



Segurança Computacional

Um breve histórico do *hacking*

André R. A. Grégio

gregio@inf.ufpr.br

Departamento de Informática
UFPR

AGENDA



- Motivar o estudo de segurança computacional
- Mostrar casos reais de ataques e os impactos às vítimas
- Discutir as implicações da segurança insuficiente/ausente

So far, so bad...



- Milhões de dólares roubados de corretoras de criptomoedas
- Brechas de segurança em redes sociais (exposição de contas), serviços de compartilhamento de edição e de arquivos, serviços na Internet
- Roubo e vazamento de propriedade intelectual
- Derrubada de nuvens

E a segurança?



No princípio, eram...



- ... as companhias telefônicas.
- Antes dos:
 - computadores pessoais
 - dispositivos móveis e *tablets*



1971

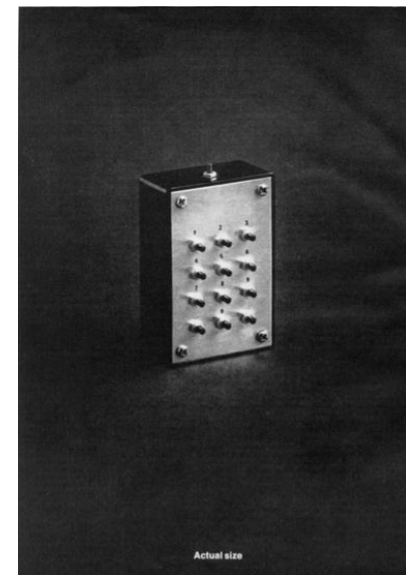


- Artigo na Esquire:

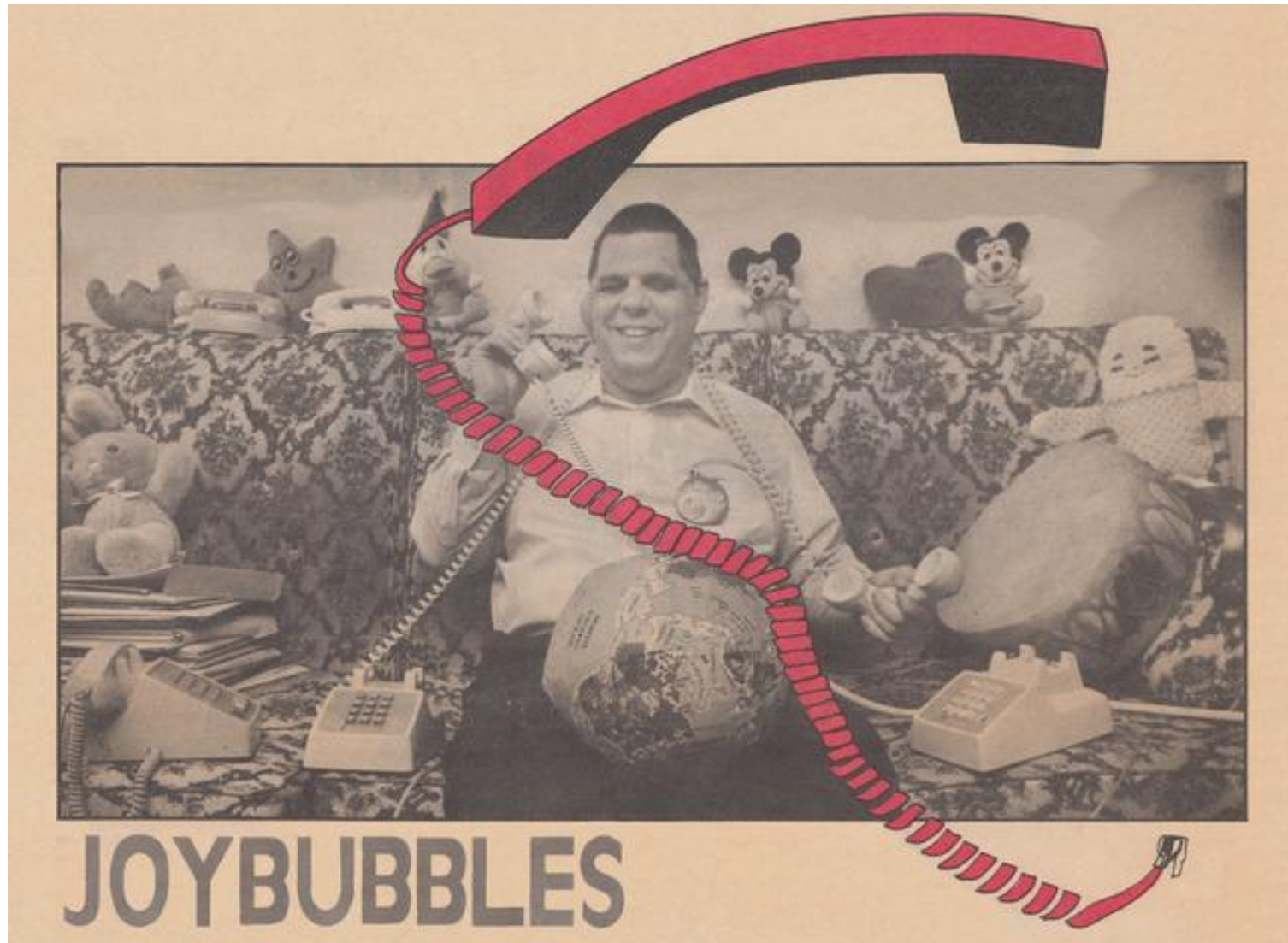
Secrets of the Little Blue Box

by Ron Rosenbaum

A story so incredible it may even make you feel sorry for the phone company



Joe Engressia Jr.



