

# Criminal Hideouts for Lease: Bulletproof Hosting Services

**Max Goncharov**

Forward-Looking Threat Research (FTR) Team



#### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

## Contents

4

### BPHS basics

5

### Popular content and services

6

### Classifying BPHSs

13

### The case of RandServers

17

### What keeps BPHS providers alive?

23

### Ongoing security challenges



Bulletproof hosting services (BPHSs) play a very crucial yet very low-key role in cybercriminal operations. When thinking about cybercrime, the focus is normally drawn to the modus operandi or the cybercriminals behind it. BPHS is relegated to an incidental detail of a much grander scheme. The reason, perhaps, is that this service stays in the background and does not overtly affect cybercrime victims. But it would be foolish to downplay its significance. Without BPHS, many, if not all major cybercriminal groups would cease to operate.

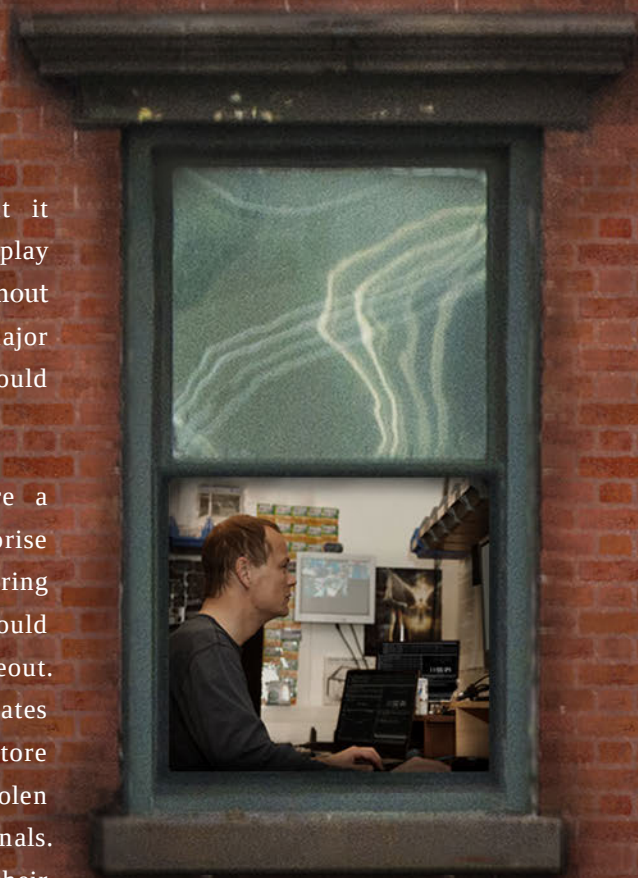
If we were to compare a cybercriminal enterprise to a real-world crime ring operation, BPHS would serve as the gang's hideout. As real-world syndicates use their hideouts to store their contraband and stolen goods, so do cybercriminals. They use BPHSs to keep their malicious tools (malware components, browser exploit kits, etc.); serve as botnet command centers; act as repositories of stolen information; or host sites used in phishing, pornography, or scams. To ensure the smooth flow of transactions, both hideouts and BPHSs must be strategically located to make them harder to seize

and be inconspicuous enough to avoid calling the attention of authorities.

Much like crime ring hideouts, BPHSs put up a legitimate facade. Real-world crooks may rent out an apartment or a shop as a front to hide the shady dealings that go on in their back rooms. The building owners will let them do whatever they want as long as they pay rent. The same applies to cybercriminals who avail of BPHSs. BPHS providers are known to allow customers to host any type of content—even if they're malicious—just as long as the latter pay. Of course, this is only one example of the BPHS business models that this paper discusses.

This paper covers all of the different types of BPHSs, how they work, and what keeps them afloat. It also includes a brief case study

featuring a popular BPHS provider and how, like a legitimate business, it strives to stay relevant and stand out from its competitors. Finally, it touches on the challenges and possibilities of taking down these cybercriminal hideouts.





## BPHS basics

Bulletproof hosting servers are hardware-, software-, or application-based hosting facilities that can store any type of content or executable code. Unlike regular hosts, bulletproof servers can primarily host malicious content like phishing sites, pornography, fake shopping and carding sites, and command-and-control (C&C) infrastructure.

BPHS operations are complex; diversifying bulletproof-hosting-server structures, much more so. On one hand, bulletproof hosts need to offer solid services that ensure stability to customers. On the other, BPHS providers aspire to appear as legitimate as possible so authorities would not shut them down. Bulletproof host owners rent hardware colocation facilities in various countries to ensure the continuity of their operations. They normally rely on countries with lax laws to minimize the risk of being blacklisted or shut down.

### Noteworthy BPHS providers

The Russian Business Network (RBN) can be considered one of the first big BPHS providers. It was rooted on free-hosting service providers like narod.ru, GeoCities.com (now Yahoo! Small Business), ucoz.ru, and tripod.com, which were ad based [1]. Tagging their service offerings “free” allowed the providers to gain popularity as hosts to small phishing campaigns and good places to store and share music and other files.

As time passed, anyone who wanted to earn from cybercrime required “professional” hosting services in the form of bulletproof servers. Though RBN provided services worldwide, it also primarily served local clients.

Perhaps the most notable BPHS-related incident recorded in history happened on March 2013 [2], when the infamous Off-sho.re and a group of attackers, all BPHS providers, targeted Spamhaus—a project established in 1998 by Steve Linford to track email spammers [3, 4]. The attack caused the site to crash.

# Popular content and services

BPHS providers in certain countries or regions specialize in hosting different kinds of content and services. What we listed below are just a few of the many content and service types:

- **Fakes shopping sites:** These include sites that sell any kind of fake products (watches, designer clothes, electronics, pharmaceuticals, etc.) to users in various countries where selling them may be prohibited and punishable by law.
- **Torrent file download sites:** These strictly follow internally structured rules that help them keep their torrent files searchable and accessible [5].
- **Blackhat search engine optimization (SEO) pseudo sites:** These are developed and maintained for fully searching engines so customers can buy or sell Web traffic, which can help them get bigger revenue from their own sites. They also act as traffic concentrators, traffic direction systems (TDSs), drop zones, or doorways. The traffic driven to customers' sites is, in most cases, obtained through malicious or fraudulent techniques and tools like malvertising, fake apps, and iframes.
- **Brute-forcing tools:** Sites that host these focus on discovering weak passwords and access credentials that can be exploited and owned to compromise email accounts, server infrastructure, Web-based services, and other online accounts. Brute-forcing tools scan networks and guess passwords to gain access.
- **C&C components:** Sites that host these have environments suited for controlling networks of infected client systems and other botnet-related infrastructure (infected file drop zones, exploit kit locations, stolen data storage sites, etc.).
- **Virtual private networks (VPNs):** These hosting facilities can act as exit points to protect their owners' privacy from security researchers and law-enforcement agencies.
- **Warez forums:** These provide information on overriding protective measures against software and hardware piracy. They refer to sites where key generators, cheat codes, and commercial software can be obtained for free.
- **Files that violate the Digital Millennium Copyright Act (DMCA) [6]:** Sites that host these contain all kinds of commercially available copyrighted content, which can be downloaded free of charge.
- **Spam:** Sites that host these also contain all kinds of tools used in mass-mailing attacks for profit or other malicious gains.

