapter 2

Why study historical records?

- Common body of knowledge
- Distinguish amateurs from professionals
- Shared history of significant events
- What has shaped development of field
- Understand references from senior people
- Put new events and patterns into perspective

Trends

- Early days: sabotage, disgruntled/dishonest employees
- Physical damage prominent threat until 1980s
- Unauthorized access common
- Telecommunications subversion popular in 1960s/70s
- Malicious software developed in 1980s
- Fax-based fraud developed in 1980s (4-1-9)
- Growth of Internet multiplied threats
- Financial crime mediated by computers & networks grew in 1990s
- New malware types developed in 1990s
- Illegitimate uses of e-mail spawned spam, phishing, 4-1-9 e-mail fraud

Rough Guesses About Sources of Damage to IT



MORAL: remember this fuzzy graph and don't trust precise statistics about computer crime!

1960s / 70s – Sabotage

- Computers can be *tools* and *targets* of crime
 - ❑ Also repositories of evidence
- 1969.02 – fire in computer center during student riot in Montréal, Québec, Canada
 - ❑ Sir George Williams University (now Concordia)
 - ❑ \$2M damages & 97 people arrested
- In 2001, survey by Novatech showed ~¼ of all computers had been physically assaulted by owner (4,200 respondents)

Albert the Saboteur (1970)



- National Farmers Union Service Corporation
 - ❑ 1970-1972
 - ❑ Burroughs B3500 mainframe
 - ❑ 56 hard disk head crashes in 2 years
 - ✓ 8 hours average downtime
- \$500,000 electrical system repairs
- Crashes continued
- Suspicion fell on Albert the Operator
 - ❑ Loyal employee
 - ❑ Night shift for many years without letup
 - ❑ Secret video-tape revealed sabotage
 - ❑ Liked the excitement of having all those people around

7

Copyright © 2014 M. E. Kabay. All rights reserved.

Impersonation



- 1970: Jerry Neal Schneider
- 1980-2003: Kevin Mitnick
- 1970s-today: Credit Card Fraud
- 1990s-today: Identity Theft Rises

8

Copyright © 2014 M. E. Kabay. All rights reserved.

1970: Jerry Neal Schneider



- Born c. 1951
- 1968: forms Creative Systems Enterprises
 - ❑ Selling electronic communications equipment
 - ❑ Dumpster® Diving for parts at PT&T
 - ❑ Found discarded (unshredded) procedures manuals
- 1971: Ordered new equipment from PT&T by pretending to be employee involved in repairs
 - ❑ Then sold it -- ~\$200K value
- 1972: Arrested and convicted of grand theft
 - ❑ 2 months + \$500 fine!

9

Copyright © 2014 M. E. Kabay. All rights reserved.

1980-2003: Kevin Mitnick (1)



- Born 1963
 - ❑ As young teenager, stole bus rides by using special punch for bus transfers
 - ❑ Phone phreaking, pranks, breakins using social engineering against DEC
- 1981: social engineering to enter PacBell
 - ❑ Juvenile court ordered psychological study
 - ❑ 1 year probation
- 1987: arrested for penetrating USCA
 - ❑ Stored stolen VAX VMS code on disks
- 1988: Arrested by FBI; sentenced 1989 to 1 year jail & 6 months rehabilitation



10

Copyright © 2014 M. E. Kabay. All rights reserved.

Kevin Mitnick (2)



- 1992: FBI tried to arrest him for stealing services from phone company computers
 - ❑ Went underground
- 1994: Insults Tsutomu Shimomura
 - ❑ Physicist & Internet security expert
 - ❑ Mitnick left rude messages on computer, voice-mail
 - ❑ Shimomura helped FBI track Mitnick
- 1995: FBI arrests Mitnick
- 1999: Convicted of wire fraud, computer fraud & illegal interception of wire communication
 - ❑ Sentenced to 46 months federal prison

11

Copyright © 2014 M. E. Kabay. All rights reserved.

Kevin Mitnick (3)



- Became cause célèbre among criminal hackers
 - ❑ FREE KEVIN defacements worldwide
 - ❑ Funniest: FREE KEVIN on Mexican Web site after release of KM
- 2000: released from prison
 - ❑ 3 years parole
 - ❑ Restricted access to computers
 - ❑ Profits from writing and speaking about criminal career used to reimburse victims
 - ❑ Founded own computer-security firm
 - ❑ Wrote books about defending against social engineering



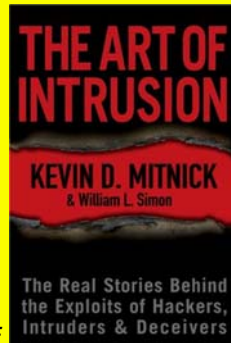
12

Copyright © 2014 M. E. Kabay. All rights reserved.

Kevin Mitnick (4)

➤ Readings about the Mitnick case

- ❑ Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick—and the Man Who Hunted Him Down*. Dell (New York). ISBN 0-440-22205-2. xix + 328.
- ❑ Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.
- ❑ Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick—The Inside Story of the Great Cyberchase*. Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.
- ❑ Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—by the Man Who Did It*. Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.



13

Copyright © 2014 M. E. Kabay. All rights reserved.

1970s-Today: Credit Card Fraud (1)

➤ Credit cards developed after WWII in USA

- ❑ 1950: Diners Club
- ❑ 1951: BankAmericard & MasterCard
- ❑ 1958: American Express
- 1960s: aggressive marketing of credit cards
 - ❑ Sending cards to unsuspecting consumers
 - ❑ Mailbox theft → surprise bills on first invoice
- 1974: Fair Credit Billing Act to reduce abuses
- 1970s-80s: expansion of electronic confirmation
- 1980s: Refusal to improve security (no pictures)

14

Copyright © 2014 M. E. Kabay. All rights reserved.

Credit Card Fraud (2)

- 1990s: massive increase in credit card & online fraud
 - ❑ US Visa/MC: \$110M in 1980 vs \$1,630M in 1995
- More recent data*:
 - ❑ Unauthorized general-purpose credit card transactions = 0.037% all card-present credit card transactions in 2012
 - ❑ Fraud = 0.092% value of transactions)
 - ❑ 0.118% all card-not-present transactions
 - ❑ 0.114% value those transactions)
 - ❑ Global fraud rates across Visa < \$0.06/\$100

* < <http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php> >
or < <http://tinyurl.com/6hdtv6> >

15

Copyright © 2014 M. E. Kabay. All rights reserved.

1990s-now: Identity Theft Rises

- One of the fastest growing crimes in USA
- Identity Theft Resource Center
 - ❑ <http://www.idtheftcenter.org/>
 - ❑ Wealth of resources
 - ✓ Victim resources
 - ✓ ID theft protection tips
 - ✓ Scams & alerts
- FBI ID Theft Resources
 - ❑ http://www.fbi.gov/about-us/investigate/cyber/identity_theft
- Statistic Brain
 - ❑ <http://www.statisticbrain.com/identity-theft-fraud-statistics/>

16

Copyright © 2014 M. E. Kabay. All rights reserved.

What ID Thieves Do

- Locate identifying data
 - ❑ Social Security Number
 - ❑ Driver's License
 - ❑ Home address, telephone number
 - ❑ Mother's maiden name
 - ❑ Or just misuse of *handle* (screen name) for forged messages
- Create new credit cards, bank accounts
- Default on loans in victim's name
- Ruin reputations, credit records

17

Copyright © 2014 M. E. Kabay. All rights reserved.

Consequences for Victims

- Credit-card expenses relatively easy to correct IFF
 - ❑ Victim checks statement immediately and
 - ❑ Reports questionable transactions within time limit
- Bank-account thefts much more difficult to correct
 - ❑ Money stolen is client's, not bank's
 - ❑ Client has great difficult recovering funds
- Bill-collectors hound victims relentlessly
- Bad credit records difficult to correct, ruin plans, cause loss of jobs or interfere with hiring
- Criminal accusations put victims at serious risk of erroneous arrest or deportation
- Victims may be nailed for child support of total strangers

18

Copyright © 2014 M. E. Kabay. All rights reserved.

Preventing ID Theft

- Prevent theft: restrict access to your SSN and other personal data
 - ❑ SSN may be required by SSA, IRS employer, financial institution, lender
 - ❑ Corner store or video rental should NOT be given SSN
- NEVER give out credit-card or other personal data over the phone to someone *who has called you*. Ask for written documents.
- Shred papers that include confidential info before discarding.
- Destroy computer media before discarding.
- Don't use DEBIT cards to buy things

Phone Phreaking

- Phone + freak = phreak
- 1950s: Single-frequency signals communicated control instructions to central switches (computers)
- Generating external tone could fool switch
- 2600 Hz tone generated by whistling, flute or whistle in Captain Crunch cereal box
 - ❑ Hence John Draper phreak became known as Cap'n Crunch
 - ❑ Able to initiate free long-distance
 - ❑ Interviewed by Equire 1971 about phreaking – arrested & convicted
 - ❑ Eventually jailed for wire fraud in 1977



John Draper then and now

Data Diddling

- Unauthorized modification of data
- Changes can occur
 - ❑ Before data input
 - ❑ During data input
 - ❑ Before output
- Records affected have included
 - ❑ Bank records
 - ❑ Payrolls
 - ❑ Inventory data
 - ❑ Credit records
 - ❑ School transcripts
 - ❑ Telephone switch configurations....

Data Diddling: The Equity Funding Fraud

- Equity Funding Corporation of America
 - ❑ From early 1960s to 1973, immensely successful firm
 - ❑ Buy insurance + invest in mutual funds
- In 1964, computer problem prevented printing final figures
 - ❑ President ordered head of DP to falsify report with expected profit
 - ❑ Profit failed to materialize
 - ❑ Invented false insurance policies to make up difference
 - ❑ Eventually “killed” nonexistent policy holders to collect payouts (\$MILLIONS)
- Discovered 1972 by SEC; officers went to jail

EQUITY FUNDING CORPORATION OF AMERICA

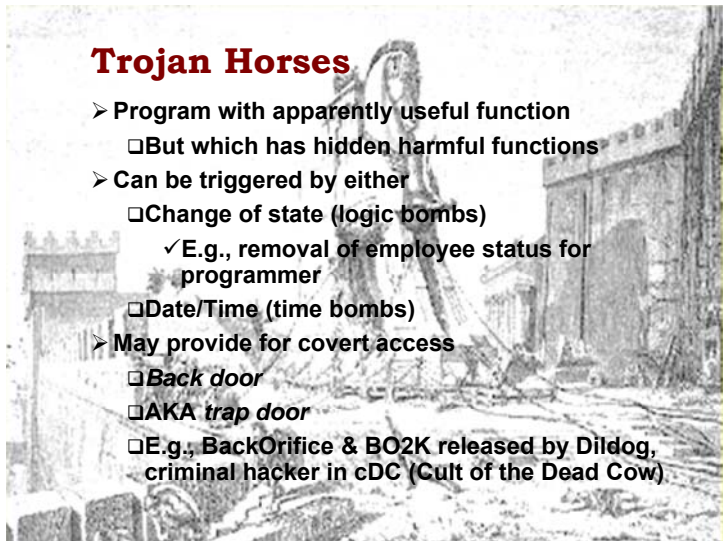
Data Diddling: Vladimir Levin vs Citibank

- In 1994, Russian programmer Vladimir Levin broke into Citibank computers
 - ❑ Transferred ~\$12M to various international bank accounts
- Spotted after 1st \$400,000 transferred in July 1994
- Citibank cooperated with FBI & Interpol
- Levin & gang eventually arrested and tried
- Convicted 1998 to 3 years prison
- Citibank hired banking industry's first CISO, Stephen R. Katz



Trojan Horses

- Program with apparently useful function
 - ❑ But which has hidden harmful functions
- Can be triggered by either
 - ❑ Change of state (logic bombs)
 - ✓ E.g., removal of employee status for programmer
 - ❑ Date/Time (time bombs)
- May provide for covert access
 - ❑ Back door
 - ❑ AKA trap door
 - ❑ E.g., BackOrifice & BO2K released by Dildog, criminal hacker in cDC (Cult of the Dead Cow)



Logic Bombs

- Jerusalem Virus of 1988
 - ❑ Duplicated itself every Friday and on 13th of month
 - ❑ On every Friday 13th after May 13, 1988, corrupted all available disks on system
- PC Cyborg
 - ❑ AIDS information diskette
 - ❑ Actually encrypted directories, filled C: drive, intercepted commands
 - ❑ Linked to extortion demand for money



Early Notorious Worms and Viruses

- 1987: Christmas Tree Worm
 - ❑ December e-mail with EBCDIC version of tree flooded IBM networks
- Nov 2, 1988: The Morris Worm
 - ❑ Robert T. Morris studying at Cornell
 - ❑ Released self-replicating autonomous code
 - ❑ Spread through Internet
 - ❑ Crashed systems all over USA (~6,000-9,000)
- Led to formation of Computer Emergency Response Team Coordination Center, CERT-CC®
- Morris convicted
 - ❑ Violated *Computer Fraud & Abuse Act of 1986*, 18 USC §1030(a)
 - ❑ 3 years probation, \$10K fines, expelled from Cornell
 - ❑ Now respected MIT professor
<http://pdos.csail.mit.edu/~rtm/>



Stuxnet Worm

- July 2010
- Zero-day threat to SCADA
 - ❑ Siemens Simatic WinCC & PCS7
 - ❑ Designed for industrial espionage
 - ❑ Also for sabotage
- Thought to have been developed by USA and Israel by 2007
- Found in ~100,000 computers
 - ❑ Iran, Indonesia, India
 - ❑ Iranian nuclear power program affected
 - ✓ Centrifuges ran too fast

Spam (not SPAM®)

- 1994: Green Card Lottery spam
 - ❑ Laurence A. Canter & Martha S. Siegel
 - ✓ Attorneys
 - ❑ Posted ad to 6,000 USENET groups
 - ✓ But did not cross-post (1 copy/user)
 - ✓ Posted to EVERY GROUP (1 copy/group)
 - ❑ Response massive
 - ✓ Complaints crashed their e-mail server ISP
 - ✓ Canter disbarred
 - ✓ Never apologized – continue to spam
- TODAY: estimates of 75-85% all email = spam

Denial of Service

- DoS = interference with availability of service
 - ❑ Resource exhaustion or
 - ❑ Destruction
- Unemailer (1996)
 - ❑ johnny [x] chaotic subscribed victims to 100s of e-mail lists
 - ❑ Led to practice of confirming subscriptions
- MafiaBoy (2000)
 - ❑ Massive attacks on Yahoo.com, Amazon.com, eBay.com, Buy.com, CNN.com – flooded
 - ❑ 15-year-old boy using modem in west end of Montréal did \$M of lost business & depressed stock prices

Hacker Underground

- Criminal-Hacker Subculture
- Chaos Computer Club
- Cult of the Dead Cow
- 2600 *The Hacker Quarterly*
- LOD
- Phrack
- MOD
- Gray-Hat Hackers
- Anonymous
- Lulz
- Web Vandalism Classics

Criminal-Hacker Subculture

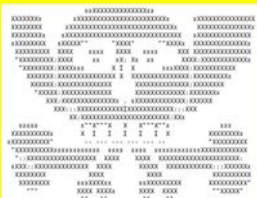
- Who?
 - ❑ Children (sub-teens, teens)
 - ❑ Adults (fewer after 18 years of age)
 - ❑ Amateurs
 - ❑ "3133T" (elite) hackers
 - ❑ Professionals
 - ❑ Organized crime
- What
 - ❑ Publications, USENET groups, lists
 - ❑ Local meetings, conventions
 - ❑ Jargon (133T5p33k)

Criminal-Hacker Subculture (2)

- Why?
 - ❑ Defining peer-group, affiliation, status
 - ❑ Rebellion, power
 - ❑ Curiosity, learning
 - ❑ Ideology, cant
- Avoid stereotypes
 - ❑ Not all creepy adolescent geeks
 - ❑ Varying levels of ethical reasoning, emotional development

Classic Hacker Group: Chaos Computer Club

- 1981: German group of computer enthusiasts
 - ❑ Radical politics
 - ❑ Demonstrated vulnerability in Bundespost videotext service
 - ❑ Generally viewed as gray-hat (non-criminal) hackers
- 1999: Opposed attempts by some computer hacker groups to disable computers in PRC
- Chaos Communications Conferences popular with some legitimate security experts



CDC – Cult of the Dead Cow

- Founded 1984 in Texas
- "Global Domination Through Media Saturation"
 - ❑ Much satire – some very funny
- Member Drunkfux founded HoHoCon hacker conference
- Political action campaigns
 - ❑ Against censorship (Goolag Campaign against GOOGLE cooperation with PRC)
 - ❑ Attacks on Church of Scientology
- Hacking tools
 - ❑ BO & BO2K



2600 The Hacker Quarterly

- Editor Eric Corley aka "Emmanuel Goldstein"
- <http://www.2600.com/>
- Founded in 1984
- Longest running & most popular hacking 'zine'
- Detailed instructions on
 - ❑ Stealing telephone services
 - ❑ Lock-picking
 - ❑ Penetration techniques
- Analysis of security issues
- History of hacking
- Political ideology



Legion of Doom (LOD)

- 1984: Phone phreakers and criminal hackers founded LOD
 - ❑ Named after enemies of DC Comics superheroes
 - ❑ Published findings in *LOD Technical Journal*
- Chris Goggans (*Eric Bloodaxe*) one of best known
 - ❑ Editor of *Phrack*
 - ❑ Became member of MOD
- Mark Abene (*Phiber Optik*) also member who moved to MOD
- Conflict with MOD = *The Great Hacker War*



Chris Goggans Then & Now

Phrack

- <http://www.phrack.com/>
- 1st edition Nov 1985
- Originally focused on phreaking
- Entirely electronic on BBS systems
- Eds: *Knight Lightning* (Craig Neidorf) & *Taran King* (Randy Tischler)
- Phrack 24 involved in *Operation Sundevil* (1990)
 - ❑ Published E911 docs
 - ❑ Actually public docs!



Craig Neidorf

Masters of Deception (MOD)

- 1989-1992 New York criminal hacker group
 - ❑ *Phiber Optik* (Mark Abene)
 - ❑ Highly visible in media
 - ✓ *Harper's*
 - ✓ *Esquire*
 - ✓ *New York Times*
 - ✓ TV (Geraldo)
 - ❑ Eventually arrested,
 - ❑ Tried for violation of CFA [18 USC §1030(a)]
 - ❑ Sentenced to 1 year in prison



Gray-Hat Hackers (1)

- **Black-Hats:** criminal hackers
 - ❑ Ignore laws
 - ❑ Test for and exploit vulnerabilities without authorization
 - ❑ Publicize vulnerabilities without delay for repair
 - ❑ Sometimes amateurish; may be experts
- **White-Hats:** penetration testers
 - ❑ Authorized to test by owners of systems
 - ❑ Maintain confidentiality and professionalism
 - ❑ Sometimes hide-bound; may be imaginative

Gray-Hat Hackers (2)

- **Gray-Hats:** professionals with black-hat backgrounds and attitudes
 - ❑ May have been members of criminal-hacking organizations
 - ❑ May continue to use hacker handles (pseudonyms)
- 2000-01: L0pht members join @Stake
 - ❑ 8 members of L0pht Heavy Industries
 - ❑ Continued to use hacker handles (e.g., Mudge, Weld Pond, Brian Oblivion, Dildog...)
- Described in glowing terms by some reputable experts
 - ❑ NTBugtraq's Russ Cooper: "The eight brilliant geniuses down at the L0pht. . ."
- Other commentators not impressed
 - ❑ John Taschek of PC Week: ". . . L0pht's history shows that the group is not ethical, maintained practices that bordered on being illegal and is simply downright scary. . ."

Web Vandalism Classics

- CIA (1996.09)
- USAF (1996.12)
- NASA (1997.03)
- AirTran (1997.09)
- UNICEF (1998.01)
- US Dept Commerce (1998.02)
- New York Times (1998.09)
- SETI site (1999)
- Fort Monmouth (1999)
- Senate of the USA (twice)(1999)
- DEFCON 1999 (!)



WELCOME TO THE TRUTH

Some Useful Links To Get You Started

INSIDE AREA 51

INFINITE VOID

42

And finally, send email to President Clinton and tell him what you really think of him

Or send email to the rash president, President Hillary

43

NORWICH UNIVERSITY

You can learn all about gov't corruption here. Learn the secrets that they don't know want you to know. We'll not really, I don't have time for that.

But trust me it's true. Like the time, and learn the truth yourself. After all information should always be free. Trust your mind not someone else's.

This is What your gov't is doing to you everyday

The thing is we all support the government whether we want to or not, as we pay taxes, etc. Why do we do this? Well the fact is we do this because we are told we have no choice, well the fact is we do have a choice, this gov't was founded on personal freedom.

Why should we give that up, for a congress of immoral greedy politicians? For a president that would be in jail other than for executive privilege. America was once a great nation, make it so again, fight back, and make this country proud again.

NORWICH UNIVERSITY

Orbiter Thermal Protection System

(H4G15 > NASA)

Greetings from the members of H4G15.

Our mission is to continue where our colleagues the ILF left off. During the next month, we the members of H4G15, will be launching an attack on corporate America. All who profit from the misuse of the internet will fall victim to our upcoming reign of digital terrorism.

Our privileged and highly skilled members will stop at nothing until our presence is felt nationwide.

Even your most sophisticated firewalls are useless. We will demonstrate this in the upcoming weeks.

THE COMMERCIALIZATION OF THE INTERNET STOPS HERE

44

It's something else.

airTran

SO WE KILLED A FEW PEOPLE, BIG DEAL

AIRTRAN INTRODUCES NEW SERVICES, BEGINS STRATEGY TO KILL ALL AMERICANS!

ATLANTA, Apr. 24, 1997. Vahjet Airlines today changed its name to AirTran Airlines and along with its merge partner AirTran Airways introduced a new business strategy designed to bring dismemberment to a broader travel audience. The airline said that its objective is to make air travel more attractive to business travelers and even more convenient for suicidal maniacs.

It seems Vahjet is attempting to pull an unethical "fast one" over on the public, while bailing out to a larger conglomerate. "Let's call ourselves AirTran then maybe someone will be dumb enough to get on board one of our flying death machines!" "We have gag orders and fuck edit in the airplane with a 2 foot long salami."

"Over the past year we've narrowed our focus on the basis of our business with safety, reliability and operational excellence as our goal," said Cox, who joined the carrier in November 1996. He previously served as an inmate in San Quentin and as prisoner number 670564, he aged 42 men. "AirTran's mission is to kill air travel customers who can actually afford to die. It's that simple. That's a significant change from our previous strategy, which was to offer the lowest-priced air transportation possible, without seatbelts or pilots," added Cox, who will be the chief executive of the merged airline and holding company.

For an untimely death
800.AIRTRAN

In the Atlanta area.
770.994.8258

In the Orlando area.
407.247.8726

45

Copyright 1997 BoW Sucks. All Rights Reserved.
Copyright © 2014 M. E. Kabay. All rights reserved.

unicef
United Nations Children's Fund

and DAMM bring you...

STARVIN' 4 KEVIN

DAMM

On here's the situation, as we see it. All one is paying attention to the picture of the underground, fine, you had ur choice, now we need business. DAMM (Dumb Against Mad Mothers) and UNICEF have formed a coalition to put an end to the mislithement of KEVIN MITNICK. Kevin has been held for over two years without trial and he has had adequate counsel. His imprisonment has been deemed unjust. All of all, Kevin is just a big kid, and that what UNICEF is all about, helping the children. speaking of children. On to the matter of our release Damz.

If Kevin is not released by Friday 2nd (goodlord's day), we begin the ultimate hijackout.

46

SUID-USA/Inet

The actual site has been redesigned for easy access to 3,000 additional phreak and hack-related phreak, greater functionality, and a whole lot more! Open to all members of SUID and all friends.

Personal msg : love u A-Y from crew4

U May Want To Be Under Her Dependence

We Show u That U Take This Thing too simply from klout

save amazony forest from senekool

Be among the strong. from Adz

& fuck dudie hulu, that's all guys

Hack'd by Rewt4

for SUID

47

NORWICH UNIVERSITY

A Service of the U.S. Department of What!
Last Modified: February 11, 1998 (stat-ua@do.gov) U.S. Department of Consensus

New York Times (1998.09)

HACKING FOR GIRL13Z

FIRST OFF, WE HAVE TO SAY.. WE OWN YER DUMB ASS. AND REMEMBER, DUMB ASS IS OFF3N CUTE 4SS. AND WE LIKE CUTE ASS.

3COND, TH3R3 AR3 80 MANY L033R3 N3R3, IT2 HARD TO PICK WHICH TO INSULT THE MOST.

SINC3 WE AR3 NOW INTERN3T TERRORIST2, W3 FIGURE WE SHOULD DEMAND 50ME RAN3OM OR SOMETHING. SO, PAY US 104 GIRLIE2, 6 BILLION IN NEWSPAPER SUBSCRIPTION2, AND HAVE A PRINTING PRESS OR SOMETHING. NOT LIK3 YOU GUYS KNOW WHAT FAIR JOURNALISM IS ANYWAY. DUMB WHOR32.

48

WANTED:



Oh phuK n0.

n0t Our b0m@

n0t Our p0rt0les smy b0m@ @@@ n0t
yuk f00. w3 0wned you.



this is d0m0r0d to all the fagg0t b0m h0ng0es
in f0rt m0n0m0uth
may y0u0t n0 b0y, st0mb0
w3ll wh0t w3 ch0d0 gr0t p0p0l. bu7 th0 w3 m0ght g0t /n0m0r0s 0n R0st, 4nd g0t 0wned by th0se m3n th0 d00ds.
all 1 h0r0 to r0y 0b07 th0se d00ds, 1s th0? It's all f0r2 g0m3 w0h0m0r0 0wns w0t f0r2. and 1000s 11k0 y0u 1000g to v0ne
h0h0h0 r0h0
h0h0h0h0h0h0 w3 0wn y0u n0w

Senate of the USA (1) (1999)



MOD K1X A\$\$
w0t 1ng0t l0st n0w d0t 0.02 b0y th0 03 w0rks 0n 0 b1g 100K0R U GUT7 (0n th0 v0l0f 0f 0h0 0f th0 03 w0rks 0n th0 FBI.
WITHOUT FURTHER DELAY, LADIES AND GENTLEMEN, BOYS AND GIRLS, PLAYERS AND PLAYERS, HATERS. WE
ANNOUNCING
MAST3RZ 0F D0WNL0ADING, GL0B0L D0M1N10N '99
The FBI may be all over the other gangs, like those g0t and 10 q000s, 00000g0 g0ll0r. M0D m0k0 b0th0 0wn00 000k 1k0 0 g0ll0g 0f
sp0c10d 0b1d0r0z @ FBI vs. M0D n '99. BR1NG IT 0N F00RZ (0TW N1FC 1Z 0L50 0RNE0)
S1M0T1M0Z U GUT7A G0 W1TH 0 N0M0 U C0N TRU5T. 4 S1M0, R0GUL0T10N 1Z 1UST 0 W0Y 0F L1F0.
0wned (0wn 10) th0 0rt 0f 0b0w0g h0w 0t0p0 0 r0ad00n c0n b0, 0n 0 00000
BIG UP 2:
M0D/L0B/P00K1/P00B/00B1/N0T
B0M/92L/00A/20040/0000/000
TH0 0R10T0L 5C000001000
SMA0 IN TH0 T00TH 2:
B0M/04010/0400/0002/000
TH0 V1L000 R000 M000100
ALL TH0 F00RZ 0T W000.M10

Senate of the USA (2) (1999.06)



ADM CON 7 is July 9-11th, 1999 on Planet Earth!
07/00/99 DEF CON taken over by the ADM Crew and renamed to ADM CON
07/00/99 Antivirus is now DEF CON 7.0 official sponsor!

Hacker Conventions

- > Blackhat < <http://www.blackhat.com/> >
- > DefCon < <http://www.defcon.org/> >
- > HOPE (Hackers on Planet Earth) < <http://www.hopenumbernine.net/> >

Criminal Hacking Gets Organized

- Profitable, low risk
- International gangs successful
 - Russian Business Network (RBN)
 - Bradley Guinen (NU BSCSIA 2013)
 - ✓ CJ341 paper published in *Network World Security Strategies* with Kabay

[http://www.mekabay.com/nwss/866_russian_cybercrime_\(guinen\)_part_1.pdf](http://www.mekabay.com/nwss/866_russian_cybercrime_(guinen)_part_1.pdf)
[http://www.mekabay.com/nwss/867_russian_cybercrime_\(guinen\)_part_2.pdf](http://www.mekabay.com/nwss/867_russian_cybercrime_(guinen)_part_2.pdf)
[http://www.mekabay.com/nwss/868_russian_cybercrime_\(guinen\)_part_3.pdf](http://www.mekabay.com/nwss/868_russian_cybercrime_(guinen)_part_3.pdf)

55

Copyright © 2014 M. E. Kabay. All rights reserved.

Chinese Cyberwar

- Significant increase in industrial espionage by PRC
- Full-time hackers employed by state
- Log off during weekend!
- Attacks, penetration, infiltration, IP theft
- See Chapter 14 from CSH6.

56

Copyright © 2014 M. E. Kabay. All rights reserved.

DISCUSSION

57

Copyright © 2014 M. E. Kabay. All rights reserved.