Black hat (computer security)

A **black hat** (**black hat hacker** or **blackhat**) is a computer hacker who violates laws or ethical standards for nefarious purposes, such as cybercrime, cyberwarfare, or malice. These acts can range from piracy to identity theft. A black hat is often referred to as a "cracker".[1]

The term originates from 1950s westerns, with "bad guys" (criminals) typically depicted as having worn black hats and "good guys" (heroes) wearing white ones. In the same way, black hat hacking is contrasted with the more ethical white hat approach to hacking. Additionally, there exists a third category, called grey hat hacking, characterized by individuals who hack, usually with good intentions but by illegal means.[2][3][4]

Description

Criminals who intentionally enter computer networks with malicious intent are known as "black hat hackers".[5] They may distribute malware that steals data (particularly login credentials), financial information, or personal information (such as passwords or credit card numbers). This information is often sold on the dark web. Malware can also be used to hold computers hostage or destroy files. Some hackers may also modify or destroy data in addition to stealing it. While hacking has become an important tool for governments to gather intelligence, black hats tend to work alone or with organized crime groups for financial gain.[2][6]

Black hat hackers may be novices or experienced criminals. They are usually competent infiltrators of computer networks and can circumvent security protocols. They may create malware, a form of software that enables illegitimate access to computer networks, enables the monitoring of victims' online activities, and may lock infected devices. Black hat hackers can be involved in cyber espionage or protests in addition to pursuing personal or financial gain.[7] For some hackers, cybercrime may be an addictive experience.[8][9]

History

One of the earliest and most notorious black hat hacks was the 1979 hacking of The Ark by Kevin Mitnick. The Ark computer system was used by Digital Equipment Corporation (DEC) to develop the RSTS/E operating system software.

The WannaCry ransomware attack in May 2017 is another example of black hat hacking. Around 400,000 computers in 150 countries were infected within two weeks. The creation of decryption tools by security experts within days limited the extortion payments to approximately $120,000, or slightly more than 1% of the potential payout.[10]

Countries initially affected by the WannaCry ransomware attack

The notable data breaches typically published by major news services are the work of black hat hackers. In a data breach, hackers can steal the financial, personal, or digital information of customers, patients, and constituents. The hackers can then use this information to smear a business or government agency, sell it on the dark web, or extort money from businesses, government agencies, or individuals.[11] The United States experienced a record number of 1,862 data breaches in 2021, according to the Identity Theft Resource Center's 2021 Data Breach Report. There has been a noticeable increase in the number of data leaks. Take the United States as an example: in 2017, there were a record 1,506 incidents;[12] in 2021, there was a new high of 1,862 incidents;[13] and in 2023, there was a record 3,205 incidents.[14] At the same time, there has been no significant decline between the peak values.

From 2013 to 2014, black hat hackers broke into Yahoo and stole 3 billion customer records, making it possibly the largest data breach ever.[15] In addition, the adult website Adult FriendFinder was hacked in October 2016, and over 412 million customer records were taken.[15] A data breach that occurred between May and July 2017 exposed more than 145 million customer records, making the national credit bureau Equifax another victim of black hat hacking.[15]

Strategies

Concealing

One of the most famous black hat methods is to utilize nasty "doorway pages", which are intended to rank highly for specific search queries. Accordingly, the substance of these doorway pages is stowed away from both the clients and the web indexes. Doorway pages are designed to deceive search engines so that they cannot index or rank a website for synonymous keywords or phrases.

Keyword stuffing

Another form of black hat search engine optimization (SEO) is known as keyword stuffing, which involves repeatedly using the same keywords to try to trick search engines. This tactic involves using irrelevant keywords on a webpage (such as on the homepage or in metadata tags) to make it appear more relevant for particular keywords, deceiving people who visit the site.[16]

Link farming

Link farming occurs when multiple websites or pages link to a particular website. This is done to profit from the pay-per-click (PPC) advertisements on these websites or pages. The issue is that the links only point to the specific website because it promises something in return, when in fact they are only there to increase traffic to the desired website and its popularity. These websites are unethical and will damage the credibility of the website's other pages, possibly reducing its income potential.