# Classifying BPHSs

Given the diversity of features that BPHSs offer, we devised a simple set of criteria below that would allow fellow researchers to better classify and analyze them:

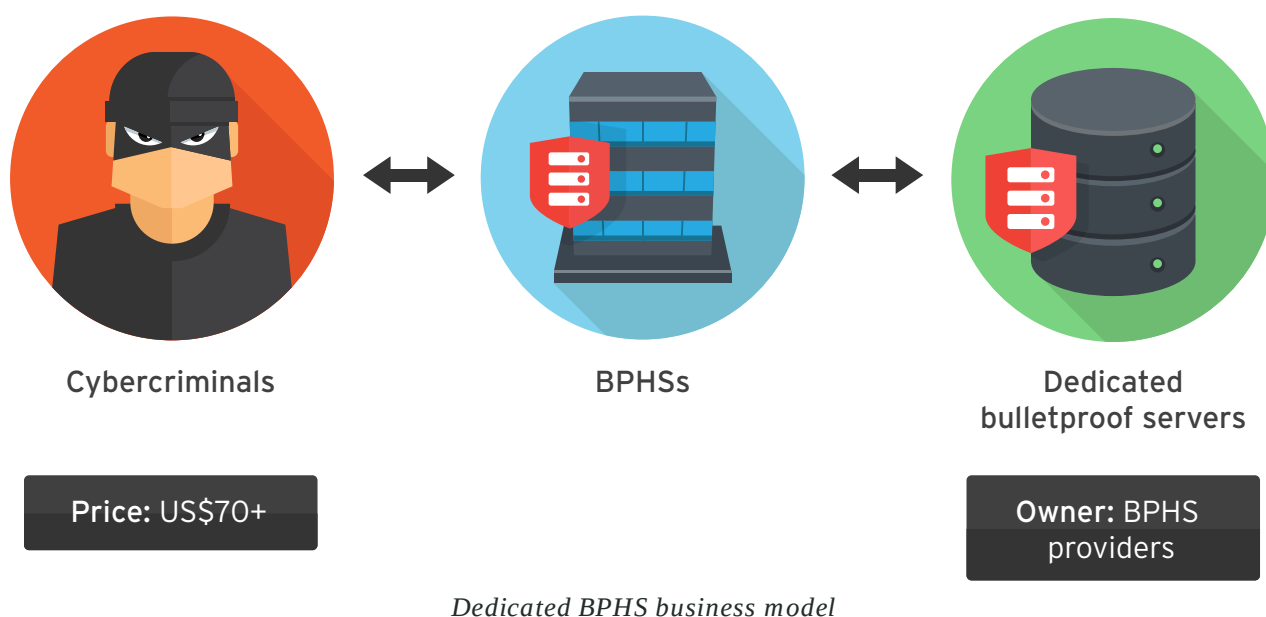
|   |                               |                                                                                         |
|---|-------------------------------|-----------------------------------------------------------------------------------------|
| 1 | <b>Business model</b>         | How do BPHS providers operate?                                                          |
| 2 | <b>Toxicity level</b>         | How malicious (toxic/dangerous) is the content/service hosted on a BPHS infrastructure? |
| 3 | <b>Geolocation</b>            | Where are the bulletproof servers physically located?                                   |
| 4 | <b>Targets and exceptions</b> | Which regions are targeted by/protected from the hosted content?                        |
| 5 | <b>Price</b>                  | How much does hosting cost?                                                             |
| 6 | <b>Popularity</b>             | How popular are BPHS providers based on customer feedback?                              |
| 7 | <b>Longevity</b>              | How long has a BPHS provider been operating?                                            |

## Business model

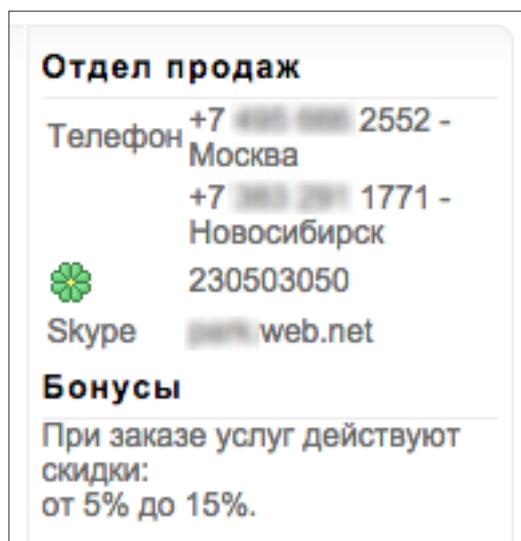
BPHS providers operate in a number of ways. We've broken them down into three simple models.

### Model 1: Dedicated bulletproof servers

Those who operate under this model know exactly what they're doing. BPHS providers who use this business model allow their customers to host content that may be considered illegal in certain countries.



These BPHS operators make their infrastructure appear as legitimate as possible to avoid arousing suspicion from law enforcement. They also make their servers as takedown-proof as possible. This is why cybercriminals often avail of their services. They will continue to make their servers available to customers unless they are mandated to stop serving bad content.

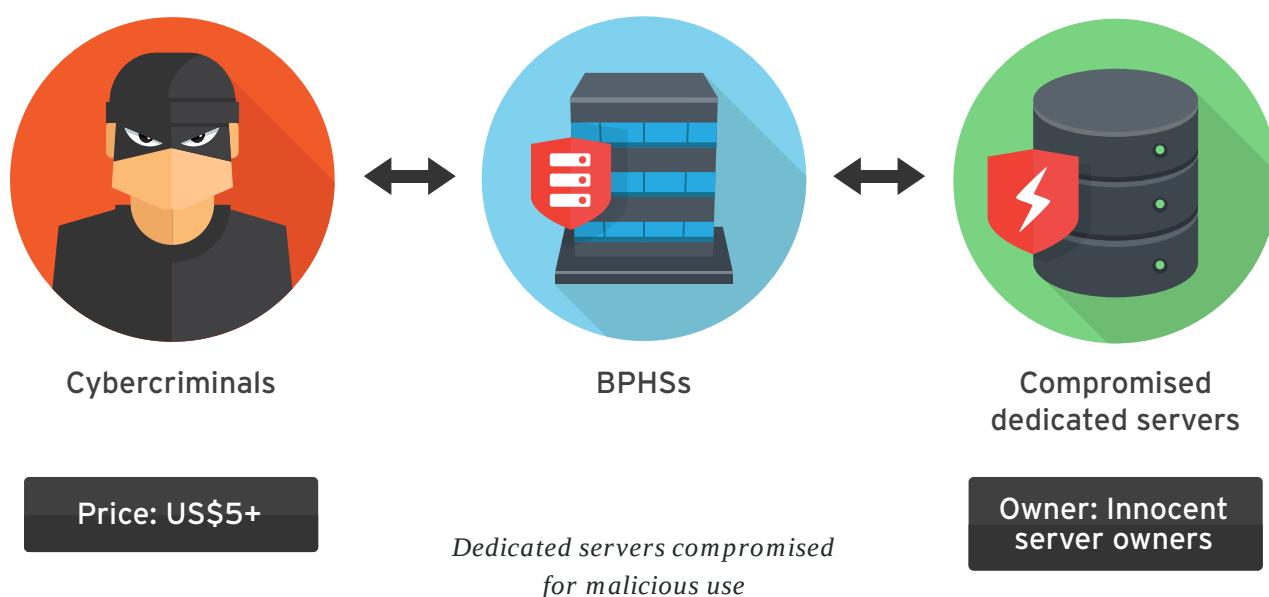


*Sample contact details of a BPHS provider*

Providers who use this model often only make their ICQ or phone number publicly available. In the given example, a provider is renting out a bulletproof server for US\$70 or more a month.

## Model 2: Compromised dedicated servers

Some BPHS providers choose to compromise dedicated servers. They then rent these out to parties who wish to host malicious content. But this is a temporary setup. Once the real owner of the compromised server detects the anomaly, the BPHS providers can no longer use the server.



Hosts of this type are often used to facilitate blackhat SEO and brute-forcing attacks. Below is a list of compromised dedicated servers ideal for brute-forcing attacks. For US\$5, a customer can rent a server for a one-time attack.

