TLP:CLEAR

Bulletproof Defense: Mitigating Risks From Bulletproof Hosting Providers

Publication: November 19, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Department of Defense Cyber Crime Center
U.S. Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Netherlands National Cyber Security Centre
New Zealand National Cyber Security Centre
United Kingdom National Cyber Security Centre

TLP:CLEAR

Introduction

This document was developed through the Joint Ransomware Task Force (JRTF), a U.S. interagency body established by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) to ensure unity of effort in combating the growing threat of ransomware attacks.

This document provides internet service providers (ISPs) and network defenders recommendations to mitigate potential cybercriminal activity enabled by bulletproof hosting (BPH) providers. This document is authored by the Cybersecurity and Infrastructure Security Agency (CISA) and the following partners:[1]

- U.S. National Security Agency (NSA)
- U.S. Department of Defense Cyber Crime Center (DC3)
- U.S. Federal Bureau of Investigation (FBI)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- Netherlands National Cyber Security Centre (NCSC-NL)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)

A **BPH provider** is an internet infrastructure provider that knowingly and intentionally markets and leases their infrastructure to cybercriminals. The authoring agencies have observed a marked increase in cybercriminal actors using BPH infrastructure to support cyber operations against critical infrastructure, financial institutions, and other high-value targets. BPH providers continue to pose a significant risk to the resilience and safety of critical systems and services.

Mitigating cybercriminal activity enabled by BPH providers requires a nuanced approach because BPH infrastructure is integrated into legitimate internet infrastructure systems, and actions from ISPs or network defenders may impact legitimate activity. The authoring agencies encourage ISPs and network defenders to apply the recommendations in this document, including curating a list of "high confidence" malicious internet resources and using the list to implement filters. By doing so, ISPs and network defenders can mitigate cybercriminal activity perpetuated by BPH infrastructure. This will help reduce the effectiveness of this infrastructure and potentially force cybercriminals to use legitimate infrastructure providers who are responsive to cyber threat abuse complaints and law enforcement takedown requests.

Bulletproof Hosting Providers

BPH providers lease their own infrastructure to cybercriminals. Increasingly, they resell stolen or leased infrastructure from legitimate hosting providers, data centers, ISPs, or cloud service providers who may unknowingly enable BPH providers to provide infrastructure to cybercriminals.

[1] Hereafter referred to as the authoring agencies.

BPH providers are able to market their infrastructure as "bulletproof" to cybercriminals because they do not engage in good faith with legal processes (such as subpoenas or court orders) and third-party or victim complaints of malicious[2] activity enabled from such infrastructure. For example, some BPH providers impose onerous documentation requirements before accommodating a third-party (i.e., law enforcement) takedown request.[3]

With the "bulletproof" assurance, cybercriminals use this infrastructure for obfuscation via fast flux techniques, command and control, malware delivery, phishing, and hosting illicit content in support of a variety of malicious cyber activities, such as ransomware, data extortion, and denial of service (DoS) attacks.

Bulletproof Hosting and Legitimate Infrastructure

BPH infrastructure is integrated into legitimate internet infrastructure systems, making it difficult for defenders to mitigate the cybercriminal activity. BPH infrastructure is part of a network or group of networks known as an Autonomous System (AS), where each AS has a unique identifier known as an Autonomous System Number (ASN). Blocking activity from the entire AS by leveraging the ASN may be ineffective in preventing malicious activity as:

The defensive filters may unduly impact legitimate traffic. Cybercriminals often spread their BPH infrastructure across multiple ASes to avoid detection and mitigation, ensuring that the BPH infrastructure forms only a small part of each AS. In cases where BPH providers operate leased infrastructure from legitimate providers, blocking all traffic corresponding to a particular ASN may filter out legitimate traffic.

BPH infrastructure is designed to dynamically avoid defenses. BPH providers can request a new ASN from an internet registry and receive it within two to five business days. The BPH provider then migrates the underlying malicious IP ranges to the new ASN, enabling BPH providers to evade ASN-based defensive filtering. Additionally, BPH-enabled activity often involves using temporary emails for responding to abuse requests and cycling through IP addresses, ASNs, nameservers, or Canonical Name (CNAME) Domain Name System (DNS) records.[4]

Mitigations

The authoring agencies urge ISPs and network defenders to apply a nuanced approach to dynamically filter ASNs, IP ranges, or individual IP addresses[5] to effectively reduce the risk of compromise from BPH provider-enabled activity. ISPs and network defenders should apply the recommendations only after weighing the associated risks, ensuring that actions taken do not unduly impact legitimate infrastructure.

---

[2] For purposes of this document, "malicious" refers exclusively to cybersecurity threats and cybersecurity risks, as those terms are defined at 6 U.S.C. § 650(7)-(8).

