SECURITY ADVISORY

CYBER STASH

November, 2025

Disrupting Adversary Infrastructure

Reducing Exposure to Bulletproof Hosting

Context

In recent years, the cyber criminal ecosystem has leaned heavily on special-purpose infrastructure known as "bulletproof hosting" (BPH) providers — operators that knowingly lease or resell hosting, IP space or Autonomous Systems to threat actors with little to no takedown response. These BPH providers offer an environment where malware-delivery, phishing, fast-flux DNS, command-and-control and data-extortion services can operate with impunity. The key enabler is that the hosting provider either ignores or actively resists abuse complaints, subpoenas or law-enforcement takedown requests — creating a safe haven for malicious actors.

Crucially, these BPH infrastructures are often blended within legitimate networks: they may lease IP blocks or Autonomous Systems from mainstream service providers, rotate Autonomous Systems Numbers rapidly, and dynamically evade filtering by moving malicious ranges across Autonomous Systems. As a result, defensive efforts must contend with the dual risk of blocking legitimate traffic or failing to disrupt the malicious infrastructure footprint.

In effect, the existence and growth of BPH providers amplify the overall cyber risk landscape by enabling a wide range of high-impact attacks — including ransomware, data extortion and large-scale phishing campaigns — with reduced operational risk for the attacker. The complicating factor is that organisations (and their upstream providers) cannot simply "turn off" all suspicious Autonomous Systems without risking collateral damage to legitimate services. Thus, the threat context for defenders is characterised by rapid infrastructure churn, asymmetric visibility, and operational complexity in attribution and disruption.

In this environment, the intelligence-driven understanding of BPH providers and their infrastructure behaviour becomes a critical enabler for proactive defence. Without tailored visibility into the malicious resource lists, traffic anomalies, and filtering strategy required, defenders are left reactive — while threat actors continue to exploit these platforms to scale and persist.

This report exposes the security risks fuelled by bulletproof hosting providers and provides clear, actionable mitigation strategies to reduce organisational exposure and improve resilience.

Infrastructure, Techniques, and Risks

Bulletproof hosting providers lease or resell Internet infrastructure specifically to criminals and refuse to respond to abuse or legal takedown requests. They deliberately configure their networks and business structures to evade detection, attribution, and shutdown. For example, Australia's cybersecurity centre notes that BPH operators lease IP address space and switch networks frequently to obscure customer activity.

Many BPHs obtain IPs from IP brokers or resellers, and then rapidly cycle or replace those addresses when service is disrupted. In practice this looks like an entire "whack-a-mole" chase: as soon as one IP block or ASN is identified and blacklisted, the provider moves its clients onto new prefixes or even registers a new Autonomous System Number (ASN) within days.

Spamhaus analysts confirm that "BPH services consistently change their Autonomous Systems and IP ranges," allowing defenders to block known malicious ASNs but requiring constant updates as adversaries rehome their infrastructure.

In short, BPH networks are designed for maximum disposability: criminals treat IPv4 space as a "disposable asset," abandoning one block and spinning up another whenever pressure arises.

IP and ASN rotation: BPH providers employ rapid network switching. They may lease multiple ASNs (often small, specialized networks) and shift IP ranges between them. When an ASN is blocked or a provider is shut down, customers' sites are migrated to fresh IP space or new ASNs almost immediately. This makes static IP blocklists only partially effective.

Reverse proxy pools (fast-flux DNS): Some BPH services offer "fast-flux" hosting as a feature. For instance, an analysis of a BPH vendor found it provided customers with a pool of hundreds of proxy IPs and "fluxes" the clients' domains across that pool at short intervals (minutes to hours) . This means a phishing or malware domain may resolve to a new IP every few minutes. Blocking one node simply means the domain resolves elsewhere moments later.

Leased and resold resources: Many BPHs do not own data centres or IP space outright. Instead they repackage legitimate services, leasing servers and IPs from downstream providers who may be unaware of the illicit end-use. These upstream providers (cloud hosts, collocation data centers, local ISPs) believe they are serving a regular customer, while the BPH resells that capacity to cybercriminals. This "nested leasing" adds layers of intermediaries and legal separation between the abused infrastructure and the actual

In some cases BPH operators even incorporate shell companies across multiple countries as fronts, so that even if one company is de-registered or raided, the criminal operation can continue under a new name in a different jurisdiction

These infrastructure tactics – rapid IP/ASN rotation, fast-flux DNS, and multi-layered reseller chains – are all designed to keep malicious services on the air. Defenders often find that taking down one node of a BPH network has little lasting effect because the operation simply reappears elsewhere. As a result, threat intelligence teams emphasize tracking not just IPs but entire ASNs and domain patterns, since historical data on known BPH networks can offer high-confidence indicators of malicious infrastructure.