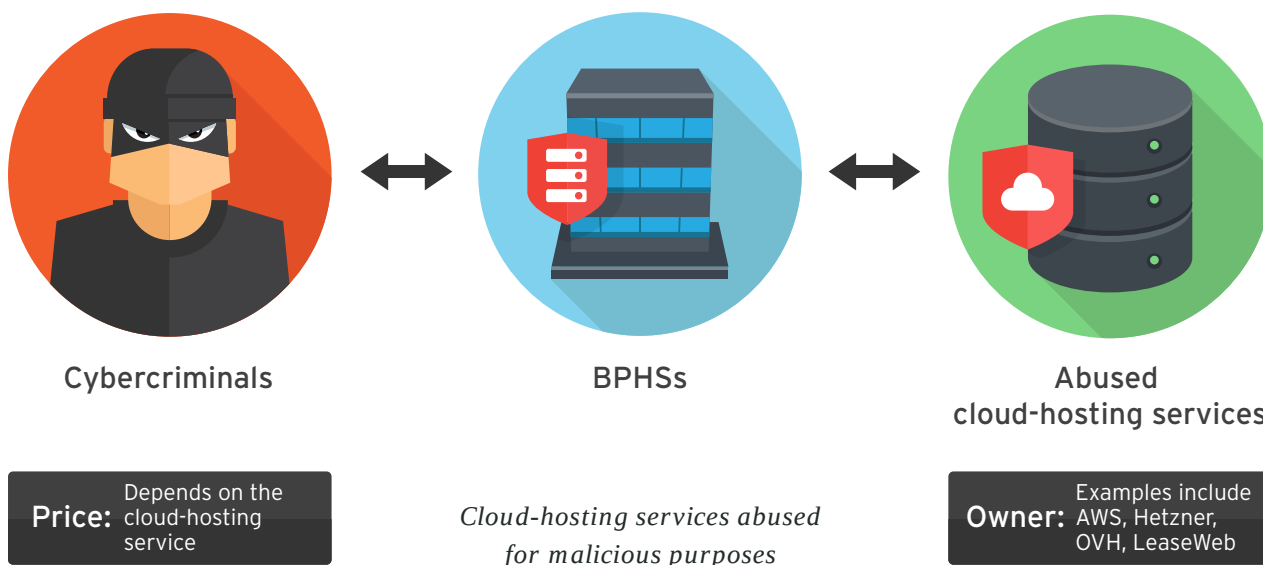
| Mask           | Country       | State                | City       | OS      | Processor                                  | RAM    | Speed                     | NAT | Admin | PayPal | Comment | Action/Result |
|----------------|---------------|----------------------|------------|---------|--------------------------------------------|--------|---------------------------|-----|-------|--------|---------|---------------|
| 178.75.***.**  | Bulgaria      |                      |            | Win7    | Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz | 4 Gb   | 15.93 / 4.1 Mbit/s        | No  | YES   | No     | ✓       | Buy (9\$)     |
| 91.219.***.**  | Netherlands   | Provincie Gelderland | Zaltbommel | Win2008 | Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz   | 16 Gb  | / Mbit/s                  | YES | No    | No     | ✓       | Buy (7\$)     |
| 69.236.***.**  | United States |                      |            | Win     | processor                                  | RAM Gb | inspeed / outspeed Mbit/s | Unk | Unk   | Unk    | ✓       | Buy (9\$)     |
| 70.167.***.**  | United States | Louisiana            | Metairie   | Win     | processor                                  | RAM Gb | inspeed / outspeed Mbit/s | Unk | Unk   | Unk    | ✓       | Buy (9\$)     |
| 173.200.***.** | United States | California           | Walnut     | Win     | processor                                  | RAM Gb | inspeed / outspeed Mbit/s | Unk | Unk   | Unk    | ✓       | Buy (9\$)     |

*Sample market list of compromised dedicated servers (Дедукс)*

These servers can also be used as a malicious traffic proxy and act as a stolen data drop zone. Due to the unstable availability of this service, it is rarely used for C&C activities.

### Model 3: Abused cloud-hosting services

Going back to our crime ring comparison, we can think of the providers in this category as strict landlords who run an honest business. They lease their units to tenants and don't tolerate rule breakers. This doesn't stop their tenants from engaging in illegal operations in the privacy of their own units though.





Legitimate providers may restrict the hosting of malicious content on their dedicated servers, but some of their customers will still find ways to abuse their infrastructure. Abusive customers are only stopped if they are reported and consequently blacklisted. In the past, we've seen providers like Amazon Web Services (AWS) [7], Hetzner [8], OVH [9], and LeaseWeb [10] have their services abused by cybercriminals. The criminals either used their infrastructure as C&C server or drop zone for stolen data.

## Toxicity

The toxicity of a bulletproof server depends on the kind of content hosted on it. The more illicit or malicious the content, the more unsafe it is to host. It is therefore much harder to find a BPHS provider that allows highly toxic content hosting.

Malicious content stored in bulletproof hosts and their corresponding toxicity

| HOSTED CONTENT                | TOXICITY LEVEL |
|-------------------------------|----------------|
| Child exploitation            | Very high      |
| C&C components                |                |
| Exploits                      | High           |
| Malware                       |                |
| Spam                          | Medium         |
| Brute-forcing tools           |                |
| Torrent file download sites   |                |
| Files that violate DMCA       | Low            |
| VPNs                          |                |
| Shopping sites for fake goods |                |
| Blackhat SEO pseudo sites     |                |
| Adult content                 |                |

*Note: Though none of the BPHS providers admit to hosting content related to child exploitation, it doesn't mean that such content may be found up on their domains.*

## Geolocation

A server's physical location is always important, especially when considering what's legal and illegal in the countries where BPHS providers operate. Deploying a blackhat SEO doorway server or establishing an online shop for fake watches may be legal in certain countries but not in others.

To minimize risks, attackers normally rent bulletproof servers that don't share their intended targets' geolocation. A BPHS customer, for instance, can attack users in the United States using an exploit kit hosted on a server in Lebanon. The geographical distance between the BPHS provider and targets slows down the reaction time on abuse reports.

BPHS users, meanwhile, who host content that violate DMCA prefer to be as near as possible to their customers in order to minimize connection latency.

Diversifying BPHS infrastructure protects providers from becoming victims of distributed denial-of-service (DDoS) attacks and blacklisting. This measure allows them to distribute resources and evade detection.

To show how diverse BPHS offerings and prices are, we analyzed a small sample. The list in the table below is by no means exhaustive, but it does show how diverse BPHSs are.

Sample BPHS offerings by host country

|                           | Panama | Lebanon | Ukraine | Russia | Iran | Netherlands | Luxembourg | Switzerland |
|---------------------------|--------|---------|---------|--------|------|-------------|------------|-------------|
| Files that violate DMCA   | x      | x       | x       | x      | x    |             | x          | x           |
| VPNs                      | x      | x       | x       | x      |      | x           |            |             |
| Fakes shopping sites      | x      | x       | x       | x      |      |             |            |             |
| Spam                      | x      | x       |         |        |      |             |            |             |
| C&C components            | x      | x       |         |        | x    |             |            |             |
| Torrent download sites    | x      | x       |         |        | x    |             |            |             |
| Blackhat SEO pseudo sites | x      | x       |         |        | x    |             |            |             |
| Warez forums              | x      | x       |         |        | x    |             |            |             |
| Brute-forcing tools       | x      |         | x       | x      |      | x           |            |             |

*The list of offerings in the table above is by no means exhaustive.  
Bulletproof hosts may operate in countries that aren't in the list.*

A lot of BPHS infrastructures have remained relatively unchanged over time, especially in countries where they are difficult to legally shut down. In stricter countries, BPHS providers move their servers around a lot to keep their services online. They also use untraceable Whois details to register servers aided by fake identification documents and/or privacy-protection legal services, which can be quite costly.



## Targets and exceptions

We've seen notifications posted on BPHS providers' sites that claim they protect the interests of the countries they operate from. Everything outside is fair game and can be considered targets. This could be due to two primary reasons:

- Local law-enforcement authorities have an easier time tracking attackers who go after victims from their host country. These attackers are, after all, under the law enforcers' jurisdiction. In such cases, BPHS providers are forced to move to other countries that have laxer laws.

A good example of this is Pirate Bay. Before it was taken down in 2009, it moved its operations to the Ukraine and has almost had no problems since then [11]. This could be due to the fact that under Ukrainian communication laws, providers are not responsible for what their customers do. It also has multiple backup servers in various countries.

- Some governments either sponsor or control a number of BPHS providers. This protects the latter from being shut down.