Captain Crunch



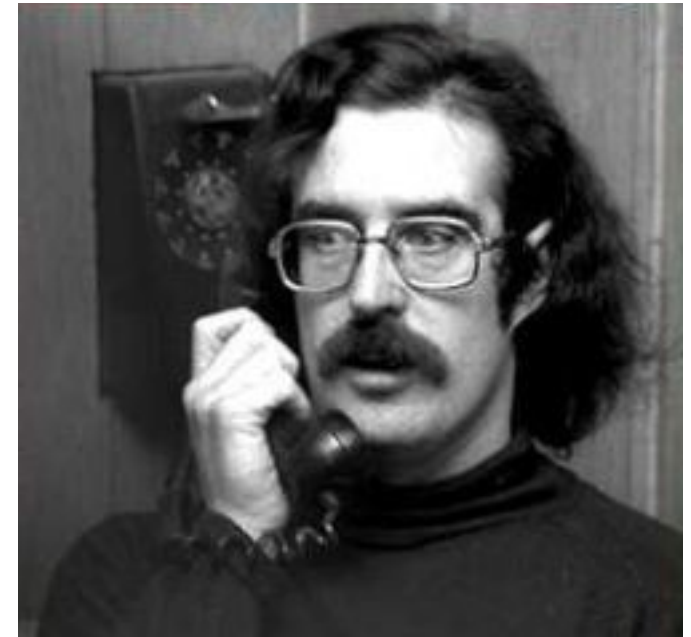
- Cereal Cap'n'Crunch:
 - Brinde dos anos 70 → apito!



Captain Crunch



- Ma Bell/AT&T:
 - Frequência de sinalização para ligações interurbanas → 2600 Hz
- John Draper:
 - Descobriu como subverter o
 - sistema de telecomunicações
 - emitindo um som na mesma
 - frequência.



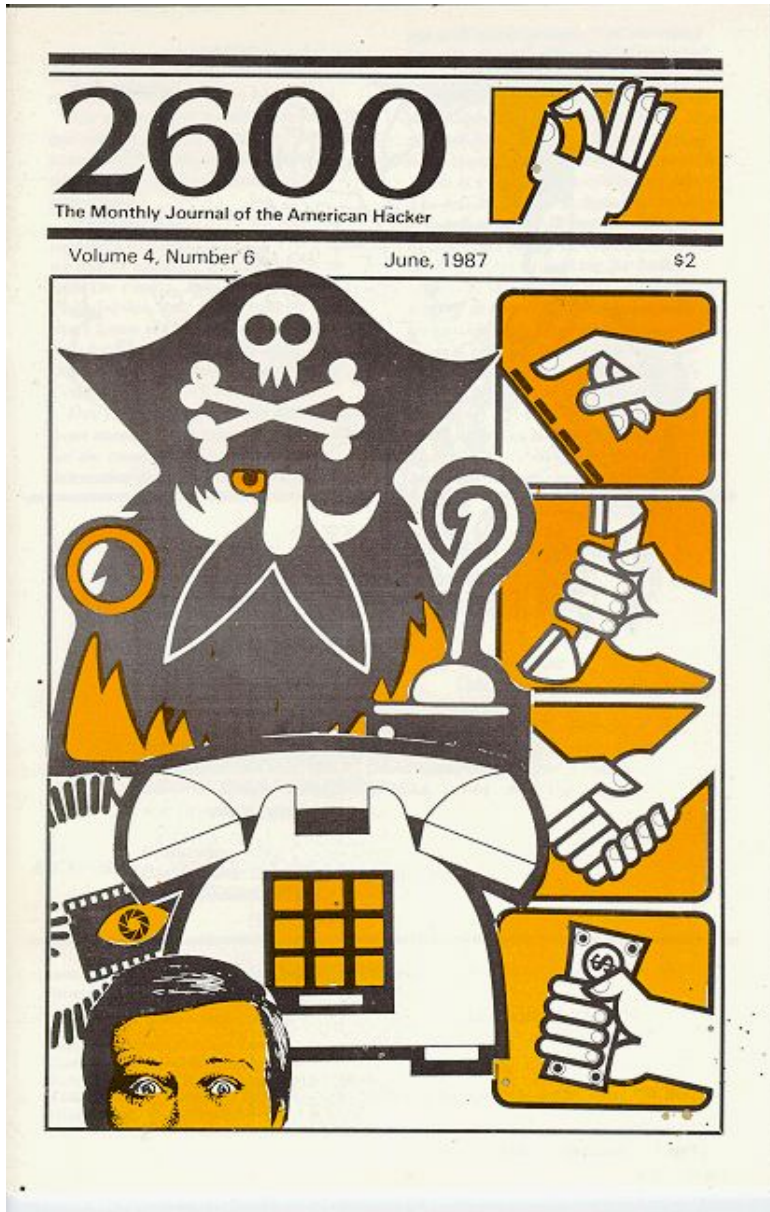
Captain Crunch



- BlueBox:
 - John Draper → Captain Crunch
 - Wozniak e Jobs (1972) → 1ª 'empresa' juntos, venda de *blueboxes* em Berkeley
 - *Phone phreakers!*



