WIKIPEDIA
The Free Encyclopedia

Bulletproof hosting

(Redirected from Bullet proof hosting)

Bulletproof hosting (BPH) is technical infrastructure service provided by an Internet hosting service that is resilient to complaints of illicit activities, which serves criminal actors as a basic building block for streamlining various cyberattacks.[1] BPH providers allow online gambling, illegal pornography, botnet command and control servers, spam, copyrighted materials, hate speech and misinformation, despite takedown court orders and law enforcement subpoenas, allowing such material in their acceptable use policies.[2][3][4]

A former NATO-bunker in the Netherlands, which housed bulletproof hosting provider CyberBunker.

BPH providers usually operate in jurisdictions which have lenient laws against such conduct. Most non-BPH service providers prohibit transferring materials over their network that would be in violation of their terms of service and the local laws of the incorporated jurisdiction, and oftentimes any abuse reports would result in takedowns to avoid their autonomous system's IP address block being blacklisted by other providers and by Spamhaus.[5]

History

BPH first became the subject of research in 2006 when security researchers from VeriSign revealed the Russian Business Network, an internet service provider that hosted a phishing group, was responsible for about $150 million in phishing-related scams. RBN also become known for identity thefts, child pornography, and botnets.[6][7][8] The following year, McColo, the web hosting provider responsible for more than 75% of global spam was shut down and de-peered by Global Crossing and Hurricane Electric after the public disclosure by then-Washington Post reporter Brian Krebs on his Security Fix blog on that newspaper.[9][10]

Difficulties

Since any abuse reports to the BPH will be disregarded, in most cases, the whole IP block ("netblock") assigned to the BPH's autonomous system will be blacklisted by other providers and third party spam filters. Additionally, BPH also have difficulty in finding network peering points for establishing Border Gateway Protocol sessions, since routing a BPH provider's network can affect the reputation of upstream autonomous systems and transit provider.[11] This makes it difficult for BPH services to provide stable network connectivity, and in extreme cases, they can be completely de-peered;[1] therefore BPH providers evade AS's reputation based fortification such as BGP Ranking and ASwatch through unconventional methodologies.[2]

Web hosting reseller

According to a report, due to their mounting difficulties, BPH providers engage in establishing reseller relationships with lower-end hosting providers; although these providers are not complicit in supporting the illegitimate activities, they tend to be lenient on abuse reports and do not actively engage in fraud detection.[1] Therefore, BPH conceals itself behind lower-end hosting providers, leveraging their better reputation and simultaneously operating both bulletproof and legitimate resells through the sub-allocated network blocks.[12] However, if the BPH services are caught, providers of BPH migrate their clients to a newer internet infrastructure—newer lower-end AS, or IP space—effectively making the blacklisted IP addresses of the previous AS ephemeral; thus continuing to engage in criminal conduct by modifying the DNS server's resource records of the listening services and making it point to the newer IP addresses belonging to the current AS's IP space.[12] Due to privacy concerns, the customary modes of contact for BPH providers include ICQ, Skype, and XMPP (or Jabber).[13][14]

Admissible abuses

Most BPH providers promise immunity against copyright infringement and court order takedown notices, notably Digital Millennium Copyright Act (DMCA), Electronic Commerce Directive (ECD) and law enforcement subpoenas. They also allow users to operate phishing, scams (such as high-yield investment program), botnet masters and unlicensed online pharmacy websites. In these cases, the BPH providers (known as "offshore providers") operate in jurisdictions which do not have any extradition treaty or mutual legal assistance treaty (MLAT) signed with the five eye countries, particularly the United States.[15][16][17] However, most BPH providers have a zero-tolerance policy towards child pornography and terrorism, although a few allow cold storage of such material given forbidden open-accessibility via the public internet.[18]

Prevalent jurisdictions for incorporation and location of the data centers for BPH providers include Russia (being more permissive),[19] Ukraine, China, Moldova, Romania, Bulgaria, Belize, Panama and the Seychelles.[20][21]