Blocking by ASN (e.g. using blocklists like ASN-DROP) can preemptively block groups of IPs, but BPHs' dynamic ASN changes limit this approach's efficacy

Abuse-Evasion Techniques

By definition, bulletproof hosts defy abuse requests. They build their reputation on "no questions asked" tolerance for illicit content. In practice this means BPH providers ignore legal subpoenas, court orders, abuse complaints, and takedown notices. A classic description notes these services are "so called because they can be depended upon to ignore abuse complaints and subpoenas from law enforcement organizations".

Even when targeted by legitimate authorities, BPH operators often drag out or refuse cooperation. For example, U.S. guidelines report that some BPHs "impose onerous documentation requirements" on law enforcement and will only consider takedown requests after burdensome hurdles.

In other cases, BPH companies simply refuse to respond at all. Australia's cybersecurity guidance emphasizes that bulletproof hosts "actively ignore law enforcement engagement, government cooperation and abuse complaints" .

- **Ignoring and delaying takedowns:** BPH operators typically have a policy of non-cooperation. If authorities or security researchers report malicious content, the provider does nothing. In rare cases they claim to require extensive paperwork before considering removal, effectively stonewalling any takedown attempt. Victims and law enforcement learn that a takedown request is usually futile.

- **Legalistic defenses:** Some bulletproof hosts use legal threats and shell companies as shields. As documented by Spamhaus, a notorious BPH once hired U.S. shell companies to procure datacenter services, then sued the datacenter when asked to remove illegal content – arguing that the ISP was not responsible for its "customer's" activity. This kind of "separation of liabilities" means even if one component is challenged, the criminal service as a whole remains insulated.

- **Obfuscating ownership:** BPH providers often hide behind layers of corporate entities. Investigations have found that their business structures deliberately span many jurisdictions, creating "firewalls of plausible deniability" between each layer. For example, a data center may subcontract to a reseller company, which in turn sublets to the actual "hosting" company that delivers services to criminals. Each entity points blame to another, so by the time abuse is reported, the trail is cold.

In short, bulletproof hosts have built-in abuse resistance at both the technical and legal levels. Defenders note that simply blocking IPs or ASNs often backfires, because the operational model itself actively thwarts takedowns. Major BPH providers advertise this impunity explicitly: underground forum ads boldly claim "We won't get taken down" and promise to "respect your privacy and don't care about your activity".

Jurisdictional and Legal Exploitation

Bulletproof hosts gravitate to jurisdictions where enforcement is weak or legal hurdles are high. Many operate out of countries with lenient cyber laws or poor cooperation with international investigations. For instance, historical research notes that BPH first flourished in contexts like the Russian Business Network (RBN) in 2006, and contemporary analysis confirms that "Russia has become a permissive environment for cybercriminal groups," where operators have close ties to local officials or simply face little scrutiny. Other common bases include Ukraine, China, Moldova, Romania, Bulgaria, and small offshore enclaves (Belize, Panama, Seychelles, etc.). These jurisdictions often lack extradition treaties or mutual legal assistance pacts with Western countries, making it very difficult for U.S./EU/Australian authorities to compel cooperation or seize assets.

- **Permissive hosting countries:** BPH providers tend to put servers in places where court orders and law enforcement have no teeth. Research and public reporting list Russia (especially St. Petersburg), Ukraine, China, and certain Eastern European or Central Asian states as hotspots.

For example, the Russian firm Media Land (St. Petersburg) was sanctioned by the US/UK/Australia in 2025 for enabling dozens of ransom ware groups, reflecting Russia's outsized role in providing BPH infra structure. In some cases providers claim to be in one country while their ownership is registered in another, complicating legal jurisdiction (e.g. a UK-based shell company fronting a Russian operator.

- **Legal loopholes and front companies:** Criminal-friendly jurisdictions often have corporate laws or regulatory gaps that the BPH can exploit. For instance, some BPHs form British or American shell companies to appear legitimate, even if their actual management and servers are abroad. Spamhaus observes that a recent trend is using "unobtrusive" UK/US entities in addition to, or instead of, known offshore havens. These Western-registered facades undergo cursory vetting and are less likely to draw attention than a Caribbean LLP. Meanwhile, true control remains with the criminals hiding behind those fronts.

- **Limited law enforcement reach:** Because of these factors, standard takedown mechanisms (like ISPs cutting connectivity after a court order) often fail. Even mutual legal assistance treaties may be hard to invoke if the provider's country is unwilling or too slow to act. Australia's advisory report notes that BPH operators often choose "permissive cyber regimes" with non-existent or lenient regulations. This is intentional: operating in such jurisdictions effectively immunizes the criminals from swift legal action.

AS Hijacking, Fast-Flux DNS, and Nested Leasing

Bulletproof hosts also employ technical network strategies to hide operations. Besides leasing IPs legitimately or via brokers, attackers sometimes hijack unused IP address blocks for their servers. Spamhaus calls a hijacked network "digital no man's land": often the original owner of the address space is defunct or merged, and the new (illicit) announcer simply operates unchallenged for years. While actual IP hijacking is somewhat rare and often eventually becomes blacklisted, it remains an attractive option because it leaves no easy paper trail to a current owner.