*Warez forum notice that bans content that can harm Russia and some Eastern European countries*

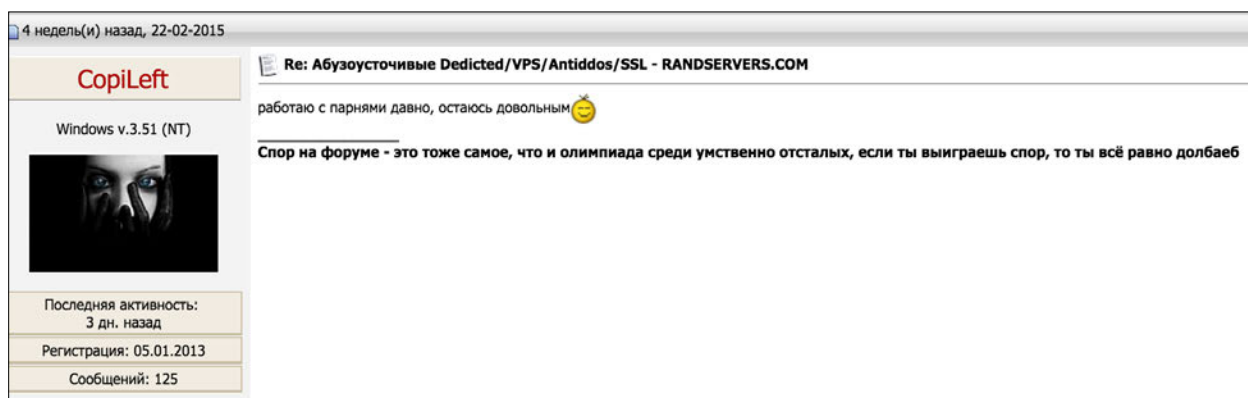
## Pricing

BPHS prices depend on the risk involved in hosting certain content:

- **Low:** BPHS providers that allow low-risk content hosting rent out their servers for as low as US\$2 per month. This kind of offer is available in several countries. Any customer found guilty of engaging in malicious or fraudulent activities can be refused service.
- **Medium:** Predominantly based in Russia and Lebanon, these servers can host both medium- and high-risk content for around US\$70 (hardware) or US\$20 (virtual private server [VPS]) per month.
- **High:** At US\$300 or more per month, a customer can host critical infrastructure projects or high-risk content in servers mostly based in China, Bolivia, Iran, and the Ukraine.

## Popularity

A BPHS provider's popularity can be determined based on forum recommendations and customer feedback. Satisfied clients usually create forum threads to show their appreciation. Novice BPHS providers who haven't had many customers yet can enhance their reputations by providing a guarantee of at least US\$1,000.



*Sample feedback from a satisfied BPHS customer*

## Longevity

The reputation of BPHS providers also relies on how long they've been serving customers in the cybercriminal underground without having to change their name or domain. Being able to keep their name or domain for a long time shows that they are able to ensure the confidentiality of their customers' activities from the prying eyes of security researchers and law enforcers. Changing names or domains could often mean that the BPHS provider keeps getting caught dealing with underground elements and eventually gets shut down. Longevity can be determined by observing forum activities and reading customer feedback.

# The case of RandServers

A good example of a BPHS provider is RandServers. We first encountered it being promoted by a forum user with the handle “sosweet.”

26.12.2014, 03:32

#1

sosweet

НЕ ПРОВЕРЕН



Регистрация: 23.12.2014  
Сообщений: 12  
DM RUR: 0.00  
Депозит: 0  
Сделок через  
ГАРАНТА: 0

😊 [Хостинг] Абузостойчивый дата-центр в Украине и Нидерландах



Доброго времени суток уважаемые форумчане.

Рады вам предложить качественные абузостойчивые сервера в Украине или Нидерландах на выбор, по низким ценам, главная наша задача - это предоставление отказоустойчивого места для размещения **ЛЮБОГО** вашего материала.

**Почему мы:**

- Мы не реселлеры, обладаем своим оборудованием, помещением, AS, блоками IP адресов, готовы собрать любую конфигурацию сервера в кратчайшие сроки.
- Наши сервера расположены в Украине и Нидерландах в очень укромном месте. Доступ на серверную получить не реально.
- В наш дата-центр заведены проверенные провайдеры, которые позволяют гарантировать 99% uptime и низкий пинг в Европу/США /Россию
- Защита от DDOS, мы используем дорогостоящее аппаратное оборудование **RadWare**, которое позволяет фильтровать мощные атаки с подменой IP адресов.
- Круглосуточная тех поддержка, в саппорте работает 4 человека, с графиком работы 12x2.
- Постоянный мониторинг сети/железа на графиках cacti/zabbix
- Мы своевременно обновляем хостинговое ПО и дистрибутивы ОС клиентов, что позволяет держать наши системы в актуальном виде, без угроз взлома.
- Мы бесплатно настраиваем сервера под ваши нужды, в том числе и отключаем логи, криптуем hdd, поднимаем VPN
- По запросу клиента, полностью резервируем его проект в том числе базы/файлы/настройки.
- Даем бесплатный тест любой нашей услуги для людей с репутацией.

**Локационное расположение:**

- Клиентам которых не устраивает локационное расположение в Украине или Нидерландах мы имеем возможность предложить сервера в других абузостойчивых дата-центрах, наших партнеров.
- **Европа (Румыния,Люксембург, Литва, Чехия, Нидерланды), Средней Африка(Египет) и Азия (Малайзия)**

*Forum post by sosweet on darkmoney.cc promoting RandServers*

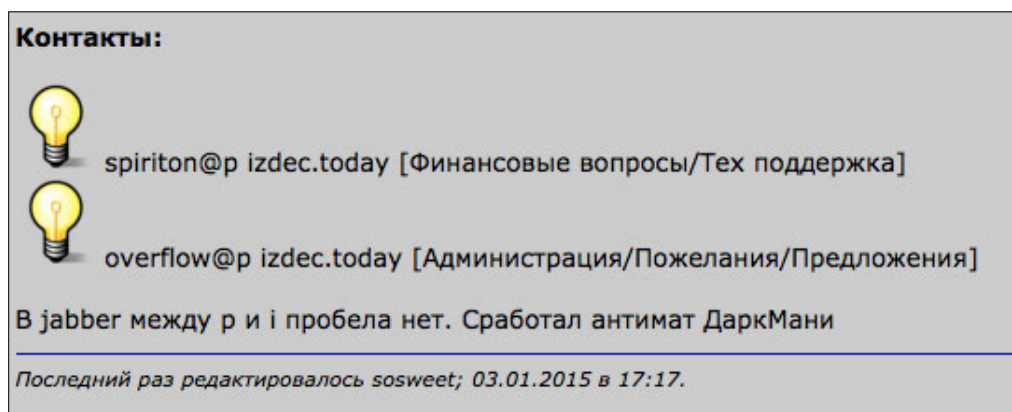
Based on the underground forum thread we found, RandServers claims it can host any type of content with some restrictions. It doesn't, for instance, allow hosting any content related to child pornography.

Availing of RandServers's services requires talking to its support team that gives potential customers a list of package offerings. All packages include the use of Radware (a DDoS-mitigation application) and Cacti or Zabbix (monitoring tools). Some also include the use of out-of-the-box solutions for hosting Zeus, Citadel, or CARBERP C&C servers. Others give customers an option to use virtual private or dedicated servers.



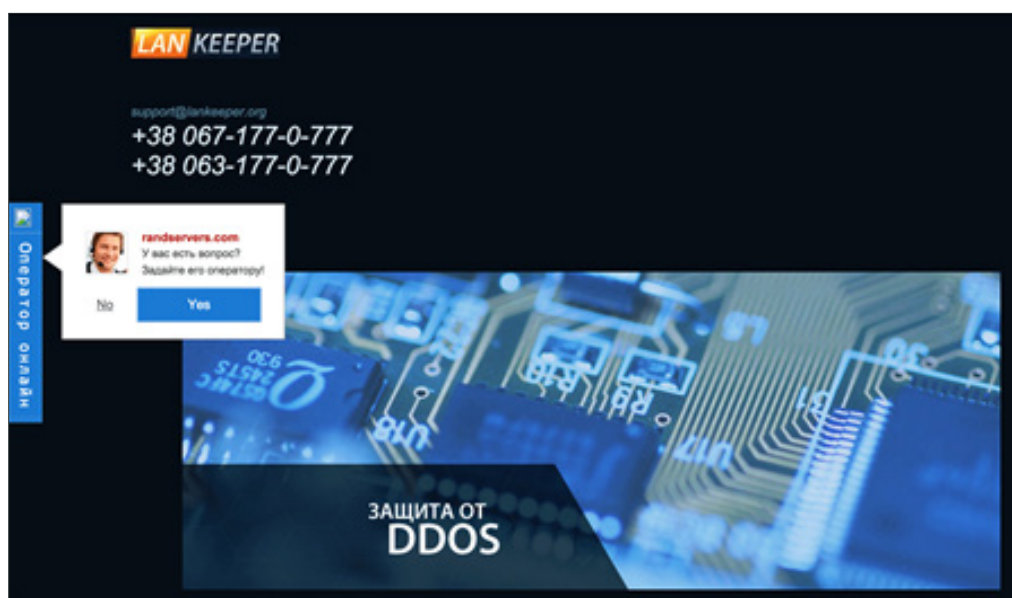
## Who are behind RandServers?