[3] "2024 Year in Review: Trends, Insights, and Lessons Learned," Silent Push, accessed April 7, 2025, https://info.silentpush.com/year-in-review.

[4] "Infrastructure Laundering: Silent Push Exposes Cloudy Behavior Around FUNNULL CDN Renting IPs from Big Tech," Silent Push, accessed September 19, 2025, https://www.silentpush.com/blog/infrastructure-laundering/.

[5] Hereafter referred to as internet resources.

The following mitigations include recommendations for both ISPs and network defenders, and recommendations tailored specifically for ISPs.

Internet Service Providers and Network Defenders

The authoring agencies recommend ISPs and network defenders take the following actions to mitigate malicious activity enabled by BPH providers:

- **Curate a list of "high confidence" malicious internet resources.** Develop this list by leveraging commercial and open source threat intelligence feeds (see the **Resources** section for examples of freely available threat feeds) and public and private information sharing channels, such as the Communications Information Sharing and Analysis Center (COMM-ISAC).
- **Conduct traffic analysis to supplement your organization's malicious internet resources list.** Establish and continuously maintain a baseline of your organization's expected network traffic and identify outlier activity.
  - Some legitimate activity, such as common content delivery network (CDN) behaviors, may look like malicious fast flux activity. Network defenders should make reasonable efforts, such as allowlisting expected CDN services, to avoid blocking or impeding legitimate content.
- **Conduct automated and regular reviews of the curated malicious internet resources list.** Promptly add new malicious internet resources to the list and remove internet resources that are reallocated to legitimate infrastructure.
- **Share threat intelligence findings.** Share information about malicious internet resources and other threat intelligence with the community via public and private information sharing channels. In addition to strengthening the ecosystem's cybersecurity posture, this provides easy confirmation for entities, showing that their traffic is not being incorrectly blocked.
- **Configure your organization's centralized event logging system to leverage the malicious internet resources list.** Configure the centralized logging system so it records both ASNs and IP addresses in log entries and issues alerts when traffic corresponding to a malicious internet resource reaches the organization network.
  - Ensure that the centralized logging system is always leveraging the most recent version of the malicious internet resource list. Refer to the logging vendor for configuration guidance.
- **Implement filters.** Implement malicious internet resource filters at the network border or appropriate policy enforcement points relevant to the system. For each internet resource on the malicious list, carefully consider the impact a filter may have on malicious traffic and possibly legitimate traffic. This risk analysis should inform whether a filter should be used, and if so, at what granularity (e.g., filtering all traffic from an ASN versus IP ranges versus individual IP addresses).
  - Establish an audit log. When each filter policy is established, document when and why that decision was made. Ensure that the log is regularly maintained.
  - Use a robust change control process for all filters. Regularly review the filters in place against the audit logs and change control documents, ensuring that the filters have not been changed in an unauthorized manner.

        - Because organizations often apply filters at an IP range or IP address level, implementing an ASN filter may involve mapping that ASN to organizational IP address blocklists. IP addresses behind an ASN can change, so refreshing the mapping is crucial for mitigating the risk of filtering IPs that are no longer associated with the malicious ASN.
    - **Develop filter feedback processes**. Establish a streamlined process for handling inquiries regarding blocked resources that mitigates the risk of incorrectly filtering legitimate traffic. Supported inquiries could include both access requests to blocked resources and requests that seek understanding of whether an entity's resources are blocked and why. Staff should leverage the audit log when answering these inquiries and engage with requesters in a timely, transparent, and collaborative manner to determine whether filter adjustments are appropriate. Finally, standardize inquiry data; track macro-level feedback trends and adjust filters, as needed.
- **Use upstream providers that follow Secure by Design principles** and mitigate the risks from BPH providers.[6]
    - Ask upstream providers for their management process of customer requests regarding blocked resources.
    - Ask upstream providers if their unblock process of an internet resource results in removing the block for only the requesting customer or for all of the provider's customers.
    - Use a risk-informed approach when asking providers to unblock likely malicious internet resources or reverse other mitigating measures.

Internet Service Providers

ISPs can play a crucial role in reducing cyber threats by taking the following actions that decrease the utility of BPH infrastructure:

- **Notify customers about malicious internet resource lists and associated filters**, ensuring they are aware of potential incidents or availability impacts.
    - Consider providing opt-out options for customers with different risk tolerances.
- **Create filters that customers can apply in their own networks.**
    - By offering optional, premade malicious internet resource filters, ISPs can help customers take further mitigation actions that may be too restrictive for an ISP to take themselves but benefit organizations with different risk tolerances.
    - If customers choose not to apply the filters, encourage customers to review the associated malicious internet resource list and validate traffic against it.
- **Form standards and norms for ISP accountability.**
    - Engage with other ISPs for sector-wide agreement on a code of conduct for BPH abuse prevention.

[6] See joint Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem for guidance on choosing secure technologies throughout the procurement cycle.

- Consider setting a timeframe (e.g., 90 days) for blocking all malicious IP ranges managed under an AS.
  - After the block period, ask the provider managing the identified AS and malicious IP ranges, or their upstream ISP, to provide updates confirming customers abusing the AS or IP ranges were removed, such as via acquisition of the range by another entity.
    - If no action is taken, conduct another block period, repeating until appropriate action is taken.
- Include the sector-wide code of conduct as binding terms and conditions in peering arrangements and contracts to reinforce accountability.

- **Establish "know your customer" capabilities.**
  - Raise the barrier for BPH providers to lease ISP infrastructure by collecting and vetting identifiable information from prospective customers.
    - Helpful information may include personal data, authenticated proof of identity, banking details (e.g., by submitting a 1 cent payment), Legal Entity Identifier (LEI), and other company details.
    - BPH providers may cycle through a series of email addresses and phone numbers that are capable of receiving messages but not sending;[7] therefore, test the legitimacy of the prospective customer's contact information by requiring them to *send* a verification code to the ISP.
  - Ensure this information is collected in compliance with relevant data privacy laws.
- **Implement internet routing security best practices**, such as those presented in the **Resources** section, to mitigate other risks from threat actors using BPH services, such as Border Gateway Protocol (BGP) hijacking.

Resources

- See the ASD's ACSC "Bulletproof" hosting providers: Cracks in the armour of cybercriminal infrastructure for more information on BPH.
- See CIRA Canadian Shield: Donning your cyber security armour for information on the Canadian Internet Registration Authority (CIRA)'s Canadian Shield. CIRA Canadian Shield is a free DNS firewall service for Canadians. Canadian Shield services include blocking connections to websites associated with known malicious internet resources.
- See the following free threat feeds:
  - The SpamHaus Project provides free blocklists of internet resources associated with spam, phishing, malware, and ransomware. See SpamHaus Project's Don't Route Or Peer Lists (DROP).

[7] "How hosting providers can battle fraudulent sign-ups," SpamHaus Project, accessed July 24, 2025, https://www.spamhaus.org/resource-hub/service-providers/how-hosting-providers-can-battle-fraudulent-sign-ups/#introduction.

  - ipapi.is provides a list of 1,000 "abusive" ASNs and 5,000 "abusive" IP ranges. See ipapi.is's Most Abusive ASNs on the Internet and Most Abusive Networks on the Internet, respectively.
  - ThreatFox, a project between abuse.ch and SpamHaus, provides threat reports for ASNs. See ThreatFox. To search for an ASN, enter the ASN number in the URL: https://threatfox.abuse.ch/asn/[ASN #].
- The authoring agencies encourage ISPs to implement routing security best practices such as those identified by NCSC-UK's Technical Report: Responsible Use of the Border Gateway Protocol (BGP) for ISP Interworking and the National Institute of Standards and Technology's SP 800-189 Rev. 1, Border Gateway Protocol Security and Resilience.
- See CISA's StopRansomware to learn more about ransomware threats and no-cost resources.
- See the joint #StopRansomware Guide for best practices to detect, prevent, respond, and recover from ransomware attacks.

Contact

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this document to CISA, FBI, NSA, and/or DC3:

- Contact CISA via CISA's 24/7 Operations Center (contact@cisa.dhs.gov or 1-844-Say-CISA [1-844-729-2472]) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- Contact DC3's DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) for DIB reporting and cybersecurity services (dc3.dcise@us.af.mil).

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing Cyber Centre at contact@cyber.gc.ca or online via the reporting tool Report a cyber incident - Canadian Centre for Cyber Security.

New Zealand organizations: Report cybersecurity incidents to incidents@ncsc.govt.nz or call 04 498 7654.

Netherlands organizations: Visit ncsc.nl for advisories, and report incidents by emailing NCSC-NL at cert@ncsc.nl.

United Kingdom organizations: Report a significant cybersecurity incident to ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Disclaimer

CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific

commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by CISA and the authoring agencies.

Acknowledgements

Amazon Web Services, Silent Push, and RedSense contributed to this guidance document.

Version History

November 19, 2025: Initial version.

References

"2024 Year in Review: Trends, Insights, and Lessons Learned." Silent Push. Accessed April 7, 2025. https://info.silentpush.com/year-in-review.

"How hosting providers can battle fraudulent sign-ups." SpamHaus Project. Accessed July 24, 2025. https://www.spamhaus.org/resource-hub/service-providers/how-hosting-providers-can-battle-fraudulent-sign-ups/#introduction.

"Infrastructure Laundering: Silent Push Exposes Cloudy Behavior Around FUNNULL CDN Renting IPs from Big Tech." Silent Push. Accessed September 19, 2025. https://www.silentpush.com/blog/infrastructure-laundering/.