More commonly, however, BPH providers use legitimate allocations (via resellers) and then move on quickly if probed. In some campaigns, criminals even abuse major content delivery networks (CDNs) for "living off trusted services": by pointing malicious domains at a CDN (e.g. Cloudflare), they make takedown extremely difficult without collateral damage.

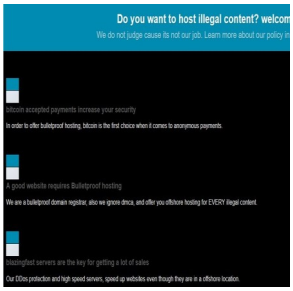
- **Fast-flux DNS and proxy services:** As noted above, providers may offer rotating proxy pools under the banner of "fast-flux" hosting. This technique changes the DNS record for a domain at very short intervals (often minutes), cycling through a large pool of front-end IPs. Each IP might itself proxy to the actual malicious server (reverse proxy), so blocking one IP only forces the actor to another. Some BPH vendors explicitly advertise these fluxing proxy networks to make their customers' sites "more resilient, harder to trace, and more resistant to takedown".
- **Autonomous System (AS) abuse:** Criminals also abuse ASNs in unconventional ways. For example, they can apply for new ASNs under fake identities; one industry report notes that BPHs can obtain a fresh ASN in as little as 2–5 business days, then transfer their IP ranges to it. This means defenders who block an ASN must watch new announcements continuously. BPH operators may also insert themselves as transit networks for each other, or spoof BGP announcements – techniques that blur the actual AS path. While outright BGP hijacking of others' traffic is less common, some BPHs have been found announcing routes to IP blocks they don't legitimately own (for example, attacking upstream filters by announcing someone else's prefixes).
- **Nested leasing and reseller chains:** A hallmark of modern BPH is the "separation of liabilities" through nested leasing. One Spamhaus analysis describes conversations where a datacenter says "ask my customer", the customer says "ask the server owner", the owner says "I only have an email and crypto wallet on file for this client". In practice, this means a BPH host may only lease physical servers, then rent virtual machines or proxy services onward, each step looking only at the next link. Some operations even sublease to shell ISPs, who in turn lease from actual carriers – producing multi-layered obscurity. Each layer shields the one below: if law enforcement subpoenas the top-level entity, it can claim it is merely a middleman with no real insight.

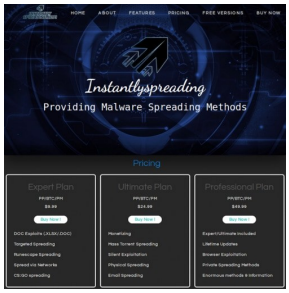
These techniques compound the difficulty of tracing a BPH operation. Even if one node (IP or domain) is identified, it typically belongs to a shifting cloud of addresses and front companies. The dynamic nature of ASNs and DNS records in these networks means defenders must rely on threat intelligence (e.g. recognized domain patterns, AS reputation, and historical routing data) to stay ahead.

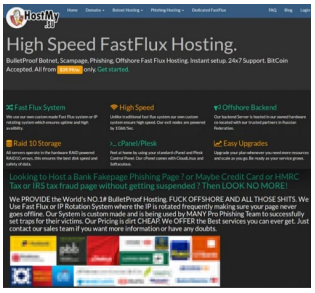
Attacker Tactics Using Bulletproof Hosting

How do criminals actually use these services? Typically, threat actors find BPH providers on underground forums, private messaging channels or hidden marketplaces, often advertised as "offshore" or "anonymous" hosting. They sign up under aliases (sometimes paying just in cryptocurrency and providing no real identity) and begin deploying malicious infrastructure. For example, a 2025 Australian report depicted a mock BPH ad boasting "Proxy networks to obfuscate client activity… C2 infrastructure for malware… Botnet C2 servers… Domain Registration… Hosting outside [police] reach," with payment accepted in Bitcoin, Tether, Ethereum, and Litecoin.

Figure: *Examples of an underground forum advertisement for bulletproof hosting services, offering proxy networks, malware C2 hosting, and acceptance of cryptocurrency payments.*







Key aspects of attacker usage include:

- **Anonymous registration and payment:** BPH providers generally require minimal information to open an account. Some have no KYC (Know Your Customer) at all – a leaked BPH operation boasted that they only collected an *email address and a crypto wallet* from each client, nothing more. Payment is almost always via cryptocurrency or other untraceable means. For instance, a 2025 industry write-up notes providers "often accept anonymous payments, like cryptocurrency, and require minimal personal information," making it "nearly impossible to trace" the real customer. This allows ransomware groups and other operators to pay for persistent hosting without revealing their identities.
- **Infrastructure setup:** Once registered, criminals configure their payloads on the BPH servers just as they would on any hosting account. They upload command-and-control (C2) servers, phishing sites, malware droppers or botnet panels to the virtual machines or dedicated servers provided. Because the host promises no takedowns, attackers feel free to run illicit services openly. Some providers even assist by pre-allocating TLS certificates or wildcard domains to their clients (often at extra cost). The client may then point their malware or spam campaigns at those C2 domains or IPs, trusting that the infrastructure will remain live despite abuse notices.

- ***Resilience tactics:*** *Finally, attackers leverage the BPH's own agility. If law enforcement or researchers do identify an active IP or domain, the client can quickly spin up a replacement. They may use domain-generation algorithms or take advantage of the host's "fast flux" to rapidly shift their service to a new address. In practice, an attacker might configure their malware to check-in with multiple backup domains, so even if one is taken down by a typo or blocking, the others still connect to the resilient BPH network.*

In short, BPH providers are sold and used as crime enablers. They let inexperienced or high-profile attackers bootstrap complex campaigns without worrying about quick shutdown. Cybercriminal forums routinely list bulletproof hosts as part of their toolkit (alongside bulletproof VPNs, anonymizing proxies, and bitcoin mixers), and veteran threat intelligence warns that "bulletproof hosting is probably the biggest enabling service" in the underground. Indeed, research indicates any group "that can afford [such] services are somewhat more sophisticated," since they trust the stability of their C2 and malware delivery infrastructure.

Types of Adversaries Using BPH

Bulletproof hosting serves a wide spectrum of malicious actors. The most prominent users are cybercrime syndicates and ransomware groups. High-profile ransomware gangs like LockBit, BlackCat (ALPHV), BlackSuit and Play have all been tied to Russian-based BPH networks, as these criminals rely on robust, uncensorable infrastructure to host leak sites and C2 servers. For example, U.S. Treasury reports confirm that Media Land (a St. Petersburg BPH) supplied infrastructure to LockBit, BlackSuit and others.

Similarly, the Aeza Group (also Russian) has provided hosting for strains of banking malware (Dridex, Zeus) and was linked to ransomware like BianLian. Criminal spam and phishing operators are another major user: they put phishing kits, credential stealers, fake bank login pages, and spam mailing scripts on BPH servers to keep campaigns alive.

Other malicious groups include cyber-espionage and APT actors who need resilient C2. While less publicized, nation-state or advanced persistent threat (APT) teams have also been known to abuse BPH services for command servers when stealth is paramount. In some cases, BPH providers with close ties to certain governments have attracted like-minded advanced threat actors.

For example, one contractor in Eastern Europe routinely advised criminal and state-linked customers to route their content behind a CDN (Cloudflare) to obscure origin. Moreover, hybrid criminal-political operators use BPH too. Recorded Future notes that the Aeza Group even played a role in pro-Kremlin disinformation ("Doppelgänger") campaigns in Europe, and UK officials have sanctioned BPH-facilitated operations spreading propaganda (e.g. Social Design Agency).

In summary, BPH infrastructure underpins "every part of cybercrime," from spam botnets and data exfiltration to extortion and disinformation. Defenders emphasize that if a threat actor's toolkit includes malware delivery, phishing, or DDoS capabilities, it is "one of the core enablers of modern cybercrime". Indeed, law enforcement actions tend to hit BPH providers when they see broad criminal use: in 2025 alone, multiple Russian bulletproof hosts (Media Land, ZServers, Lolek) were dismantled or sanctioned after global partnerships identified them as backbone platforms for ransomware and malware networks.

Defender Challenges and Mitigation

Protecting networks from bulletproof-hosted threats is uniquely challenging. BPH infrastructure is highly dynamic and entwined with legitimate services, broad blocks risk collateral damage. As one mitigation guide warns, simply blacklisting an entire ISP or CDNs runs the risk of "impacting legitimate activity".

For example, defenders might see a malicious domain suddenly moving to Cloudflare or another popular CDN – shutting off the CDN would disable many benign sites as well. Similarly, traditional IP-based firewall rules can be circumvented by fast-flux techniques: if you block IP X today, tomorrow the same domain is at IP Y.

The Intel471 team notes that defenders must maintain up-to-date lists of known BPH ASNs and IPs, but even this is a chase – BPHs rotate ASNs at will.

- ***Uncertainty of attribution:*** *Since BPH networks span multiple ASNs and countries, identifying a malicious host requires correlating many signals (AS reputation, domain history, hosting patterns). A domain's WHOIS or an ASN's registrant info is often fake or outdated. Investigators have reported that even registering front companies in the UK or US creates a false sense of legitimacy – these shell entities reveal little about who really controls the IP space.*
- ***Dynamic infrastructure:*** *Malicious actors exploit the speed of change. A Cybersecurity and Infrastructure Security Agency (CISA) advisory points out that BPH operators can obtain a new ASN within days and remap all their services, making static filters obsolete. Similarly, BPH clients often use temporary email accounts and frequently update DNS records or CNAMEs, so defenders may not see the same artifact twice. In practice, this means that automated blocklists must be refreshed constantly, and real-time intelligence sharing is crucial to keep pace with the adversary.*

- ***Balancing blocklists and accessibility:*** *If organizations block all traffic to an entire ASN known for bulletproof hosting, they risk cutting off legitimate customers hosted there. U.S. guidance explicitly recommends that any filtering be "nuanced" and carefully weighed against business needs. One example is using layered defenses: combine IP/ASN blacklists with domain-based filters (so legitimate mail servers at that ASN aren't blocked, only known malicious domains are). Many defenders also implement "long-tail" blocking: they block small ASNs dedicated to BPH while avoiding large mixed-use ASNs. Intel analysts suggest that a newly minted ASN used by known BPH actors can often be fully blacklisted with minimal collateral, because it carries only criminal traffic.*

Finally, there is the systemic challenge of cross-border enforcement. Because BPH operators exploit jurisdictional gaps, network defenders alone cannot stop them. International collaboration is required. Recent coordinated sanctions against Media Land and Aeza (US/UK/AUS and others) highlight that law enforcement is now targeting BPH providers directly.

Cybersecurity agencies have published mitigation guides and are sharing threat intelligence on BPH networks (e.g. CISA's 2025 guide, ASD's alerts) to help organizations block bulletproof infrastructure proactively.

Yet even with these steps, experts warn that complete takedowns are unlikely – BPH operators have shown resiliency by spinning up replacements. Instead, defenders focus on making BPH hosting as unattractive as possible, by cutting off affiliates (e.g. pressuring downstream data centres or transit providers to drop suspicious clients) and by systematically devoting resources to tracking and naming these services.

CyberStash emphasises that targeting adversary infrastructure — combined with exception handling for trusted services — is key to reducing exposure without impacting legitimate business operations.

Case Studies

The following table presents ten high-confidence case studies where advanced persistent threat (APT) groups deliberately leveraged bulletproof hosting (BPH) infrastructure to support operations spanning espionage, financial theft, malware delivery, and long-term command-and-control. These are not isolated incidents, but strategic infrastructure choices that underpin entire campaigns.

While each APT group differs in terms of geopolitical alignment, technical sophistication, and mission objectives, they all converge on one foundational need: infrastructure that offers resilience, anonymity, and resistance to takedown. Bulletproof hosting provides precisely that — acting as the digital equivalent of a safehouse for malicious operations.

Where these actors diverge is in their method of exploitation. Some rely on fast-flux DNS and rotating IP infrastructure to evade detection and increase scalability. Others abuse offshore ASNs and legal havens, exploiting jurisdictions that are slow to act on abuse complaints. More advanced threat actors, particularly those aligned with state objectives, often blend BPH nodes with compromised infrastructure or legitimate cloud services — creating hybrid environments that complicate attribution and disruption.

Across these cases, BPH is not a convenience — it's a force multiplier. It enables attackers to persist, adapt, and escalate with reduced operational risk. By studying these examples, defenders gain critical insight into how infrastructure decisions shape threat capabilities, and why mitigating exposure to bulletproof networks is essential to strategic risk reduction.

APT Group	Bulletproof Hosting Service / Infrastructure	Attack Information	TTPs Related to BPH Usage	Key Aspects / Notes
APT-C-36 (Blind Eagle)	Proton66 OOO (Russia)	Spear-phishing Latin American gov & financial targets with downloaders & RATs.	Use of Russian BPH ASNs, DDNS domains, rotating C2 IPs, malware hosting.	Direct attribution: Proton66 IP 45.135.232(.)0/24 used for C2 & phishing landing pages.
Lazarus Group (North Korea)	BPH providers in Malaysia, India, Bulgaria, Seychelles	Financial theft, crypto exchange intrusions, SWIFT fraud.	Fast-flux DNS, disposable VPS nodes, multi-hop proxy networks.	Lazarus uses criminal BPH networks to hide high-risk financial C2 infrastructure.
Turla (Russia / FSB)	Long-term use of compromised servers + offshore BPH nodes	Espionage targeting EU/Middle East ministries.	Hosting C2 proxies on bulletproof hosts + hijacked servers blended.	Turla maintains redundant C2 hosted in permissive jurisdictions with weak takedown.
Gamaredon (FSB-aligned, Russia)	Russian & Crimean BPH networks	Rapid-fire phishing + mass malware distribution.	Fast-moving C2 IP rotation, use of "burner" ASNs with no abuse response.	Known for high-volume infrastructure churn and reliance on BPH services.
TA505 (FIN11, Russian-speaking)	LolekHosted, YalvHost & anonymous EU BPHs	Ransomware deployment (Clop), large phishing waves.	Hosting C2 & droppers on servers that ignore abuse requests, rapid domain rotation.	DOJ indictment confirmed use of LolekHosted for ransomware ops.
MuddyWater (Iran)	Criminal VPS hosts in Pakistan, India, Turkey	Espionage, destructive malware disguised as ransomware.	Use of cheap offshore VPS that ignore subpoenas, multi-stage proxying.	Known for blending BPH nodes with compromised servers to stretch attribution.

Table: APT Use of Bulletproof Hosting Infrastructure

Mitigation Strategy

5-Step Risk Reduction Plan

Effective exposure reduction begins with understanding where threats originate and how they interact with your environment. The following five steps outline a structured approach that any organisation can use to identify high-risk sources, validate legitimate needs, and implement targeted controls that reduce exposure over time.

First, we correlate known threat indicators to uncover hostile infrastructure patterns. Next, we build a threat landscape profile tailored to the organisation's real attack activity. We then validate legitimate business traffic to ensure essential services remain unaffected. Once validated, tactical block policies are applied to restrict risky infrastructure categories. Finally, this process is repeated at regular intervals, gradually reducing the organisation's exposure and improving overall resilience.

Figure: *Steps to Reduce Risk from Bulletproof Hosting Providers*

In the next section, we examine how CyberStash brings this framework to life through the Eclipse.XDR Technology Stack — transforming a high-level methodology into a fully automated, intelligence-driven defence capability.

Mitigation Strategy

Reducing Exposure to Bulletproof Hosting Through Intelligence-Driven Blocking

Bulletproof hosting infrastructure succeeds because most organisations treat malicious traffic as random, isolated events. In reality, the vast majority of attacks originate from repeatable patterns — the same ASNs, the same TLD clusters, the same geo-regions and proxy networks used by criminal and APT groups. CyberStash's defensive methodology is built around making these patterns visible, quantifiable, and then operationalised into proactive control.

Our approach focuses on reducing an organisation's exposure footprint to the hostile parts of the Internet where BPH providers operate, without disrupting legitimate business needs. CyberStash achieves this through a multi-stage, intelligence-driven methodology:

Step 1: Correlate Known Threat Indicators Against Infrastructure to Determine High-Risk Sources

We begin by analysing the organisation's live threat telemetry — including DNS, Web, Proxy, VPN, Email, and Endpoint alerts — and correlate every malicious or suspicious indicator against:

- *Autonomous System Numbers (ASNs) known to host malware, phishing, C2 infrastructure, or BPH networks.*
- *Top-Level Domains (TLDs) with disproportionate abuse rates (e.g., .top, .xyz, .support, .rest, .cam).*
- *Geo-IP / Country intelligence that identifies high-risk jurisdictions with permissive cyber-crime environments.*
- *Hosting provider lineage, including nested resellers, VPS brokers, and IP brokers used by BPH operators.*

This correlation stage reveals where the organisation is actually being targeted — not the abstract, global threat landscape, but their personal threat map.

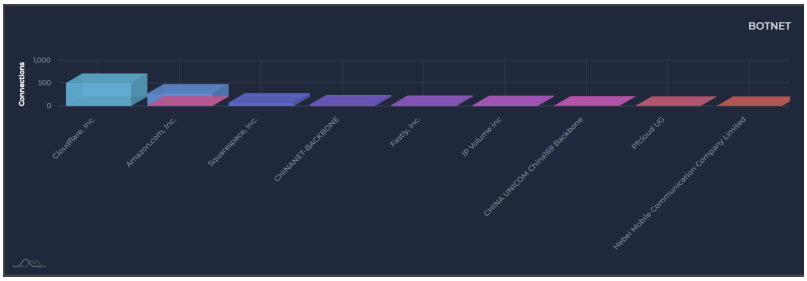


Figure: *Top Botnet ASNs (Source: CyberStash Eclipse.XDR)*

Step 2: Build an Environment-Specific Threat Landscape Profile for the Organisation

By aggregating these correlations, we generate a threat distribution heatmap that shows:

- *Which ASNs are most frequently attacking or probing the environment*
- *Which countries are responsible for the majority of malicious traffic*
- *Which TLDs appear in repeated phishing, malware delivery, or callback attempts*
- *Whether the patterns align with known bulletproof hosting operations*

This produces a data-backed view of the organisation's exposure, replacing guesswork with measurable adversary infrastructure patterns. Most organisations discover that 5–10 ASNs, 5–7 countries, and a handful of TLDs account for 70–95% of their malicious inbound activity — the exact infrastructure classes used by BPH networks.

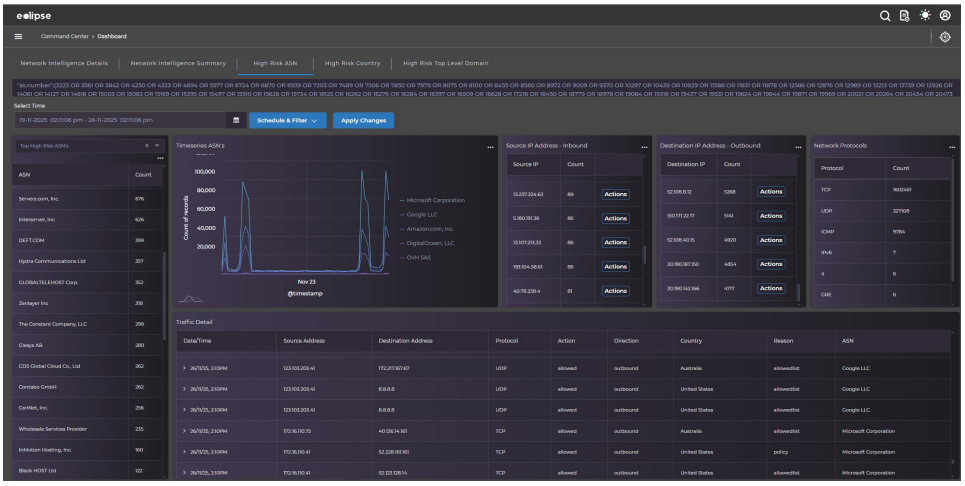


Figure: *ASNs Analytics (Source: CyberStash Eclipse.XDR)*

Step 3: Validate Legitimate Business Requirements

Before enforcing policy controls, we conduct a business validation layer:

- *Identify whether any legitimate applications, partners, or suppliers operate within the "high-risk" infrastructure.*
- *For any required exceptions, we add precise, narrowly scoped allowances (specific IP ranges, subnets, or domains), not broad exclusions.*

This step ensures that security controls are high-confidence and business-safe — the organisation blocks adversaries while preserving legitimate operations.

Step 3: Validate Legitimate Business Traffic to Define Safe Exceptions

Before enforcing policy controls, we conduct a business validation layer:

- *Identify whether any legitimate applications, partners, or suppliers operate within the "high-risk" infrastructure.*
- *For any required exceptions, we add precise, narrowly scoped allowances (specific IP ranges, subnets, or domains), not broad exclusions.*

This step ensures that security controls are high-confidence and business-safe — the organisation blocks adversaries while preserving legitimate operations.

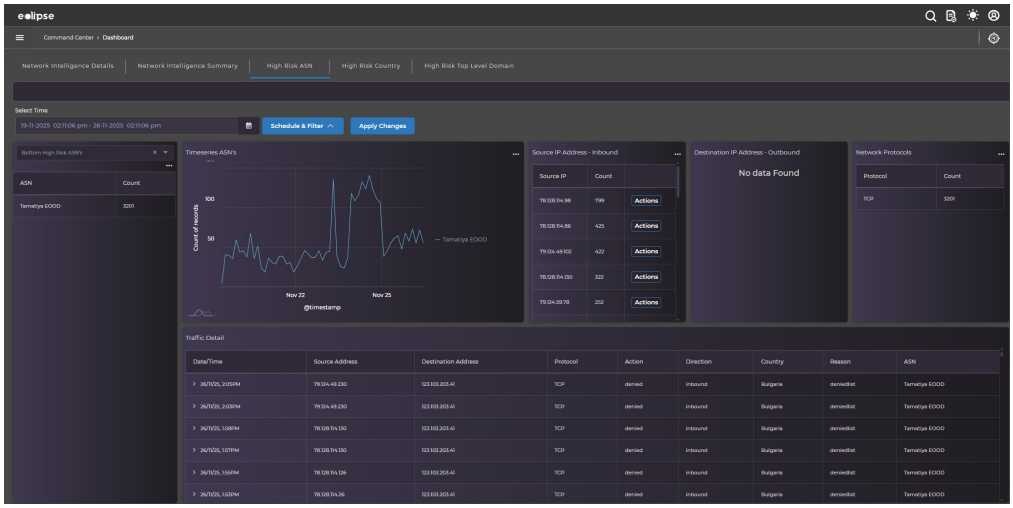


Figure: *ASNs Filtered Analytics (Source: CyberStash Eclipse.XDR)*

The above figure illustrates how filtering at the ASN level enables proactive risk reduction. In this example, we have isolated ASN Tamatiya EOOD (AS50360).

Over the past seven days, all observed traffic associated with this ASN has been inbound, and every event has already been correlated against CyberStash threat -intelligence block lists — meaning the XDR Gateway is already blocking these connections.

AS50360 contains more than ***5,300 IP addresses****, despite its size, no legitimate traffic to or from any of the 5,300+ IP addresses within AS50360 has been observed in the organisation's environment. Given this pattern, and the fact that all inbound interactions have been classified as malicious, the ASN can be safely blocked in its entirety. By doing so, we get ahead of any future attacks that may originate from any other IP address within this high-risk ASN.*

This methodology allows us to enforce tactical blocks without disrupting legitimate business traffic or user applications. Most importantly, it breaks the dependency on having prior knowledge of an attacker's specific IP address or domain before we can act. By blocking at the infrastructure level — ASN, country, or TLD — we stay ahead of future attacks that may originate from any other IP within this high-risk network.

Step 4: Deploy Tactical Block Policies for the High-Risk Infrastructure

Once validated, CyberStash applies a targeted enforcement layer on the XDR Gateway:

- *Country-level blocks on regions with no legitimate business value but high malicious density.*
- *ASN blocking, surgically removing entire hostile networks used by BPH operators.*
- *TLD blocking, cutting off high-abuse domain categories popular with phishing kits and C2 setups.*
- *Real-time feedback loop, where new indicators update and refine block policies continuously.*

This shifts the organisation from reactive detection to proactive exposure elimination — shutting down entire infrastructure classes before attackers even attempt to connect.

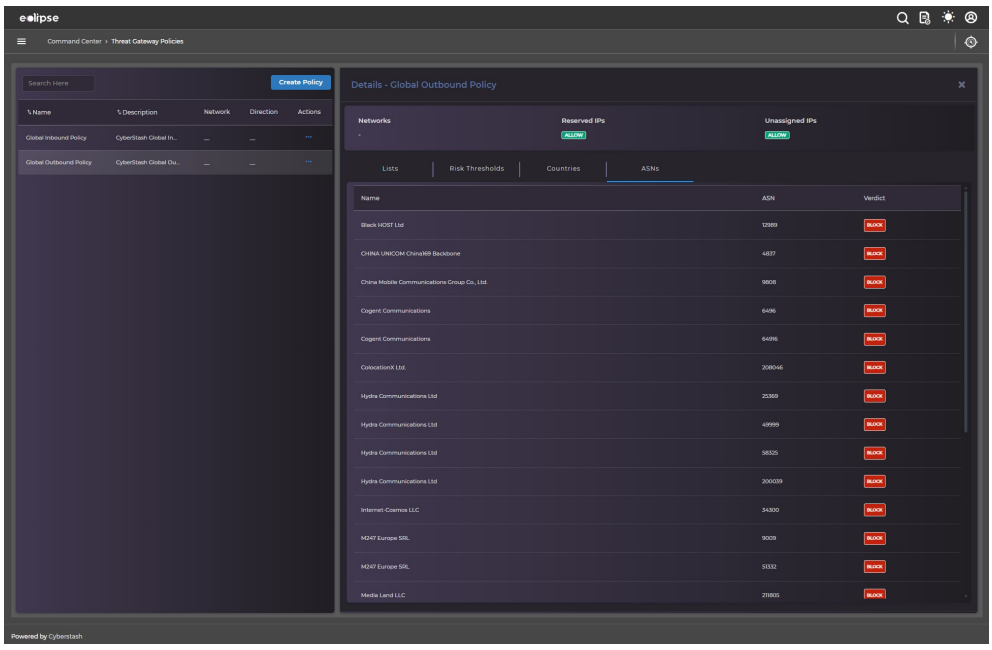


Figure: *ASNs Blocking Policy (Source: CyberStash Eclipse.XDR)*

Step 5: Continuous Reduction of Exposure Over Time

As malicious ASNs, TLDs, and countries are blocked:

- *The attack surface shrinks rapidly*
- *Unwanted traffic drops significantly*
- *Malware delivery and exploitation attempts lose their infrastructure pathways*
- *Organisations experience fewer alerts, fewer incidents, and fewer investigation demands*

CyberStash's clients typically see a 70–95% reduction in permitted hostile traffic within weeks, with exposure continuing to decline as block policies mature.

Why This Works Against Bulletproof Hosting

Bulletproof hosting providers survive because defenders allow their networks to reach internal systems by default. By blocking the hostile infrastructure rather than the attack artefact, CyberStash eliminates:

- *The attacker's ability to deliver payloads*
- *The callback path for malware*
- *The communication channel for C2*
- *The delivery infrastructure for phishing and credential harvesting*

This is how we "get ahead of the attacker" — by dismantling the infrastructure they rely on, not just detecting the symptoms they produce.

References

- Australian Cyber Security Centre / Cyber.gov.au: “Bulletproof Defense: Mitigating risks from bulletproof hosting providers” https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/network-hardening/bulletproof-defense-mitigating-risks-from-bulletproof-hosting-providers
- Australian Cyber Security Centre / Cyber.gov.au: ““Bulletproof” hosting providers: Cracks in the armour of cybercriminal infrastructure” https://www.cyber.gov.au/about-us/view-all-content/publications/bulletproof-hosting-providers
- IC3.gov (U.S. Internet Crime Complaint Center) / CISA joint publication (PDF): “Mitigating Risks From Bulletproof Hosting Providers” https://www.ic3.gov/CSA/2025/251119.pdf
- The Spamhaus Project: “The anatomy of bulletproof hosting – past, present, future” https://www.spamhaus.org/resource-hub/bulletproof-hosting/the-anatomy-of-bulletproof-hosting-past-present-future-/
- The Spamhaus Project: “Bulletproof hosting – there’s a new kid in town” https://www.spamhaus.org/resource-hub/bulletproof-hosting/bulletproof-hosting-theres-a-new-kid-in-town/
- KrebsOnSecurity: “Meet the World’s Biggest ‘Bulletproof’ Hoster” https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/
- The Record (Recorded Future News): “US, allies sanction Russian bulletproof hosting services for ransomware support” https://therecord.media/bulletproof-hosting-sanctions-ransomware