Forum posts on RandServers don't contain contact information. Clicking any of the two light bulbs though takes users to the BPHS provider's site, <https://randservers.com>, which contains details on its service offerings.



*The light bulbs point to RandServers's site that showcases its service offerings*

We dug a little and found an open folder with some of the content from the provider's old site (<http://randservers.com/lc/>). This folder, however, has now been removed.



*Site of LanKeeper.org, a DDoS-mitigation service provider based in Kharkiv, Ukraine*

We conducted an open source intelligence (OSINT) investigation to find out more about sosweet. This person posted RandServers ads and most likely responded to technical and sales queries on forum pages. Sosweet, whose Jabber username is “OVERFLOW@PIZDEC.TODAY,” answered questions related to RandServers’s service offerings.

A complaint by a user named “Fsystem” on a forum thread revealed information on sosweet, particularly the latter’s WebMoney wallet ID, “Z186456037356.” Users don’t usually give out this ID number to just anyone.

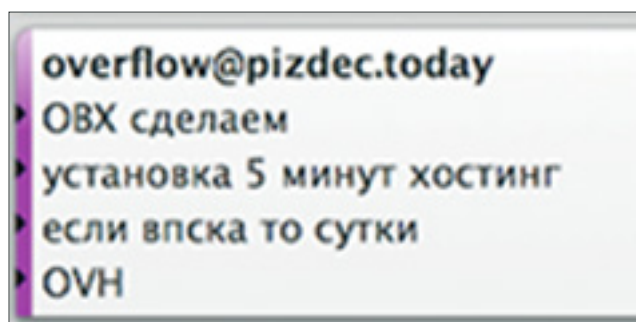
|                                          |                   |
|------------------------------------------|-------------------|
| <b>Fsystem</b>                           | 24.09.2014, 10:30 |
| Прошу принять меры.                      |                   |
| <b>\$1d</b>                              | 24.09.2014, 16:32 |
| <a href="#">sosweet</a> статус выставлен |                   |
| <b>Fsystem</b>                           | 24.09.2014, 19:46 |
| Кошелек крысы<br>Z186456037356           |                   |

*Sosweet’s WebMoney wallet details exposed on exploit.in*

This information allowed us to obtain more details on sosweet, including his name, birth date, address, and mobile number.

A look at pastebin.com for information on sosweet turned up the document, <http://pastebin.com/1UiJ4tZe>, which was most likely a virtual host configuration file for Nginx. It contained the email address, [overflowpps@gmail.com](mailto:overflowpps@gmail.com). A look at the reset parameter for the email address showed the mobile number “\*\*\*\*\*9,” which was likely sosweet’s mobile number tied to his WebMoney wallet ID.

We chatted with the owner of [overflowpps@gmail.com](mailto:overflowpps@gmail.com) in the guise of a possible customer looking for IP addresses or an ISP based in Western Europe. The person suggested RandServers. A sales representative who owned the address confirmed that the provider rents colocation services from OVH to serve customers’ needs.



*Jabber chat with overflowpps@gmail.com*

The following table sums up our findings on RandServers:

| CRITERIA               | DETAILS                                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business model         | RandServers follows both models 1 and 3. It has its own infrastructure that allows it to host all kinds of content, but it also rents small colocation environments from well-known ISPs like OVH. |
| Toxicity level         | RandServers is highly toxic since it allows customers to host all kinds of content, including malicious content.                                                                                   |
| Geolocation            | The servers are physically located in a part of the Ukraine that is difficult to locate and reach. The rented ones are located in the Netherlands and Canada.                                      |
| Targets and exceptions | RandServers's customers aren't required to have preferred country targets though the provider strictly disallows attacks against any entity with ties to the Ukraine.                              |
| Pricing                | Service offerings cost from US\$100 a month (VPSs) to US\$300 a month (dedicated servers).                                                                                                         |
| Popularity             | We saw complaints regarding 24 x 7 support availability and VPS instability.                                                                                                                       |
| Longevity              | Three years                                                                                                                                                                                        |



# What keeps BPHS providers alive?

## Technical support

The scale of a BPHS provider's operation isn't really important to its customers; what matters more is its ability to provide immediate support. Strong BPHS providers have a very good support team who communicates with clients via ICQ, Jabber, or their own JavaScript™-based messaging service. Like legitimate providers, their support team uses a ticketing system to process queries.

## Infrastructure migration due to blacklisting

Law enforcement agencies, security vendors, and root-hosting service providers commonly blacklist BPHS providers. This is why BPHS providers are very interested in feeds from organizations like Spamhaus and security vendors. They constantly check if their IP subnets or addresses have been categorized as malicious. In case these have, BPHS providers immediately move their infrastructure while conducting internal investigations to find out which customer violated their rules.

## Protection against DDoS attacks

BPHS infrastructure can be the subject of serious DDoS attacks due to various reasons. Perhaps the most common is abusive customers. As such, high-end BPHS providers offer DDoS protection as part of their standard package.

## Software to control VPSs

BPHS clients need full control over the physical or VPSs they rent from providers. Experienced clients can manage servers using the command-line interface though others need Windows® and a mouse to do so. Most BPHS providers offer such for free or a fee via Web-based interfaces, which usually have installations for File Transfer Protocol (FTP), virtual hosts, Apache, PHP, Cron, email configuration, Secure Sockets Layer (SSL), proxy, and one-click content management systems (CMSs).

Today's markets have several applications that allow users to fully control most of the services normally found on physical or VPSs like cPanel, ISPmanager, DirectAdmin, and Parallels Plesk.

## Proxying visibility using whitehat-provided services

BPHS providers sometimes hide their IP addresses behind whitehat-provided proxy services. This isn't very common, but techniques to protect real BPHS IP addresses from detection work, especially when they are used to deploy and run exploits. A good example of this involves CloudFlare, which was used as a proxy by those behind the Fiesta Exploit Kit [12].

## Multilevel proxying via distributed VPS presence

Some BPHS providers allow clients to build networks of multilayer VPSs with Nginx Reverse Proxy technology. This enables HTTP requests to pass through and allows the modification of headers and content (as in man-in-the-middle [MitM] attacks) to hide the address of real destination servers. Strong bulletproof protection requires a multilayer structure and specifically configured A or CNAME Domain Name System (DNS) records with multiple IP addresses and fully qualified domain names (FQDNs) with high SEO scores, if possible [13, 14]. That way, losing one VPS or FQDN due to detection and takedown from a chain of domains and servers doesn't affect the core VPS.

Multilevel and distributed VPS and FQDN infrastructures normally drive up hosting costs but ensure stability. An example of a professional BPHS provider that provides multilevel VPS proxy services is Eurobyte.

## Advertising

Every BPHS provider relies on advertising to gain potential clients. But because they need to stay under the radar, they do so only on underground forums and similar venues. At present, two types of BPHS ads exist:

- **Legitimate ads:** These appear as search results for a query on BPHS providers. They don't, however, reveal ties to malicious activity. When clicked, the links lead to Web pages with more information on the providers' offerings, including contact details (normally ICQ, Jabber, or Skype IDs).
- **Forum ads:** Because these only appear on underground forums, BPHS providers can opt to include details on shadier offerings. They normally take the form of clickable banners linked to forum threads where more detailed information like that normally seen on legitimate providers' sites is given. BPHS providers who use these rely on "thank you" messages from clients to widen their client bases.