Shrouding

Shrouding involves showing different content to clients and web search tools. A website may present search engines with information irrelevant to the website's real content. This is done to boost the website's visibility in search results.

Spamdexing

Spamdexing is a form of black hat SEO that involves using software to inject backlinks to a website into search engine results. This is done solely to raise the website's ranking in search engines.

Unethical redirects

A redirect link is considered unethical if it takes the user to a webpage different from the one indicated in the link. For instance, it is unethical to have a link that should take the user to the website "ABC" but instead takes them to "XYZ". Users are tricked into following an unintended path, even though they might not be interested in the website they land on.

Examples of famous black hats


Kevin Mitnick

- Kevin Mitnick is one of the most well-known black hat hackers. At one point, he was the most wanted cybercriminal in the world. He hacked into over forty major corporations, including Motorola and IBM, and even the US National Defense warning system. He was taken into custody and incarcerated in 1995. He became a cybersecurity consultant after his release in 2001, utilizing his hacking expertise for white hat hacking.[17]
- Vladimir Levin is a Russian hacker who, while working with a dial-up connection and a laptop from his Saint Petersburg apartment in 1994, accessed the accounts of several large corporate customers of Citibank, stealing USD$10.7 million. He ended up spending three years in jail. However, in 2005, an anonymous hacker group claimed responsibility for the theft, stating that they only sold Vladimir the data needed to steal the money.[18]

Other hat types

White hat

An ethical security hacker is referred to as a white hat or white hat hacker. The term "ethical hacking" is meant to mean more than just penetration testing. White hat hackers aim to discover any flaws in the current system with the owner's permission. Many organizations engage white hat hackers to enhance their network security through activities such as vulnerability assessments. Their primary objective is to assist the organization.[19]

Grey hat

A grey hat is a hacker who typically does not have malicious intent but often violates laws or common ethical standards. A vulnerability will not be illegally exploited by a grey hat, nor will it instruct others on how to do so; however, the grey hat may trade this information for personal gain.[20] A special group of gray hats are hacktivists, who hack to promote social change.[3]

The ideas of "white hat" and "black hat" hackers led to the use of the term "grey hat" at the end of the 1990s.

Another difference between these types of hackers is how they find vulnerabilities. The black hat will break into any system or network to uncover sensitive information for personal gain, whereas the white hat does so at the request of their employer or with explicit permission to determine how secure it is against hackers. The grey hat typically possesses the white hat's skills and intentions and the black hat's disregard for permission or laws.[4] A grey hat hacker might request organizations for voluntary compensation for their activities.[21]

