invotra
enabling evolution

Evolution of cyber security

invotra
enabling evolution

Invotra

Digital Workplace, Intranet and Extranet

700 bc

Scytale used by Greece and Rome to send messages

And kids ever since..

Image Source: https://commons.wikimedia.org/wiki/File:Skytale.png

1467

Alberti Cipher was impossible to break without knowledge of the method.

This was because the frequency distribution of the letters was masked and frequency analysis - the only known technique for attacking ciphers at that time was no help.

Image Source: https://commons.wikimedia.org/wiki/File:Alberti_cipher_disk.JPG

1797

The Jefferson disk, or wheel cypher as Thomas Jefferson named it, also known as the Bazeries Cylinder.

It is a cipher system using a set of wheels or disks, each with the 26 letters of the alphabet arranged around their edge.

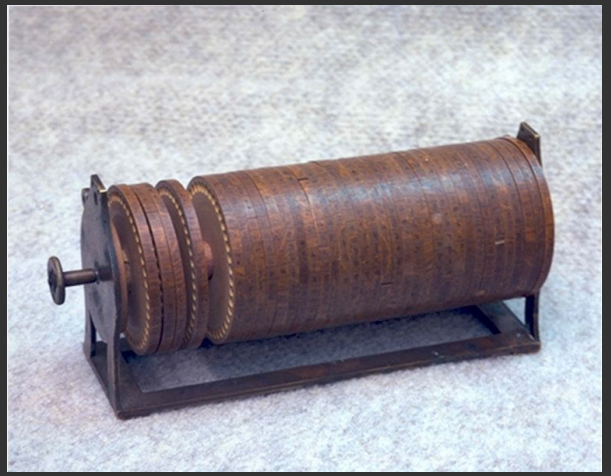


Image Source:
https://en.wikipedia.org/wiki/Jefferson_disk#/media/File:Jefferson%27s_disk_cipher.jpg

1833

Augusta Ada King-Noel, Countess of Lovelace was an English mathematician and writer, chiefly known for her work on Charles Babbage's proposed mechanical general-purpose computer, the Analytical Engine.

She is widely seen as the world's first programmer

Image Source: https://commons.wikimedia.org/wiki/File:Ada_Lovelace_portrait.jpg

1903

Magician and inventor Nevil Maskelyne interrupted John Ambrose Fleming's public demonstration of Marconi's purportedly secure wireless telegraphy technology.

He sent insulting Morse code messages through the auditorium's projector.

Image Source:
https://en.wikipedia.org/wiki/Nevil_Maskelyne_(magician)#/media/File:Nevil_Maskelyne_circa_1903.jpg

1918

The **Enigma Machine**.

It was developed by Arthur Scherbius in 1918 and adopted by the German government and the nazi party

Image Source: https://commons.wikimedia.org/wiki/File:Kriegsmarine_Enigma.png

1932

Polish cryptologists Marian Rejewski, Henryk Zygalski and Jerzy Różycki broke the Enigma machine code.

Germans eventually added more complexity and the polish could not keep up as it was too expensive.

Image Source: https://commons.wikimedia.org/wiki/File:MR_1932_small.jpg

1939

Alan Turing, Gordon Welchman and Harold Keen worked to develop the Bombe (on the basis of Rejewski's work).

The Enigma machine's use of a reliably small key space makes it vulnerable to brute force.

Image Source: https://commons.wikimedia.org/wiki/File:Alan_Turing_Aged_16.jpg

1943

René Carmille, comptroller general of the Vichy French Army, hacked the punched card system used by the Nazis to locate Jews.

Image Source: https://commons.wikimedia.org/wiki/File:Carmille.jpg

1949

The roots of the computer virus date back as early as 1949, when the Hungarian scientist John von Neumann published the "Theory of self-reproducing automata"

Image Source:https://en.wikipedia.org/wiki/File:JohnvonNeumann-LosAlamos.gif

1955

At MIT, “hack” first came to mean fussing with machines.

The minutes of an April, 1955, meeting of the Tech Model Railroad Club state that

"Mr. Eccles requests that anyone working or hacking on the electrical system turn the power off to avoid fuse blowing."

Image Source: unknown

1957

Joe "Joybubbles" Engressia, a blind seven-year-old boy with perfect pitch, discovered that whistling the fourth E above middle C would interfere with AT&T's telephone systems.

Inadvertently opening the door for phreaking.