## Forum ads for bulletproof blackhat-SEO-related services

Hosting sites for blackhat-SEO-related purposes is easy. It doesn't require a really powerful server unless the operation involves a TDS. All it requires are permanent links and additional doorways for crawlers.

[Новости](#)
[Клиентам](#)
[Сотрудничество](#)
[Компания](#)
[F.A.Q.](#)
[Блог](#)

## Надежное качество за разумные деньги

Аренда абозустойчивых серверов/ВДС/хостинга.

[Главная](#)
[Акции](#)
[Контакты](#)
[Отзывы](#)

**Контакты**

Менеджер - 768360  
[manager@blackservers.org](mailto:manager@blackservers.org)  
 Слуппорт - 8880594

Сервера

VDS

Хостинг

Дополнительные услуги

### Space Plan

**\$300.00 /мес.**

- CPU: Intel DualCore E5700
- RAM: 4GB
- HDD: 500GB SATA
- LAN: 100Mb/s
- Срок установки: до 3 дней

ЗАКАЗАТЬ

### Business Plan

**\$340.00 /мес.**

- CPU: Intel Core2Quad q8300
- RAM: 4GB
- HDD: 500GB SATA
- LAN: 100Mb/s unlimited
- Срок установки: до 3 дней

ЗАКАЗАТЬ

### Maximum Plan

**\$370.00 /мес.**

- CPU: Intel Core2Quad q8300
- RAM: 8GB
- HDD: 2x500GB SATA
- LAN: 100Mb/s unlimited
- Срок установки: до 3 дней

ЗАКАЗАТЬ

13.05.2014

#### Наши отзывы!

Уважаемые клиенты, с отзывами качества нашей работы вы можете ознакомиться здесь — [Акция!](#)

- По всем возникшим вопросам пишите Менеджер — 768360

В скором времени будет запущен Жабер. На данный момент действуют скидки:

- хостинг — от 15y.e. (5 аккаунтов)
- ВДС — от 50y.e. (5 ВДС)
- сервера — от 200y.e. (5 серверов)

Будем рады видеть вас в качестве наших клиентов!!!

05.04.2012

#### Уважаемые клиенты!

Уважаемые клиенты! Мы не устанавливаем ваше ПО!!! Только ОС и панель по требованию! Все остальное либо вы сами либо за дополнительную ПЛАТУ!

Канал 1Gb доступен каждому!

Чем больше, тем дешевле

Круглосуточный суппорт

Unlimited

**Безлимитный трафик? Пожалуйста!**

Уважаемые клиенты, все наши услуги (хостинг, VDS, выделенные сервера) имеют неограниченный трафик. Все сервера имеют стандартное подключение 100Mb. (VDS, Выделенные сервера) У нас вам не придется платить за трафик.

*BPHS provider with expensive offerings*

## Forum ads for bulletproof VPN services

Almost every BPHS provider rents out machines that can be used as VPN exit nodes. Bad actors, however, often use stolen machines as VPN exit nodes. The second option is actually cheaper and quite stable. Bad actors can have 2–5 exit points for less if they avail of a real BPHS provider’s offerings.

Changer871

Пользователь

Регистрация: 29.09.2014

Сообщений: 6

Вес репутации: 0

Репутация: 0

Dedicated Server[Дедки]Выделенный сервер

DEDICATED SERVERS

SKYPE CHANGER871

Приветствую, предлагаю сервис по продаже выделенных серверов (дедиков)

Страны в наличии: Уточнять у оператора.

Наши гарантии и преимущества:

- Не дорого.
- Возможен манибек.
- Дедики всегда проверяются на работоспособность перед продажей.
- Приобретая дедик на нем гарантированно будет рабочий интернет.
- В отличии от магазинов, у нас никогда не получите дедик с DesktopLocker'ом.
- Один дедик в одни руки.
- Работает через гарантов.
- Конфиденциальность клиентов.

Наши положения:

- Бесплатно создаю для вас учетку с админ.правами.
- Гарантируется манибек в размере 100% в случае если на момент выдачи деда отсутствует коннект или пароль оказался недействителен.
- Мы не оказываем манибек/замену дедиков в случаях: 1)если администратор обнаружил вашу активность. 2)ваша учетная запись была удалена/заблокирована(по вашей пингуется/не коннектится) 4)вашу учетную запись обнулили.
- Мы предоставляем учетные записи на которых установлены админ. права(даже если логин например Test или 123)
- Сервер с учеткой без админ.прав 50% от полной стоимости(если есть в наличии)
- Оператор не обязан предупреждать клиента о наличии антивируса/особой политики безопасности/отсутствия патч/улучш. спец. настроек на серверах. Не занимаюсь рус.
- При добавлении в скайп рекомендую не молчать, а сразу указывать необходимый сервер.

Дополнительные услуги:

- Залить браузер Chrome на дедик(иногда в IE установлена повышенная безопасность, которая не позволяет скачивать файлы). - 0.3\$
- Создание дополнительной учетки(с админ.правами) (первая учетка с админкой выдается бесплатно) - 0.2\$
- Снятие ограничения времени пребывания на дедике (бывает когда дисконнектишься с дедика, через 5 минут заходишь - все проги закрыты, дед как перезагрузили) - 0.3\$
- Предоставление основной учетки(с админ.правами) (необходимо в случае если вашу 1ую учетку удалят/отключат/сменят пароль. - 1\$

*Forum post advertising access to compromised dedicated servers that have been checked*

## Forum ads for BPHS for sites that violate DCMA

A Romania-based BPHS provider called “Hostimvse.ru” specializes in sites that host torrent files and files that violate DMCA.

HOME

ХОСТИНГ

О НАС

ДОМЕНЫ

КЛИЕНТУ

УСЛУГИ

КОНТАКТЫ

Вход для клиентов

Логин

Пароль

Регистрация

Забыли пароль?

HostimVse!

разместим любые проекты

VPS / VDS сервера

Абузоустойчивый хостинг

Dedicated сервера

Виртуальный хостинг сайтов

Абузоустойчивые VPS / VDS сервера

Локация: UA

Собственный ДЦ

Трафик: от 3 ТБ/мес (канал 100 мбит)

Стоимость: от 29\$/мес

Абузоустойчивые VPS (VDS) сервера — это физический сервер разделенный на несколько виртуальных серверов. Абузоустойчивость за счет размещения в собственном ДЦ — мы за свободу слова, информации, против копиратов и прочих глупых законов ограничивающих свободу слова и информацию. Тем не менее, мы придерживаемся интернет этикета, сотрудничаем только с теми, кто чтит **хакерские ценности**, а не ворует бабушкину пенсию с её карточки.

Мы работаем с двумя технологиями виртуализации: **OpenVZ** и **KVM**. Первая стоит дешевле, последняя позволяет развернуть любую ОС, включая **Windows**.

Для управления VPS мы предоставляем панель управления **Proxmox**, с её помощью есть возможность удаленной перезагрузки и переустановки ОС. При заказе абузоустойчивой VPS на технологии виртуализации OpenVZ можно выбрать практически любую Linux ОС (Ubuntu, Debian, CentOS...), при заказе VPS на KVM — любая ОС, включая Windows.

*Sample BPHS provider known for sites that host DMCA violators and torrent files*



## Forum ads for bulletproof botnet-hosting services

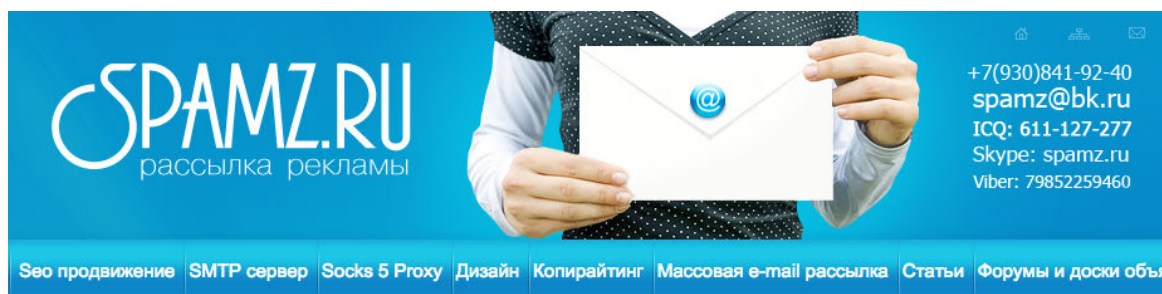
My.Galkahost.com is an example of a distributed bulletproof hosting provider, which specializes in botnet C&C and SEO hosting. Service prices are determined on a case-to-case basis, but can be as low as US\$10. Based on forum reviews, they sublease hosting facilities from Hetzner in Germany.

