The Hacker Infrastructure and Underground Hosting: Cybercrime Modi Operandi and OpSec

Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin

TREND MICRO | research

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.

Published by
Trend Micro Research

Written by
Vladimir Kropotov,
Robert McArdle,
Fyodor Yarochkin

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents

4
Bulletproof Hosting (BPH)

20
How Criminals Secure Assets Like Criminal Forums

26
Case Study: Dynamics of Criminal Forums and Communities Hosting

34
Weaknesses of Bulletproof Hosting Providers

36
Conclusion

40
Appendix

At the core of any online business lies a solid, reliable infrastructure. An online commercial business can be the most innovative and profitable in its market, but if the hosting infrastructure on which it relies goes offline, none of that matters. Having an online business means exactly that — being online. The same applies to cybercrime — whether it is a botnet owner needing the command and control (C&C) infrastructure to control victims or an online shop selling stolen credit cards — they all need to stay online to be successful.

Cybercrime businesses, however, have additional concerns. Of course, a hard drive may fail or a server may have network issues, but few legitimate businesses have to worry about the constant threat of takedowns or seizures. So keeping their business online no matter what is critical for cybercriminals, and nowhere is this truer than when we talk about those selling these infrastructure offerings in the first place.

The first part of our Underground Hosting series detailed how criminal infrastructure markets operated.[1] The second part continued this by covering each service offered, how they operate, and how criminals use them.[2] Our series concludes with an examination of what makes a network-hosting provider one that offers "bulletproof hosting." We also discuss what characteristics make for a prolific and successful underground bulletproof hosting provider versus the common mistakes made by providers with shorter longevity. Each part of the series also includes an appendix of definitions and concepts, serving as a glossary of terms.

Bulletproof Hosting (BPH)

The key to understanding this paper is to learn about the concept of "bulletproof hosting" (BPH), which is also known as abuse-resistant services. We previously defined bulletproof hosting as any service that is provided to host components or infrastructure to conduct malicious and criminal activity. In light of this definition, we would like to further elaborate on the semantics of the "bulletproof" concept. The name largely speaks for itself — a bulletproof host is a hosting service that allows activities commonly disallowed by legitimate hosting providers (i.e., hosting of malware, restricted content, stolen materials).

Bulletproof hosting providers will either ignore abuse requests or give an early warning to customers of such requests so they have time to adapt their business. In some cases, they also provide additional features that would either allow the perpetrator of these activities to hide their true identity from investigators.

Many bulletproof hosts that use fast-flux infrastructure and/or stolen or compromised assets have a high level of resistance to abuse (after all, they do not own those resources). However, any host in their network could be removed at any time (after the detection of compromise by the original owners), and criminal users of such services should be prepared for this. Typically, threat actors use such hosting systems for short-lived activities like spam distribution, hosting of reverse proxies, mass scanning, and credential brute-forcing. This way, they would only lose a small part of their information if a system is taken down.

While some hosting providers do own their hardware such as servers, server racks, and data centers, a large number of BPHs do not own the servers and data centers. They simply act as a marketplace. These groups resell hosting services from "suitable" providers to customers that require hosting services meeting particular requirements. The "bulletproofness" of such services lies in the reseller's ability to accurately match requests and demands, as well as their good understanding and relationship with a variety of legal hosting providers when handling abuse requests.

Often, hosts do short-term leases of hosting resources from larger hosting providers and resell them. Such relationships, for example, could be observed in forum discussions on certain providers that are likely subleasing servers from former hosts. The same forum discussions also claim that this scenario ultimately led providers to go out of business after some of their servers were seized.

In some cases, intermediate hosting resellers can also act as a mediator between the hosting service provider and service consumer in case of any business-related conflicts or disputes.

Figure 1 shows a breakdown of variations in bulletproof hosting services and specific features that might come with them.

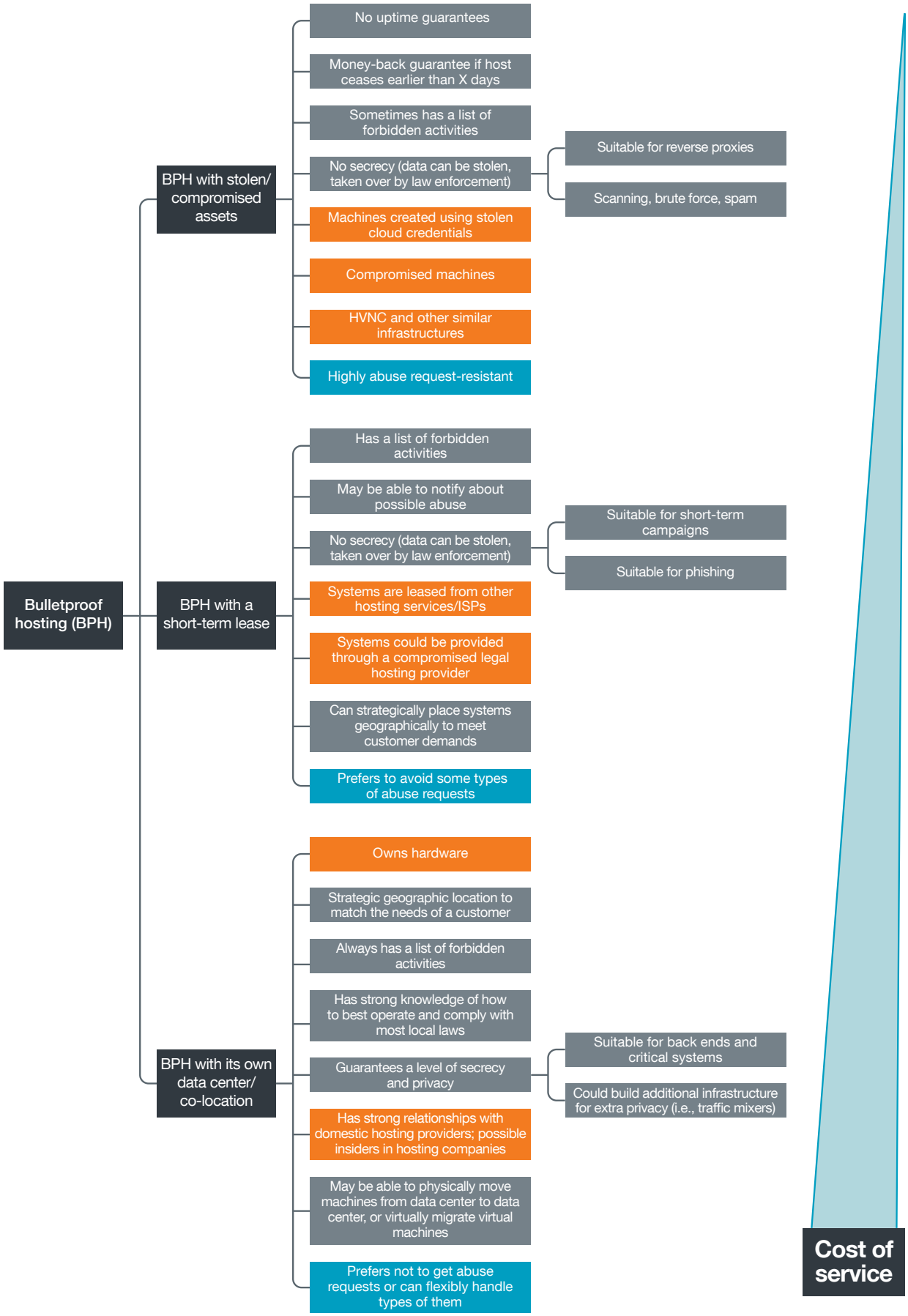


Figure 1. Breakdown of BPH hosting providers

The diagram of hosting providers in Figure 1 shows that hosting on compromised assets is the cheapest available hosting option. However, these hosts do not live long. For systems that require longer periods of availability, hosting in data centers where the service provider owns the infrastructure is a more viable approach.

While some hosts leverage compromised assets for their abuse resistance (or for short-lived attacks), other BPHs tend to strategically allocate their resources and build or rent infrastructure globally, taking into account the local legal regulations, geographical and national characteristics, the professionalism of local law enforcement agencies, and level of corruption among various state institutions. Both cases are guided by the business model and the requirements of the criminals.

Let us examine some of these aspects. We will start this analysis with a universal claim: In our experience in the underground, no criminal hosting provider can provide services to customers for all sorts of criminal activities. Depending on their agreements and negotiations with upstream providers or regulations, there will always be some type of activity that will remain strictly forbidden and activities that are considered tolerable. We will see that the experiences of different hosts differ drastically based on their setups. Some providers support customers by sharing early notifications of received abuse requests and even automatically moving them to another IP space operated by the same host but in a different jurisdiction. This is all done while assuring the person who made the abuse request that action has been taken.

Some hosts deliberately provide illegal services from their infrastructure. These are often novice players in the hosting business. We frequently observe that this kind of direct violation of domestic laws usually ends up with the BPH service being shut down and its equipment seized. Typically, it is only a matter of time before this happens (i.e., when domestic law enforcement has collected sufficient proof of crime). We have seen multiple cases of large BPH operations being shut down this way, including CyberBunker,[3] and multiple BPH service providers in Latvia.[4]

More professional BPH providers can change their upstream internet providers when needed. We identified that some BPH providers peer with other peers, controlled by the same physical person or business entity. These BPH providers can shut down the business and create new shell companies as a part of their "abuse request response" procedure. Since autonomous systems (AS) are technically controlled by the same group but formally belong to different organizations located in different jurisdictions, the shutdown of a BPH AS will appear as a proper response to an abuse request.

For example, an autonomous system of a BPH service could be registered in Seychelles, while an IP space is allocated to another AS located in Ukraine. The upstream peer could be another legitimate-looking company in Seychelles. When the upstream provider receives a critical number of abuse requests, they could simply reallocate IP ranges to new companies and shut the older companies down.

Other hosts make extensive use of virtualization options and run virtual private server (VPS) platforms in several geographical locations. When an abuse request is received, they could move a VPS from one

location to another, ensuring that the malicious service continues to operate while also making it difficult for law enforcement to seize the actual system. When bundled with front-end reverse proxies, this hosting model is perfect for high-availability BPH services.

Other hosts, such as "Yalishanda,"[5] have been able to survive in this business by managing to carefully navigate domestic and international laws and strictly controlling the type of services provided to their customers.

Some BPHs have become so high-profile that they can cause issues for their major upstream providers' reputations and simply get disconnected from the internet, as was the case with McColo.[6]

Cross-jurisdictional issues and specifics of local laws in particular countries play an important role in the BPH ecosystem. The next section focuses on the regional specifics that underground actors use for their services.

Bulletproof Hosting Regional Differences

As previously mentioned, many bulletproof hosting providers attempt to build or rent their hosting infrastructure to meet their customers' requirements. They often do so by carefully selecting regional locations, company registration information, as well as network peering partners. This section explains how the geographical location of the hosting services impacts the type of services that are deemed acceptable by a hosting provider.

The close relationship between a country's laws and the services that a BPH can offer from servers in that location naturally causes several regional differences, which we will outline next. Observations of acceptability of activities based on geographical location are shown in the Table 1.

Disclaimer: It should be noted that this table and the section that follows is compiled based on BPH provider feedback/feature reviews gathered from criminal discussion forums, and in some cases, expresses the practical experience of BPH customers, which might contradict legal regulations in a country. Also, not all countries are represented, rather the countries are sampled from their region. The following table is based on the feedback that underground actors provide on the forums and threads related to BPH.

Activities	Countries																		
	RU	UA	CA	US	BZ	NL	PH	LU	CZ	PL	SE	RO	CN	MD	UK	DE	MY	FR	CH
Spam	M	M	M	Y						N			Y			M			
Online spam/SEO	Y	Y		Y						Y				Y					
Phishing	M		M	Y		M	Y			N	M		Y				M		
C&C hosting/ malware	M	M	M	M		M							Y			M	M	M	M
Brute force/ scanning	M		M			N		M					Y				Y		M
Political content	M	M	Y	Y		Y		Y					N						
Restricted content in other countries	N	N	Y	Y		Y						Y	N	Y	Y	M			
Gambling	N			M	Y	Y	Y	Y	N		Y	Y	N	Y					
Copyrighted materials	M			N		Y					Y	Y	Y	Y		Y	Y		
Pharmaceutical products			Y	N						Y	Y	Y		Y		Y			

Table 1. Preferred criminal hosting locations by country and activity, based on underground actors' feedback on hosting

Note: [Y]es: Underground actors mention this location; [N]o: Underground actors actively suggest not using this location; [M]aybe: Underground actors sometimes mention this location along with restricted factors, like the targeted region

For example, we have seen a lot of BPH services located in **Ukraine**, and there are several reasons for this. For one thing, some of the customers may be local or may be located in a neighboring country. Ukraine state regulations and law enforcement may be less strict compared to its neighboring countries, but law enforcement actions may be less predictable to the owner of the business. There are known cases where domestic security services (such as the Security Service of Ukraine) have proactively investigated and arrested a bulletproof host.[7]

In another example,[8] **Switzerland** and the **Netherlands** have also been discussed as suitable locations for creating shell companies to proxy hosting operations. We believe the main reason for this is the fact that the host will likely receive an early tip-off (in the form of a search warrant or police visit) and would have time to relocate systems at its offshore locations.

Several investigative reports suggest that the earlier mentioned "Yalishanda" was likely operating their infrastructure out of **China** while using both domestic and international infrastructures to provide their service. One of the interesting legal aspects of operating a BPH service in China is that many activities that are deemed illegal in other countries may be considered acceptable within the region and vice versa. For example, email spam is largely tolerated, as with network scanning, as long as it does not go against domestic targets. The same could be said for other activities. However, gambling — especially gambling that targets local customers — and political content or political satire are big no-nos in China and may attract the attention of domestic regulators.

In **Canada**, complex paperwork requirements make this country attractive to BPH services, as a court order is required to seize content.[9] However, a host like "cadedic," which was advertised as operating out of Canada, was forced to shut down. Their official reason given in underground threads states a lack

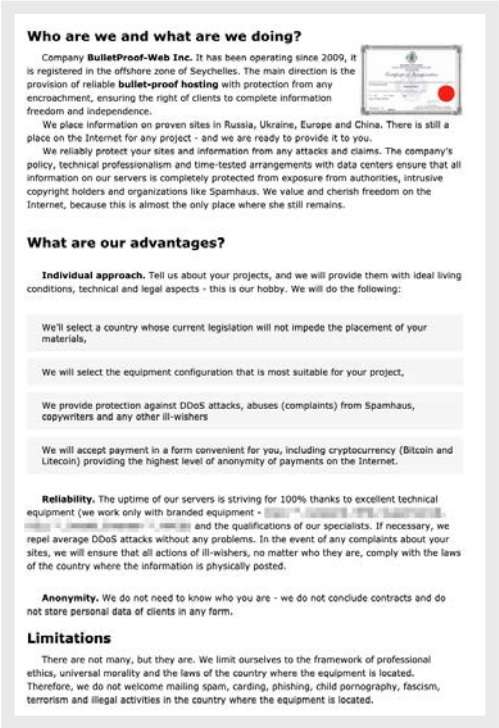
of interest in Canadian servers from European customers. However, the real reason is more likely to be related to experiencing legal problems domestically.

In advertisements of hosting from the United States, adult or pornographic material and other restricted content in some countries are widely acceptable, with the strong exception of Child Sexual Abuse Material (CSAM). In contrast, however, spam is not easily acceptable in the US, as well as network scanning and brute-force attacks, which will generate numerous abuse requests that the provider usually handles appropriately.

Some companies in the US (like Amazon/AWS) proactively detect such activities and may shut systems down even without an abuse request. Political content is usually accepted, while content violating the Digital Millennium Copyright Act (DMCA) is not.

Russia is very strict about pornographic materials, and most pornographic content is not allowed. Based on criminal hosting advertisements, illegal drug-related materials are also not allowed. Russia is very sensitive to political content. However, users of such providers have noted that some hosts could be flexible in providing early abuse request notifications. Other hosts are more accepting of malicious activity as long as it does not target domestic users.

Seychelles, **Belize**, **Dominican Republic**, and **Panama** received positive reviews from criminal discussions for having a strong mix of good internet connectivity and local legal or resource issues that delay any timely response to internet threats. As such, it comes as no surprise that some BPH providers advertise their presence in these geographical locations as proof of their status:



Who are we and what are we doing?

Company **BulletProof-Web Inc.** It has been operating since 2009, it is registered in the offshore zone of Seychelles. The main direction is the provision of reliable **bullet-proof hosting** with protection from any encroachment, ensuring the right of clients to complete information freedom and independence.

We place information on proven sites in Russia, Ukraine, Europe and China. There is still a place on the Internet for any project - and we are ready to provide it to you.

We reliably protect your sites and information from any attacks and claims. The company's policy, technical professionalism and time-tested arrangements with data centers ensure that all information on our servers is completely protected from exposure from authorities, intrusive copyright holders and organizations like Spamhaus. We value and cherish freedom on the Internet, because this is almost the only place where she still remains.

What are our advantages?

Individual approach. Tell us about your projects, and we will provide them with ideal living conditions, technical and legal aspects - this is our hobby. We will do the following:

We'll select a country whose current legislation will not impede the placement of your materials,

We will select the equipment configuration that is most suitable for your project,

We provide protection against DDoS attacks, abuses (complaints) from Spamhaus, copywriters and any other ill-wishers

We will accept payment in a form convenient for you, including cryptocurrency (Bitcoin and Litecoin) providing the highest level of anonymity of payments on the Internet.

Reliability. The uptime of our servers is striving for 100% thanks to excellent technical equipment (we work only with branded equipment - [redacted] and the qualifications of our specialists. If necessary, we repel average DDoS attacks without any problems. In the event of any complaints about your sites, we will ensure that all actions of ill-wishers, no matter who they are, comply with the laws of the country where the information is physically posted.

Anonymity. We do not need to know who you are - we do not conclude contracts and do not store personal data of clients in any form.

Limitations

There are not many, but they are. We limit ourselves to the framework of professional ethics, universal morality and the laws of the country where the equipment is located. Therefore, we do not welcome mailing spam, carding, phishing, child pornography, fascism, terrorism and illegal activities in the country where the equipment is located.

Figure 2. A BPH provider calling out the unique selling point of operating over a decade based in Seychelles. It also offers distributed denial-of-service (DDoS) protection, as well as stating the services they cannot allow.

We can see a preference for some previously mentioned geographical locations when we look at the hosting history of some criminal discussion portals such as ShadowCarders (a site with a tagline that reads, “infamous carding forum”), which sells credit cards and other stolen documents.

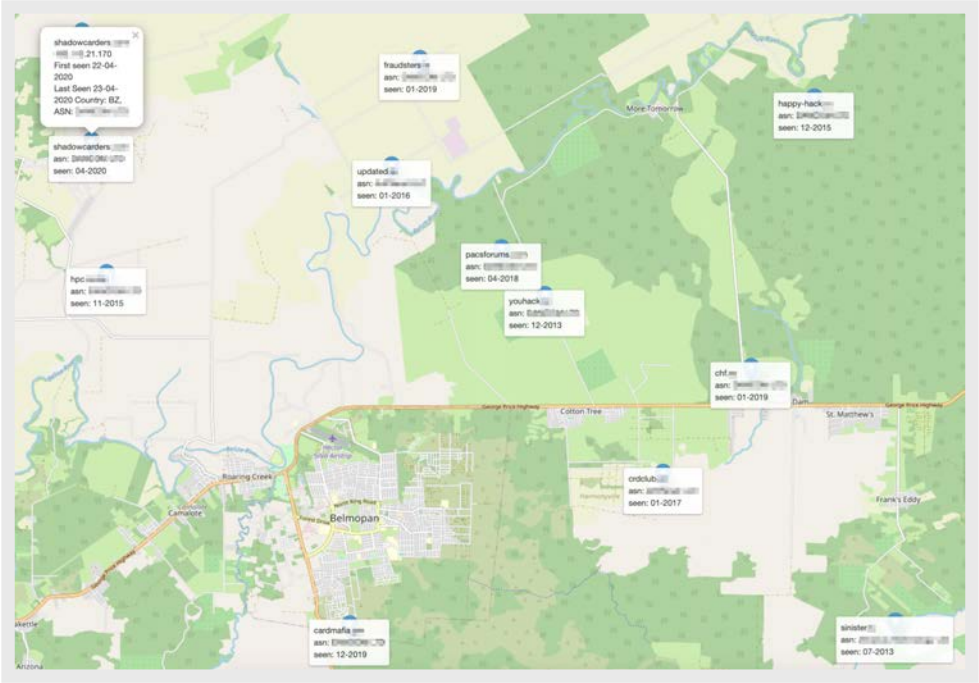


Figure 3. A screenshot that visualizes the registration information of IP addresses’ geographical locations for the ShadowCarders forum

The forum was recently hosted by a provider that was likely physically located in the Russian Federation; however, the declared geolocation, as well as location information available in databases like MaxMind, points to an address located in Belize.

The lookup through IPIP[.]net, a public service that aggregates information of several geolocation providers, confirms our theory:

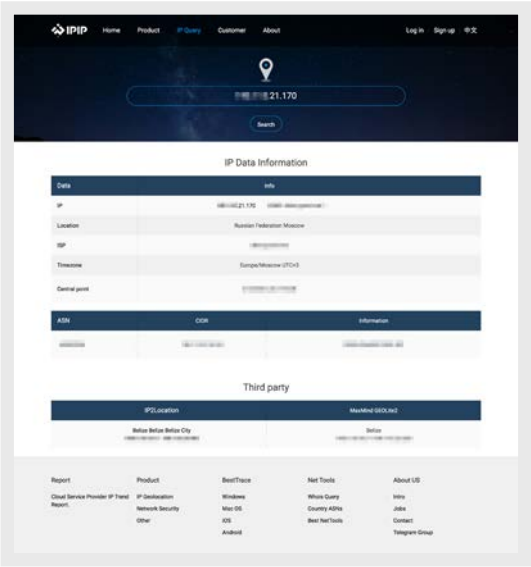


Figure 4. A geolocation lookup on the provider

In the first map, it can be noted that it is not a single case, as this hosting provider is also very popular with several other criminal forums, including CardMafia, CrdClub, YouHack, and Fraudsters. These types of locations are so popular that the cybercrime underground has created another name for such BPH services: “offshore hosting.”

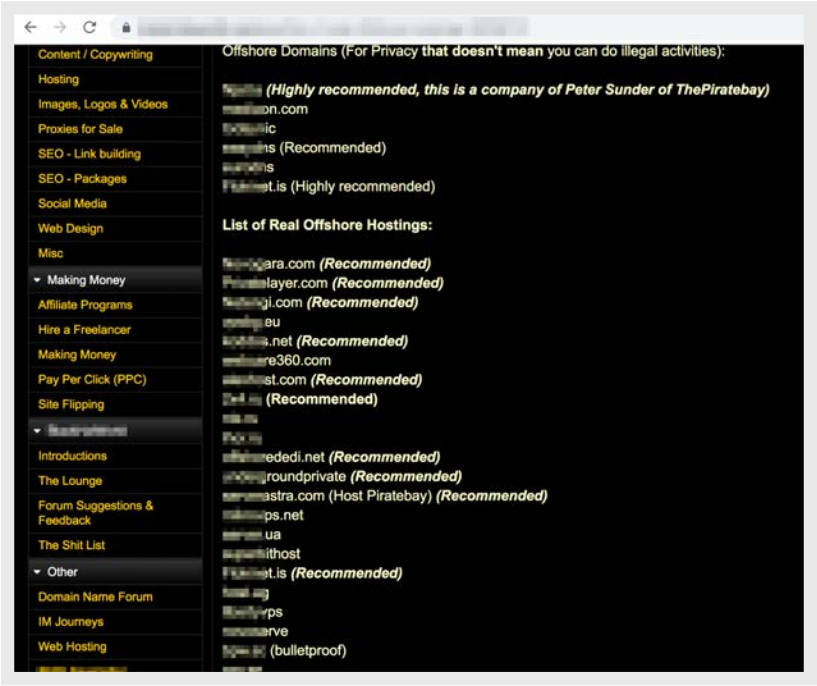


Figure 5. A list of popular and recommended offshore hostings

During our research, we noticed that some of the listed hosts were physically based in the **Netherlands**; however, the companies behind them were registered to offshore locations. In general, the Netherlands has a reputation — at least among criminals — of being a country that requires a court order for a takedown to occur. It is also perceived as a country that is accepting of several types of material that are not allowed to be hosted in other locations. For example, in criminal hosting advertisements related to the Netherlands, general pornographic materials are easily accepted. Online portals related to the sex trade (e.g., prostitution, web camera services) also seem to be generally accepted, as do drug trading platforms.

Online gambling is another type of content that is not widely allowed. There are some countries in Europe, such as **Luxembourg**, that are known to be friendly to gambling content in underground discussions, but many countries have rigid laws that make it difficult for hosts. In the **Philippines**, online gambling is also acceptable and legal, as long as domestic residents are not allowed to participate.

The many differences in restrictions and services based on location have allowed the most serious underground threat actors to combine the benefits of each to maximize their business models. For example, hosting the parts of their operations that require strong reliability in one region, while keeping parts where privacy is key in another. It comes as no surprise, therefore, that many of the BPH advertisements we see specify not only the type of hosting (i.e., VPS, dedicated server) but also the country where the equipment is physically located.

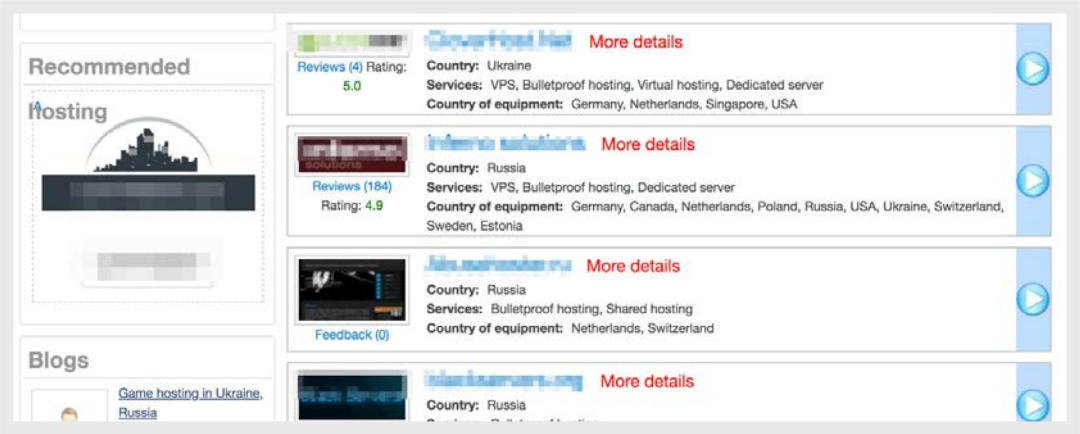


Figure 6. An example of a BPH advertisement

Legal Awareness of BPH

BPH threat actors generally know what is considered to be legal in a particular country or jurisdiction, what is illegal but safe (rarely punished), and what kind of activity is illegal and penalized in certain geographical locations. They also appear to be well-versed on the capabilities of different law enforcement agencies, and how different agencies cooperate internationally. For example, in the following discussion, a forum member provides legal advice to the topic starter on doing proper OpSec (Operational Security) while conducting illegal activity:

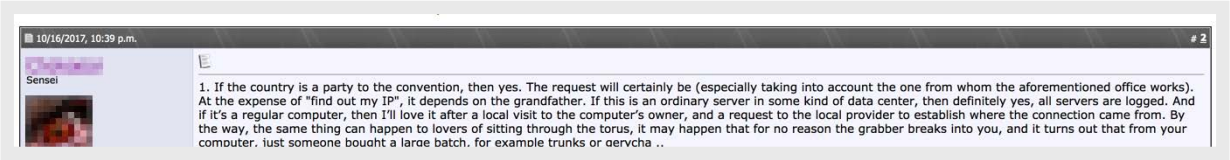
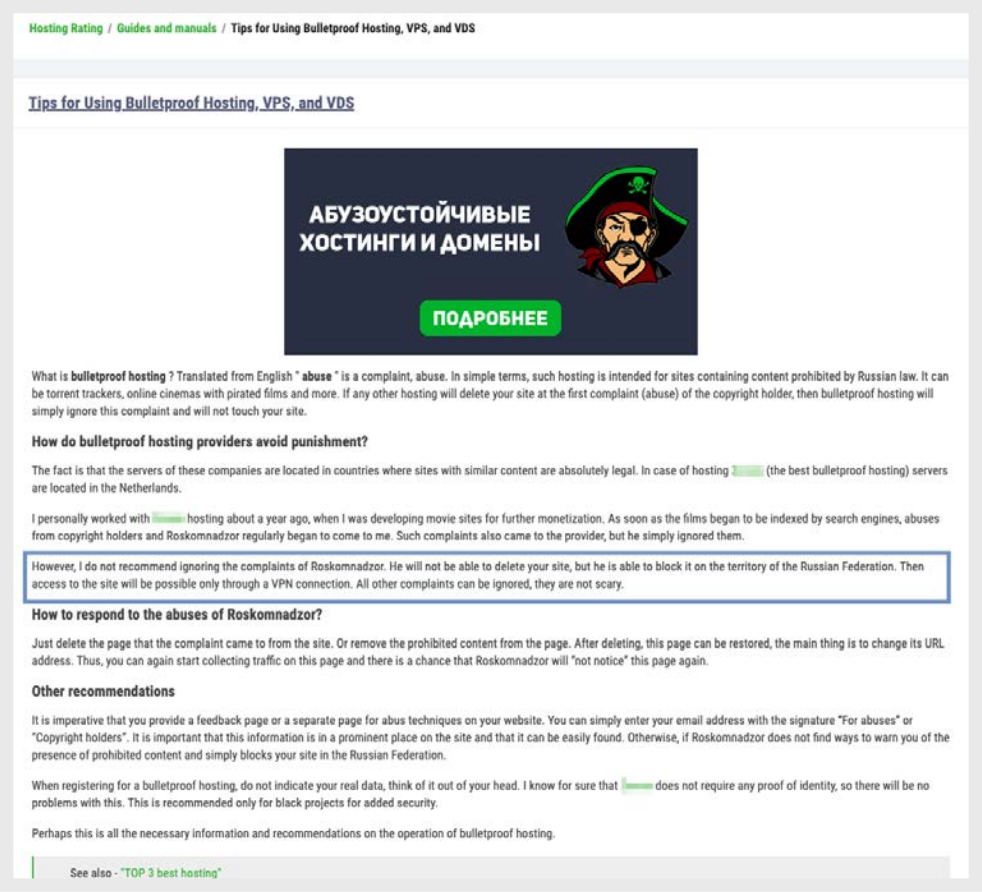


Figure 7. Advice from a senior forum member on hosting legalities (machine-translated)

Indeed, in many of the Russian-speaking forum sections related to bulletproof hostings, it is possible to find survival guides for bulletproof hosts. These guides offer advice on how to choose jurisdictions based on the hosting content and provide suggestions on how to best respond to different sorts of abuse requests. From reading these tutorials, we can see that criminal hosting providers gain a healthy "respect" for certain enforcement agencies over time. The author of the post below strongly recommends not to ignore abuse requests from Russian authority "Roscomnadzor," otherwise known as the Federal Service for Supervision of Communications, Information Technology and Mass Media. The agency is responsible for censorship of media or telecommunications.

He suggests immediately deleting or modifying non-permitted content from the particular page that the abuse request flagged; otherwise, this authority can block the content of the whole website on a country-wide scale.



Hosting Rating / Guides and manuals / Tips for Using Bulletproof Hosting, VPS, and VDS

Tips for Using Bulletproof Hosting, VPS, and VDS

АБУЗОУСТОЙЧИВЫЕ ХОСТИНГИ И ДОМЕНЫ

ПОДРОБНЕЕ

What is **bulletproof hosting** ? Translated from English " **abuse** " is a complaint, abuse. In simple terms, such hosting is intended for sites containing content prohibited by Russian law. It can be torrent trackers, online cinemas with pirated films and more. If any other hosting will delete your site at the first complaint (abuse) of the copyright holder, then bulletproof hosting will simply ignore this complaint and will not touch your site.

How do bulletproof hosting providers avoid punishment?

The fact is that the servers of these companies are located in countries where sites with similar content are absolutely legal. In case of hosting (the best bulletproof hosting) servers are located in the Netherlands.

I personally worked with hosting about a year ago, when I was developing movie sites for further monetization. As soon as the films began to be indexed by search engines, abuses from copyright holders and Roskomnadzor regularly began to come to me. Such complaints also came to the provider, but he simply ignored them.

However, I do not recommend ignoring the complaints of Roskomnadzor. He will not be able to delete your site, but he is able to block it on the territory of the Russian Federation. Then access to the site will be possible only through a VPN connection. All other complaints can be ignored, they are not scary.

How to respond to the abuses of Roskomnadzor?

Just delete the page that the complaint came to from the site. Or remove the prohibited content from the page. After deleting, this page can be restored, the main thing is to change its URL address. Thus, you can again start collecting traffic on this page and there is a chance that Roskomnadzor will "not notice" this page again.

Other recommendations

It is imperative that you provide a feedback page or a separate page for abus techniques on your website. You can simply enter your email address with the signature "For abuses" or "Copyright holders". It is important that this information is in a prominent place on the site and that it can be easily found. Otherwise, if Roskomnadzor does not find ways to warn you of the presence of prohibited content and simply blocks your site in the Russian Federation.

When registering for a bulletproof hosting, do not indicate your real data, think of it out of your head. I know for sure that does not require any proof of identity, so there will be no problems with this. This is recommended only for black projects for added security.

Perhaps this is all the necessary information and recommendations on the operation of bulletproof hosting.

See also - "TOP 3 best hosting"

Figure 8. A guide that suggests not to ignore abuse requests from a Russian authority

Most BPH providers are willing to sacrifice the content of some customers for the greater good of the survival of the overall business. While survivability is the main driving factor for most hosting providers, understanding how they look into doing this can also give investigators some avenues to better tackle this problem.

Bulletproof: A Customer Perspective

Looking at criminal infrastructure from the criminals' point of view allows us to understand it better. In this section, we will detail the typical setup for a criminal that builds and deploys botnets to help illustrate the thought process that must go into such a business.

Any botnet has several components that are of some value to this cybercrime operator:

- The backend C&C system
- The botnet distribution components
- Exploit kit-serving infrastructure
- Search engine optimization (SEO)/landing page infrastructure (which brings victim traffic to exploit kits)
- Systems used for spam distribution
- Systems used for online forums and social media flooding
- Network scanning and brute-force systems

All of these systems contain information of different values and interact differently with the rest of the internet. Therefore, the botnet operator would invest differently to protect these systems and their identity based on their core values to the criminal business model. In many ways, this is similar to how a legitimate business would prioritize security solutions for parts of their corporate network based on the risk and importance to the business. Let us examine some of these:

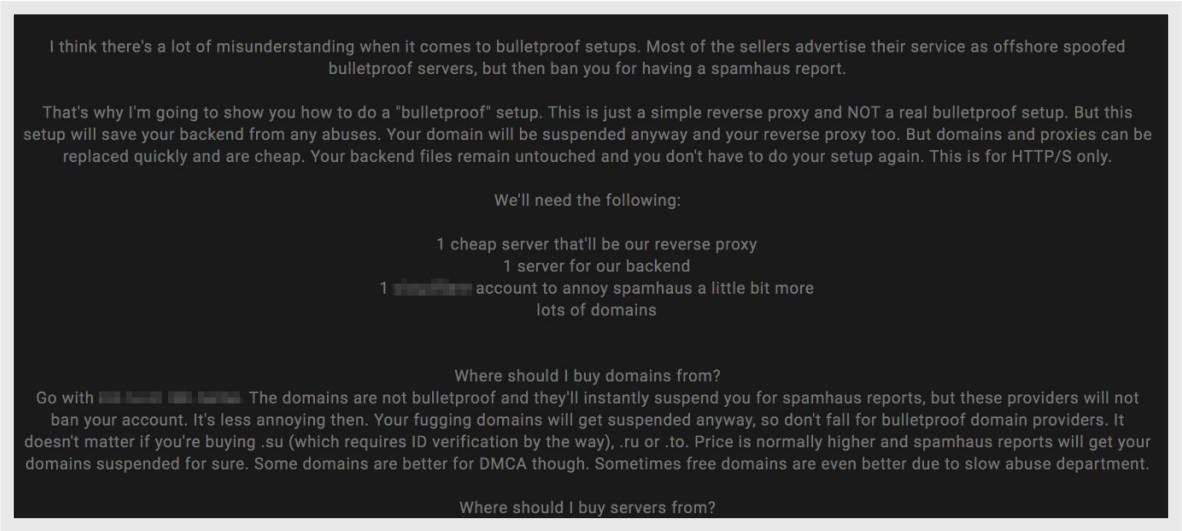
The backend panel or a C2 system will likely contain:

- The C&C panel code
- Some records of activities
- Possibly samples of distributed malicious software
- System access logs

The system will also likely contain other information, which, if collected by law enforcement, could lead to the takedown of the botnet, potential monetary loss, and even identification and arrest of the operator. Thus, the operator needs to protect this resource. Of course, clever operators of such systems can take additional precautions from unexpected takedowns by minimizing the amount of useful (for law enforcement or investigators) log files and accessing the system from anonymous sources like Tor networks. Operators also typically use encryption to make the forensic analysis of the system difficult.

We should also keep in mind that the actual operator does not often do the backend setup; this job is usually outsourced to other individuals. Recreating the backend system would normally be time-consuming and require additional funds. This could be likened to protecting the core trade secrets of a legitimate business.

The following “bulletproof” tutorial discusses some of the aspects that we have seen underground actors widely use:


I think there's a lot of misunderstanding when it comes to bulletproof setups. Most of the sellers advertise their service as offshore spoofed bulletproof servers, but then ban you for having a spamhaus report.

That's why I'm going to show you how to do a "bulletproof" setup. This is just a simple reverse proxy and NOT a real bulletproof setup. But this setup will save your backend from any abuses. Your domain will be suspended anyway and your reverse proxy too. But domains and proxies can be replaced quickly and are cheap. Your backend files remain untouched and you don't have to do your setup again. This is for HTTP/S only.

We'll need the following:

1 cheap server that'll be our reverse proxy
1 server for our backend
1 [redacted] account to annoy spamhaus a little bit more
lots of domains

Where should I buy domains from?
Go with [redacted]. The domains are not bulletproof and they'll instantly suspend you for spamhaus reports, but these providers will not ban your account. It's less annoying then. Your fugging domains will get suspended anyway, so don't fall for bulletproof domain providers. It doesn't matter if you're buying .su (which requires ID verification by the way), .ru or .to. Price is normally higher and spamhaus reports will get your domains suspended for sure. Some domains are better for DMCA though. Sometimes free domains are even better due to slow abuse department.

Where should I buy servers from?

Figure 9. How underground actors see bulletproof setups

This tutorial's author recommends using a chain of disposable reverse proxies in front of the backend system. One well-known DDoS protection solution is mentioned in the tutorial as well, despite it being common knowledge in the underground community that this provider cooperates with law enforcement when abuse requests are submitted.

The exploit-kit, SEO, and doorway-serving infrastructure are likely to benefit from the same level of protection. However, most exploit kit vendors have recently turned to software as a service (SaaS)-like infrastructure and are implementing protection mechanisms by themselves. SEO and doorway providers can use disposable domains or web servers, as they commonly do not require complex setups.

Spam and social media flooding tools produce unsolicited outgoing traffic, thus the botnet operator would need a network of outgoing proxies or traffic mixer services to protect the system from getting blocklisted. The same goes for *scanning and credential brute-force systems*. The operator would lose a portion of their log information in case such a system is taken down or seized by domestic law enforcement agencies. Due to the visibility of such systems, an operator will typically only access them from an anonymized source (like the Tor network) to ensure that they have as little identifiable information on the operator as possible.

Another important aspect of picking a bulletproof host for a threat actor is the geographical location targeted for criminal activities. Many hosting platforms, online forums, and service providers strictly prohibit "work" in their regions. This is very common for former USSR countries and China, and is mainly done to safeguard the whole chain (i.e., online forum, service provider, service consumer) against conflicts with local law enforcement agencies.

Examples of such rules can be seen in the following screenshots. For example, CrdClub strictly forbids any discussion of work targeting victims within former USSR/CIS territories:

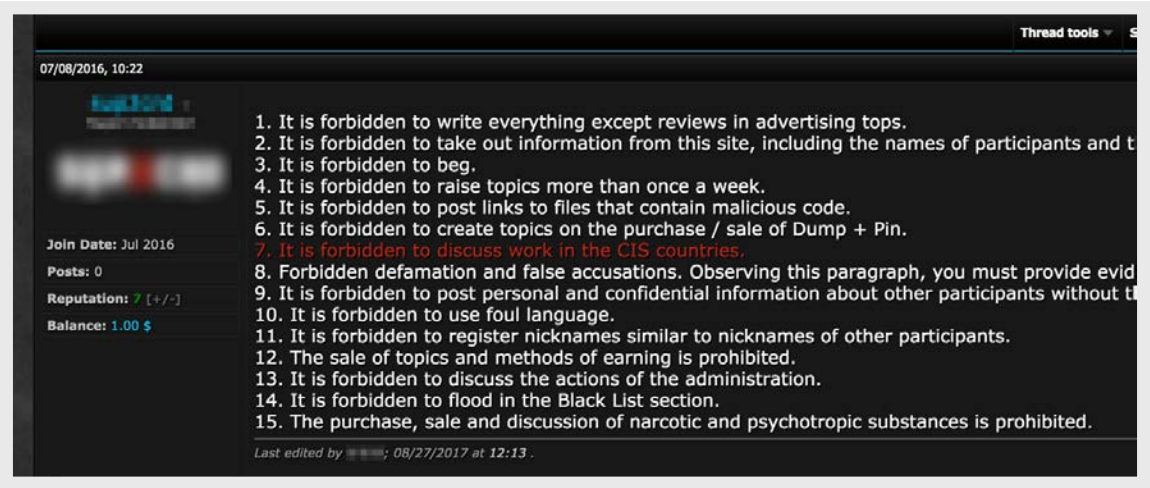


Figure 10. CRDCLUB forum rules

The seller of the Taurus Project data stealer strictly insists that their build does not work in former CIS countries:

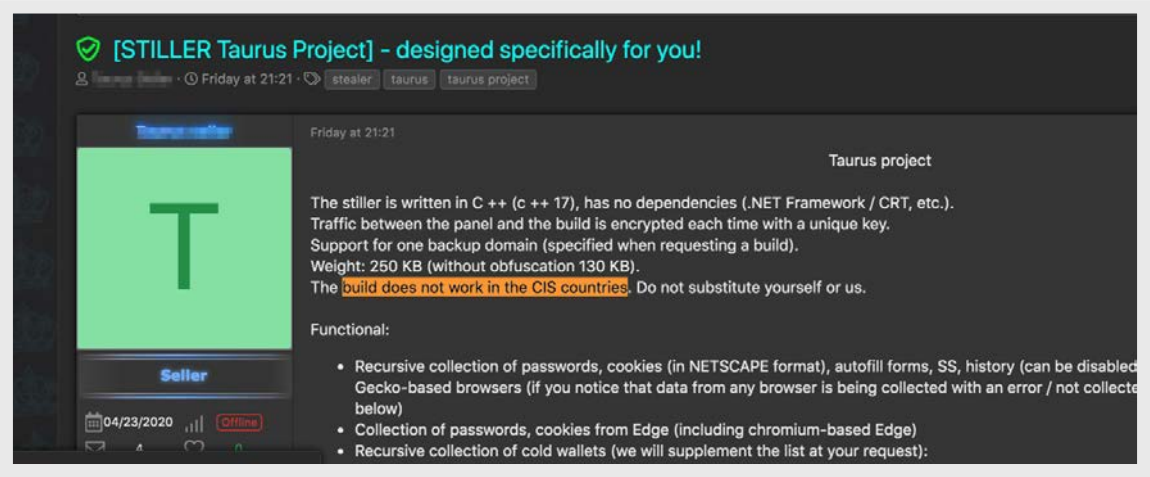


Figure 11. Advertisement of a stealer build, which does not work in CIS countries

Categorizing Hosting Providers

Once a criminal customer determines the hosting requirements for each aspect of their business, like any other buyer, they will wish to compare the options available in the market. One site we examined integrated information from more than 1,000 hosting services (both legitimate and questionable), breaking them down into different categories and features and offering detailed customer reviews. This portal surprisingly had a dedicated page related to bulletproof hosting for English-speaking and "no-abuse" hosting for Russian-speaking users, with a "Bulletproof Rating" given for each one:

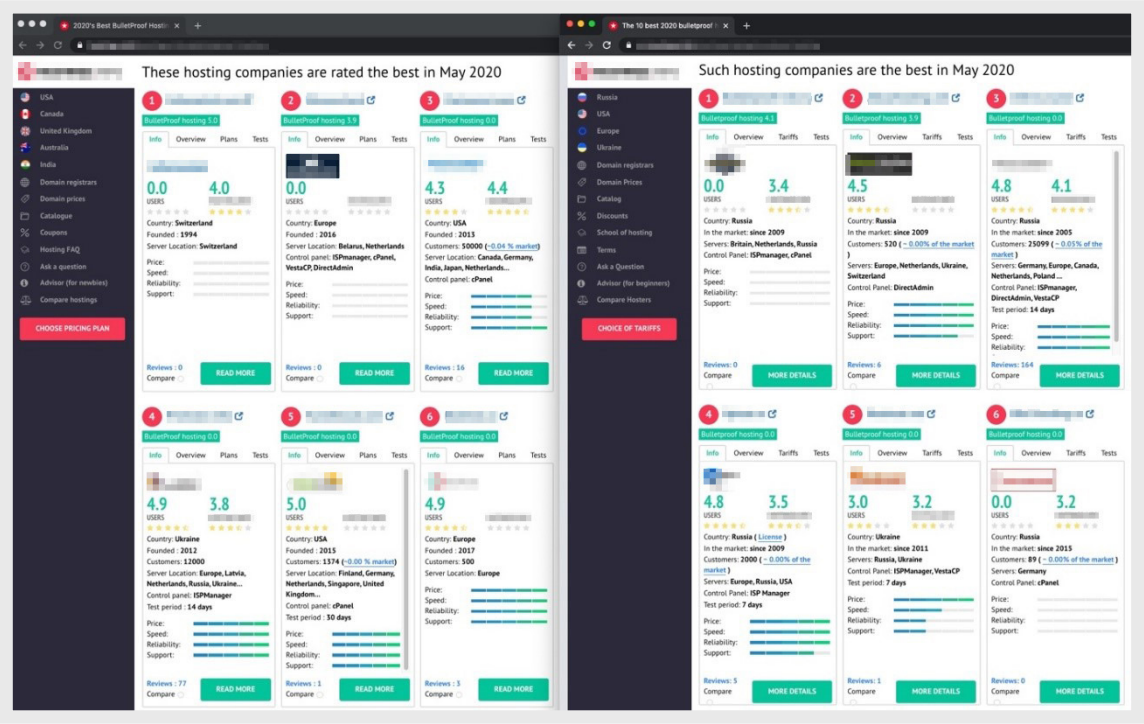


Figure 12. An example of a ranking page for bulletproof hosting services

(list of service offerings for English speakers [left], Russian [right])

This website shows different rankings for hosting depending on the language used by the viewer. For example, for Russian speakers, there is an alternative ranking that includes hosts in Russian-speaking locations (in line with the importance of geographical location highlighted earlier).

This example illustrates a general tendency related to bulletproof hosting services:

- Different geographical locations and groups that speak different languages often have their preferred hosting providers
- Preferred hosting providers sometimes even cross language barriers
- Often, the customers of hosting providers in country A are not aware of providers in country B
- Favored hosting providers for country A sometimes cannot work for country B due to political, legal, or other reasons

For example, the hosting of gambling sites for target users in mainland China is often in Taiwan; if the target users are in Taiwan, the hosting is carried out in mainland China. But these countries cannot switch roles — gambling sites for China cannot be hosted legally in China, for the same reason that we can see entirely different leaders for Russian- and English-speaking customers in the screenshots above.

Major Survival Principles for Hosting Providers

Throughout several years of our research in the cybercrime underground, we have observed that some BPHs continue to strive and operate, while others only operated for a short time before disappearing —either voluntarily or due to takedown or arrest. We think it is important to understand the factors that allow some hosts to survive longer, not to provide advice to such groups but to assist those who look to disrupt them.

We believe there are a few criteria that increase hosting providers' survivability. For starters, a clear discretion in allowed operations is very important. Many of the BPH providers that show longevity have stringent and distinct rules of operation and proactively take down systems of any customers who violate their policies. This policing is key for them to protect their business. For example, we observed that many hosts strictly demand no sale or monetization of stolen credit card data from their infrastructure.

Agility and adaptability are two other important characteristics of a successful BPH provider. We have seen several cases where service providers would move or migrate their servers and/or virtual machines (VMs) from one country to another when sudden legal problems appear in one of their countries of operation. The ability to operate globally and rapidly move resources, in our observations, had a significant impact on a host's survivability.

Criminals consider the ability to accept anonymous payments without requiring additional personal information from the customer to be one of the most important characteristics when selecting a hosting platform for illegal (or potentially illegal) activities. BPH providers often highlight this anonymity factor in their advertisements, as could be seen from offerings like the one below.

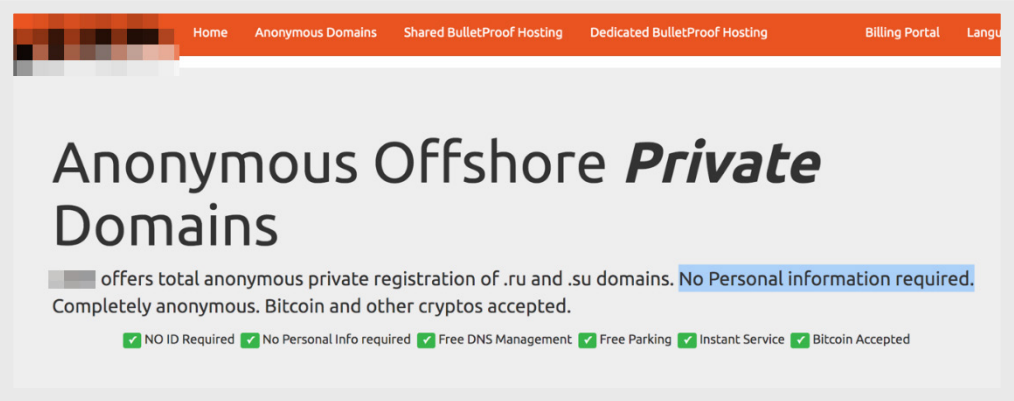


Figure 13. An “anonymous” hosting offering

We also observed that some legitimate hosting platforms would purposely advertise similar anonymity. For example, Domains by Proxy bases its business on concealing its customer’s identities from most public queries. However, it should be noted that the company does respond to legal or law enforcement requests (such as disclosing the site owner details) in cases of copyright violation claims.[10]

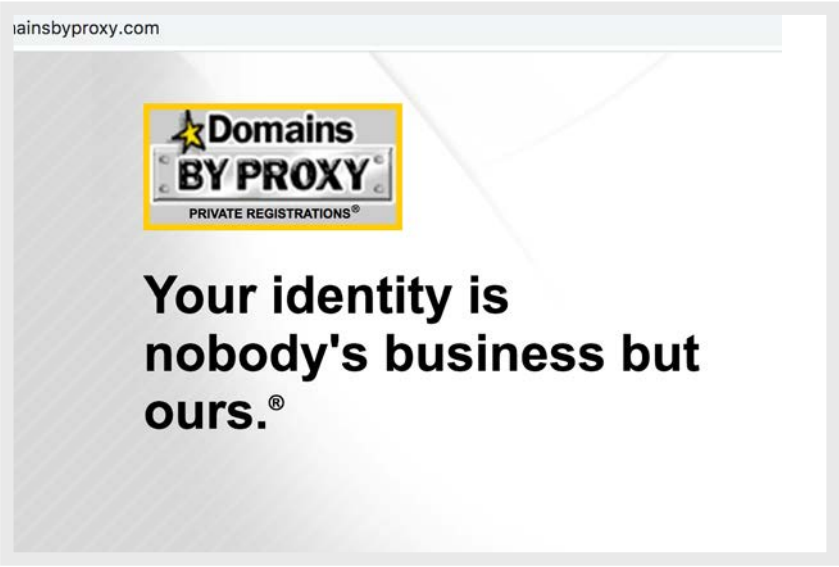


Figure 14. A screenshot of Domains by Proxy

Like any successful business, BPH companies survive by carefully tailoring the location of their hosting infrastructure to their customers’ needs. For example, the following provider has a specific service that offers to host DMCA-violating content with its Anti-DMCA tariff by using servers in countries where such laws do not apply.

Our service provides various services and tariffs. Each of them has its own individual rules and restrictions. Please read them at the rate or service that interests you.

About the prohibition policy

Despite the large list of prohibitions described below, which are based on the prohibition of only crime and black promotion methods, our hosting has a lot of room for creativity. If your project does not fall under any of the described prohibitions, then you can safely post it without fear of blocking. For example, are you tired of blocking other hosts from complaints from copyright holders, competitors, haters, those whom you annoyed? Stay with us!

Absolutely all tariffs are subject to a general ban on : spam, child pornography (and models that look younger than 18+), phishing, fakes, viruses, hacking and port scans of servers, hacking, carding, fraud, brute, DDoS, botnets, spam house, drugs (mixture powders, etc.)

What is prohibited on AntiDMCA tariffs

In addition to the general prohibitions, it is prohibited for UA-AntiDMCA :
1. any

+ general prohibitions specified above

In addition to general prohibitions , the following is prohibited on CH-AntiDMCA :
1.

+ general prohibitions specified above

In addition to the general prohibitions , the following are prohibited on NL-AntiDMCA :
1. replicas of goods (hours

2. clothes

3. shoes, etc.)

4. pharma

5. public vpn services

6. proxying sites with traffic over 5TB / month (for VPS and proxy service)

+ general prohibitions specified above

1. Everything else is ALLOWED .
2. If you receive a complaint that is not prohibited by these rules, then it is simply ignored.
3. For a deliberate violation of these rules, instant blocking without returning any funds.
4. We do not require the closure of anything if you have not violated our rules.
5. We are not a court or prosecutor's office and do not respond to unreasonable complaints of any parties, such letters are regarded as spam.
6. We undertake not to disclose any customer data to any party (except Interpol and the local police) and guarantee 100% anonymity for customers.

Despite the fact that a lot is allowed here, do not neglect security: place your projects only at those tariffs in those countries other than those of your target audience. So you are guaranteed to avoid the interest of the local police in your business at the request of visitors or competitors. Local police refers to the police storing the server location. Recall we ignore police requests from other countries (except for the local interpol) since we act in accordance with the legislation of the country where the server is located.

What is prohibited on OpenVPN

1. OUTGOING email spam.

2. Using xrumer.

3. Hacking servers, hacking, botnets, brute, DDoS (incoming and outgoing), IRC, PPI.

4. Consumption of a large amount of traffic (torrents, movies, etc.).

5. Fraud, carding

1. Everything else is ALLOWED.
2. If you receive a complaint that is not prohibited by these rules, then it is simply ignored.
3. For a deliberate violation of these rules, instant blocking without returning any funds.
4. We do not require the closure of anything if you have not violated our rules.
5. We are not a court or prosecutor's office and do not respond to unreasonable complaints of any parties, such letters are regarded as spam.
6. We undertake not to disclose any customer data to any party and guarantee 100% anonymity to customers.

Figure 15. Anti-DMCA tariff offering

To summarize, the key survival principles for a BPH to stay in business include:

- Discretion for their customers
- Adaptability to the ever-changing threat environment
- Good operational security for their customers' protection: anonymous payments, early alerts on takedown attempts, use of fake identities for registration of legal entities, and payments through banking transactions

How Criminals Secure Assets Like Criminal Forums

For operators of online criminal forums, ensuring that they have a solid networking infrastructure that keeps their site online is only half the battle. Just like any other website on the internet, they may become a target of cyberattacks ranging from denial of service (DoS) to hacking attempts and application-level abuse. The likelihood that they will experience this is higher than a normal website; after all, any site may have disagreements with their users or competitors, but it is uncommon for normal sites to have users who make a career in cybercrime and would carry out such attacks.

Operators of these sites are well-aware of these threats and are quite versed in implementing protection mechanisms to defend their resources. For instance, we frequently observed them adopting common security principles, such as defense-in-depth.

In the previous section, we discussed and gave insights into the types of hosting services used in underground forums. This section covers the different ways underground actors protect their infrastructure at the application level (as opposed to the network level). We cover several mechanisms, including DDoS protection and automated forum scraping protection. It concludes with an example of how some configuration errors in an underground site could allow direct access to the site without solving a Captcha.

Use of DDoS Protection Services

Underground forums are common targets of DDoS attacks by disgruntled forum members and competitors, so proper DDoS protection mechanisms must be in place. For example, the forum Darkode came under a series of heavy DDoS attacks, requiring it to employ DDoS protection.[11]

Downtime during a DDoS attack could affect a forum's reputation, causing members to move to competitor forums and consequently leading to a downturn of usage. This sort of downturn can be a vicious spiral. As people leave the site, activity decreases, which has a knock-on effect on the operators' revenue, from sale commissions to advertisements. A successful defense against DDoS attacks can have the opposite effect, significantly improving a forum's reputation among users as a stable and well-trusted platform.

These DDoS attacks can be conducted on different layers of the Open Systems Interconnection (OSI) model. Typically, DDoS carried out at higher OSI layers require more sophisticated capabilities from the threat actor but can also be harder to thwart. That is why many websites use professional services that protect them from DoS attacks at the application layer, and criminal forums are no different.

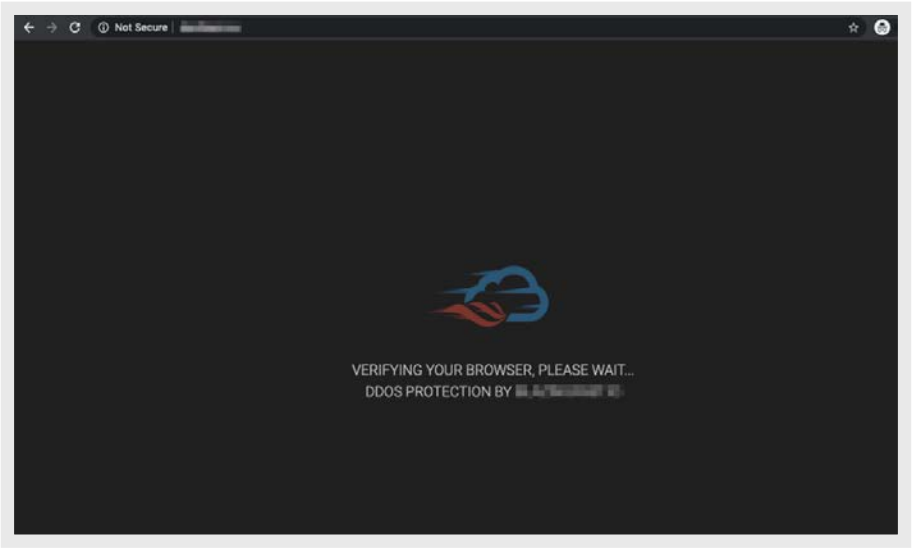


Figure 16. An underground forum protected by a DDoS protection service

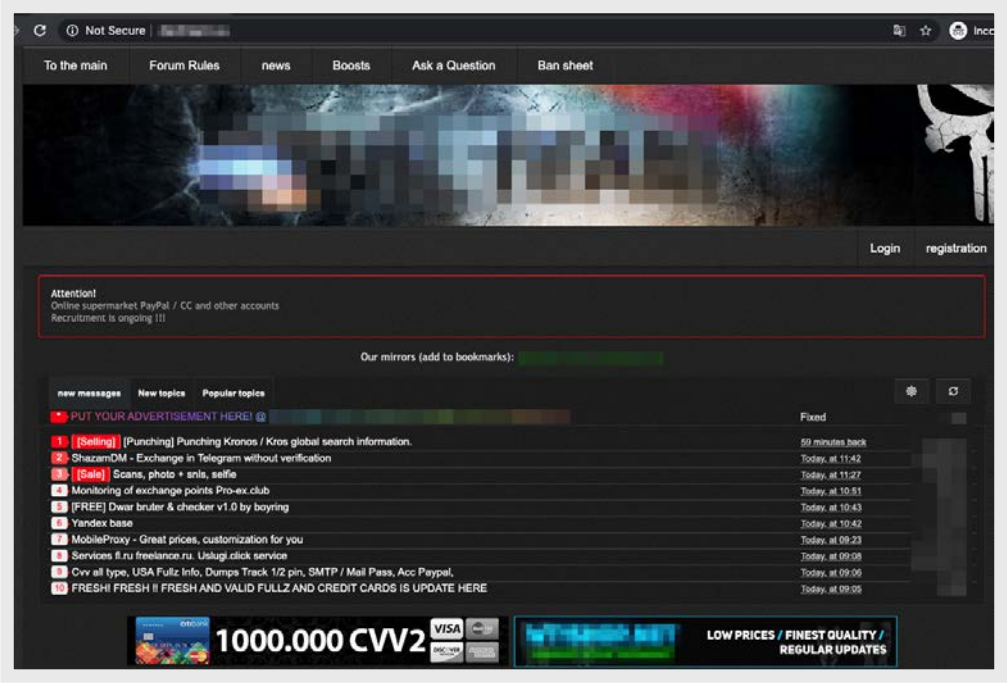


Figure 17. The same underground forum after DDoS protection has been verified

We identified dozens of underground forums that have implemented DDoS protection at the application layer during this research. Forum operators wanting to protect their websites from these attacks are not the only ones who use it; almost any other web-based portal that accommodate criminal infrastructure also require such protection.

For example, even hosting providers that advertise themselves as bulletproof are often forced to protect their web assets. After all, any sort of downtime of a hosting provider's website could lead to significant reputation loss and operational issues.

Mechanisms for Avoiding Forum Scraping by Bots and Humans

Another problem that criminal forum operators face while selecting their hosting is that many search engines, organizations, law enforcement, and researchers attempt to automate the scraping of their content (saving it offline for later analysis).

The collected information is often later exposed in similar threat intelligence reports or used in law enforcement investigations. This information can undermine the OpSec of underground actors, draw unwanted attention, and damage the forum's reputation. In this section, we show several examples of security mechanisms used to prevent automatic forum scraping and keep less-skilled users or even non-native speakers from accessing the forum.

Security mechanisms are often applied to the more sensitive or exclusive sections of the forum. These could include rules that require users to have a particular number of posts or level of reputation in the forum before being able to see sensitive content.

How these controls are implemented varies quite a bit. The forum shown in Figure 18, the forum allows users to see 10 pages without authorization during a 24-hour timeframe. This means that strangers who only need to read several threads do not need to register, but more active users might find it more comfortable to work on the forum with authorization. This benefits the forum operator by making scraping more difficult (or at least slower) and helps the forum by preventing a flood of temporary accounts that users might create to view several threads.

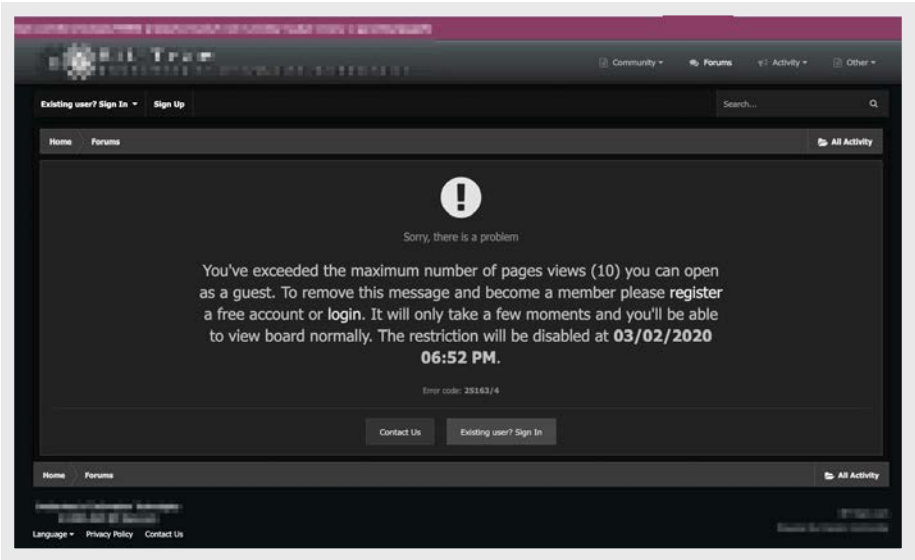


Figure 18. Forum scraping protection in an underground forum

Some forums include measures to prevent data exfiltration by researchers via automated queries in the search section. Search queries can also lead to a high load on the servers and expose forums to different types of attacks based on user input.[12]

Along with input validation, two security mechanisms are often used by underground actors to minimize this impact. The first is timeout-based, which is a mechanism that allows a second query only after a timeout, usually after 5-30 seconds. The following screenshot shows an example of such a measure:

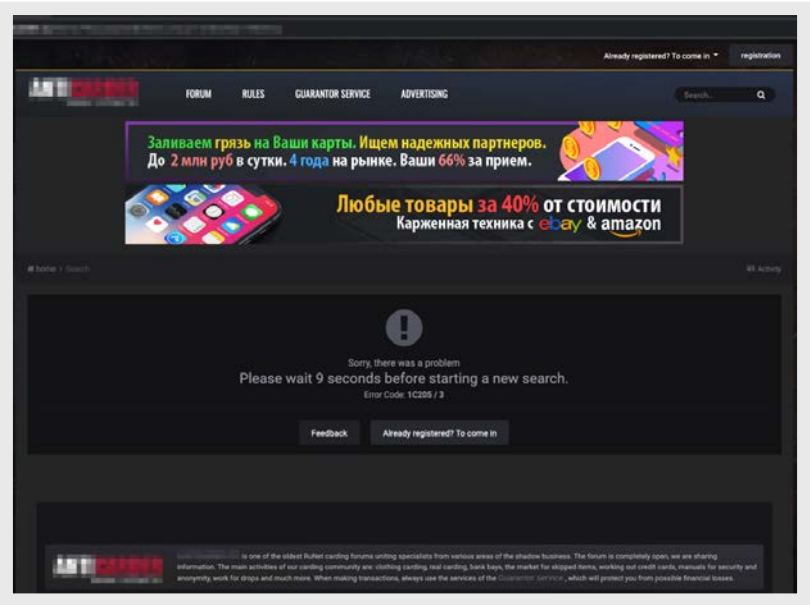


Figure 19. Flood control for search terms

Captcha is another well-known option used to protect automated access to the forum and limit search queries. Captcha is a contrived acronym for “Completely Automated Public Turing test to tell Computers and Humans Apart.” In simple terms, it is a type of challenge-response test used in computing to determine whether a user is human or not.

Captcha is a widely used security mechanism for protecting web pages from automatic scraping and visits by search engines and bots. Many legitimate sites also use Captcha.

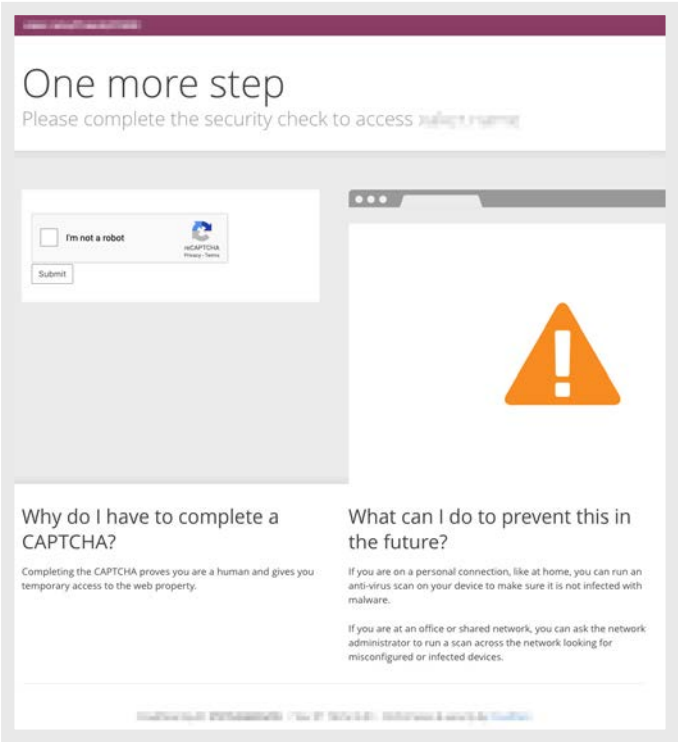


Figure 20. Sample of a Captcha in an underground forum

Criminal forums also offer a variety of services for automated Captcha-solving through a combination of computer automation and low-wage human services that know how to bypass automatic captcha-solving mechanisms. As a result, forum operators cannot normally use standard Captchas, which are seen as "unprofessional" and detrimental to the reputation of the forum owners. To address this situation, some forum owners have come up with creative replacements for well-known Captcha systems.

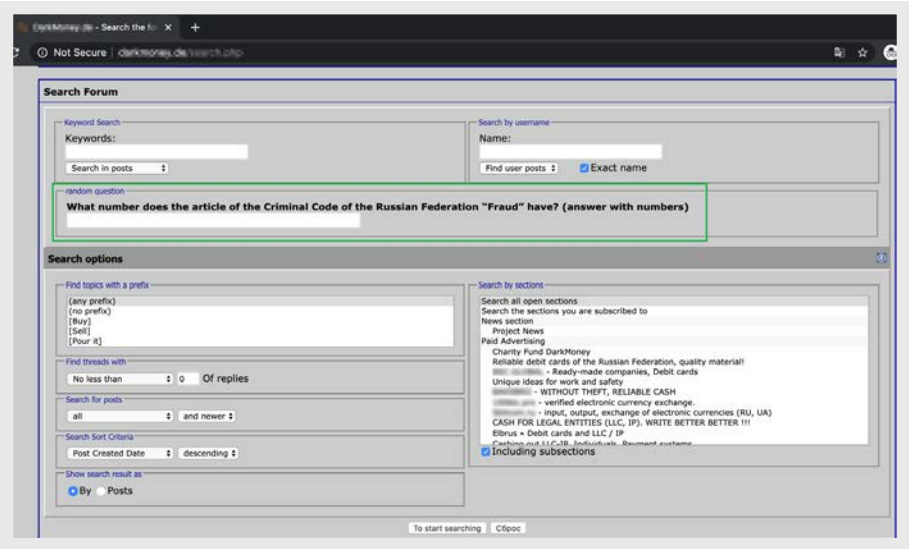


Figure 21. A random question system used to keep out bots and script kiddies

Instead of using a typical Captcha system, some sites ask random questions related to different application fields or ones that require knowledge of the cultural background of their target audience.

In this example, the first group of questions are meant to prevent automated Captcha-solving and keep out script kiddies. The questions in this section can even be related to Mathematics, Physics, information technology (IT), or History. The following screenshot shows examples of some of the questions:

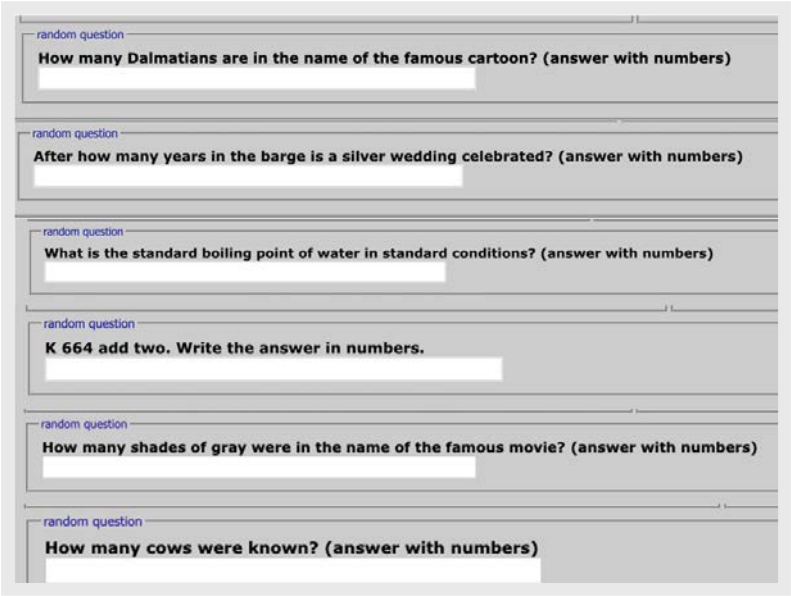


Figure 22. Examples of questions used instead of Captcha

The second category of questions intends to protect the forum from non-native speakers who use machine translation or do not understand the culture of the forum's target audience. Many underground forums cater to a particular type of audience for membership (e.g., individuals from former USSR territories). It is extremely important to enforce "communal" rules like "we do not attack victims in the former USSR territory" (as discussed in previous sections) for the safety of both forum members and the platform.

It is common for threat actors to target foreign countries in their criminal activities for a variety of reasons such as patriotic or safety concerns (i.e., so they're more inaccessible to local law enforcement and/or organized crime groups). So for forums, it is important to maintain uniform membership, where all of the forum members would be willing to accept the same guiding principles.

In the Captcha shown above, some of the questions, particularly the last one, looks confusing after machine translation. Even for a native speaker, it is barely possible to understand the nature of the question if they only see the English translation. This is because the English translation does not "click" with the cultural background knowledge.

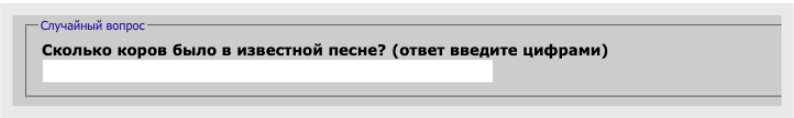


Figure 23. The original question with a completely different meaning

When read by a native speaker, as opposed to automated translation, this question should be translated as "How many cows were in the famous song?". The context is tricky to guess when in English, while the Russian wording hints at the "33 Cows" song from the 1983 "Mary Poppins, Goodbye" movie[13] filmed in the USSR.

Case Study: Dynamics of Criminal Forums and Communities Hosting

To illustrate many of the aspects we have highlighted in this Underground Hosting series, we carried out a historical case study of some of the most notorious online forums that focus on illicit ways to make money online. To do this, we used several passive domain name systems (DNSs) to reconstruct historical records of how these online portals selected their hosting locations over time. Please note that some of these portals simultaneously use hosting in the dark web (i.e., onion sites, Tor), but due to the nature of the networks, we cannot confirm whether the dark web version (the .onion domain) of the same portal actually uses the same hosting.

We started our research by visualizing hosting geographical locations. The following diagram shows the locations of these portal hostings for five years. Note that the information could vary for each forum, depending on our ability to collect particular protective domain name system (PDNS) information. Depending on visualization, we are choosing different time-scales to highlight particularly important points.

Figure 24. Geolocation of IP addresses used by an underground forum between January and April 2020

Note: Pins on this map point to a particular IP address of an underground site. Circles are clusters of IP addresses located in a particular country. The color of each circle varies depending on the density of IP addresses located in a particular country.

Looking into the way these forums were changing their hosting locations revealed several interesting patterns. For instance, the hosting pattern of BlackService showed that this host was able to operate continuously from a hosting location within the United States in 2016, while in other years, the host has been actively jumping across different countries.

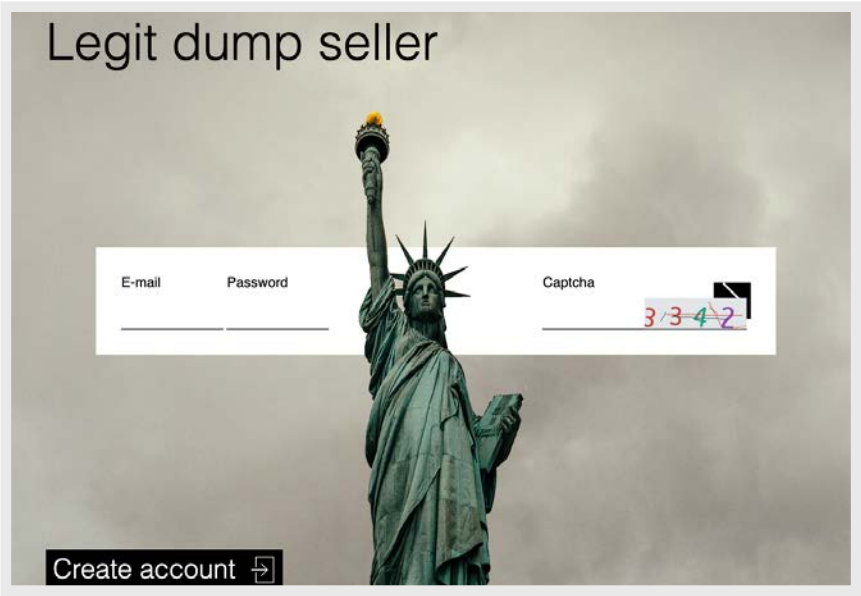


Figure 25. The underground site's front page

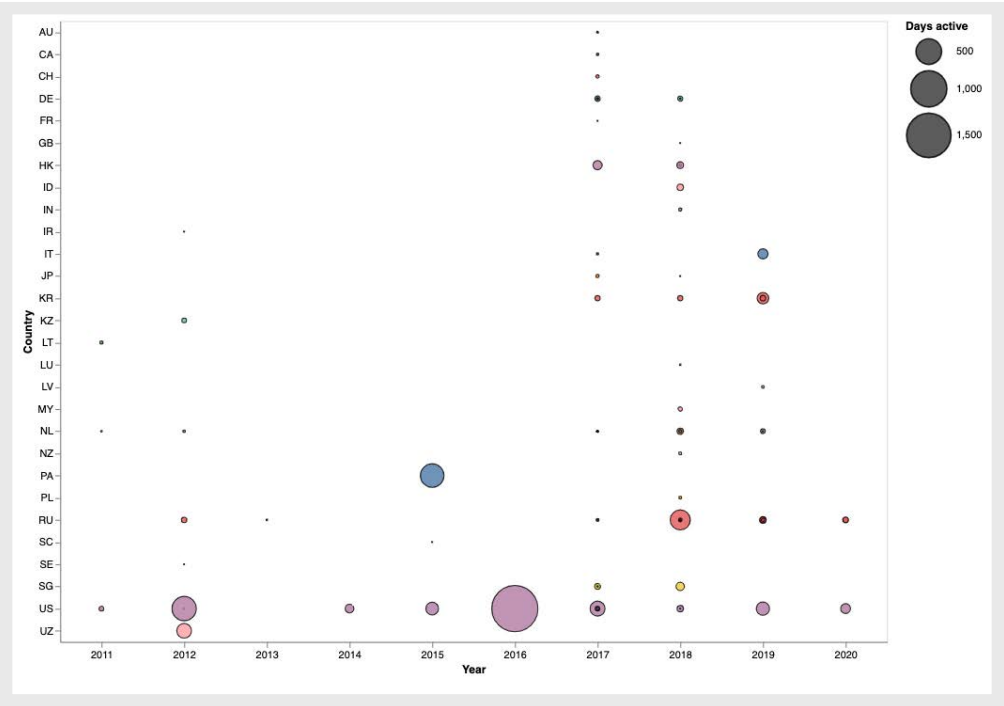


Figure 26. Locations of BlackService's hosting over time and the number of days active, grouped by the time it was last seen (i.e., the largest circle in 2016 indicates that it was active for 1,500 days and the IP was last seen in December 2019)

If we drill down and look into one year, for example, in 2018, we can see that certain hosts were able to provide hosting to the platform for a prolonged period.

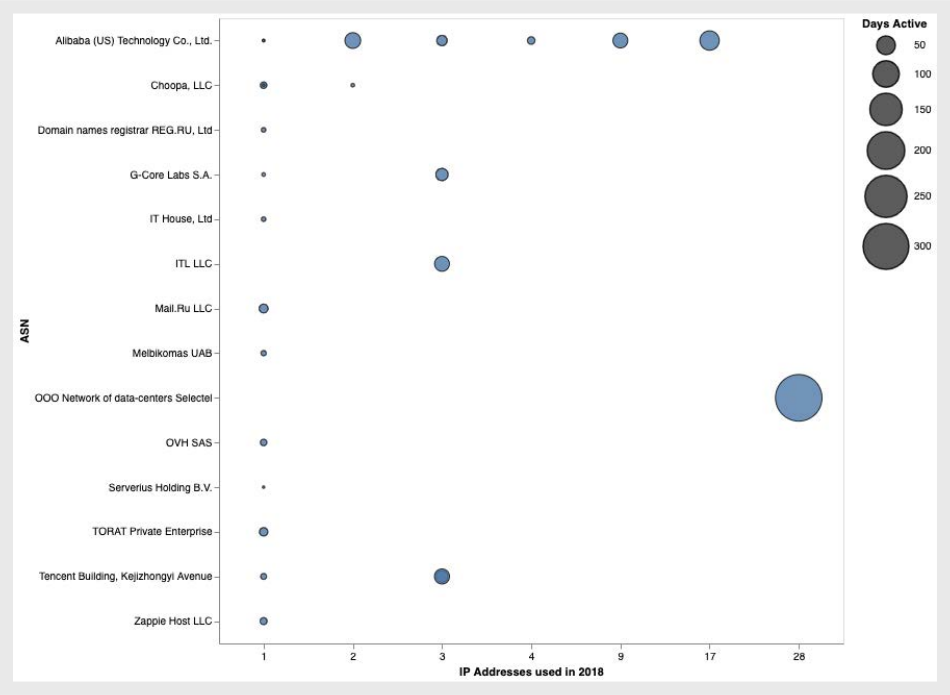
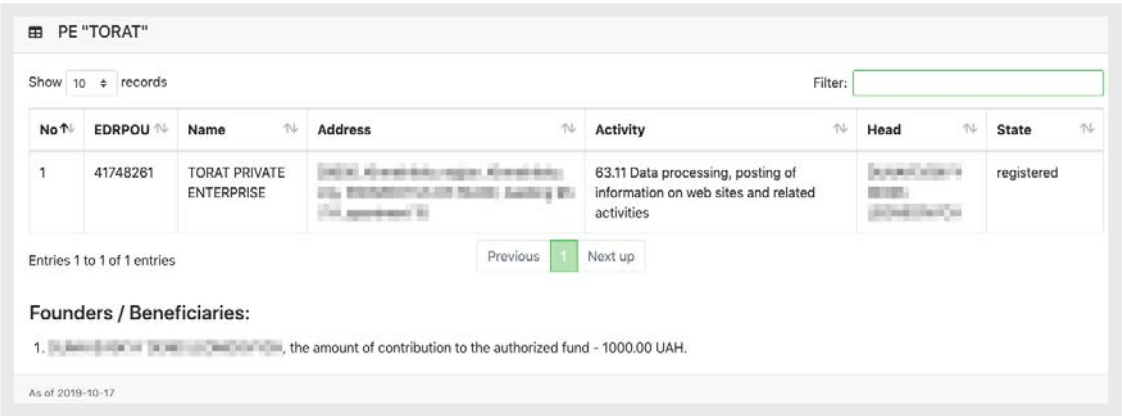


Figure 27. The number of IP addresses used in particular autonomous system numbers (ASNs) by BlackService in 2018

The graph in Figure 27 shows that several ASNs have more than one pool of IP addresses (see the x-axis). This means that IP pools from the same ASN were located in different countries.

Some of these ASN owners do have questionable reputations, whereas others are more legitimate in nature. For example, let's look into the short-lived Torat Private Enterprise[14] (which we believe to be related to the still-live Online Data Ltd. and IT-Softkom Private Enterprise,[15] which are both registered to an address in Seychelles and have taken over IP space previously owned by Torat). Other organizations have also stated this link.[16] There is reason to believe that a company with the same name based in Ukraine likely owned this ASN.



PE "TORAT"

Show 10 records

Filter:

No	EDRPOU	Name	Address	Activity	Head	State
1	41748261	TORAT PRIVATE ENTERPRISE	[redacted]	63.11 Data processing, posting of information on web sites and related activities	[redacted]	registered

Entries 1 to 1 of 1 entries

Previous 1 Next up

Founders / Beneficiaries:

1. [redacted], the amount of contribution to the authorized fund - 1000.00 UAH.

As of 2019-10-17

Figure 28. Information about the Ukrainian Torat company

The owner of the company has several other companies registered to its name based on public records, and some of the companies were named as a subject of several copyright violation court decision documents in Russia.[17]

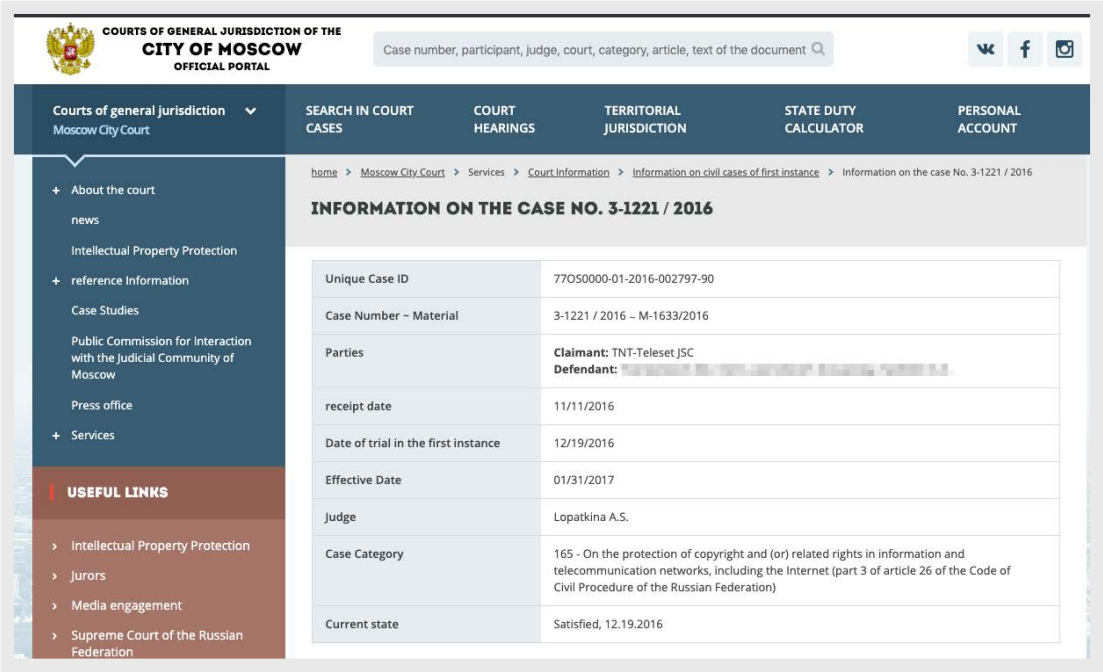


Figure 29. Court cases related to hosting of copyright-protected content

Both customers of BPHs and ASNs that provide BPHs tend to require agile and dynamic switching of company names, locations, and registration details. This agility is one of the factors that make them difficult to investigate and take down, but over time, it also leaves a paper trail that can be followed and used as evidence:

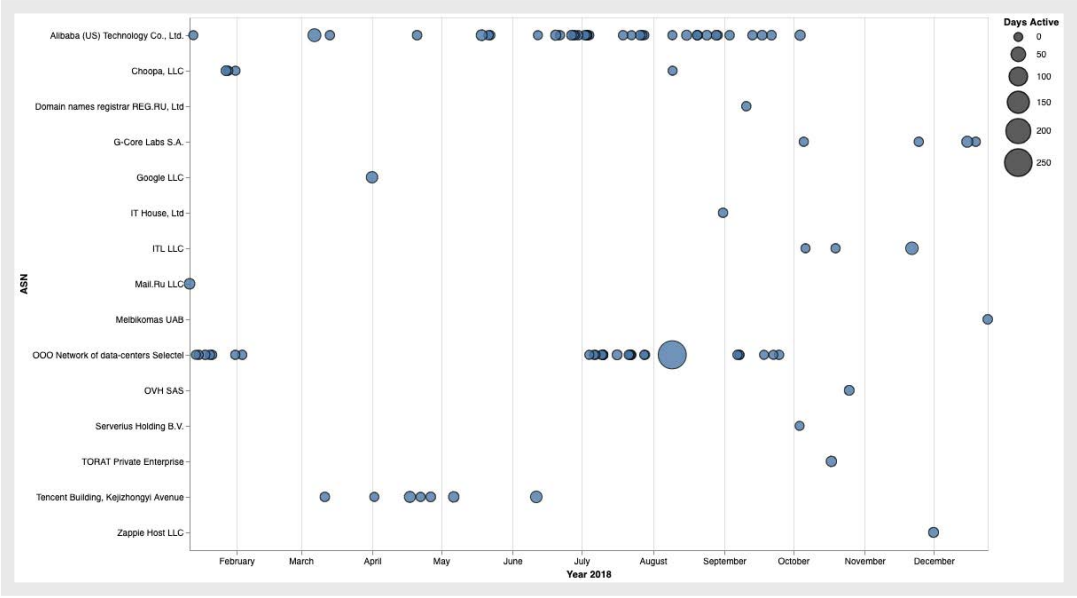


Figure 30. Transitions between ASNs by BlackService in 2018

The next example looks at the forum “Sky-Fraud,” which has been online since at least 2015. Visualizing the data of their hosting patterns reveals a very different hosting setup.

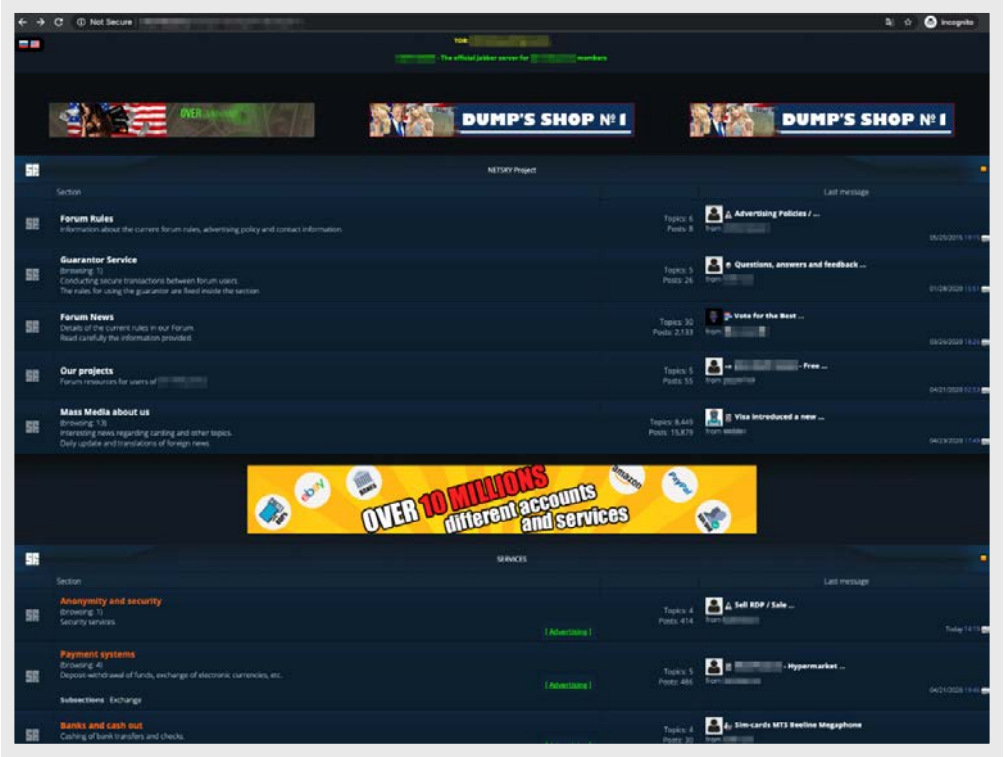


Figure 31. Sky-Fraud forum’s front page

This forum has had different hosting patterns over the years, as seen in Figure 32.

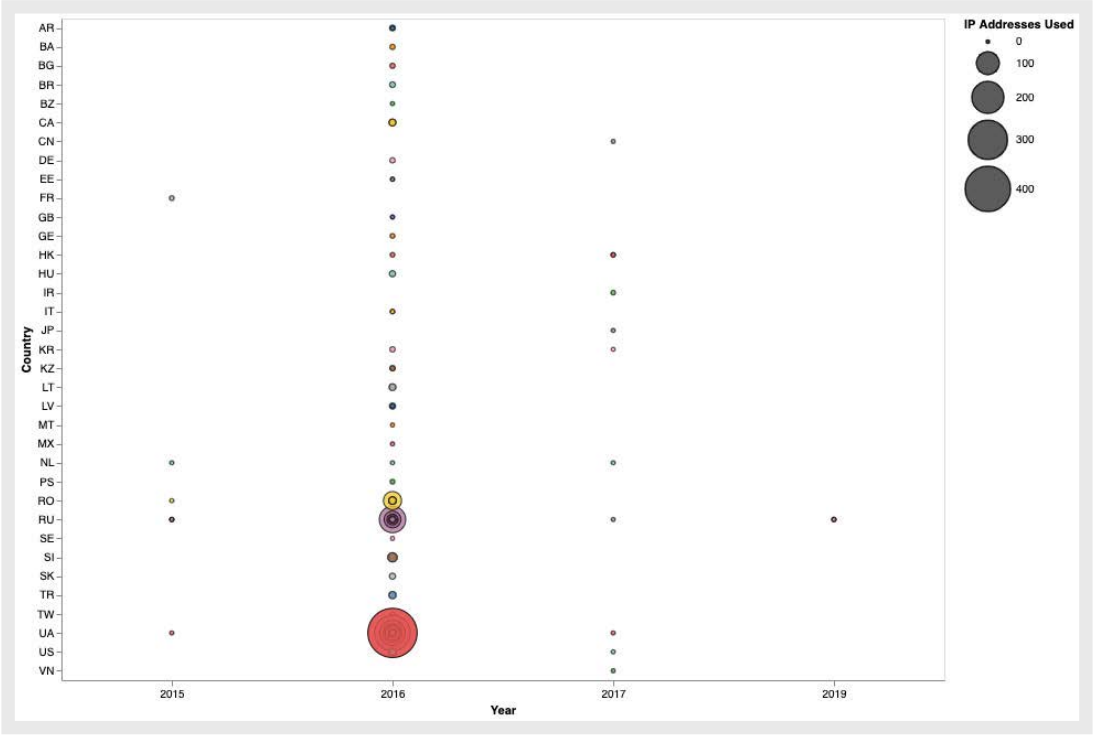


Figure 32. Number of IP addresses used by Sky-Fraud forum

In 2015, it was hosted in five countries, using a small number of IP addresses in each. The following year, there is a considerable spike in both the number of countries and the number of IP addresses used. The same anomaly was visible after using another criterion of how long IP addresses from a particular ASN space were used.

The graph on the left side of Figure 33 shows a huge amount of short-lived hosting across a wide range of ASNs and countries (almost a solid line of small circles). In contrast, the graph on the right side, which excludes 2016, looks more in line with what we saw with BlackService — hosting for several hundred days at a time in any given ASN.

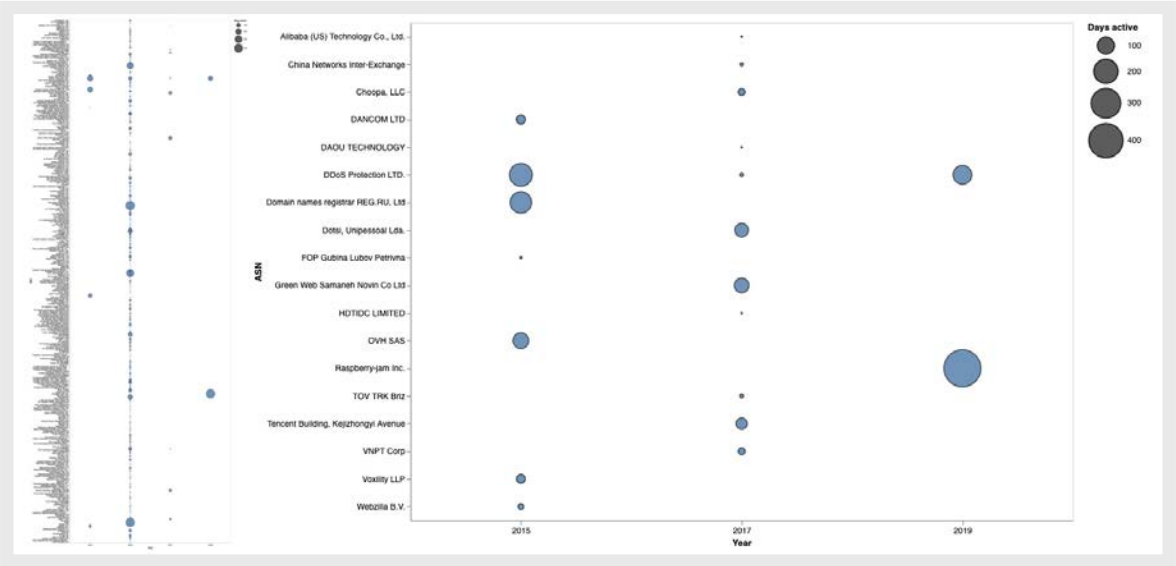


Figure 33. Autonomous systems used by Sky-Fraud forum overall (left) and excluding 2016 (right)

To analyze this 2016 anomaly, we zoomed into particular days of the year to visualize the ASNs that hosted this site. The spike occurred at the end of September 2016, when several thousand IP addresses distributed more than two hundred ASNs in nine days.

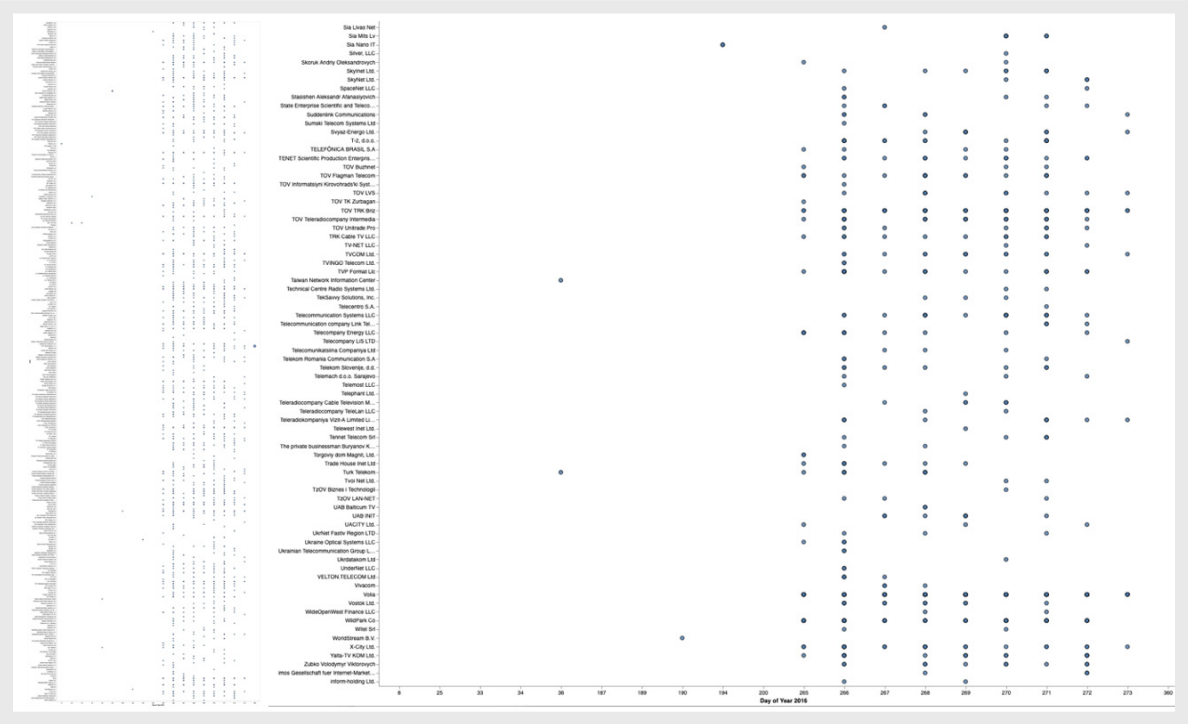


Figure 34. Autonomous systems used by Sky-Fraud forum in 2016, full drawing (left), and a zoomed-in view of the end of September (right)

This kind of agility is typically associated with **fast-flux**-based infrastructure, which was likely used in this case. Fast-flux is a technique that ensures high availability of services through high-frequency switching of domain resolution to a pool of IP addresses or proxies. The forum's real IP address may be relatively static (or moving in a similar pattern to those seen in other years), but it was obfuscated behind the layer of ever-changing proxies.

The forum operators' reasons for using this strategy for less than two weeks before reverting to a more traditional setup is not fully known, but we saw that these forums use different strategies for hosting and are often forced to change these strategies over time. This is likely due to external circumstances such as abuse requests or law enforcement investigations. As a final example, we can see this change of hosting strategy in the case of the forum CrdClub.

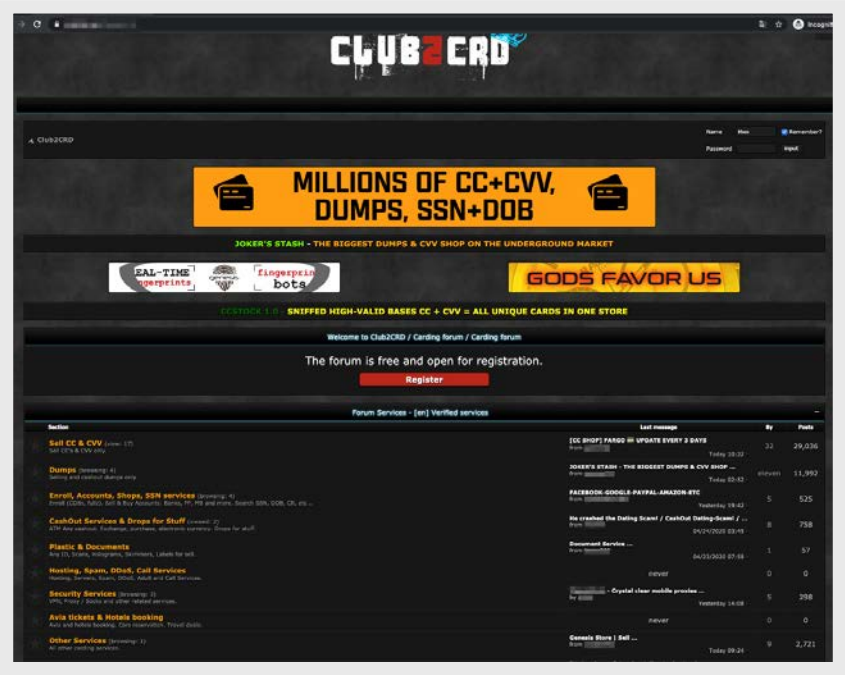


Figure 35. Underground forum CrdClub's front page, hosted at the same ASN for over a year

Figure 36 allows us to observe several stages of the forum's hosting lifecycle. During the earlier days of the forum's existence, it used several ASNs within the same year.

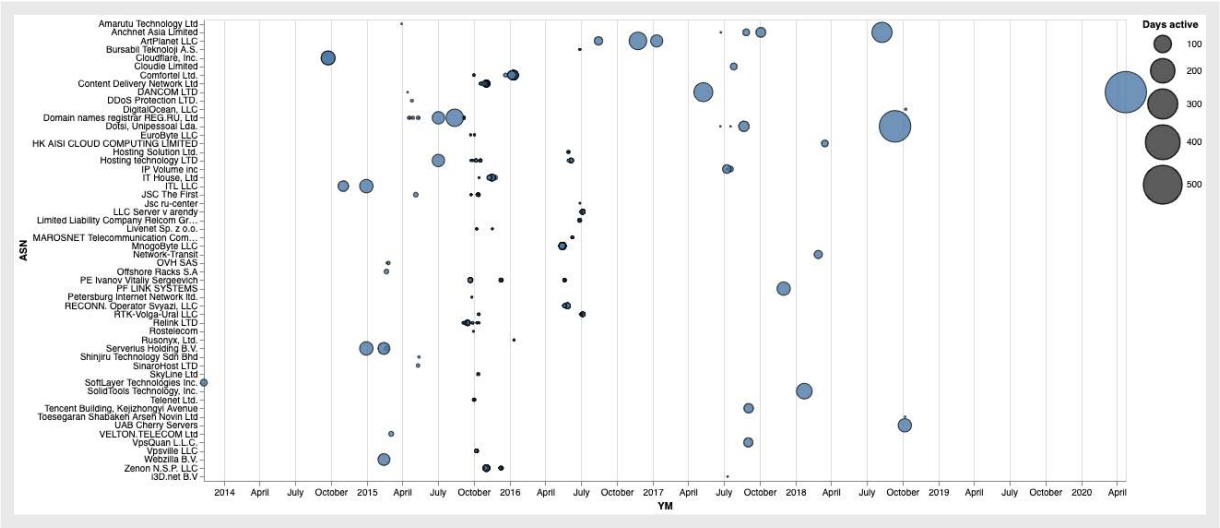


Figure 36. Hosting of CrdClub forum over time

We witnessed a significant transition between multiple ASNs within a short period from the tail end of 2015 to mid-2016. For the last two years, however, we see that the forum reverted to using only a few ASNs for a long period. It appears that the actors behind the forum have found a successful hosting relationship, following the constant need for reliability.

Weaknesses of Bulletproof Hosting Providers

Based on existing work and our own experience, these are a few key indicators that can be used to help identify hosts, including:

- Many BPH service providers rent a space or sub-space from a legitimate hosting provider or a peer with a legitimate ISP, while often creating subsidiaries on offshore locations as a cover-up for BPH IP allocation ownerships. Through past research, Trend Micro has found a significant presence of certain IP ranges in public blocklists and a large number of public abuse requests for a particular IP segment. The allocation range may signify that a BPH service could use it. However, the BPH providers are very agile at handling abuse requests by moving the subjects of blocklists/abuse to a different location, so time correlation is a very important factor.
- Another way to identify a BPH is through analysis of autonomous system behavior and peering information. Many BPH providers pair with trusted upstream providers that can handle abuse requests without disconnecting the BPH from the internet. In many cases, the autonomous systems used by actual hosts are short-lived and are frequently renewed, often reusing the same IP space. Looking into a host's AS is an effective way to affect their business; however, a BPH provider might be able to find new peers to connect with — turning the takedown of a BPH host into a cat-and-mouse game.
- Many hosts replicate their configuration on multiple hosts. If one host belonging to a BPH service can be identified, carrying out machine fingerprinting and searching for similar machines on the internet can yield additional network ranges belonging to the same provider. This includes, but is not limited to, commonly open ports, versions of services running on the machine, unique SSH keys, and SSL certificates. An example of such configuration errors can be found in a short case study in the Appendix.

Once identified, disruption of a BPH service is key, and this does not always have to involve a search and seizure or takedown of their servers. Other approaches should also be considered:

- Properly submitting and documenting abuse requests to both the suspected hosting provider and its upstream peers could be an effective way of having a deterrent effect on a host. This is particularly true when the services of a legitimate hosting provider are resold, and the hosting provider is not aware that its infrastructure is being used for BPH services. Many hosting providers prefer to avoid incidents with law enforcement because server takedowns and arrests may lead to significant loss of revenue due to downtime and client compensations.
- In addition to contacting hosts and their upstream providers, adding the BPH network ranges to well-established blocklists can also have a significant effect on the profitability of the BPH service. For example, the Spamhaus's Don't Route or Peer (DROP) lists[18] are used by many ISPs to limit internet traffic going to malicious actors.
- There are two particularly strong ways to disrupt a BPH. The first of these is to make the business unprofitable by causing a significant financial overhead. Many BPH providers operate with slim margins, so even a slight increase in their operational costs could affect them negatively. Any operations that can drive up their costs are likely to have a major effect on their stability.
- A second related approach is to target the BPH provider's reputation among its customer base. Reputation is vital for any business, but it's critically important in the world of cybercrime as the anonymous nature of customers and service providers means that reputation often serves as the key factor in a customer's buying decisions. There are several ways to undermine this trust, like the use of covert accounts to call into question the security of the criminal hosting provider or unfounded rumors related to their collaboration with authorities.

For those interested in reading more work in this field, we have included recommended references and summaries in the Appendix: Additional Reading.

Conclusion

Over the course of this series, we hope that we have successfully painted a picture of the current state of the cybercrime infrastructure. Starting with a look into the marketplace for these services[19] to an in-depth look at the technical offerings available to criminals,[20] we conclude here with a look into the various ways cybercriminals and service providers operate their businesses. Over this series, you will have gained knowledge of what aspects are important to successful criminal hosting and infrastructure, as well as areas where they may fail.