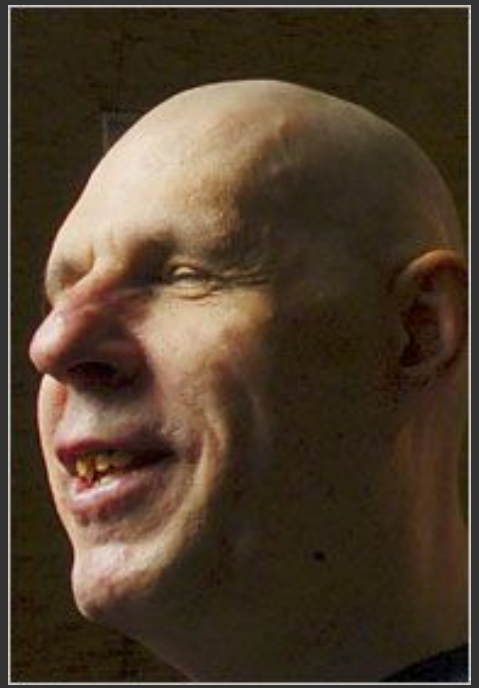
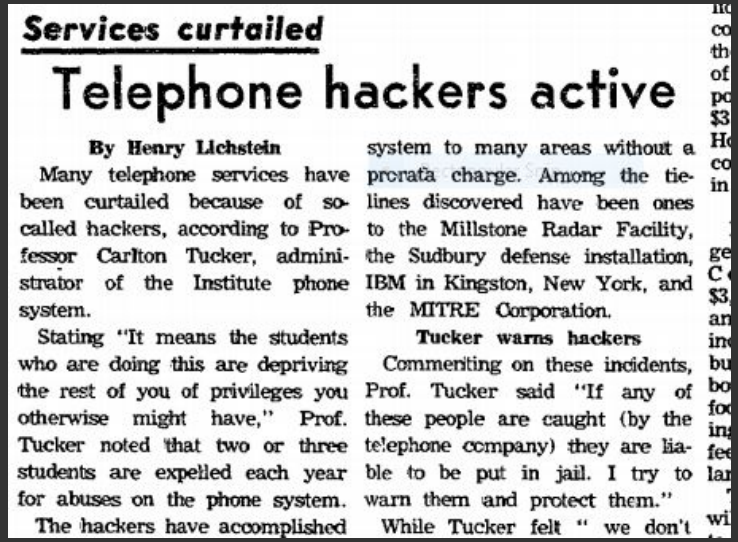


Image source: https://www.findagrave.com/cgi-bin/fg.cgi?page=mr&GRid=23683554&MRid=46480146&

1963

The first ever reference to malicious hacking is 'telephone hackers' in MIT's student newspaper,

The Tech of hackers trying up the lines with Harvard, configuring the PDP-1 to make free calls, war dialing and accumulating large phone bills.



Services curtailed

Telephone hackers active

By Henry Lichstein

Many telephone services have been curtailed because of so-called hackers, according to Professor Carlton Tucker, administrator of the Institute phone system.

Stating "It means the students who are doing this are depriving the rest of you of privileges you otherwise might have," Prof. Tucker noted that two or three students are expelled each year for abuses on the phone system.

The hackers have accomplished system to many areas without a prorata charge. Among the tie-lines discovered have been ones to the Millstone Radar Facility, the Sudbury defense installation, IBM in Kingston, New York, and the MITRE Corporation.

Tucker warns hackers

Commenting on these incidents, Prof. Tucker said "If any of these people are caught (by the telephone company) they are liable to be put in jail. I try to warn them and protect them."

While Tucker felt " we don't

Image Source: **http://tech.mit.edu/V83/PDF/V83-N24.pdf**

1965

William D. Mathews from MIT found a vulnerability in a CTSS running on an IBM 7094.

The standard text editor on the system was designed to be used by one user at a time, working in one directory, and so created a temporary file with a constant name for all instantiations of the editor.

The flaw was discovered when two system programmers were editing at the same time and the temporary files for the message-of-the day and the password file became swapped, causing the contents of the system CTSS password file to display to any user logging into the system.

Image Source: https://commons.wikimedia.org/wiki/File:IBM_7094_console2.agr.JPG

1971

John T. Draper (later nicknamed Captain Crunch), his friend Joe Engressia, and blue box phone phreaking hit the news with an Esquire Magazine feature story.

First known computer virus appeared in 1971 and was dubbed the "Creeper virus".This computer virus infected Digital Equipment Corporation's (DEC) PDP-10 mainframe

Image Source: https://commons.wikimedia.org/wiki/File:20151004_Captain_Crunch_at_Maker_Faire_Berlin_IMG_1282_by_sebaso.jpg

1979

Kevin Mitnick breaks into his first major computer system, the Ark.

The computer system Digital Equipment Corporation (DEC) used for developing their RSTS/E operating system software.

Image Source: https://commons.wikimedia.org/wiki/File:ROYAL_food,_NY.jpg

1980

New york times first reports on hackers as a result of the FBI going in to investigate a breach in NCSS (mainframe time sharing company)

Image Source: https://commons.wikimedia.org/wiki/File:The_New_York_Times_logo.png

1981

Chaos Computer Club forms in Germany.

Ian Murphy aka Captain Zap, was the first cracker to be tried and convicted as a felon. Murphy broke into AT&T's computers in 1981.

Image Source: unknown

1982

TCP/IP protocol suite is agreed.

Internet as we know it begins.

NSA “seem” to have influenced Vint Cerf and Bob Kahn to make sure that TCP/IP was not encrypted

Image Source:By Paul Morse - White House News & Policies photo (direct image URL [2])., Public Domain, https://commons.wikimedia.org/w/index.php?curid=2225190

1983

The cover story of Newsweek with the title "Beware: Hackers at play".

The group KILOBAUD.

The movie WarGames introduces the wider public.

In his Turing Award lecture, Ken Thompson mentions "hacking" and describes a security exploit that he calls a "Trojan horse".

Image Source : https://commons.wikimedia.org/wiki/File:The_game_screen_for_DEFCON.jpg

1984

Someone calling himself Lex Luthor founds the Legion of Doom.

The Comprehensive Crime Control Act gives the Secret Service jurisdiction over computer fraud.

Cult of the Dead Cow forms .

The hacker magazine 2600.

The Chaos Communication Congress, is held in Hamburg, Germany.

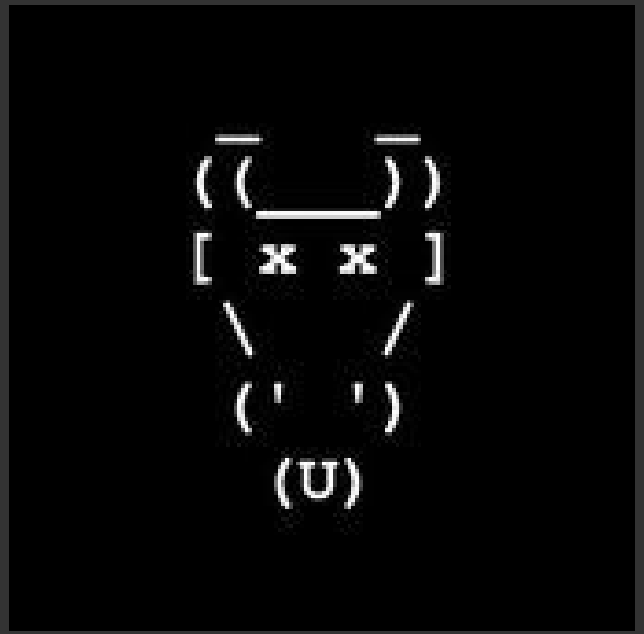


Image Source: cdc

1985

The online 'zine Phrack is established.

The Hacker's Handbook is published in the UK

The FBI, Secret Service, Middlesex County NJ Prosecutor's Office and various local law enforcement agencies execute seven search warrants concurrently across New Jersey under a newly passed criminal statute.

Image Source: http://www.phrack.org/

1986

The first IBM PC compatible "in the wild" computer virus, and one of the first real widespread infections, was "Brain"

Robert Schifreen and Stephen Gold are convicted under the Forgery and Counterfeiting Act 1981 in the United Kingdom

The Mentor arrested. He published a now-famous Hacker's Manifesto in the e-zine Phrack.

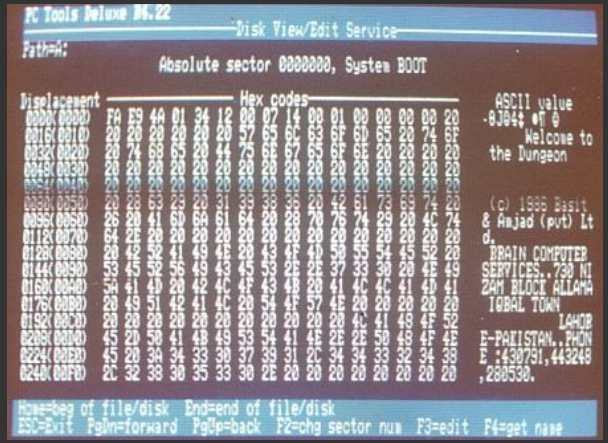


Image Source: https://en.wikipedia.org/wiki/Brain_(computer_virus)

1987

The Christmas Tree EXEC "worm" causes major disruption to the VNET, BITNET and EARN networks.

McAfee founded McAfee Associates

Image Source:
https://commons.wikimedia.org/wiki/File:John_McAfee_Def_Con_(14902350795).jpg

1988

The Morris Worm spreads to 6,000 networked computers, clogging government and university systems.

First National Bank of Chicago is the victim of $70-million computer theft.

The Computer Emergency Response Team (CERT) is created by DARPA to address network security.

The Father Christmas (computer worm) spreads over DECnet networks

Image Source: unknown

1989

Jude Milhon launches Mondo 2000 in Berkeley, California.

The politically motivated WANK worm spreads over DECnet.

Dutch magazine Hack-Tic begins.

The detection of AIDS (Trojan horse) is the first instance of a ransomware detection.

1989 - Quantum cryptography experimentally demonstrated in a proof-of-the-principle experiment by Charles Bennett et al.

Tim Berners-Lee initiates HTTP protocol

Image Source:By Trescabehling - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=48652371

1990

Operation Sundevil introduced in 14 U.S. cities.

The Electronic Frontier Foundation is founded

Electron and Nom are the first in the world to use a remote data intercept to gain evidence for a computer crime prosecution.

The Computer Misuse Act 1990 is passed in the United Kingdom, criminalising any unauthorised access to computer systems.

Image Source: https://commons.wikimedia.org/wiki/File:EFF-logo-plain-black.svg

1991

Kevin Poulsen Arrested

He took over all of the telephone lines for Los Angeles radio station KIIS-FM, guaranteeing that he would be the 102nd caller and win the prize of a Porsche 944

Phil Zimmermann releases the public key encryption program PGP along with its source code, which quickly appears on the Internet.

Image Source: police

1992

Release of the movie Sneakers, in which security experts are blackmailed into stealing a universal decoder for encryption systems.

One of the first ISPs MindVox opens to the public.

Bulgarian virus writer Dark Avenger wrote 1260, the first known use of polymorphic code..

Image Source:
https://commons.wikimedia.org/wiki/File:Dan_Aykroyd_wearing_an_Alekas_Attic_T-Shirt_in_the_Movie_%22Sneakers%22.jpg

1993

The first DEF CON hacking conference takes place in Las Vegas.

AOL gives its users access to Usenet.

Image Source: By ArnoldReinhold - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=50713931

1994

Russian crackers siphon $10 million from Citibank lead by Vladimir Levin

AOHell is released,

IP spoofing attack by Kevin Mitnick, on expert Tsutomu Shimomura started "My kung fu is stronger than yours".

RC4 cipher algorithm is published on the Internet

SSL encryption protocol released by Netscape.

Image Source: **https://www.computerhope.com/people/vladimir_levin.htm**

1995

The movies The Net and Hackers are released.

The FBI raids the "Phone Masters".

Vladimir Levin arrested

Kevin Mitnick Arrested

NSA publishes the SHA1 hash algorithm as part of its Digital Signature Standard.

Image Source: https://commons.wikimedia.org/wiki/File:Lamo-Mitnick-Poulsen.png

1996

Hackers alter sites of the US Department of Justice, CIA , Air Force.

Hackers attempted to break into Defense Department 250,000. times in 1995 alone. About 65 percent of the attempts were successful

The MP3 format gains popularity.

Cryptovirology is born, later form the basis of modern ransomware.

Image Source: https://commons.wikimedia.org/wiki/File:MP3_logo.png

1997

A 15-year-old Croatian youth penetrates computers at a U.S. Air Force base in Guam.

First high-profile attacks on Microsoft's Windows NT operating system

OpenPGP specification (RFC 2440) released

Digital Millennium Copyright Act (DMCA) becomes law

First definition of HTTP/1.1

Image Source: By U.S. Government - Extracted from PDF version of Our Flag, available here (direct PDF URL here.), Public Domain, https://commons.wikimedia.org/w/index.php?curid=41373752

1998

Natasha Grigori was one of the pioneers of the female hacking, started found antichildporn.org.

The Internet Software Consortium proposes the use of DNSSEC.

L0pht testify in front of the US congress

Information Security publishes Survey, finding that nearly three-quarters of organizations suffered a security incident in the previous year

Hacking exposed published

Image Source: unknown

1999

Everyone hacked Windows 98

Bill Clinton announces a $1.46 billion initiative to improve government computer security.

The "Legion of the Underground" declares "war" against Iraq & China.

The Melissa worm is released and quickly becomes the most costly malware outbreak to date.

July: Cult of the Dead Cow releases Back Orifice 2000 at DEF CON.

Image Source: By Bob McNeely, The White House

2000

The ILOVEYOU worm infected millions of computers

Jonathan James became the first juvenile to serve jail time for hacking.

U.S. Government announce restrictions on export of cryptography

RSA Security Inc. released their RSA algorithm into the public domain,

UK Regulation of Investigatory Powers Act requires anyone to supply their cryptographic key to a duly authorized person on request

Image Source: unknown

2001

DNS paths that take users to Microsoft's websites are corrupted.

Dutch cracker releases the Anna Kournikova virus

Russian programmer Dmitry Sklyarov is arrested at the annual Def Con hacker convention (DMCA).

Belgian Rijndael algorithm selected as the U.S. Advanced Encryption Standard (AES)

Microsoft and its allies vow to end "full disclosure" of security vulnerabilities by replacing it with "responsible" disclosure guidelines

Image Source: https://commons.wikimedia.org/wiki/File:Dmitry_Sklyarov_it-sa_2010.jpg

2002

Bill Gates decrees that Microsoft will secure its products and services.

Klez.H, becomes the biggest malware outbreak in terms of machines infected.

Chris Paget publishes "shatter attacks", detailing how Windows' unauthenticated messaging system can be used to take over a machine.

The International Information Systems Security Certification Consortium - $(ISC)^2$ - confers its 10,000th CISSP certification.

PGP Corporation formed, purchasing assets from NAI.

Image Source: https://commons.wikimedia.org/wiki/File:Bill_Gates_June_2015.jpg

2003

The hacktivist group Anonymous was formed.

Cult of the Dead Cow and Hacktivismo are given permission by the United States Department of Commerce to export software utilizing strong encryption.

Adrian Lamo Alias: The Homeless Hacker arrested

Kim Vanvaeck arrested

HD Moore builds metasploit

Image Sources: unknown

2004

North Korea claims to have trained 500 hackers who successfully crack South Korean, Japanese, and their allies' computer systems.

The hash MD5 is shown to be vulnerable to practical collision attack

The first commercial quantum cryptography system becomes available from id Quantique.

Image Source:
https://commons.wikimedia.org/wiki/File:North_Korea-Rungrado_May_Day_Stadium-01.jpg

2005

Rafael Núñez (aka RaFa) arrested for breaking into the Defense Information Systems Agency computer system

Gary Mckinnon arrested for hacking US Military and NASA over 13 months.

Potential for attacks on SHA1 demonstrated

Agents from the U.S. FBI demonstrate their ability to crack WEP using publicly available tools

Image Source: https://commons.wikimedia.org/wiki/File:Gary_McKinnon.jpg

2006

Joanna Rutkowska presents vista hack at Black Hat Briefings conference in Las Vegas

Jeanson James Ancheta receives a 57-month prison sentence, and is ordered to pay damages amounting to $15,000.00 for damage done due to DDoS attacks and hacking.

The largest defacement in Web History as of that time is performed by the Turkish hacker iSKORPiTX who successfully hacked 21,549 websites in one shot.

Image Source:
https://commons.wikimedia.org/wiki/File:LinuxCon_Europe_Joanna_Rutkowska_01.jpg

2007

CN Girl Security Team come to the fore lead by Xiao Tian

FBI Operation Bot Roast finds over 1 million botnet victims

A spear phishing incident at the Office of the Secretary of Defense steals sensitive U.S. defense information, leading to significant changes in identity and message-source verification at OSD.

United Nations website hacked by Turkish Hacker Kerem125.

Image Source: http://wikis.fdi.ucm.es/ELP/Xiao_Tian

2008

Anonymous attacks Scientology website servers around the world.

Around 20 Chinese hackers claim to have gained access to the world's most sensitive sites, including The Pentagon. They operated from an apartment on a Chinese Island.

Trend Micro website successfully hacked by Turkish hacker Janizary (aka Utku).

Owen Thor Walker - Alias: AKILL Arrested

Image Source:
http://seputtarinternet.blogspot.co.uk/2016/01/15-hacker-paling-berbahaya-di-dunia.html

2009

Conficker worm infiltrated millions of PCs worldwide including many government-level top-security computer networks.

Bitcoin network was launched.

Hackers steal data on Pentagon's newest fighter jet

Twitter becomes major target for enumeration attack, Obama account hacked.

Defcon attendees hacked by atm

Image Source: http://thechive.com/2011/01/14/atm-wtf-18-photos/

2010

Stuxnet The Stuxnet worm is found by VirusBlokAda became clear that it was a cyber attack on Iran's nuclear facilities.

The first Malware Conference, MALCON took place in India. Founded by Rajshekhar Murthy.

Anna Chapman and Kristina Vladimirovna Svechinskaya- Arrested

The master key and the private signing key for the Sony PlayStation 3 game console are recovered and published using separate

Image Source: https://www.soldierx.com/hdb/Kristina-Vladimirovna-Svechinskaya
https://commons.wikimedia.org/wiki/File:Anna_Chapman_2011_at_the_iCamp_conference_in_Kazan_(Tatarstan,_Russia)_008.jpg

2011

The hacker group Lulz Security is formed.

Bank of America hacked, 85,000 credit card numbers and accounts stolen.

Computer hacker sl1nk releases information of his penetration in the servers of the Department of Defense (DoD), Pentagon, NASA, NSA, US Military, Department of the Navy, Space and Naval Warfare System Command etc.

TiGER-M@TE made a world record in defacement history by hacking 700,000 websites in a single shot.

The YouTube channel of Sesame Street was hacked, streaming pornographic content for about 22 minutes.

Image Source: https://en.wikipedia.org/wiki/File:Lulz_Security.svg

2012

Iranian hackers retaliate by releasing Shamoon, a virus that damages 35,000 Saudi AramCo computers

A Saudi hacker, 0XOMAR, published over 400,000 credit cards online

Israeli hacker published over 200 Saudi's credit cards online.

The social networking website LinkedIn has been hacked and the passwords for nearly 6.5 million user accounts are stolen by cybercriminals

Image Source:http://www.ibtimes.co.uk/arab-israel-cyberwar-0xomar-ministry-construction-opfreepalestine-298238

2013

The social networking website Tumblr is attacked by hackers , 65,469,298 unique emails and passwords were leaked from Tumblr.

Raven Alder presents at defcon

Dual_EC_DRBG is discovered to have a NSA backdoor.

NSA publishes Simon and Speck lightweight block ciphers.

Edward Snowden discloses a vast trove of classified documents from NSA.

Image Source: http://yegs.org/yegs-hall-of-fame-raven-alder-1976-2/

2014

The bitcoin exchange Mt.Gox filed for bankruptcy after $460 million was apparently stolen by hackers due to "weaknesses in [their] system" and another $27.4 million went missing from its bank accounts.

The White House computer system was hacked It was said that the FBI, the Secret Service, and other U.S. intelligence agencies categorized the attacks "among the most sophisticated attacks ever

The website of the Philippine telecommunications company Globe Telecom was hacked to acquaint for the poor internet service they are distributing.

Image Source: https://commons.wikimedia.org/wiki/File:MtGox.png

2015

Kaspersky labs hacked.

the records of 21.5 million people, including social security numbers, dates of birth, addresses, fingerprints, and security-clearance-related information, are stolen from the United States Office of Personnel Management.

The Wall Street Journal and the Washington Post report that government sources believe the hacker is the government of China.

The servers of extramarital affairs website Ashley Madison were breached

Image Source: https://en.wikipedia.org/wiki/Eugene_Kaspersky#/media/File:Eugene_Kaspersky_-_Kaspersky_Lab.jpg

2016

The 2016 Bangladesh Bank heist attempted to take US$951 million from Bangladesh Bank, and succeeded in getting $101 million - although some of this was later recovered.

Wikileaks published the documents from the 2016 Democratic National Committee email leak.

US Election hacked

The 2016 Dyn cyberattack is being conducted with a botnet consisting of IOTs infected with Mirai

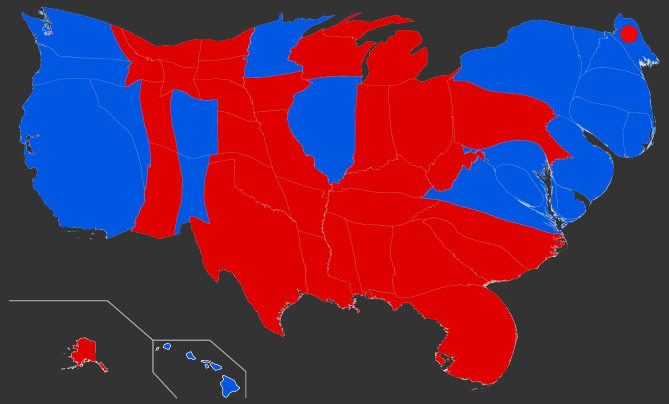


Image Source: By Ali Zifan - Own work by using ArcGIS., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=53232016

2017

A hacker group calling itself "The Dark Overlord" posted unreleased episodes of Orange Is the New Black from Netflix.

May: WannaCry ransomware attack started on Friday, 12 May 2017, and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries.

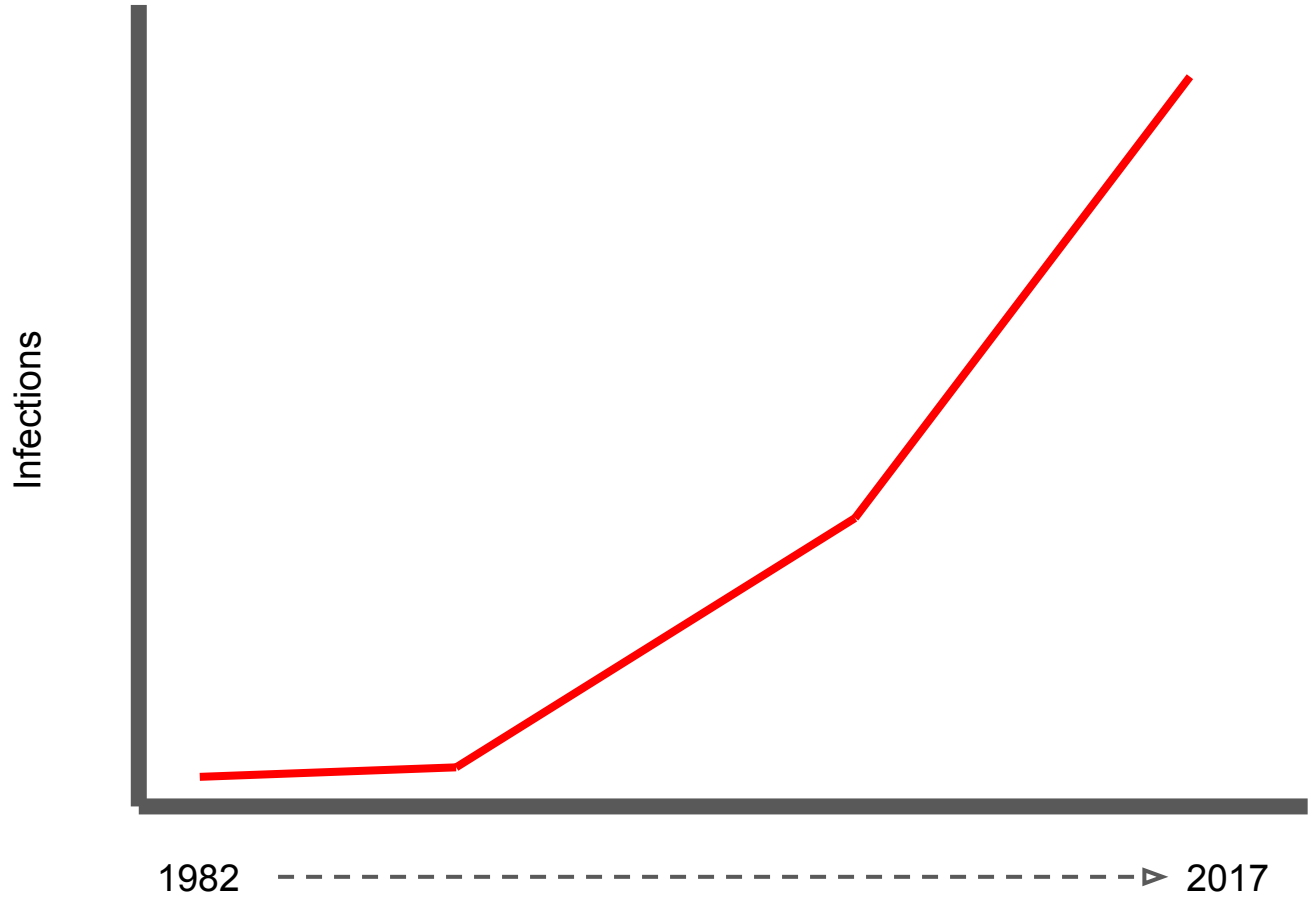
Petya cyberattack brings ransomware mainstream and takes out NHS and others

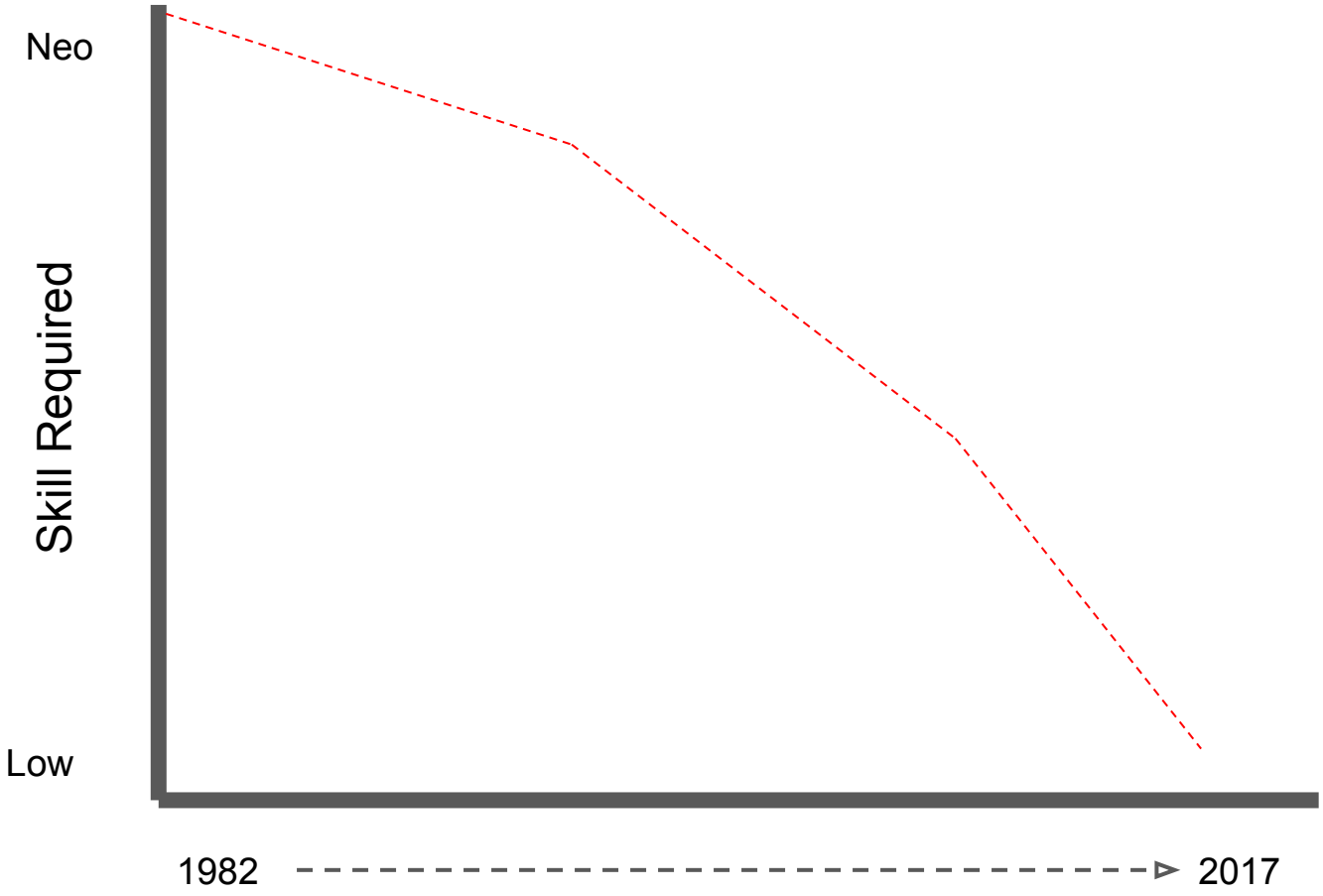
Equifax Hack (more this afternoon)

Las Vegas Casino Hack with a fishtank

Image Source:
https://commons.wikimedia.org/wiki/File:Fish_Tank_@_Honolulu_Aquarium_(4671604664).jpg

invotra
enabling evolution




Neo
Skill Required
Low
1982
2017

invotra
enabling evolution

http://map.norsecorp.com/#/

Thank you....

invotra
enabling evolution

Fintan Galvin
CEO Invotra
Twitter: @suncao
Linkedin: https://www.linkedin.com/in/johnfgalvin
Blogs: https://www.invotra.com/users/fintan-galvin

Digital Workplace, Intranet and Extranet

invotra
enabling evolution

Invotra

Digital Workplace, Intranet and Extranet