The screenshot shows the homepage of My.Galkahost.com. At the top is a dark blue navigation bar with links: HOME, ANNOUNCEMENTS, KNOWLEDGEBASE, NETWORK STATUS, AFFILIATES, CONTACT US, and ACCOUNT. Below this is a light gray section titled "Choose a Domain..." with a subtext: "Start your web hosting experience with us by entering the domain name you want to register, transfer or simply purchase hosting for below...". There is a text input field with the placeholder "eg. yourdomain.com". Below the input field is a CAPTCHA area with the text: "Please enter the characters you see in the image below into the text box provided. This is required to prevent automated submissions." The CAPTCHA image shows the characters "1PY46". Below the CAPTCHA are three buttons: "Check Availability" (blue), "Transfer" (green), and "Order Hosting Only" (gray). Below this section are two columns. The left column is titled "Order New Services" and contains the text: "Visit the Order Form to browse the Products & Services we offer. Existing customers can also purchase optional extras and addons here." Below this text is a button "Go to Order Form »". The right column is titled "Manage Your Account" and contains the text: "Already registered with us? If so, click the button below to login to our client area from where you can manage your account." Below this text is a button "Secure Client Login »". Below these columns is a section titled "Latest Announcements" with three entries: "15/03/2011 - New shared hosting plans" (with a link to "New shared hosting plans"), "24/02/2011 - New Dell servers in USA and Netherlands" (with a link to "New Dell servers in USA and Netherlands"), and "21/10/2010 - Virtual hosting in Europe." (with a link to "Virtual hosting in Europe."). Below the announcements is a footer section with a Twitter icon and the text "Loading Retrieving latest tweet...", a language selector set to "English", a copyright notice "Copyright © 2014 Galkahost. All Rights Reserved.", and a "Back to Top" link.

*Sample BPHS provider known for providing botnet-hosting services*

## Forum ads for bulletproof spam-sending IP addresses

An example of a known spam-related BPHS provider is Spamz.ru. Customers can avail of its offerings for US\$70. It comes with anti-DDoS-attack support and free services for seven days.

The banner features the Spamz.ru logo on the left, a central image of hands holding an envelope with an '@' symbol, and contact information on the right. The contact details include a phone number (+7(930)841-92-40), email (spamz@bk.ru), ICQ (611-127-277), Skype (spamz.ru), and Viber (79852259460). A navigation bar at the bottom lists services: Seo продвижение, SMTP сервер, Socks 5 Proxy, Дизайн, Копирайтинг, Массовая e-mail рассылка, Статьи, and Форумы и доски объявлений.

**SPAMZ.RU**  
рассылка рекламы

+7(930)841-92-40  
spamz@bk.ru  
ICQ: 611-127-277  
Skype: spamz.ru  
Viber: 79852259460

Seo продвижение | SMTP сервер | Socks 5 Proxy | Дизайн | Копирайтинг | Массовая e-mail рассылка | Статьи | Форумы и доски объявлений

*E-mail спам рассылка поможет быстро продать любой товар или услугу.*

*Спам хостинг на 7 дней бесплатно при заказе любой рассылки.*

Как добиться видимых результатов в продажах, заполучить новых клиентов, которые стали бы постоянными, сделать ресурс популярным, но, при этом, не тратить огромных денег? Ответ на этот вопрос один — массовая e-mail рассылка рекламы, как ни один другой вид интернет рекламы, лучше всего справиться с поставленной задачей. За считанные часы электронные письма разлетятся в почтовые ящики миллионов пользователей интернета, из которых наверняка найдутся Ваши клиенты.

### *Стоимость e-mail рассылки, основные базы:*

| Регион                | База             | Кол-во адресов | Стоимость                     |
|-----------------------|------------------|----------------|-------------------------------|
| Москва и область      | Фирмы, ЧП, info@ | 1 216 000      | 6 500 руб.                    |
|                       | Физические лица  | 8 702 000      | 32 000р./все; 5 500р./1 млн.  |
| Санкт-Петербург (СПБ) | Юридические лица | 318 000        | 3 500р.                       |
|                       | Физические лица  | 2 237 000      | 9 500р.; 5 500р./1 млн.       |
| Россия                | Юридические лица | 8 673 000      | 32 000р./все; 5 500р./1 млн.  |
|                       | Физические лица  | 37 619 000     | 115 000р./все; 5 500р./1 млн. |
| Украина — Киев        | Юр. фирмы        | 986 000        | 5 500р.                       |
|                       | Физические лица  | 6 418 000      | 24 000р./все; 5 500р./1 млн.  |
| Беларусь — Минск      | Юр. компании     | 247 300        | 3 500р. (60\$ долларов)       |
|                       | Физ. лица        | 3 324 000      | 12 000р./все; 5 500р./1 млн.  |
| Казахстан — Астана    | Юр. лица         | 208 000        | 3 500р. (60\$ долларов)       |
|                       | Физ. лица        | 4 927 000      | 19 000р./все; 5 500р./1 млн.  |

- [E-mail рассылки по городам России;](#)
- Массовая **e-mail рассылка по Вашей собственной базе от 500 руб.**, гарантированная доставка во «Входящие»;
- Сбор тематической e-mail базы по заданным параметрам от 500 руб.;
- Спам рассылка по нашим базам, объемом до 500 тысяч e-mail адресов, стоит 3200 рублей или 60\$ долларов, 1 млн. — 5500 рублей или 100\$, хорошие скидки при больших объемах;
- Поддержка всех форматов электронных писем, в том числе рассылает письма с вложением;
- Предоставляем отчет с подробной статистикой;
- Скорость рассылки 50.000 — 100.000 e-mail сообщений в час;
- Бесплатная возможность заказать спам тест на 20 Ваших e-mail адресов;
- Способы оплаты рассылки: Qiwi, WebMoney, Яндекс.Деньги, наличными в Москве, безналичный расчет для юр. лиц.