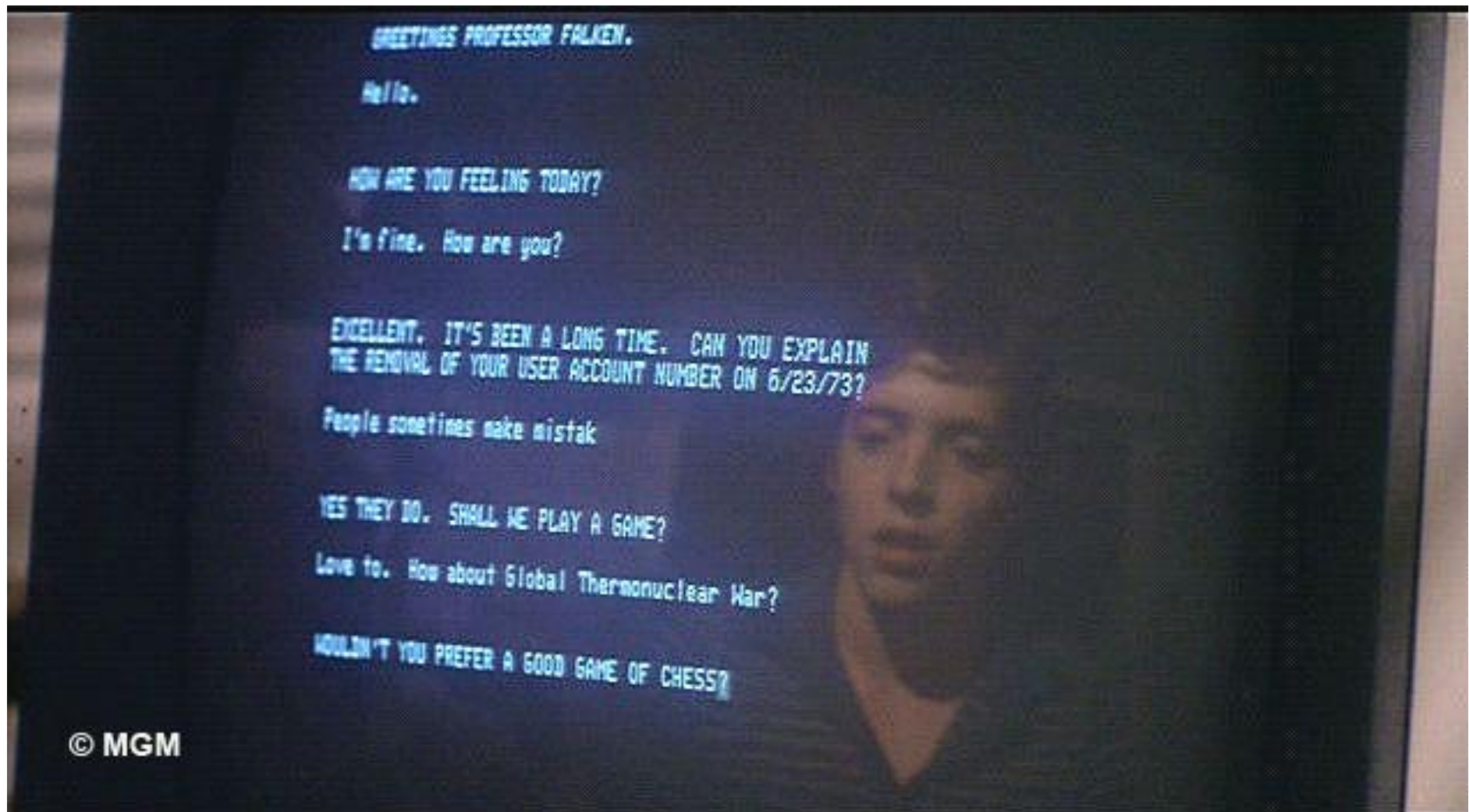
Revista 2600



Phone phreaking

- Durou entre os anos 50 e 70
- Preocupação da cia. telefônica → **segurança física**, não remota
- Falta de autenticação
- Cultura da época
- Motivação:
 - *status*
 - curiosidade

Anos 80: *War dialing*



War dialing



- . Discagem de “faixas” de números de telefone
- . Descoberta de:
 - Linhas ativas
 - Fax
 - *Modems*
- . Programas para controle remoto habilitados:
 - porta de entrada via discagem!
- . “Ocorrências” nos anos 80 e 90 causaram a criação de leis...

<http://www.imdb.com/title/tt0086567/>

War driving



War driving



```
Kismet Sort View Windows
Name      BSSID      T C  Ch Freq  Pkts  Size  Bcn%  Sig  Cnt  Manuf      Cty  Seen By
TRENDnet  00:14:D1:5F:97:12 A 0  1 2417    1    0B   ---   ---  1 TrendwareI --- wlan0
linksys_SES_45997 00:16:B6:1B:E4:FF A 0  6 2432    1    0B  10% -78  1 Cisco-Link --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N  ---  ---    2    0B   ---   0  1 IntelCorpo --- wlan0
linksys  00:1A:70:D9:BC:13 A N  6 2437    2    0B  10% -86  1 Cisco-Link --- wlan0
MPA41  00:1F:90:E6:E0:84 A W  11 2462    3    0B   ---  -86  1 ActiontecE --- wlan0
6SI03  00:1F:90:FA:F4:C8 A W  --- 2412    3    0B   ---  -83  1 ActiontecE --- wlan0
TFS  00:09:5B:D7:9D:B2 A N  --- 2462    4    0B   ---  -68  1 Netgear --- wlan0
Xu Chen 00:18:01:F9:70:F0 A N  6 2437    4    0B   0% -75  1 ActiontecE US wlan0
TK421  00:18:01:FE:68:77 A 0  6 2437    4    0B   ---  -79  1 ActiontecE --- wlan0
meskas  00:18:01:F5:65:E1 A 0  11 2462    5    0B  10% -71  1 ActiontecE US wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0  11 2462    7    0B  10% -45  1 Netgear --- wlan0
7J4R0  00:1F:90:E6:04:F1 A W  11 2462    7    0B   ---  -80  1 ActiontecE --- wlan0
Pickles  00:1F:33:F3:C5:4A A 0  2 2422    8    0B   ---  -75  1 Netgear --- wlan0
BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
38c8  00:16:CE:07:60:77 A W  6 2447    19    0B   ---  -82  1 NonHalPrec --- wlan0
Danish_Penguin 00:13:10:35:59:CB A W  9 2462   331    2K  50% -32  5 Cisco-Link --- wlan0

No GPS info (GPS not connected)
45

0

INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect

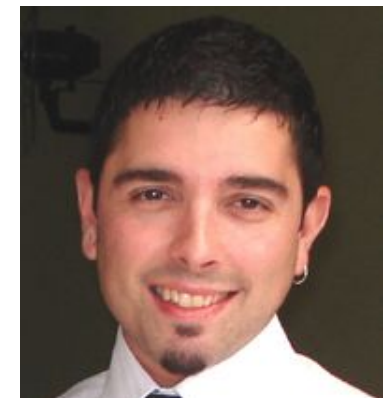
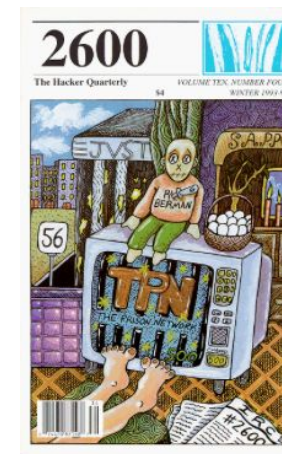
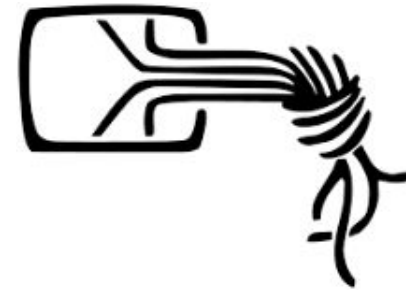
Packets
Data
wlan0
9
```

<http://kismetwireless.net>

Grupos de *Hackers*



- CCC → Chaos Computer Club (1981)
 - Maior grupo europeu; Karl Koch
 - Quebraram o TouchID (iPhone 5s)
- CdC → Cult of Dead Cow (1984)
 - BackOrifice (insegurança Win98)
- LoD → Legion of Doom (1984-1990)
 - Jornais técnicos para disseminar conhecimento
 - Hackers e Phreakers
- MoD → Masters of Deception
 - Dissidência da LoD; fim dos 80's-1993
- LoD/MoD
 - Perseguidos pelo FBI e serviço secreto
 - Processados e presos/condicional
 - Mark Abene, a.k.a *Phiber Optik*



■ (1 ano preso, 3 cond., 600h serviços comunitários)

Clifford Stoll



- . Astrônomo, começou a trabalhar como administrador de redes no LBNL (1986)
- . Problema:
 - erro de **contabilidade** de 75 cents → usuário não autorizado usufruiu de **9 segundos** de tempo de computador sem pagar!
 - como o sistema de cobrança poderia falhar?
- . Causa:
 - conta de usuário sem centro de custo atrelado
 - invasão de uma conta de superusuário “inativa”

Clifford Stoll



- Investigação envolveu “morar” no LBL aos fins de semana e conectar os terminais com impressoras para traçar a origem do intruso
- Conexão via modem; impressão dos comandos dados pelo intruso:
 - Uso do computador invadido como trampolim
 - Busca por arquivos com palavras-chave:
 - SDI (*Strategic Defense Initiative*)
 - Nuclear, NORAD
 - KH-11 (satélite espião americano)

(KH-11)



1. Construção de porta-aviões em Kiev
2. Bombardeiro chinês
3. Fábrica de fármacos no Sudão

Clifford Stoll

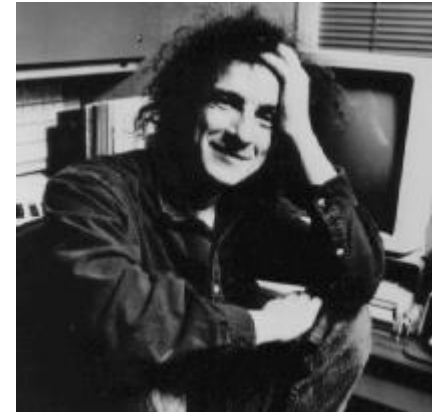


- Descobriu que o atacante fazia ataques de dicionário que funcionavam mesmo em redes militares → **senhas padrão não modificadas!**
 - Usuário *guest* sem senha
- Várias agências contactadas:
 - NSA, CIA, Força Aérea (investigações especiais)
 - FBI não se interessou porque não havia uma quantia monetária substancial envolvida
- Auxiliado, traçou o intruso até a Alemanha Ocidental
- 1º *honeypot*: conta com dados falsos sobre contrato de mísseis para atrair o atacante.

Clifford Stoll



- Desfecho:
 - Stoll testemunhou contra Markus Hess na Alemanha, culpado por espionagem
 - Venda de informações para a KGB soviética



Hackers found guilty of selling computer codes

CELLE (West Germany), Fri. - Three West German hackers were found guilty yesterday of selling Western military computer codes to the Soviet KGB and given suspended sentences ranging from 14 months to two years.

Dirk Brzezinski, Peter Carl and Markus Hess were arrested in March after an investigation by US and West German officials revealed the three had obtained passwords and codes giving them access to key military and research computers in the United States, Western Europe and Japan.

A fourth man, 30-year-old Karl Koch, who was also arrested in the case, committed suicide in May.

At the trial, which began Jan 11, all three admitted guilt in obtaining the codes to sell them to a Soviet KGB agent in East Berlin.

In yesterday's decision, Chief Judge Leopold Spiller said the three were given suspended sentences because "it could not be proven that substantial damage had been done to the Federal Republic (West Germany) or its Nato partners". But Mr Spiller also said the three sold the computer codes for money.

Carl was sentenced to 24 months, Hess 20 months and Brzezinski 14 months.

All three men were freed on suspended sentences as long as they stay out of trouble with the law for the duration of their terms.

Carl, 35, told the court during the trial that he could only identify the KGB agent he dealt with as "Serge" and said he did not wish to reveal anything more about the Soviets in open court for fear of reprisals.

Court records show that Carl made at least 25 contacts with the Soviets and received a total 90,000 marks (about M\$144,000) for the computer information, which was split among the hackers, amateurs who figure out ways to access private computer systems.

Brzezinski, 30, told the court that Koch had the original idea of selling the information to the KGB.

According to Brzezinski, Koch claimed he had gained access to the US Defence Department general databank known as Optimus.

US and West German news media reported the hackers also gained access to a Nasa and a "Star Wars" research computer, and computers linked to nuclear weapons and energy research. . . AP



Dirk



Peter



Markus



Karl

"sucidou-se"

New Straits Times, 17/02/1990 →

Clifford Stoll



- Invasão no LBL ([estratégia do atacante](#))
 - Problema na configuração do *Emacs*¹ do LBL (`movemail` instalado com `SETUID root`) → **Má prática do *sysadmin*!**
 - **SETUID**: atributo para garantir direitos de acesso:
 - Usuário pode executar um programa com as permissões do *owner* do programa (e elevar privilégio) → **escalada se houver bug!**
 - Ex.: *ping*, *passwd*
 - O programa não foi projetado para isso, criando uma brecha:
 - Pôde ser utilizado para mover arquivos para qualquer lugar
 - O atacante substituiu o programa `atrun` e executou como root, criando uma conta administrativa (escalou privilégios)
 - `atrun`: roda serviços enfileirados periodicamente
 - O `atrun` modificado (Trojan) pelo atacante é o **ovo do cuco**.

¹https://www.gnu.org/software/emacs/manual/html_node/efaq/Security-risks-with-Emacs.html

Honeypots/Honeynet



- *Honeypot* passou a ser o nome do recurso computacional utilizado para “enganar” um atacante (e monitorar suas atividades)
- 1999 → Projeto Honeynet:
 - Pesquisa (análise de dados, KYE etc.)
 - Disseminação de conhecimento
 - Ferramentas para a comunidade
- Vários “capítulos” ao redor do globo
- GSoC (<https://www.honeynet.org/gsoc/>)

Robert T. Morris, Jr.



- . Estudante na Cornell University (PhD → CC)
- . Aos 23 anos, em 02/11/1988, liberou um programa na “Internet” a partir do MIT:
 - “**Objetivo**”: medir o tamanho da rede
 - Considerado o 1º *worm* da Internet
 - Internet da época = +- 60 mil computadores
 - . Ambiente de troca de informações
 - . Não havia preocupação com segurança
 - Infectou ~10% da rede
 - . Custo de desinfecção: USD 200–53 mil por *site* (prejuízos podem ter chegado a 10M)
 - . Experimento que deu errado...



Robert T. Morris, Jr.



- . Experimento que deu errado:
 - Problema de projeto
- . O *worm* não possuía código “malicioso”:
 - Não tinha comportamento destrutivo
 - Na corte, Morris explicou que queria mostrar as vulnerabilidades de segurança presentes na rede pela exploração de *bugs* que ele achou.
- . Professor no MIT
 - Sistemas Distribuídos



Robert T. Morris, Jr.



- . *Bugs* explorados para propagação:
 - `rsh` com mesmo usuário/senha local/remoto
 - *Buffer overflow* no `fingerd` → *shell* remoto
 - Sendmail com DEBUG → interpretou (executou) o corpo do e-mail (cópia do *worm* e comandos para compilar e executar)
- . *Bugs* presentes no Internet *worm*:
 - Verificava se já havia sido instalado
 - . Objetivo: evitar **cópias infinitas** no mesmo alvo, esgotando seus recursos
 - Para evitar contra-medida → resposta SIM falsa
 - . Programou uma taxa de 1/7 para **ignorar** a resposta

Robert T. Morris, Jr.



- 1º indiciado pelo *Computer Fraud and Abuse Act* de 1986:
 - Multa (10.050,00 dólares)
 - Liberdade condicional (3 anos)
 - Serviço comunitário (400 horas)
- Embora tenha tentado ocultar sua origem, ao ver que o experimento saiu do controle, buscou por ajuda e tentou avisar os *sysadmins*.
- Causou a criação do CERT na CMU pela DARPA



Software Engineering Institute
Carnegie Mellon

Kevin Mitnick



- . *a.k.a.* Condor. Famoso nos anos 90
 - Preso por 5 anos, +3 sem usar a Internet
- . Anos 70, aos 13, ônibus de graça em L.A.:
 - Engenharia social → descobriu onde comprar perfurador de cartões de ônibus
 - Mergulho no lixo → encontrou cartões de transferência não utilizados perto da garagem
- . Anos 80, prisões e liberdade condicional:
 - 1982: 1 ano de cond. → B&E PacBell; 6 meses prisão juvenil → uso ilegal dos PCs da USC
 - 1987: 3 anos de con. → B&E SCO
 - 1988: 1 ano de cadeia → B&E DEC + roubo de software



Kevin Mitnick



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: (NOC/ 3721460021)

NAME:MITNICK, KEVIN DAVID

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

DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:VAN HOUTS, 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:D02G02PM3104PM39PM9

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: 9311-1112-015A-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)336-6102; (24 hour telephone center) NLETS access code is VLSMOO00.

PROR. EDITIONS ARE OBSOLETE AND NOT TO BE USED

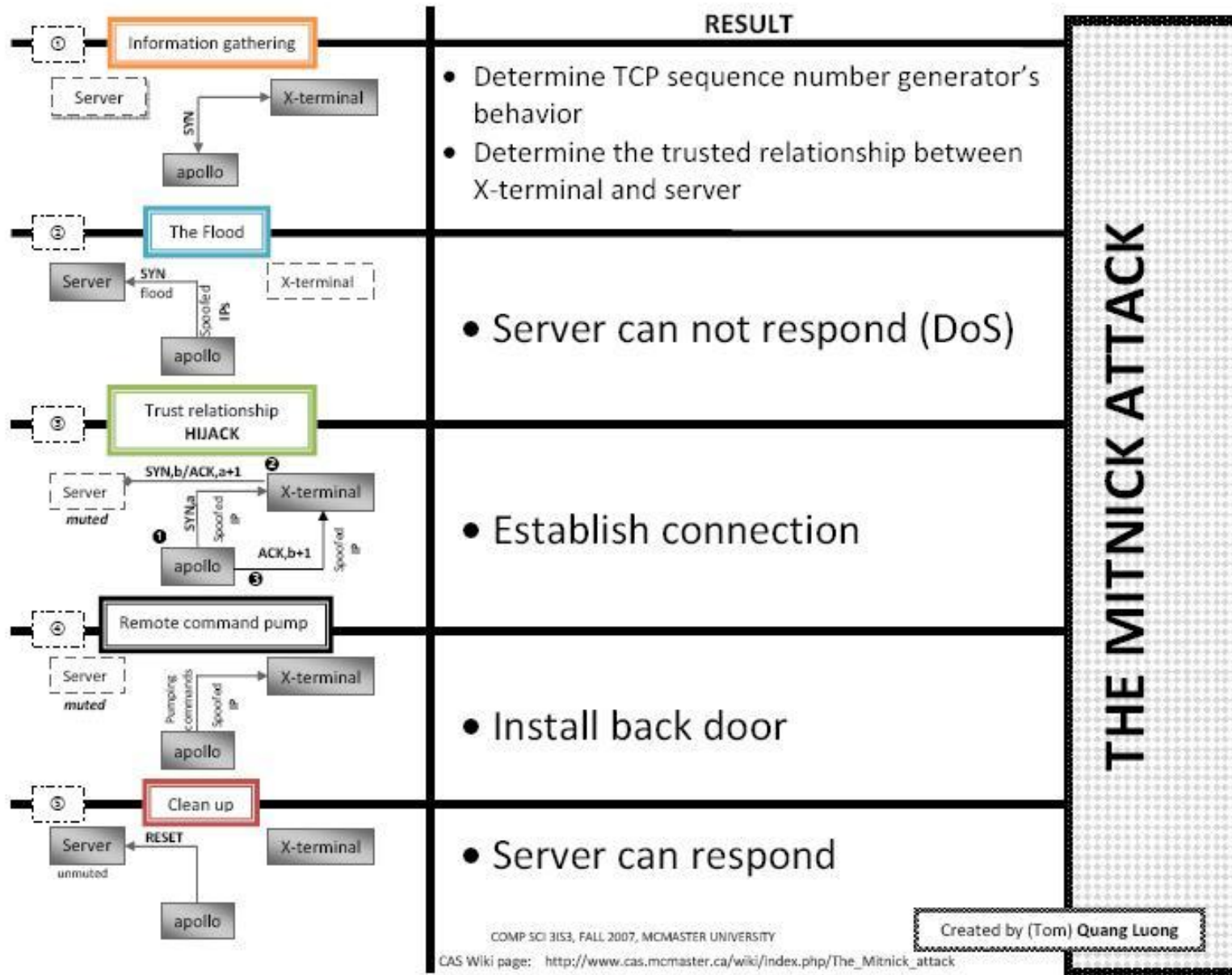
Form UTM-132
(Rev. 1/1982)

November 1992



- 1992: violação da condicional → fugitivo
- 1994: Procurado → Cal. DMV oferece **USD 1M** por sua cabeça (fraudes usando licença para dirigir)
- Natal de 94 → Acusado de invadir o San Diego Supercomputer Center
 - Preso em fev./1995 pelo FBI com o auxílio de Tsutomu Shimomura
 - Grampeou os agentes que o perseguiram
 - 100+ celulares clonados, IDs falsos
 - 8 meses na solitária porque o promotor convenceu o juiz de que ele podia **começar uma guerra nuclear da prisão assoviando em um telefone...**
 - Atualmente é consultor de segurança

Kevin Mitnick



Kevin Mitnick



OBITUARY

Kevin David Mitnick

AUGUST 6, 1963 – JULY 16, 2023



IN THE CARE OF

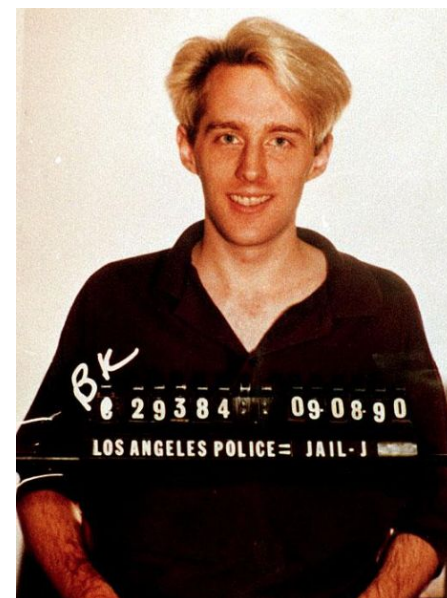
King David Memorial Chapel & Cemetery

<https://www.dignitymemorial.com/obituaries/las-vegas-nv/kevin-mitnick-11371668>

Kevin Poulsen



- *a.k.a.* Dark Dante
 - *Phreaker* nos anos 80/90, subverteu todas as linhas telefônicas de um rádio de LA → 102ª chamada ganhava um Porsche
 - Invadiu computadores federais e obteve informações de operações secretas do FBI
 - Preso em 1995 por fraudes, lavagem de \$, obstrução da justiça, invasão (pena: 51 meses de prisão e US\$ 51 mil de restituição)
 - Virou jornalista investigativo: SecurityFocus, Wired News, Threat Level:
 - Identificou 700+ “tarados” no MySpace
 - Cobriu a história de Bradley Manning e Adrian Lamo sobre WikiLeaks
 - Criou software para comunicação segura entre jornalistas e suas fontes (SecureDrop)



WikiLeaks (2006-...)



- [Adrian Lamo](#): preso por invasão do NYT, Yahoo! e Microsoft, dedurou Manning
- [Chelsea Manning](#): sentenciada em 2013 a 35 anos de prisão por violação do ato de espionagem e do CFAA
- [Julian Assange](#): exilado na Embaixada do Equador em Londres desde 2012 (anos 90: 25 acusações de *hacking* na Austrália)
- [Edward Snowden](#): Acusado de violação do ato de espionagem e roubo de propriedade do governo; exilado na Rússia (2012)



Vitek Boden



- Preso em 2001 após invadir o sistema de controle de esgoto em Queensland-AU
- 46 tentativas de ataque entre 03-04/2000
 - Milhões de litros de esgoto foram vazados
 - Morte de vida marinha, escurecimento de riachos, mau odor insuportável na cidade
 - Motivo: rejeitado em vaga de emprego
 - *Insider* → trabalhou na empresa que instalou o sistema computacional

<https://www.acsac.org/2008/program/case-studies/Abrams.pdf>

http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Stuxnet



- *Malware* descoberto no Irã em 2010
- Alvo: programa nuclear Iraniano-enriquecimento de urânio
- *Air gap* → *pendrive* usado para instalar código malicioso nos sistemas da usina (busca por *software* da Siemens)
 - 4 *zero-days*, *exploits*, certificados roubados, *rootkits* (um para PLC), destruição física de 1000 das 6000 centrífugas
- Atribuído aos **governos** dos EUA e Israel

National Security

Stuxnet was work of U.S. and Israeli experts, officials say

By Ellen Nakashima and Joby Warrick June 2, 2012

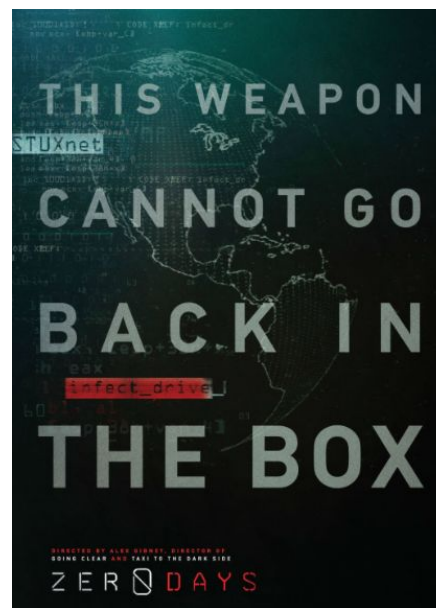
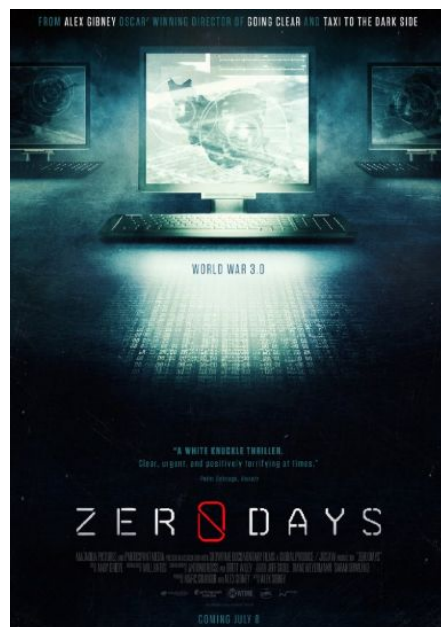


The Washington Post

Stuxnet



- Outro “experimento” que saiu do controle
- Documentário recente cobre a história
- <http://www.imdb.com/title/tt5446858/>



Hacktivismo



. Anonymous

- Criado em 2003
- DDoS coordenados contra *sites* de governos, religiosos e corporativos
- *Defacements* com vídeos



. Lulzsec

- Criado em 2011
- Invasões e exposição de credenciais e outras informações sensíveis
- Dissidentes do Anonymous



- . Derrubaram `brasil.gov.br`,
`presidencia.gov.br` e Petrobrás



Ataques recentes



. 2011

- Citigroup: 200K+ nomes, info de contato, contas de consumidores; roubo → 2,7M (CC)
- PSN: dezenas de milhões de usuários → info pessoal e de dados de cartão (crédito/débito)
 - . Dano estimado: 1 – 2 bilhões de dólares

. 2012

- Anonymous expõe e-mail de oficiais britânicos (militares, policiais, intel., OTAN)
- Tentativas de DoS a sites da Rio+20

Ataques recentes



. 2013

- *Defacement* (membro do Anonymous) em sites de partidos/governo de Singapura motivado por novas regras de censura para Web sites

. 2014

- JPMorgan Chase → 83M contas vazadas

. 2015

- *CyberCaliphate* tomou a programação da rede francesa TV5Monde
- CPF de militares do EB

Ataques recentes



. 2016

- Ransomware cresceu 172% só no 1s.
- Ataques contra instituições financeiras
 - . Banco de Bangladesh, SWIFT
- Mirai: DDoS via ELF malware em IoT
- Credential stuffing (500M+ contas de usuários comprometidas do Yahoo)
- Sequestro de VPN em cias de energia na Ucrânia (malware BlackEnergy apagou/crashou sistemas SCADA) → 3h, 250K consumidores afetados

Ataques recentes

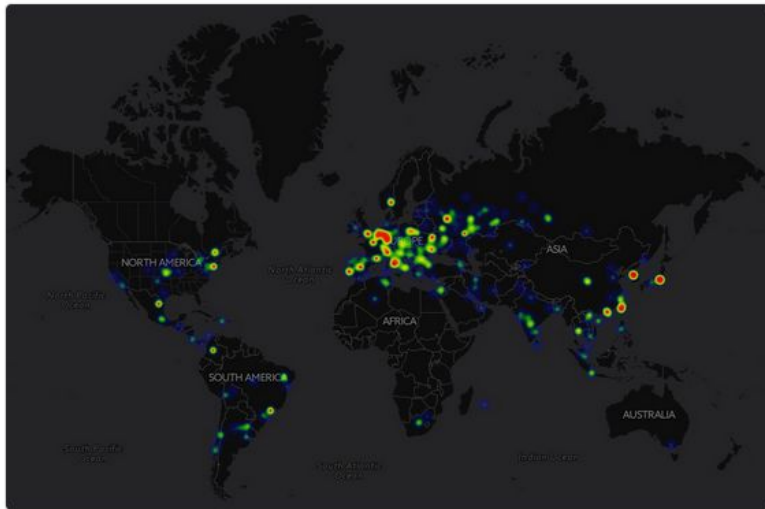


MalwareHunterTeam

@malwrhunterteam

Follow

Fresh IDR based heatmap for WanaCrypt0r 2.0 ransomware (WCry/WannaCry). Also follow @MalwareTechBlog's tracker: intel.malwaretech.com/botnet/wcrypt



11:07 AM - 12 May 2017

422 Retweets 235 Likes



2017

- Ataque cibernético por ransomware roubado do arsenal da NSA (WannaCry)
- Kaspersky registrou mais de 45K ataques em 99 países (UK, Rússia, Ucrânia, Índia, China, Itália, Egito, Espanha)
- Infectou hospitais e companhias telefônicas
- Já houve casos de pagamento (hosp. LA) em bitcoin como resgate (17K USD)
- Prefeituras brasileiras foram afetadas...

Ataques recentes



. 2017

- Verizon anuncia que todas as 3 bilhões de contas do Yahoo foram comprometidas
- ShadowBrokers disponibilizou vários gadgets da NSA → EternalBlue (Windows Server 2008/2012, Vista, 7, 8, 10)

. 2018

- UnderArmor (150M usernames/passwd/email)
- Facebook (87M de registros de usuários)

Ataques recentes



- 2019-2022:
 - *Ransomware*, vazamentos, *clouds*, IoT, 5G, *blockchain*, FinTechs, dados de **saúde**.
 - Companhias de defesa, energia e nuclear
 - Comprometimento da cadeia de suprimentos
 - Novos *ransomware*
 - Ataques com vulnerabilidades de vida curta

- https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf
- <https://www.kaspersky.com/blog/secure-futures-magazine/2020-cybersecurity-predictions/32068/>
- <https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-predictions-2019.pdf>
- <https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/>

Ataques recentes



- 2023:
 - *Ransomware-as-a-service*
 - <https://www.picussecurity.com/resource/blog/october-2023-key-threat-actors-malware-and-exploited-vulnerabilities>
 - Escalada de privilégio em nuvens
 - <https://aws.amazon.com/security/security-bulletins/AWS-2023-011/>
 - Evasão de mecanismos de segurança (autenticação, controle de acesso, anti-malware, anti-phishing, IDS)
 - <https://blog.qualys.com/qualys-insights/2023/09/26/qualys-survey-of-top-10-exploited-vulnerabilities-in-2023>
 - Impressão multi-dispositivo (*PaperCut*)
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a>

Alguns filmes

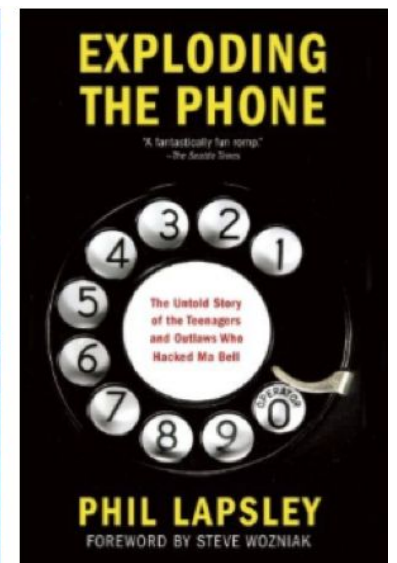
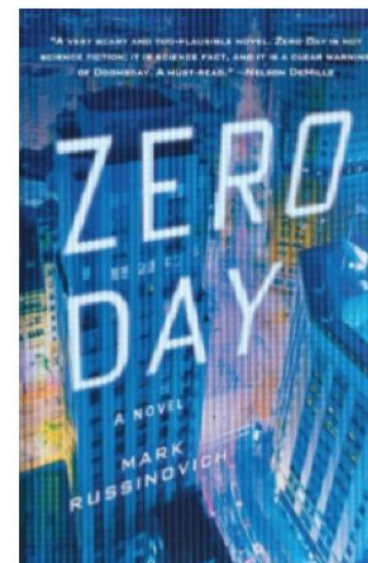
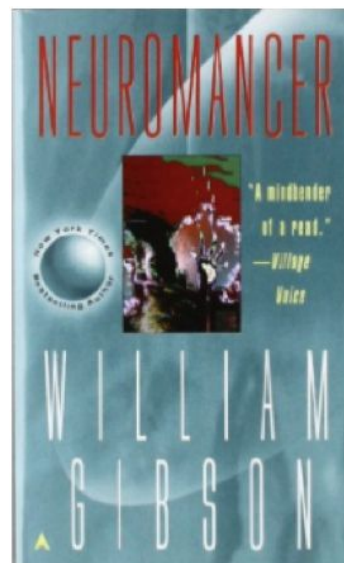
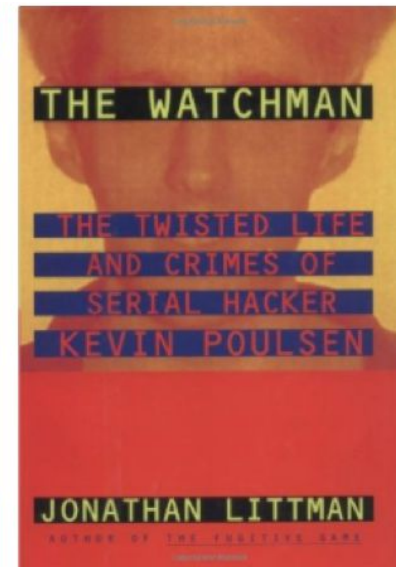
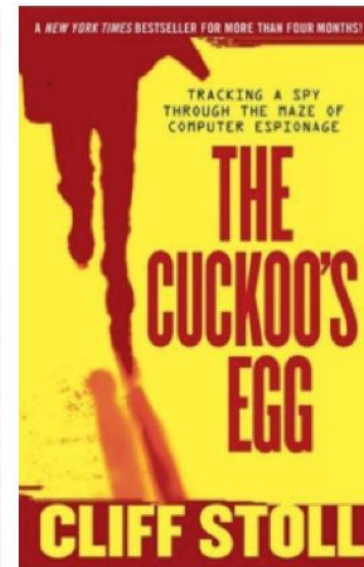
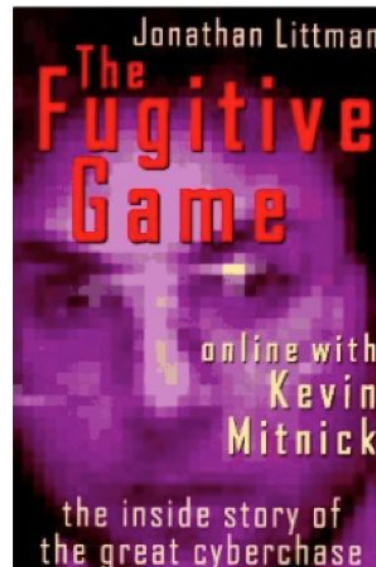


- WarGames (<http://www.imdb.com/title/tt0086567/>)
- Sneakers (<http://www.imdb.com/title/tt0105435/>)
- Hackers (<http://www.imdb.com/title/tt0113243/>)
- The Net (<http://www.imdb.com/title/tt0113957/>)
- Takedown (<http://www.imdb.com/title/tt0159784/>)
- Matrix (<http://www.imdb.com/title/tt0133093/>)
- Swordfish (<http://www.imdb.com/title/tt0244244/>)
- Privacidade Hackeada (Netflix)

Livros interessantes



- Fugitive game
- Cuckoo's egg
- Watchman
- Neuromancer
- Zero day
- Exploding the phone



Referências utilizadas



- http://www.slate.com/articles/technology/the_spectator/2011/10/the_article_that_inspired_steve_jobs_secrets_of_the_little_blue_.html
- <http://myoldmac.net/FAQ/TheBlueBox-1.htm>
- <http://www.blinkenlights.com/pc.shtml>
- <http://www.2600.com>
- <https://www.sans.org/reading>
- https://en.wikipedia.org/wiki/KH-11_Kennen
- <http://www.nytimes.com/1990/01/24/us/from-hacker-to-symbol.html?src=pm>
- <https://www.ccc.de/en/>
- <http://www.cultdeadcow.com>
- <http://www.wired.com/1994/04/phiber-optik-goes-to-prison/>
- <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/a-rundown-of-the-biggest-cybersecurity-incidents-of-2016>

Disclaimer



- . **Imagens:** o professor não detém os direitos sobre nenhuma imagem. Se alguém se sentir ofendido ou lesado pelo uso educacional de alguma das imagens utilizadas, favor entrar em contato que esta será retirada
- . *Hacking* pode ser crime!
 - Quase todos os indivíduos citados foram presos, ficaram em liberdade condicional, pagaram multas e/ou processados.
 - **No Brasil (Lei 12737 de 30/11/2012):**
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
- . O professor **não** incentiva ou recomenda, e nem está de acordo com nenhuma prática que viole as legislações vigentes.

Avaliações



1. 2 provas escritas, 35 pontos cada
2. 1 apresentação de projeto, 20 pontos
3. N trabalhos práticos, 10 pontos total

- Comunicação: via Moodle da disciplina
- Horário de atendimento:
 - **SOMENTE COM AGENDAMENTO**

Projeto de Pesquisa - Participe!!!



VERIFICAÇÃO DE VIABILIDADE E DESAFIOS DA AUTENTICAÇÃO CONTÍNUA DE USUÁRIOS DE SISTEMAS COMPUTACIONAIS

Link para a página do projeto: <https://www.inf.ufpr.br/mfbotacin/pesquisa/>

[Download da Versão Linux/Desktop](#)

[Download da Versão Android](#)