Impacts

BPH services act as vital network infrastructure providers for activities such as cybercrime and online illicit economies,[22] and the well-established working model of the cybercrime economies surrounds upon tool development and skill-sharing among peers.[23] The development of exploits, such as zero-day vulnerabilities, are done by a very small community of highly-skilled actors, who encase them in convenient tools which are usually bought by low-skilled actors (known as script kiddies), who make use of BPH providers for carry out cyberattacks, usually targeting low-profile unpretentious network services and individuals.[24][25] According to a report produced by Carnegie Mellon University for the United States Department of Defense, low-profile amateur actors are also potent in causing harmful consequences, especially to small businesses, inexperienced internet users, and miniature servers.[26]

Criminal actors also run specialized computer programs on BPH providers knowns as port scanners which scan the entire IPv4 address space for open ports, services run on those open ports, and the version of their service daemons, searching for vulnerable versions for exploitation.[27] One such notable vulnerability scanned by the port scanners is Heartbleed, which affected millions of internet servers.[28] Furthermore, BPH clients also host click fraud, adware (such as DollarRevenue), and money laundering recruitment sites, which lure untried internet users into honey trapping and causing financial losses to the individuals while unrestrictedly keeping their illicit sites online, despite court orders and takedown attempts by law enforcement.[29]

Counterinitiatives against BPH

The Spamhaus Project is an international nonprofit organization that monitors cyber threats and provides realtime blacklist reports (known as the "Badness Index") on malicious ASs, netblocks, and registrars that are involved in spam, phishing, or cybercrime activities. The Spamhaus team works closely with law enforcement agencies such as National Cyber-Forensics and Training Alliance (NCFTA) and Federal Bureau of Investigation (FBI), and the data compiled by Spamhaus is used by the majority of the ISPs, email service providers, corporations, educational institutes, governments and uplink gateways of military networks.[30][31][32] Spamhaus publishes various data feeds that list netblocks of the criminal actors, and is designed for use by gateways, firewalls and routing equipments to filter out (or "nullroute") traffic originating from these netblocks:[11]

- **Spamhaus Don't Route Or Peer List (DROP)** lists netblocks allocated by an established Regional Internet Registry (RIR) or National Internet Registry (NIR) that are used by criminal actors, and doesn't include abused IP address spaces sub-allocated netblocks of a reputable AS.[33]
- **Spamhaus Domain Block List (DBL)** lists domain names with poor reputation in DNSBL format.[34]
- **Spamhaus Botnet Controller List (BCL)** lists single IPv4 addresses of botnet masters.[35]

Notable closed services

The following are some of the notable defunct BPH providers:

- CyberBunker, taken down in September 2019.[36]
- McColo, taken down in November 2008.[37]
- Russian Business Network (RBN), taken down in November 2007.[38]
- Atrivo, taken down in September 2008.[39]
- 3FN, taken down by FTC in June 2009.[40][41][42]
- Proxiez, taken down in May 2010.[43]

See also

- Freedom Hosting
- Fast flux
- Security theater

References

1. McCoy, Mi & Wang 2017, p. 805.
2. Konte, Feamster & Perdisci 2015, p. 625.
3. Han, Kumar & Durumic 2021, p. 4.
4. "Host of Internet Spam Groups Is Cut Off" (https://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html). *The Washington Post*. 12 November 2008. Archived (https://web.archive.org/web/20200622154458/https://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html) from the original on 22 June 2020. Retrieved 4 December 2021.
5. Han, Kumar & Durumic 2021, p. 5-6.
6. Kerbs, Brian (13 October 2007). "Shadowy Russian Firm Seen as Conduit for Cybercrime" (https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html). *Washington Post*. Archived (https://web.archive.org/web/20210915131046/https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html) from the original on 15 September 2021. Retrieved 5 January 2022.
7. Warren, Peter (15 November 2007). "Hunt for Russia's Web Criminals" (https://web.archive.org/web/20211125005824/https://www.theguardian.com/technology/2007/nov/15/news.crime). *The Guardian*. Archived from the original (https://www.theguardian.com/technology/2007/nov/15/news.crime) on 25 November 2021. Retrieved 5 January 2022.
8. Stone-Gross, Brett; Kruegel, Christopher; Almeroth, Kevin; Moser, Andreas (11 December 2009). *FIRE: FInding Rogue nEtworks*. Annual Computer Security Applications Conference. *Proceedings of the ... Annual Computer Security Applications Conference*. Institute of Electrical and Electronics Engineers. p. 231. doi:10.1109/ACSAC.2009.29 (https://doi.org/10.1109%2FACSAC.2009.29). ISBN 978-1-4244-5327-6. ISSN 1063-9527 (https://www.worldcat.org/issn/1063-9527).
9. Krebs, Brain (12 November 2008). "Host of Internet Spam Groups Is Cut Off" (https://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html). *The Washington Post*. Archived (https://archive.today/20120527042932/http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html) from the original on 27 May 2012. Retrieved 5 January 2022.

10. Krebs, Brain. "Major Source of Online Scams and Spams Knocked Offline" (https://web.archive.org/web/20210930120212/http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html). Archived from the original (http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html) on 30 September 2021. Retrieved 5 January 2022.
11. Spamhaus Research Team (19 December 2019). "Bulletproof hosting – there's a new kid in town" (https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town). The Spamhaus Project. Archived (https://web.archive.org/web/20210422115122/https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town) from the original on 22 April 2021. Retrieved 21 December 2021.
12. McCoy, Mi & Wang 2017, p. 806.
13. McCoy, Mi & Wang 2017, p. 811.
14. Goncharov, Max (15 July 2015). "Criminal Hideouts for Lease: Bulletproof Hosting Services" (https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf) (PDF). Trend Micro. Archived (https://web.archive.org/web/20210719111342/https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf) (PDF) from the original on 19 July 2021. Retrieved 5 December 2021.
15. Leporini 2015, p. 5.
16. Clayton & Moore 2008, p. 209.
17. Konte, Feamster & Jung 2008, p. 10.
18. Kopp, Strehle & Hohlfeld 2021, p. 2432.
19. Caesar, Ed (27 July 2020). "The Cold War Bunker That Became Home to a Dark-Web Empire" (https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire). *The New Yorker*. Archived (https://web.archive.org/web/20210929052936/https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire) from the original on 29 September 2021. Retrieved 5 December 2021.
20. Thomas, Elise (8 August 2019). "Inside the bulletproof hosting providers that keep the world's worst websites in business" (https://www.abc.net.au/news/2019-08-09/shining-light-on-the-bulletproof-web-hosts-lurking-in-the-sha/11396986). *ABC News*. Archived (https://web.archive.org/web/20210904052140/https://www.abc.net.au/news/2019-08-09/shining-light-on-the-bulletproof-web-hosts-lurking-in-the-sha/11396986) from the original on 4 September 2021. Retrieved 5 November 2021.
21. Richardson, Ronny; North, Max M. (1 January 2017). "Ransomware: Evolution, Mitigation and Prevention" (https://digitalcommons.kennesaw.edu/facpubs/4276/). *International Management Review*. **13** (1). Kennesaw State University: 13.
22. Collier & Hutchings 2021, p. 1.
23. Collier & Hutchings 2021, p. 1-2.
24. Bradbury 2010, p. 17.
25. Collier & Hutchings 2021, p. 2.
26. Mead, Nancy R.; Hough, Eric; Stehney, Theodore R. (31 October 2005). Security Quality Requirements Engineering (SQUARE) Methodology (https://kilthub.cmu.edu/articles/journal_contribution/Security_Quality_Requirements_Engineering_SQUARE_Methodology/6583673/1) (Report). Carnegie Mellon University. doi:10.1184/R1/6583673.v1 (https://doi.org/10.1184%2FR1%2F6583673.v1).
27. Durumeric, Zakir; Bailey, Michael; Halderman, J. Alex (August 2014). *An internet-wide view of internet-wide scanning* (https://dl.acm.org/doi/10.5555/2671225.2671230). USENIX conference on Security Symposium. USENIX. pp. 65–66.
28. Heo, Hawnjo; Shin, Seungwon (May 2018). *Who is knocking on the Telnet Port: A Large-Scale Empirical Study of Network Scanning* (https://dl.acm.org/doi/abs/10.1145/3196494.3196537). Asia Conference on Computer and Communications Security. pp. 625–626. doi:10.1145/3196494.3196537 (https://doi.org/10.1145%2F3196494.3196537).
29. Watson, David (2007). "The evolution of web application attacks" (https://www.sciencedirect.com/science/article/pii/S1353485808700394). *Network Security*. **2007** (11): 7–12. doi:10.1016/S1353-4858(08)70039-4 (https://doi.org/10.1016%2FS1353-4858%2808%2970039-4). ISSN 1353-4858 (https://www.worldcat.org/issn/1353-4858).

30. Nandi O. Leslie; Richard E. Harang; Lawrence P. Knachel; Alexander Kott (30 June 2017). "Statistical models for the number of successful cyber intrusions" (https://journals.sagepub.com/doi/abs/10.1177/1548512917715342). *The Journal of Defense Modeling and Simulation*. **15** (1). United States: United States Army Research Laboratory: 49–63. arXiv:1901.04531 (https://arxiv.org/abs/1901.04531). doi:10.1177/1548512917715342 (https://doi.org/10.1177%2F1548512917715342). S2CID 58006624 (https://api.semanticscholar.org/CorpusID:58006624). Retrieved 22 December 2021.
31. Grauer, Yael (17 January 2016). "Security News This Week: Tim Cook Demands That the White House Defend Encryption" (https://www.wired.com/2016/01/security-news-this-week-tim-cook-demands-that-the-white-house-support-encryption/). *Wired*. Archived (https://web.archive.org/web/20210423130650/https://www.wired.com/2016/01/security-news-this-week-tim-cook-demands-that-the-white-house-support-encryption/) from the original on 23 April 2021. Retrieved 22 December 2021.
32. "Corporate Documents: About Spamhaus" (https://www.spamhaus.org/organization/). Archived (https://web.archive.org/web/20211214192203/https://www.spamhaus.org/organization/) from the original on 14 December 2021. Retrieved 22 December 2021.
33. "The Spamhaus Don't Route Or Peer Lists" (https://www.spamhaus.org/drop/). The Spamhaus Project. Archived (https://web.archive.org/web/20211221203320/https://www.spamhaus.org/drop/) from the original on 21 December 2021. Retrieved 22 December 2021.
34. "The Domain Block List (DBL)" (https://www.spamhaus.org/dbl/). The Spamhaus Project. Archived (https://web.archive.org/web/20211221203312/https://www.spamhaus.org/dbl/) from the original on 21 December 2021. Retrieved 22 December 2021.
35. "Spamhaus Botnet Controller List" (https://www.spamhaus.org/bcl/). The Spamhaus Project. Archived (https://web.archive.org/web/20200826014515/https://www.spamhaus.org/bcl/) from the original on 26 August 2020. Retrieved 22 December 2021.
36. Krebs, Brian (28 September 2019). "German Cops Raid 'Cyberbunker 2.0', Arrest 7 in Child Porn, Dark Web Market Sting" (https://krebsonsecurity.com/2019/09/german-cops-raid-cyberbunker-2-0-arrest-7-in-child-porn-dark-web-market-sting/). *Krebs on Security*. Retrieved 10 June 2021.
37. "Major Source of Online Scams and Spams Knocked Offline" (http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html), *The Washington Post*, November 2008.
38. "Security Fix - Russian Business Network: Down, But Not Out" (http://voices.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html). *The Washington Post*. Retrieved 2016-10-07.
39. "Scammer-Heavy U.S. ISP Grows More Isolated" (http://voices.washingtonpost.com/securityfix/2008/09/scam-heavy_us_isp_grows_more_i.html), *The Washington Post*, September 2009.
40. "The Fallout from the 3FN Takedown" (http://voices.washingtonpost.com/securityfix/2009/06/the_fallout_from_the_3fn_taked.html), *The Washington Post*, June 2009.
41. "ISP shuttered for hosting 'witches' brew' of spam, child porn" (https://www.theregister.co.uk/2010/05/19/3fn_permanently_shuttered/), *The Register*, May 2010
42. "Rogue ISP ordered to liquidate, pay FTC $1.08 million" (https://arstechnica.com/tech-policy/news/2010/05/rogue-isp-ordered-to-liquidate-owes-ftc-108-million.ars), *Ars Technica*, May 2010.
43. 'Bulletproof' ISP for crimeware gangs knocked offline (https://www.theregister.co.uk/2010/05/14/zeus_friendly_proxiez_mia/), , *The Register*, May 2010.

Bibliography

- McCoy, Damon; Mi, Xianghang; Wang, Xiofeng (26 June 2017). "Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks" (https://ieeexplore.ieee.org/document/7958611). *2017 IEEE Symposium on Security and Privacy (SP)*. New York University. pp. 805–823. doi:10.1109/SP.2017.32 (https://doi.org/10.1109%2FSP.2017.32). ISBN 978-1-5090-5533-3. S2CID 1593958 (https://api.semanticscholar.org/CorpusID:1593958). {{cite book}}: |journal= ignored (help)
- Han, Catherine; Kumar, Deepak; Durumic, Zakir (2021). "On the Infrastructure Providers that Support Misinformation" (https://zakird.com/papers/misinfo-infra-preprint.pdf) (PDF). Stanford University. Archived (https://web.archive.org/web/20210825043611/https://zakird.com/papers/misinfo-infra-preprint.pdf) (PDF) from the original on 25 August 2021. Retrieved 4 December 2021.
- Konte, Maria; Feamster, Nick; Perdisci, Roberto (17 August 2015). "ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes" (https://dl.acm.org/doi/10.1145/2829988.2787494). *SIGCOMM*

Association for Computing Machinery. **45** (4). New York, United States. doi:10.1145/2829988.2787494 (https://doi.org/10.1145%2F2829988.2787494). ISSN 0146-4833 (https://www.worldcat.org/issn/0146-4833).

- Leporini, Dino (2015). *Architectures and protocols powering illegal content streaming over the Internet* (https://digital-library.theiet.org/content/conferences/10.1049/ibc.2015.0013). *University of Pisa*. Amsterdam, Netherlands: International Broadcasting Convention. p. 7. doi:10.1049/ibc.2015.0013 (https://doi.org/10.1049%2Fibc.2015.0013). ISBN 978-1-78561-185-8.
- Clayton, Richard; Moore, Tyler (22 December 2008). "The Impact of Incentives on Notice and Take-down" (https://link.springer.com/chapter/10.1007%2F978-0-387-09762-6_10). *Managing Information Risk and the Economics of Security*. Boston: Springer Publishing. pp. 199–223. doi:10.1007/978-0-387-09762-6_10 (https://doi.org/10.1007%2F978-0-387-09762-6_10). ISBN 978-0-387-09761-9.
- Kopp, Daniel; Strehle, Eric; Hohlfeld, Oliver (November 2021). "CyberBunker 2.0 - A Domain and Traffic Perspective on a Bulletproof Hoster" (https://dl.acm.org/doi/abs/10.1145/3460120.3485352). *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, Brandenburg University of Technology. pp. 2432–2434. arXiv:2109.06858 (https://arxiv.org/abs/2109.06858). doi:10.1145/3460120.3485352 (https://doi.org/10.1145%2F3460120.3485352). ISBN 9781450384544. S2CID 237503582 (https://api.semanticscholar.org/CorpusID:237503582).
- Collier, Benjamin; Hutchings, Alice (15 April 2021). "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies" (https://academic.oup.com/bjc/article/61/5/1407/6226588). *The British Journal of Criminology*. **61** (5). Oxford University Press. doi:10.1093/bjc/azab026 (https://doi.org/10.1093%2Fbjc%2Fazab026). hdl:20.500.11820/68a9a01b-f7c3-4fcb-9128-66caf04a4684 (https://hdl.handle.net/20.500.11820%2F68a9a01b-f7c3-4fcb-9128-66caf04a4684).
- Bradbury, Danny (15 October 2010). "Digging up the hacking underground" (https://www.sciencedirect.com/science/article/pii/S175445481070084X). *Infosecurity*. **7** (5): 14–17. doi:10.1016/S1754-4548(10)70084-X (https://doi.org/10.1016%2FS1754-4548%2810%2970084-X). ISSN 1754-4548 (https://www.worldcat.org/issn/1754-4548).
- Konte, M.; Feamster, N.; Jung, J. (January 2008). "SAC 025: SSAC Advisory on Fast Flux Hosting and DNS" (https://www.icann.org/en/system/files/files/sac-025-en.pdf) (PDF). *Security and Stability Advisory Committee (SSAC)* (1). Internet Corporation for Assigned Names and Numbers. Archived (https://web.archive.org/web/20211122051539/https://www.icann.org/en/system/files/files/sac-025-en.pdf) (PDF) from the original on 22 November 2021. Retrieved 12 December 2021.

-