*Sample ad for bulk-mail-sending support services*

## Ongoing security challenges

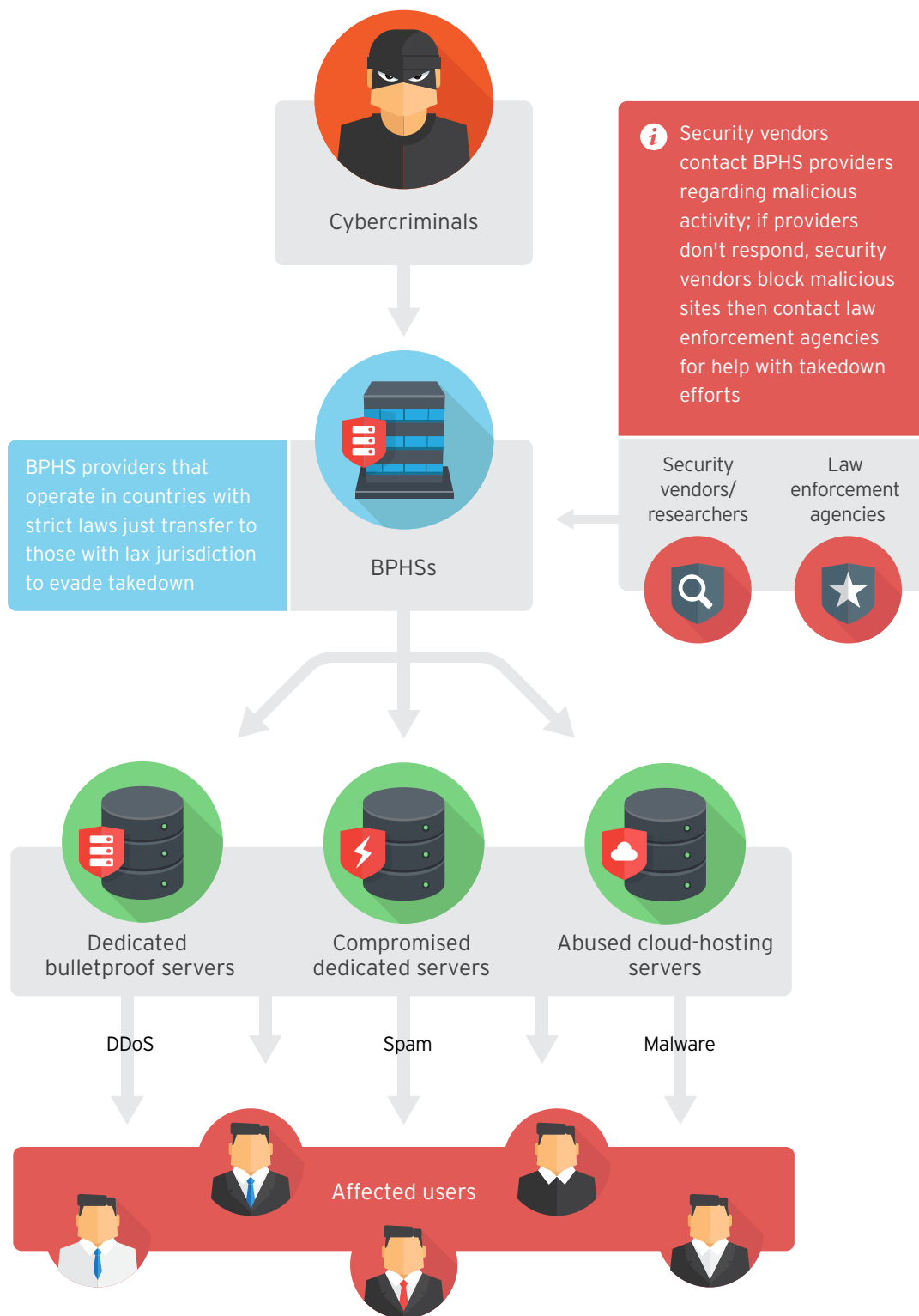
Given the complexity of bulletproof hosting, is it really possible to shut down BPHS operations?

In early 2013, a group of individuals with ties to the Gozi malware attacks were prosecuted for their cybercriminal activities. One of these men was the then 28-year-old Romanian, Mihai Ionut “Virus” Paunescu, administrator of Power Host. He provided the Gozi operation’s BPHS needs. Paunescu leased around 130 servers from legitimate hosting operations then resold them for cybercriminal use. He reportedly made €190 per month for every server he resold. Because of his negligence though, the Romanian police were able to indict him.



*Screenshot of the Power Host site taken in 2012*

Though Power Host was taken down after Paunescu's arrest, accessing its domain name now redirects to CloudFlare—a legitimate U.S. company, which interestingly provides DDoS protection and content delivery network (CDN) services.



*The role that law enforcement agencies and security vendors play in BPHS takedowns*



Power Host's case shows that it is possible to take down BPHS operators, but doing so will require political will and the cooperation of security vendors. Security providers like Trend Micro identify BPHS sites that host malicious content and block access to them to protect customers. We also cooperate with law enforcement by passing on our research findings so they can take action as quickly as possible.

Law enforcement can place external pressure on companies that host malicious content. This kind of pressure works well on service providers that follow the third business model. These are mostly legitimate enterprises that don't want to get shut down. Some hosting companies based in friendly countries like Germany often comply to avoid any inconvenience.

In the case of providers that follow the first business model—meaning their bulletproof servers are dedicated to hosting malicious content, and are most probably based in countries with lax regulations—international law enforcement will have a much harder time putting pressure on them. There is an exception though. Many BPHS providers explicitly state that they don't allow hosting any material that exploits children. Most countries condemn that kind of content and actively work together with law enforcement to put a stop to hosting services that allow it.

The very nature of BPHSs is that they protect malicious activity against law enforcement, giving cybercriminals the much-needed loophole to wriggle out of and escape from the clutches of both law enforcement and the security industry. That loophole unfortunately largely remains open today.

Unless major changes happen in the way international laws protect or turn a blind eye to services like these, BPHSs will continue to exist, and cybercriminals will continue to thrive. For our part, FTR will continue to work with security colleagues in international law enforcement to drive up the cost of carrying out cybercrime in order to make the world safe for the exchange of digital information.

“The very nature of BPHSs is that they protect malicious activity against law enforcement, giving cybercriminals the much-needed loophole to wriggle out of and escape from the clutches of both law enforcement and the security industry. That loophole unfortunately largely remains open today.”

—**Robert McArdle**,  
*Trend Micro FTR Senior Manager*

## References

1. David Bizeul. (20 November 2011). "Russian Business Network Study." Last accessed on 29 April 2015, [http://www.bizeul.org/files/RBN\\_study.pdf](http://www.bizeul.org/files/RBN_study.pdf).
2. Sean Gallagher. (29 March 2013). *Ars Technica*. "How Spamhaus's Attackers Turned DNS into a Weapon of Mass Destruction." Last accessed on 29 April 2015, <http://arstechnica.com/information-technology/2013/03/28/how-spamhaus-attackers-turned-dns-into-a-weapon-of-mass-destruction/>.
3. The Spamhaus Project Ltd. (2015). *Spamhaus*. "About Spamhaus." Last accessed on 29 April 2015, <https://www.spamhaus.org/organization/>.
4. Brian Krebs. (20 May 2013). *Krebs on Security*. "Conversations with a Bulletproof Host." Last accessed on 29 April 2015, <http://krebsonsecurity.com/2013/05/conversations-with-a-bulletproof-host/>.
5. TechTerms.com. (3 October 2007). *TechTerms.com*. "Torrent." Last accessed on 5 May 2015, <http://techterms.com/definition/torrent>.
6. "The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary." (December 1998). Last accessed on 3 July 2015, <http://www.copyright.gov/legislation/dmca.pdf>.
7. Dan Goodin. (19 June 2014). *Ars Technica*. "AWS Console Breach Leads to Demise of Service with 'Proven' Backup Plan." Last accessed on 26 June 2015, <http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/>.
8. Nicole Henderson. (7 June 2013). *Whir*. "Hetzner Security Breach Exposes Customer Passwords, Payment Information." Last accessed on 26 June 2015, <http://www.thewhir.com/web-hosting-news/hetzner-security-breach-exposes-customer-passwords-payment-information>.
9. Steve Ragan. (23 July 2013). *CSO*. "Multistage Attack Compromises Customers of French Web Host OVH." Last accessed on 26 June 2015, <http://www.csoonline.com/article/2133775/malware-cybercrime/multi-stage-attack-compromises-customers-of-french-webhost-ovh.html>.
10. Lucian Constantin. (7 October 2013). *PC World*. "Hosting Provider LeaseWeb Falls Victim to DNS Hijacking." Last accessed on 26 June 2015, <http://www.pcworld.com/article/2052680/hosting-provider-leaseweb-falls-victim-to-dns-hijacking.html>.
11. Bobbie Johnson. (5 January 2010). *The Guardian*. "Internet Pirates Find 'Bulletproof' Havens for Illegal File Sharing." Last accessed on 5 May 2015, <http://www.theguardian.com/technology/2010/jan/05/internet-piracy-bulletproof>.
12. GitHub, Inc. (2 December 2014). *GitHub Gist*. "Fiesta Exploit Kit Domains." Last accessed on 11 May 2015, <https://gist.github.com/xanda/ef6a73d9oadcd88boce7>.
13. Aetrium LLC. (2015). *DNSimple*. "Differences Between the A, CNAME, ALIAS, and URL Records." Last accessed on 11 May 2015, <https://support.dnsimple.com/articles/differences-between-a-cname-alias-url/>.
14. The Trustees of Indiana University. (17 October 2014). *Indiana University*. "What Is a Fully Qualified Domain Name (FQDN)?" Last accessed on 11 May 2015, <https://kb.iu.edu/d/aiuv>.



Created by:

**TrendLabs**

The Global Technical Support and R&D Center of **TREND MICRO**

**TREND MICRO™**

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud