Security hacker

A **security hacker** is someone who explores methods for breaching defenses and exploiting weaknesses in a computer system or network.[1] Hackers may be motivated by a multitude of reasons, such as profit, protest, information gathering,[2] challenge, recreation,[3] or evaluation of a system weaknesses to assist in formulating defenses against potential hackers. The subculture that has evolved around hackers is often referred to as the "computer underground".[4]

Longstanding controversy surrounds the meaning of the term "hacker". In this controversy, computer programmers reclaim the term *hacker*, arguing that it refers simply to someone with an advanced understanding of computers and computer networks[5] and that ***cracker*** is the more appropriate term for those who break into computers, whether computer criminals (black hats) or computer security experts (white hats).[6][7] A 2014 article noted that "the black-hat meaning still prevails among the general public".[8]

History

Bruce Sterling, author of *The Hacker Crackdown*

Birth of subculture and entering mainstream: 1960's-1980's

The subculture around such hackers is termed network hacker subculture, hacker scene, or computer underground. It initially developed in the context of phreaking during the 1960s and the microcomputer BBS scene of the 1980s. It is implicated with *2600: The Hacker Quarterly* and the *alt.2600* newsgroup.

In 1980, an article in the August issue of *Psychology Today* (with commentary by Philip Zimbardo) used the term "hacker" in its title: "The Hacker Papers". It was an excerpt from a Stanford Bulletin Board discussion on the addictive nature of computer use. In the 1982 film *Tron*, Kevin Flynn (Jeff Bridges) describes his intentions to break into ENCOM's computer system, saying "I've been doing a little hacking here". CLU is the software he uses for this. By 1983, hacking in the sense of breaking computer security had already been in use as computer jargon,[9] but there was no public awareness about such activities.[10] However, the release of the film *WarGames* that year, featuring a computer intrusion into NORAD, raised the public belief that computer security hackers (especially teenagers) could be a threat to national security. This concern became real when, in the same year, a gang of teenage hackers in Milwaukee, Wisconsin, known as The 414s, broke into computer systems throughout the United States and Canada, including those of Los Alamos National Laboratory, Sloan-Kettering Cancer Center and Security Pacific Bank.[11] The case quickly grew media attention,[11][12] and 17-year-old Neal Patrick emerged as the spokesman for the gang, including a cover story in *Newsweek* entitled "Beware: Hackers at play", with Patrick's photograph on the cover.[13] The *Newsweek* article appears to be the first use of the word *hacker* by the mainstream media in the pejorative sense.

Pressured by media coverage, congressman Dan Glickman called for an investigation and began work on new laws against computer hacking.[14][15] Neal Patrick testified before the U.S. House

of Representatives on September 26, 1983, about the dangers of computer hacking, and six bills concerning computer crime were introduced in the House that year.[15] As a result of these laws against computer criminality, white hat, grey hat and black hat hackers try to distinguish themselves from each other, depending on the legality of their activities. These moral conflicts are expressed in The Mentor's "The Hacker Manifesto", published 1986 in *Phrack*.

Use of the term hacker meaning computer criminal was also advanced by the title "Stalking the Wily Hacker", an article by Clifford Stoll in the May 1988 issue of the *Communications of the ACM*. Later that year, the release by Robert Tappan Morris, Jr. of the so-called Morris worm provoked the popular media to spread this usage. The popularity of Stoll's book *The Cuckoo's Egg*, published one year later, further entrenched the term in the public's consciousness.

Classifications

In computer security, a hacker is someone who focuses on security mechanisms of computer and network systems. Hackers can include someone who endeavors to strengthen security mechanisms by exploring their weaknesses and also those who seek to access secure, unauthorized information despite security measures. Nevertheless, parts of the subculture see their aim in correcting security problems and use the word in a positive sense. White hat is the name given to ethical computer hackers, who utilize hacking in a helpful way. White hats are becoming a necessary part of the information security field.[16] They operate under a code, which acknowledges that breaking into other people's computers is bad, but that discovering and exploiting security mechanisms and breaking into computers is still an interesting activity that can be done ethically and legally. Accordingly, the term bears strong connotations that are favorable or pejorative, depending on the context.

Subgroups of the computer underground with different attitudes and motives use different terms to demarcate themselves from each other. These classifications are also used to exclude specific groups with whom they do not agree.

Cracker

Eric S. Raymond, author of *The New Hacker's Dictionary*, advocates that members of the computer underground should be called crackers. Yet, those people see themselves as hackers and even try to include the views of Raymond in what they see as a wider hacker culture, a view that Raymond has harshly rejected. Instead of a hacker/cracker dichotomy, they emphasize a

spectrum of different categories, such as white hat, grey hat, black hat and script kiddie. In contrast to Raymond, they usually reserve the term *cracker* for more malicious activity.

According to Ralph D. Clifford, a *cracker* or *cracking* is to "gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system".[17] These subgroups may also be defined by the legal status of their activities.[18]

White hat

A white hat hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client, or while working for a security company which makes security software. The term is generally synonymous with ethical hacker, and the EC-Council,[19] among others, have developed certifications, courseware, classes, and online training covering the diverse arena of ethical hacking.[18]

Black hat

A black hat hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005).[20] The term was coined by Richard Stallman, to contrast the maliciousness of a criminal hacker versus the spirit of playfulness and exploration in hacker culture, or the ethos of the white hat hacker who performs hacking duties to identify places to repair or as a means of legitimate employment.[21] Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".[22]

Grey hat

A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.[22] Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

Elite hacker

A social status among hackers, *elite* is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.[23]

Script kiddie

A script kiddie (also known as a *skid* or *skiddie*) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), hence the term script (i.e. a computer script that automates the hacking) kiddie (i.e. kid, child an individual lacking knowledge and experience, immature),[24] usually with little understanding of the underlying concept.

Neophyte

A neophyte ("newbie", or "noob") is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.[22]

Blue hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term *BlueHat* to represent a series of security briefing events.[25][26][27]

Hacktivist

A hacktivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

Hacktivism can be divided into two main groups:

- Cyberterrorism – Activities involving website defacement or denial-of-service attacks; and,
- Freedom of information – Making information that is not public, or is public in non-machine-readable formats, accessible to the public.

Nation state

Intelligence agencies and cyberwarfare operatives of nation states.[28]

Organized criminal gangs

Groups of hackers that carry out organized criminal activities for profit.[28] Modern-day computer hackers have been compared to the privateers of by-gone days.[29] These criminals hold computer systems hostage, demanding large payments from victims to restore access to their own computer systems and data.[30] Furthermore, recent ransomware attacks on industries, including energy, food, and transportation, have been blamed on criminal organizations based in or near a state actor – possibly with the country's knowledge and approval.[31] Cyber theft and ransomware attacks are now the fastest-growing crimes in the United States.[32] Bitcoin and other cryptocurrencies facilitate the extortion of huge ransoms from large companies, hospitals and city governments with little or no chance of being caught.[33]

Attacks

Hackers can usually be sorted into two types of attacks: mass attacks and targeted attacks.[34] They are sorted into the groups in terms of how they choose their victims and how they act on the attacks.[34]

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.[35]

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness.[36] Common examples of security exploits are SQL injection, cross-site scripting and cross-site request forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through File Transfer Protocol (FTP), Hypertext

Transfer Protocol (HTTP), PHP, SSH, Telnet and some Web pages. These are very common in Web site and Web domain hacking.

Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

Finding vulnerabilities

Hackers may also attempt to find vulnerabilities manually. A common approach is to search for possible vulnerabilities in the code of the computer system then test them, sometimes reverse engineering the software if the code is not provided. Experienced hackers can easily find patterns in code to find common vulnerabilities.

Brute-force attack

Password guessing. Brute-force attacks are very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used, because of the time a brute-force search takes.[37]

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. Common approaches include repeatedly trying guesses for the password, trying the most common passwords by hand, and repeatedly trying passwords from a "dictionary", or a text file with many passwords.[38]

Packet analyzer

A packet analyzer ("packet sniffer") is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a trusted system by a user or another program – usually to fool programs, systems or users into revealing confidential information, such as user names and passwords.

Rootkit

A rootkit is a program that uses low-level, hard-to-detect methods to subvert control of an operating system from its legitimate operators. Rootkits usually obscure their installation and attempt to prevent their removal through a subversion of standard system security. They may include replacements for system binaries, making it virtually impossible for them to be detected by checking process tables.

Social engineering

In the second stage of the targeting process, hackers often use social engineering tactics to get enough information to access the network. They may contact the system administrator and pose as a user who cannot get access to his or her system. This technique is portrayed in the 1995 film *Hackers*, when protagonist Dade "Zero Cool" Murphy calls a somewhat clueless employee in charge of security at a television network. Posing as an accountant working for the same company, Dade tricks the employee into giving him the phone number of a modem so he can gain access to the company's computer system.

Hackers who use this technique must be familiar with their target's security practices in order to trick the system administrator into giving them information. In some cases, a help-desk employee with limited security experience will answer the phone and be relatively easy to trick. Another approach is for the hacker to pose as an angry supervisor, and when his/her authority is questioned, threaten to fire the help-desk worker. Social engineering is very effective, because users are the most vulnerable part of an organization. No security devices or programs can keep an organization safe if an employee reveals a password to an unauthorized person.

Social engineering can be broken down into four sub-groups:

- ***Intimidation*** As in the "angry supervisor" technique above, the hacker convinces the person who answers the phone that their job is in danger unless they help them. At this point, many people accept that the hacker is a supervisor and give them the information they seek.
- ***Helpfulness*** The opposite of intimidation, helpfulness exploits many people's natural instinct to help others solve problems. Rather than acting angry, the hacker acts distressed and concerned. The help desk is the most vulnerable to this type of social engineering, as (a.) its general purpose is to help people; and (b.) it usually has the authority to change or reset passwords, which is exactly what the hacker wants.[39]
- ***Name-dropping*** The hacker uses names of authorized users to convince the person who answers the phone that the hacker is a legitimate user him or herself. Some of these names, such as those of webpage owners or company officers, can easily be obtained online. Hackers have also been known to obtain names by examining discarded documents ("dumpster diving").

- ***Technical*** Using technology is also a way to get information. A hacker can send a fax or email to a legitimate user, seeking a response that contains vital information. The hacker may claim that he or she is involved in law enforcement and needs certain data for an investigation, or for record-keeping purposes.

Trojan horses

A Trojan horse is a program that seems to be doing one thing but is actually doing another. It can be used to set up a back door in a computer system, enabling the intruder to gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder into a protected area.)

Computer virus

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. By doing this, it behaves similarly to a biological virus, which spreads by inserting itself into living cells. While some viruses are harmless or mere hoaxes, most are considered malicious.

Computer worm

Like a virus, a worm is also a self-replicating program. It differs from a virus in that (a.) it propagates through computer networks without user intervention; and (b.) does not need to attach itself to an existing program. Nonetheless, many people use the terms "virus" and "worm" interchangeably to describe any self-propagating program.

Keystroke logging

A keylogger is a tool designed to record ("log") every keystroke on an affected machine for later retrieval, usually to allow the user of this tool to gain access to confidential information typed on the affected machine. Some keyloggers use virus-, trojan-, and rootkit-like methods to conceal themselves. However, some of them are used for legitimate purposes, even to enhance computer security. For example, a business may maintain a keylogger on a computer used at a point of sale to detect evidence of employee fraud.

Attack patterns

Attack patterns are defined as series of repeatable steps that can be applied to simulate an attack against the security of a system. They can be used for testing purposes or locating potential vulnerabilities. They also provide, either physically or in reference, a common solution pattern for preventing a given attack.

Tools and Procedures

A thorough examination of hacker tools and procedures may be found in Cengage Learning's E|CSA certification workbook.[40]

Notable intruders and criminal hackers

Notable security hackers

- Andrew Auernheimer, sentenced to 3 years in prison, is a grey hat hacker whose security group Goatse Security exposed a flaw in AT&T's iPad security.
- Dan Kaminsky was a DNS expert who exposed multiple flaws in the protocol and investigated Sony's rootkit security issues in 2005. He spoke in front of the United States Senate on technology issues.
- Ed Cummings (also known as Bernie S) is a longstanding writer for *2600: The Hacker Quarterly*. In 1995, he was arrested and charged with possession of technology that could be used for fraudulent purposes, and set legal precedents after being denied both a bail hearing and a speedy trial.
- Eric Corley (also known as Emmanuel Goldstein) is the longstanding publisher of *2600: The Hacker Quarterly*. He is also the founder of the Hackers on Planet Earth (HOPE) conferences. He has been part of the hacker community since the late 1970s.
- Susan Headley (also known as Susan Thunder), was an American hacker active during the late 1970s and early 1980s widely respected for her expertise in social engineering, pretexting, and psychological subversion.[41] She became heavily involved in phreaking with Kevin Mitnick and Lewis de Payne in Los Angeles, but later framed them for erasing the system files at US Leasing after a falling out, leading to Mitnick's first conviction.[42]
- Gary McKinnon is a Scottish hacker who was facing extradition to the United States to face criminal charges. Many people in the UK called on the authorities to be lenient with McKinnon, who has Asperger syndrome. The extradition has now been dropped.[43]
- Gordon Lyon, known by the handle Fyodor, authored the Nmap Security Scanner as well as many network security books and web sites. He is a founding member of the Honeynet Project and Vice President of Computer Professionals for Social Responsibility.
- Guccifer 2.0, who claimed that he hacked into the Democratic National Committee (DNC) computer network
- Jacob Appelbaum is an advocate, security researcher, and developer for the Tor project. He speaks internationally for usage of Tor by human rights groups and others concerned about Internet anonymity and censorship.

- Joanna Rutkowska is a Polish computer security researcher who developed the Blue Pill rootkit and Qubes OS.
- Jude Milhon (known as St. Jude) was an American hacker and activist, founding member of the cypherpunk movement, and one of the creators of Community Memory, the first public computerized bulletin board system.[44]
- Kevin Mitnick is a computer security consultant and author, formerly the most wanted computer criminal in United States history.[45]
- Len Sassaman was a Belgian computer programmer and technologist who was also a privacy advocate.
- Meredith L. Patterson is a well-known technologist and biohacker who has presented research with Dan Kaminsky and Len Sassaman at many international security and hacker conferences.
- Kimberley Vanvaeck (known as Gigabyte) is a Belgian hacker recognized for writing the first virus in C#.[46]
- Michał Zalewski (lcamtuf) is a prominent security researcher.
- Solar Designer is the pseudonym of the founder of the Openwall Project.
- Kane Gamble, sentenced to 2 years in youth detention, who is autistic, gained access to highly sensitive information and "cyber-terrorised" high-profile U.S. intelligence officials such as then CIA chief John Brennan or Director of National Intelligence James Clapper.[47][48][49]

Customs

The computer underground[3] has produced its own specialized slang, such as 1337speak. Writing software and performing other activities to support these views is referred to as hacktivism. Some consider illegal cracking ethically justified for these goals; a common form is website defacement. The computer underground is frequently compared to the Wild West.[50] It is common for hackers to use aliases to conceal their identities.

Hacker groups and conventions

The computer underground is supported by regular real-world gatherings called hacker conventions or "hacker cons". These events include SummerCon (Summer), DEF CON, HoHoCon (Christmas), ShmooCon (February), BlackHat, Chaos Communication Congress, AthCon, Hacker Halted, and HOPE. Local Hackfest groups organize and compete to develop their skills to send a

team to a prominent convention to compete in group pentesting, exploit and forensics on a larger scale. Hacker groups became popular in the early 1980s, providing access to hacking information and resources and a place to learn from other members. Computer bulletin board systems (BBSs), such as the Utopias, provided platforms for information-sharing via dial-up modem. Hackers could also gain credibility by being affiliated with elite groups.[51]

Consequences for malicious hacking

India

Section	Offence	Punishment
65	*Tampering with computer source documents* – Intentional concealment, destruction or alteration of source code when the computer source code is required to be kept or maintained by law for the time being in force	Imprisonment up to three years, or/and with fine up to 20000 rupees
66	Hacking	Imprisonment up to three years, or/and with fine up to 50000 rupees

Netherlands

- Article 138ab of Wetboek van Strafrecht prohibits *computervredebreuk*, which is defined as intruding an automated work or a part thereof with intention and against the law. Intrusion is defined as access by means of:
  - Defeating security measures
  - By technical means
  - By false signals or a false cryptographic key
  - By the use of stolen usernames and passwords.

Maximum imprisonment is one year or a fine of the fourth category.[52]

United States

18 U.S.C. § 1030 (https://www.law.cornell.edu/uscode/text/18/1030) , more commonly known as the Computer Fraud and Abuse Act, prohibits unauthorized access or damage of "protected computers". "Protected computers" are defined in 18 U.S.C. § 1030(e)(2) (https://www.law.cornell.edu/uscode/text/18/1030#e_2) as:

- A computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government.
- A computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

The maximum imprisonment or fine for violations of the *Computer Fraud and Abuse Act* depends on the severity of the violation and the offender's history of violations under the *Act*.

The FBI has demonstrated its ability to recover ransoms paid in cryptocurrency by victims of cybertheft.[53]

Hacking and the media

Hacker magazines

The most notable hacker-oriented print publications are *Phrack*, *Hakin9* and *2600: The Hacker Quarterly*. While the information contained in hacker magazines and ezines was often outdated by the time they were published, they enhanced their contributors' reputations by documenting their successes.[51]

Hackers in fiction

Hackers often show an interest in fictional cyberpunk and cyberculture literature and movies. The adoption of fictional pseudonyms,[54] symbols, values and metaphors from these works is very common.[55]

Books

- The cyberpunk novels of William Gibson – especially the Sprawl trilogy – are very popular with hackers.[56]

- Helba from the *.hack* manga and anime series
- Merlin of Amber, the protagonist of the second series in *The Chronicles of Amber* by Roger Zelazny, is a young immortal hacker-mage prince who has the ability to traverse shadow dimensions.
- Lisbeth Salander in *The Girl with the Dragon Tattoo* by Stieg Larsson
- Alice from *Heaven's Memo Pad*
- *Ender's Game* by Orson Scott Card
- *Evil Genius* by Catherine Jinks
- *Hackers* (anthology) by Jack Dann and Gardner Dozois
- *Little Brother* by Cory Doctorow
- *Neuromancer* by William Gibson
- *Snow Crash* by Neal Stephenson

Films

- *Antitrust*
- *Blackhat*
- *Cypher*
- *Eagle Eye*
- *Enemy of the State*
- *Firewall*
- *Girl With The Dragon Tattoo*
- *Hackers*
- *Live Free or Die Hard*
- *The Matrix* series
- *The Net*
- *The Net 2.0*
- *Pirates of Silicon Valley*
- *Skyfall*

- *Sneakers*
- *Swordfish*
- *Terminator 2: Judgment Day*
- *Terminator Salvation*
- *Take Down*
- *Tron*
- *Tron: Legacy*
- *Untraceable*
- *WarGames*
- *Weird Science*
- *The Fifth Estate*
- *Who Am I – No System Is Safe (film)*

Non-fiction books

- *The Art of Deception* by Kevin Mitnick
- *The Art of Intrusion* by Kevin Mitnick
- *The Cuckoo's Egg* by Clifford Stoll
- *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* by Kevin Mitnick
- *The Hacker Crackdown* by Bruce Sterling
- *The Hacker's Handbook* by Hugo Cornwall (Peter Sommer)
- *Hacking: The Art of Exploitation Second Edition* by Jon Erickson
- *Out of the Inner Circle* by Bill Landreth and Howard Rheingold
- *Underground* by Suelette Dreyfus

See also

- Cracking of wireless networks
- Cyber spying
- Cyber Storm Exercise

- Cybercrime
- Hacker culture
- Hacker (expert)
- Hacker Manifesto
- IT risk
- Mathematical beauty
- Metasploit Project
- Penetration test
- Technology assessment
- Vulnerability (computing)

References

1. *Gao, Xing (2015). "Information security investment for competitive firms with hacker behavior and security requirements". Annals of Operations Research. **235**: 277–300. doi:10.1007/s10479-015-1925-2 (https://doi.org/10.1007%2Fs10479-015-1925-2) . S2CID 207085416 (https://api.semanticscholar.org/CorpusID:207085416) .*
2. *Winkler, Ira. Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day. John Wiley & Sons. 2005. pg. 92. ISBN 9780764589904.*
3. *Sterling, Bruce (1993). "Part 2(d)". The Hacker Crackdown. McLean, Virginia: IndyPublish.com. p. 61. ISBN 1-4043-0641-2.*
4. *Blomquist, Brian (May 29, 1999). "FBI's Web Site Socked as Hackers Target Feds" (http://archive.nypost.com/a/475198) . New York Post.*
5. *"The Hacker's Dictionary" (http://jargon-file.org/archive/jargon-1.5.0.dos.txt) . Retrieved May 23, 2013.*
6. *Political notes from 2012: September–December (http://stallman.org/archives/2012-sep-dec.html#06_December_2012_%28Ecuadorian_white_hat_cracker_freed%29) . stallman.org.*
7. *Raymond, Eric S. "Jargon File: Cracker" (http://catb.org/jargon/html/C/cracker.html) . "Coined ca. 1985 by hackers in defense against journalistic misuse of hacker."*
8. *Yagoda, Ben (March 6, 2014). "A Short History of 'Hack' " (http://www.newyorker.com/tech/elements/a-short-history-of-hack) . The New Yorker. Retrieved June 21, 2019. "Although Lifehacker and other neutral or positive applications of the word [hack] are increasingly prominent, the black-hat meaning still prevails among the general public."*

9. See the 1981 version of the Jargon File (http://www.catb.org/jargon/oldversions/jarg1-81-MM-DD.txt) , entry "hacker", last meaning.
10. "Computer hacking: Where did it begin and how did it grow?" (http://www.windowsecurity.com/whitepapers/Computer_hacking_Where_did_it_begin_and_how_did_it_grow_.html) . WindowSecurity.com. October 16, 2002.
11. Elmer-DeWitt, Philip (August 29, 1983). "The 414 Gang Strikes Again" (https://web.archive.org/web/20071202043840/http://www.time.com/time/magazine/article/0,9171,949797,00.html) . Time. p. 75. Archived from the original (http://www.time.com/time/magazine/article/0,9171,949797,00.html) on December 2, 2007.
12. Detroit Free Press. September 27, 1983. `{{cite news}}`: Missing or empty `|title=` (help)
13. "Beware: Hackers at play". Newsweek. September 5, 1983. pp. 42–46, 48.
14. "Timeline: The U.S. Government and Cybersecurity" (https://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html) . Washington Post. May 16, 2003. Retrieved April 14, 2006.
15. Bailey, David (April 1984). "Attacks on Computers: Congressional Hearings and Pending Legislation" (https://ieeexplore.ieee.org/document/6234796) . 1984 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE: 180–186. doi:10.1109/SP.1984.10012 (https://doi.org/10.1109%2FSP.1984.10012) . ISBN 978-0-8186-0532-1. S2CID 15187375 (https://api.semanticscholar.org/CorpusID:15187375) .
16. Caldwell, Tracey (July 22, 2011). "Ethical hackers: putting on the white hat". Network Security. **2011** (7): 10–13. doi:10.1016/s1353-4858(11)70075-7 (https://doi.org/10.1016%2Fs1353-4858%2811%2970075-7) .
17. Clifford, D. (2011). Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime. Durham, North Carolina: Carolina Academic Press. ISBN 978-1594608537.
18. Wilhelm, Douglas (2010). "2". Professional Penetration Testing. Syngress Press. p. 503. ISBN 978-1-59749-425-0.
19. EC-Council (http://www.eccouncil.org/) . eccouncil.org
20. Moore, Robert (2005). Cybercrime: Investigating High Technology Computer Crime. Matthew Bender & Company. p. 258. ISBN 1-59345-303-5.Robert Moore
21. O'Brien, Marakas, James, George (2011). Management Information Systems. New York, NY: McGraw-Hill/Irwin. pp. 536–537. ISBN 978-0-07-752217-9.
22. Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 978-1-59345-303-9.
23. Thomas, Douglas (2002). Hacker Culture (https://archive.org/details/hackerculture00thom_0) . University of Minnesota Press. ISBN 978-0-8166-3346-3.

24. *Andress, Mandy; Cox, Phil; Tittel, Ed – (2001). CIW Security Professional. New York, NY: Wiley. p. 638. ISBN 0-7645-4822-0.*

25. *"Blue hat hacker Definition" (https://web.archive.org/web/20130308110959/http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3Dblue+hat+hacker%26i%3D56321%2C00.asp) . PC Magazine Encyclopedia. Archived from the original (https://www.pcmag.com/encyclopedia_term/0,2542,t=blue+hat+hacker&i=56321,00.asp) on March 8, 2013. Retrieved May 31, 2010. "A security professional invited by Microsoft to find vulnerabilities in Windows."*

26. *Fried, Ina (June 15, 2005). "Blue Hat summit meant to reveal ways of the other side" (http://news.cnet.com/Microsoft-meets-the-hackers/2009-1002_3-5747813.html) . Microsoft meets the hackers. CNET News. Retrieved May 31, 2010.*

27. *Markoff, John (October 17, 2005). "At Microsoft, Interlopers Sound Off on Security" (https://www.nytimes.com/2005/10/17/technology/17hackers.html?pagewanted=1&_r=1) . The New York Times. Retrieved May 31, 2010.*

28. *Chabrow, Eric (February 25, 2012). "7 Levels of Hackers: Applying An Ancient Chinese Lesson: Know Your Enemies" (http://www.govinfosecurity.com/blogs.php?postID=1206&rf=2012-02-27-eg) . GovInfo Security. Retrieved February 27, 2012.*

29. *Egloff, Florian. Cybersecurity and the Age of Privateering. (https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch14.pdf) In: Understanding Cyber Conflict: Fourteen Analogies, Chapter 14, George Perkovich and Ariel E. Levite, Eds., Georgetown University Press, 2017.*

30. *Tidy, Joe. Ransomware: Should paying hacker ransoms be illegal? (https://www.bbc.com/news/technology-57173096) BBC 20 May 2021.*

31. *Morrison, Sara. What you need to know about ransomware and the future of cyberattacks (https://www.vox.com/recode/22527272/ransomware-cyberattacks-bitcoin-explained) . Vox, Jun 16, 2021.*

32. *Abigail Summerville, Protect against the Fastest-Growing Crime: Cyber Attacks (https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html) , CNBC (July 25, 2017).*

33. *Myre, Greg. How Bitcoin Has Fueled Ransomware Attacks. (https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks) NPR, June 10, 2021.*

34. *Dey, Debabrata; Lahiri, Atanu; Zhang, Guoying (2011). "Hacker Behavior, Network Effects, and the Security Software Market" (https://dx.doi.org/10.2139/ssrn.1838656) . SSRN Electronic Journal. doi:10.2139/ssrn.1838656 (https://doi.org/10.2139%2Fssrn.1838656) . ISSN 1556-5068 (https://www.worldcat.org/issn/1556-5068) .*

35. *Gupta, Ajay; Klavinsky, Thomas and Laliberte, Scott (March 15, 2002) Security Through Penetration Testing: Internet Penetration (http://www.informit.com/articles/article.aspx?p=25916) . informit.com*

36. *Rodriguez, Chris; Martinez, Richard. "The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security" (https://www.htbridge.com/publication/the_growing_hacking_threat_to_websites.pdf) (PDF). Frost & Sullivan. Retrieved August 13, 2013.*

37. *Kerner, Sean Michael. "Sentry MBA Uses Credential Stuffing To Hack Sites." Eweek (2016): 8. Academic Search Complete. Web. 7 Feb. 2017.*

38. *Weir, Matt, Sudhir Aggarwal, Breno de Medeiros, Bill Glodek. 2009. "Password Cracking Using Probabilistic Context-Free Grammars". 2009 30th IEEE Symposium on Security and Privacy: 391-405.*

39. *Thompson, Samuel T. C. "Helping The Hacker? Library Information, Security, And Social Engineering." Information Technology & Libraries 25.4 (2006): 222-225. Academic Search Complete. Web. 7 Feb. 2017.*

40. *Press, EC-Council (2011). Penetration Testing: Procedures & Methodologies. Clifton, NY: CENGAGE Learning. ISBN 978-1435483675.*

41. *"DEF CON III Archives - Susan Thunder Keynote" (https://www.defcon.org/html/defcon-3/defcon-3.html) . DEF CON. Retrieved August 12, 2017.*

42. *Hafner, Katie (August 1995). "Kevin Mitnick, unplugged" (http://www.tomandmaria.com/ST297/Readings/mitnick%20esquire.htm) . Esquire. **124** (2): 80.*

43. *"Gary McKinnon extradition ruling due by 16 October" (https://www.bbc.co.uk/news/uk-19506090) . BBC News. September 6, 2012. Retrieved September 25, 2012.*

44. *"Community Memory: Precedents in Social Media and Movements" (http://www.computerhistory.org/atchm/community-memory-precedents-in-social-media-and-movements/) . Computer History Museum. February 23, 2016. Retrieved August 13, 2017.*

45. *"Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution ..." (https://web.archive.org/web/20090926231348/http://www.usdoj.gov/criminal/cybercrime/mitnick.htm) (Press release). United States Attorney's Office, Central District of California. August 9, 1999. Archived from the original (https://www.usdoj.gov/criminal/cybercrime/mitnick.htm) on September 26, 2009. Retrieved April 10, 2010.*

46. *Holt, Thomas J.; Schel, Bernadette Hlubik (2010). Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (https://books.google.com/books?id=LAIjG_OGuIMC&pg=PA146) . IGI Global. p. 146. ISBN 9781616928056.*

47. *"British teenager who 'cyber-terrorised' US intelligence officials gets two years detention (https://www.independent.co.uk/news/uk/british-teen-hacker-kane-gamble-us-intelligence-officials-jailed-cia-fbi-a8315126.html) ". The Independent. 21 April 2018.*

48. *"British teen Kane Gamble accessed accounts of top US intelligence and security officials (http://www.dw.com/en/british-teen-kane-gamble-accessed-accounts-of-top-us-intelligence-and-security-officials/a-42230614) ". Deutsche Welle. 21 January 2018.*

49. *"Kane Gamble: Teenager with autism on Leicestershire housing estate took classified information by fooling people into thinking he was FBI boss (https://www.independent.co.uk/news/uk/crime/us-intelligence-cia-fbi-american-government-john-brennan-mark-giuliano-crackas-with-attitude-latest-a8170561.html) ". The Independent. 21 January 2018.*

50. *Jordan, Tim; Taylor, Paul A. (2004). Hacktivism and Cyberwars (https://archive.org/details/hacktivismcyberw0000jord/page/133) . Routledge. pp. 133–134 (https://archive.org/details/hacktivismcyberw0000jord/page/133) . ISBN 978-0-415-26003-9. "Wild West imagery has permeated discussions of cybercultures."*

51. *Thomas, Douglas (2003). Hacker Culture. University of Minnesota Press. p. 90. ISBN 978-0-8166-3346-3.*

52. *Artikel 138ab (http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum_27-12-2012) . Wetboek van Strafrecht, December 27, 2012*

53. *Nakashima, Ellen. Feds recover more than $2 million in ransomware payments from Colonial Pipeline hackers. (https://www.washingtonpost.com/business/2021/06/07/colonial-pipeline-ransomware-payment-recovered/) Washington Post, June 7, 2021.*

54. *Swabey, Pete (February 27, 2013). "Data leaked by Anonymous appears to reveal Bank of America's hacker profiling operation" (http://www.information-age.com/it-management/risk-and-compliance/123456840/data-leaked-by-anonymous-appears-to-reveal-bank-of-america-s-hacker-profiling-operation) . Information Age. Retrieved February 21, 2014.*

55. *"Hackers and Viruses: Questions and Answers" (http://www.scienzagiovane.unibo.it/English/hackers/6-faq.html) . Scienzagiovane. University of Bologna. November 12, 2012. Retrieved February 21, 2014.*

56. *Staples, Brent (May 11, 2003). "A Prince of Cyberpunk Fiction Moves Into the Mainstream" (https://www.nytimes.com/2003/05/11/opinion/editorial-observer-a-prince-of-cyberpunk-fiction-moves-into-the-mainstream.html) . The New York Times. "Mr. Gibson's novels and short stories are worshiped by hackers"*

Further reading

- Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau (March 2022). "Hacker types, motivations and strategies: A comprehensive framework" (https://www.sciencedirect.com/science/article/pii/S245195882200001X) . *Computers in Human Behavior Reports*. **5**. ISSN 2451-9588 (https://www.worldcat.org/issn/2451-9588) . Retrieved January 27, 2022.
- Apro, Bill; Hammond, Graeme (2005). *Hackers: The Hunt for Australia's Most Infamous Computer Cracker*. Rowville, Vic: Five Mile Press. ISBN 1-74124-722-5.
- Beaver, Kevin (2010). *Hacking for Dummies* (https://books.google.com/books?id=rIOxAmsA6hQC&pg=PP1) . Hoboken, NJ: Wiley Pub. ISBN 978-0-7645-5784-2.

- Conway, Richard; Cordingley, Julian (2004). *Code Hacking: A Developer's Guide to Network Security*. Hingham, Mass: Charles River Media. ISBN 978-1-58450-314-9.
- Freeman, David H.; Mann, Charles C. (1997). *At Large: The Strange Case of the World's Biggest Internet Invasion* (https://archive.org/details/atlargestrangeca00free) . New York: Simon & Schuster. ISBN 0-684-82464-7.
- Granville, Johanna (Winter 2003). "Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions" (https://www.scribd.com/doc/14361572/Dotcon-Dangers-of-Cybercrime-by-Johanna-Granville) . *Australian Journal of Politics and History*. **49** (1): 102–109. doi:10.1111/1467-8497.00284 (https://doi.org/10.1111%2F1467-8497.00284) . Retrieved February 20, 2014.
- Gregg, Michael (2006). *Certified Ethical Hacker*. Indianapolis, Ind: Que Certification. ISBN 978-0-7897-3531-7.
- Hafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (https://archive.org/details/cyberpunk00kati) . New York: Simon & Schuster. ISBN 0-671-68322-5.
- Harper, Allen; Harris, Shon; Ness, Jonathan (2011). *Gray Hat Hacking: The Ethical Hacker's Handbook* (https://books.google.com/books?id=jMmpLwe2ezoC) (3rd ed.). New York: McGraw-Hill. ISBN 978-0-07-174255-9.
- McClure, Stuart; Scambray, Joel; Kurtz, George (1999). *Hacking Exposed: Network Security Secrets and Solutions* (https://archive.org/details/hackingexposedne00mccl) . Berkeley, Calif: Mcgraw-Hill. ISBN 0-07-212127-0.
- Russell, Ryan (2004). *Stealing the Network: How to Own a Continent*. Rockland, Mass: Syngress Media. ISBN 978-1-931836-05-0.
- Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. London: Routledge. ISBN 978-0-415-18072-6.

External links

Wikibooks has a book on the topic of: ***Hacking***

Wikimedia Commons has media related to ***Hackers***.

- CNN Tech PCWorld Staff (November 2001). Timeline: A 40-year history of hacking from 1960 to 2001 (http://edition.cnn.com/2001/TECH/internet/11/19/hack.history.idg/index.html)
- Can Hackers Be Heroes? (http://video.pbs.org/video/2365039353/) Video produced by Off Book (web series)

Last edited 4 months ago by Toadspike