See also

- BlueHat
- Cybercrime
- Cyberwarfare

References

1. Sheikh, Ahmed (2021), "Introduction to Ethical Hacking" (https://dx.doi.org/10.1007/978-1-4842-7258-9_1), *Certified Ethical Hacker (CEH) Preparation Guide*, Berkeley, CA: Apress, pp. 1–9, doi:10.1007/978-1-4842-7258-9_1 (https://doi.org/10.1007%2F978-1-4842-7258-9_1), ISBN 978-1-4842-7257-2, S2CID 239755067 (https://api.semanticscholar.org/CorpusID:239755067), retrieved 2024-03-08
2. "What is a Black-Hat hacker?" (https://www.kaspersky.com/resource-center/threats/black-hat-hacker). *www.kaspersky.com*. 2022-02-09. Retrieved 2022-11-27.
3. testovaniebezpecnosti (2017-11-10). "Hackers are not just the bad guys – brief history and classification" (https://hacktrophy.com/en/hackers-history-and-classification/). *HackTrophy* (in Slovak). Retrieved 2022-11-27.
4. Luciano, Michael (2018-09-05). "What Are the Three Types of Hackers?" (https://www.designworldonline.com/what-are-the-three-types-of-hackers/). *Design World*. Retrieved 2022-11-27.
5. "Black hat, White hat, and Gray hat hackers – Definition and Explanation" (https://www.kaspersky.com/resource-center/definitions/hacker-hat-types). *www.kaspersky.com*. 2022-05-11. Retrieved 2022-11-27.
6. "Kevin Mitnick - Once the world's most wanted hacker, now he's getting paid to hack companies legally | Black Hat Ethical Hacking | Black Hat Ethical Hacking" (https://www.blackhatethicalhacking.com/articles/hacking-stories/kevin-mitnick-once-the-worlds-most-wanted-hacker-now-hes-getting-paid-to-hack-companies-legally/). 2020-09-14. Retrieved 2024-01-09.
7. "What is a black hat hacker?" (https://www.techtarget.com/searchsecurity/definition/black-hat). *SearchSecurity*. Retrieved 2022-11-27.
8. "Teen hackers study considers link to addiction" (https://www.bbc.com/news/technology-37752800). *BBC News*. 2016-10-24. Retrieved 2024-08-12.
9. "How European authorities want to tackle child hacking" (https://www.euronews.com/next/2023/06/12/are-the-kids-alright-how-european-authorities-want-to-tackle-child-hacking). *euronews*. 2023-06-12. Retrieved 2024-08-12.
10. "What is WannaCry ransomware?" (https://www.kaspersky.com/resource-center/threats/ransomware-wannacry). *www.kaspersky.com*. 2022-02-09. Retrieved 2022-11-27.

11. Espinosa, Christian (2018-03-09). "Black Hat vs White Hat Hackers" (https://www.alpinesecurity.com/blog/black-hat-vs-white-hat-hackers/). *Alpine Security*. Retrieved 2022-11-27.
12. "Archived Graphs" (https://www.iii.org/graph-archive/213434). *III*. Retrieved 2025-08-26.
13. "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises" (https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/). *ITRC*. Retrieved 2025-08-26.
14. "Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High" (https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/). *ITRC*. 25 January 2024.
15. "Biggest Data Breaches in US History [Updated 2022] | UpGuard" (https://www.upguard.com/blog/biggest-data-breaches-us). *www.upguard.com*. Retrieved 2022-11-27.
16. "Black hat SEO" (https://www.twaino.com/en/definition/b/black-hat-seo/). *Twaino*. 2022-06-06. Retrieved 2022-11-27.
17. Greenberg, Andy. "Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits" (https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Retrieved 2022-11-27.
18. Podcast, Malicious Life. "Malicious Life Podcast: The Real Story of Citibank's $10M Hack" (https://www.cybereason.com/blog/malicious-life-podcast-the-real-story-of-citibanks-10m-hack). *Cybereason Blog*. Retrieved 2024-11-30.
19. Banda, Raphael; Phiri, Jackson; Nyirenda, Mayumbo; Kabemba, Monica M. (2019-03-07). "Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools" (https://doi.org/10.33260%2Fzictjournal.v3i1.74). *Zambia ICT Journal*. **3** (1): 40–51. doi:10.33260/zictjournal.v3i1.74 (https://doi.org/10.33260%2Fzictjournal.v3i1.74). ISSN 2616-2156 (https://search.worldcat.org/issn/2616-2156).
20. "What is an ethical hacker and what does the work entail?" (https://www.techtarget.com/searchsecurity/definition/ethical-hacker). *SearchSecurity*. Retrieved 2022-11-27.
21. Hanusch, Yonnique Francesca (2021-04-03). "Financial institutions should decline hackers' requests for voluntary compensation" (https://dx.doi.org/10.1080/02580136.2021.1933733). *South African Journal of Philosophy*. **40** (2): 162–170. doi:10.1080/02580136.2021.1933733 (https://doi.org/10.1080%2F02580136.2021.1933733). ISSN 0258-0136 (https://search.worldcat.org/issn/0258-0136). S2CID 235676146 (https://api.semanticscholar.org/CorpusID:235676146).