Ultimately, a perfect bulletproof hosting setup does not exist. What we have observed is that there are many available setups based on reliability, location, required services, and expected time to live (TTL) of the hosting; each criminal group leverages services that best fit their custom business model. The real power of today's BPH setup lies in its flexibility, professionalism, and the range of services that it provides.

BPH is also a time game: Hosts do not expect to be online forever. The idea is to keep things online as long as they are needed, then ideally either kill it (for short-term living services) or move it (for services that need to be online for a longer period). This behavior is very much like the classic cups-and-balls trick — virtualization and cloud technologies now make this game happen quickly (in the old days, criminal hosts had to move machines physically or copy them to new hosts).

This final part highlights the different ways that cybercriminals need to adapt their infrastructure setups, to not only protect themselves from security researchers and law enforcement but also from their fellow cybercriminals. Like any business market, cybercrime is a very competitive one, but unlike other markets, all of the players here have very questionable ethics. We strongly believe that many sources exist for understanding the underground marketplace and for thwarting those who take part in it.

Our goal for this series is to shed light on this crucial part of today's cybercrime business and to help educate those who would investigate it or seek to defend against related activities. While many aspects of criminal infrastructure have remained fairly stable since our last paper on the subject five years ago,[21] other areas have seen significant and sometimes unforeseen changes. As much as we have tried to outline some of our expected changes at the end of this report, there will doubtlessly be innovations that we could not have anticipated. However, with this solid baseline of understanding, we trust our readers will be well-positioned to deal with that new and ever-changing future.

So, where does BPH move from now? Cybercrime and its related infrastructures are continually evolving. We covered emerging threats in part two of our series, but let us recap these key developments.

While it is always hard to predict the future of any form of crime, we believe there are three core areas wherein we expect to see some changes:

Cloud

Enterprise organizations are actively adopting cloud platforms, and larger criminal organizations are no exception. We have observed numerous instances where criminals were using cloud-based services for a variety of functions, from running C&C on the services to exfiltrating data or sending phishing emails. There are several reasons for this shift, including the ease of use the services provide. With the wider adoption of cloud platforms, traffic to and from the cloud infrastructure becomes extremely common on corporate networks. As a result, threat actors can easily masquerade their activities as normal traffic without attracting too much attention, thus making these platforms an attractive option for criminals.

However, major cloud providers often perform their detection of malicious activities (for example, Amazon proactively detects abusive VMs), and many respond to abuse requests very efficiently, along with law enforcement requests for information. In this context, we also noticed another developing tendency in the underground hosting market: Threat actors frequently use smaller cloud providers for hosting malicious infrastructure. There is likely an economic explanation for that. The price pressure from larger cloud infrastructure providers is pushing smaller cloud providers to diversify their offerings. For example, many smaller infrastructure providers are readily taking bitcoin or other anonymous forms of payment, while some are slow to respond to abuse requests (likely also due to resource issues).

We also observed some criminal actors renting infrastructure from such services in bulk, then reselling access to the resources via cryptocurrency in underground markets — effectively becoming unknown resellers of the service. Such criminals often exploit political cross-country complications to ensure that they would not be easily reached by law enforcement based on the geographical location of the systems, which host malicious content.

Cloud services offer another attractive angle to cybercriminals. We have seen service providers that are capable of moving a hosted VM from one data center to another (often, in another country) with minimal downtime when an abuse request is received. Such flexibility greatly benefits cybercriminals as it allows them to rapidly move their infrastructure from one geographical region to another, escaping law enforcement acquisition of their assets. Even in cases when a server is taken down, the infrastructure could be easily recreated from system images.

The elasticity of cloud services benefits cybercriminals in other ways as well. Since many cybercrime activities are conducted in the form of periodic campaigns, such as email phishing campaigns, the threat actors can start up their infrastructure when they need it for a campaign and terminate the instances when those are no longer needed — cutting costs in the process.

New devices for hosting

We also noticed that some BPH service providers are shifting to provide more granular services, allowing them to serve certain niches in the market. These include customized devices for BPH activities, virtual workspaces, and mobile phone hosting or proxies.

Internet of things (IoT) devices are also of high interest to threat actors. We have observed multiple IoT botnets for rent, but even these business models are in their infancy and could be enhanced. For example, IoT botnet-based fast-flux services are easy to deploy and very realistic. IoT devices provide a perfect anti-forensic platform since they often operate on in-memory filesystems, thus traces of activity may disappear after reboot. We have already seen some BPH providers use such routers as a means to provide anonymous traffic aggregation services, and we expect to see more of this in the future.

Many industrial IoT (IIoT) devices these days come with connectivity options (i.e., embedded SIM cards), and such connectivity will be even more widespread in the age of 5G. IIoT devices with embedded SIM cards, when compromised by threat actors, might be too expensive to take down, fix, or replace.

Alternative networks

The usage of alternative networks and decentralized infrastructures may also become more widespread. We have already seen wide adoption of blockchain technology for domain name service provision within the cybercriminal community. Threat actors could also adopt other services such as ZeroNet. When the imageboard 8chan was taken offline, a mirror site for it appeared on the ZeroNet network.

Further, telecommunication networks have been highly interesting to threat actors, and some components of such networks could be adopted for mobility and anonymity. For example, satellite communication links allow threat actors to receive network traffic without accurately revealing their physical locations. Likewise, 3G, 4G, and other connectivity dongles could become more common in providing anonymous internet access to systems that execute malicious actions. Threat actors could also use general packet radio service (GPRS) roaming exchanges that exist in parallel to the internet if the infrastructure comes under a malicious actor's control.

We conclude this paper with a call to action to our readers. If you are an asset owner, a greater precaution should be taken in monitoring and analyzing your asset behavior, regardless if it's a cloud asset (i.e., an API key, a set of VMs) or physical hardware. We have demonstrated that it is very common in the BPH market to resell compromised assets, which can then be used to victimize others as part of the global cybercrime supply chain.

If you are an investigator or a researcher, please collaborate with peers. Working on taking down the cybercrime infrastructure as a group makes us stronger. There are private trust groups who facilitate such investigations; if you do not know who to talk to, talk to us.

If you are a member of a law enforcement organization, you, more than anyone, are key to combating cybercrime. Many of the actions, such as the takedown of threat actor servers or seizure of system logs, require legal support. International collaboration — especially those that include private industry partners — and fast response are more important than ever.

Finally, the fight against cybercrime is not lost. While we have seen that bulletproof hosting has significantly evolved and will for sure continue to improve, so will those who fight cybercrime. Companies like Trend Micro, individual researchers, and law enforcement who combat it will always strive to make the world safer for the exchange of digital information.

Appendix

Definitions and Concepts

Here are several major concepts used throughout the paper, defined for the reader's benefit:

- **Autonomous system number (ASN):** A unique identifier for each network on the internet
- **Bulletproof hosting (BPH):** Refers to several categories of hosting providers, including those who deliberately ignore abuse and legal requests, those who exist in countries with lax cybercrime laws, or even legitimate services with a poor abuse-handling record
- **Dedicated hosting service, dedicated server, or managed hosting service:** A type of internet hosting whereby the client leases an entire server not shared with anyone else
- **Domain generation algorithm (DGA):** A computer program that generates domains to contact systematically or programmatically
- **Fast flux:** A domain name service obfuscation technique that botnets use to hide their servers behind an ever-changing network of compromised machines or proxies (see **proxy**)
- **Internet service provider (ISP):** An organization that provides services for accessing or using the internet
- **Peer-to-peer:** Refers to infrastructure that operates as a network of computers, with each acting as a server to others, sharing access to files or network traffic without the need for a central server; often seen in VPN setups
- **Proxy:** A computer that functions as a relay between a client and server, offering a degree of obfuscation to the client's true location; one well-known type uses a protocol known as SOCKS
- **Remote Desktop Protocol (RDP):** A Microsoft-developed protocol that provides a user with a graphical interface for a computer being connected across a network; virtual network computing (VNC) is a similar standard
- **Traffic Direction System (TDS):** A system that uses a network of connected landing pages or servers that direct internet traffic to its ultimate end goal based on a variety of criteria such a geographic location, operating system, browser, and language
- **Virtual private network (VPN):** A private network overlaid virtually on top of a public network such as the internet
- **Virtual private server (VPS):** A virtual machine sold as a service by an internet hosting provider

Additional Reading

The wide adoption of BPH platforms for all kinds of malicious activities makes it important to understand how authorities can identify bulletproof hosts and their presence on the internet, and how they can address and possibly mitigate them. Several excellent research have already been carried out in this field, and we will summarize some of them, which we think merit further reading:

- An early work by Konte, Perdisci, and Feamster[22] discussed the design of the ASwatch system to identify autonomous systems that are likely used for bulletproof hosting. However, this paper lacked the essential component of the business models of BPHs and underground hosts. Our opinion echoes the views of several of the authors here: The best way to disrupt a bulletproof host is to make the business unprofitable by causing a significant financial overhead.
- In the following work by Noroozian et al.,[23] the authors looked into the operations of a BPH host named MaxiDed. The authors pointed at operational cost as one of the weak points of a BPH host. In an attempt to identify the potential choke points, the authors analyzed BPH forensic data, including database dumps and source code, attempting to reconstruct the operation model of the criminal enterprise.

  In the analysis of the hosts' reseller model, the authors conclude that many BPHs operate with slim margins, so even a marginal increase of BPH providers' operational costs may lead to negative consequences for them.

  MaxiDed maintained a marketplace where available hosting options could list available resources, as well as what kind of content is allowed to be hosted on them. As part of this business model, MaxiDed dealt with customer outreach, handling payments, and customer interactions. The paper provides a unique study of a BPH through analysis of data, which was collected from servers recovered from the BPH infrastructure.
- The follow-up doctoral thesis by Noroozian[24] discusses generalized security practices by hosting providers and their responsiveness to handling abuse requests while using MaxiDed as one of the case studies.
- In another paper by Alrwais et al.,[25] the authors examined how BPH behavior could be detected by analyzing Whois information and cross-referencing these with other sources such as Spamhaus to detect and validate malicious sub-allocations. Many BPHs rent a space or sub-space from a legitimate hosting provider or a peer with a legitimate ISP, while often creating subsidiaries on offshore locations as a cover-up for BPH IP allocation ownerships.

  The authors identify key features that could be used to detect malicious sub-allocations and use a classifier to first train, using labeled data, and then analyze and validate potentially malicious IP allocations using IP Whois information provided by all five major regional internet registries (RIRs).

Case Study: Infrastructure Configuration Mistakes

In this paper, we discussed several security mechanisms that are used by underground actors at the application layer to protect their infrastructure, but we also highlighted that errors in configuration could be the weaknesses that are leveraged to identify such infrastructure.

This appendix discusses a short case study about the consequences of errors in the website's security configuration and setup mistakes.

For example, a carding forum that was originally located behind a content delivery network (CDN) protection required solving a Captcha to access.

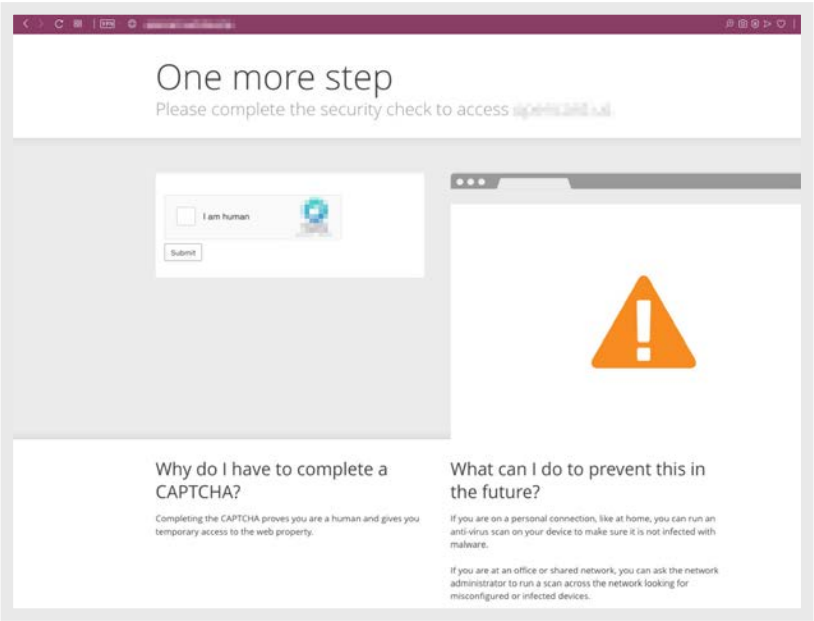


Figure 37. The access process to the underground forum as owners expected

After the Captcha is solved, it is possible to see the main page of the forum. The domain used by the forum resolved to an IP range belonging to a well-known CDN, and so far, this situation matched the operator's expectations.

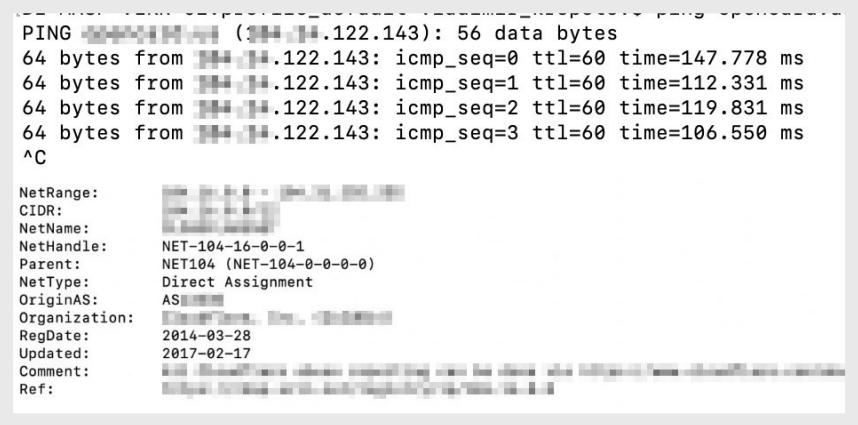


Figure 38. The underground site indexed on the IP address's front-end located behind CDN

However, due to a configuration error, the true location of the web server was exposed by the IP address, which was indexed by the Google search engine, along with the normal domain-based access. This can be found by searching for unique strings from the forum's main page.

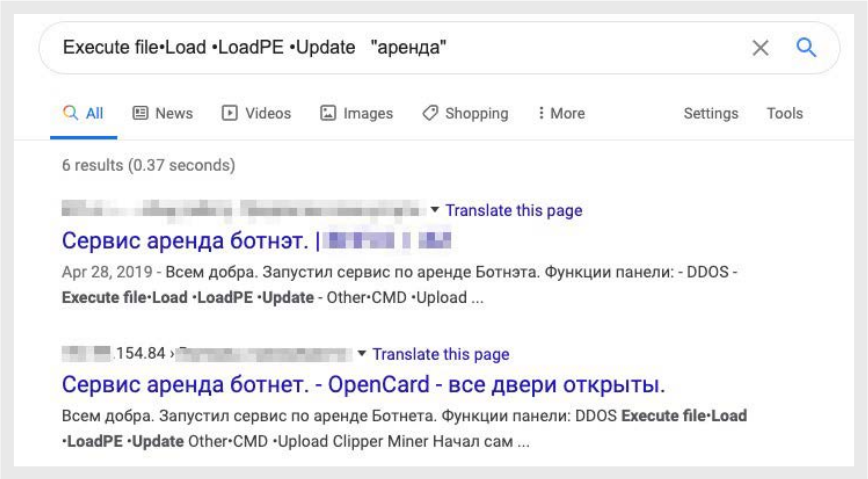


Figure 39. The IP address of the underground forum's site revealed in search engine

The IP range of the forum found via Google search does not match the IP ranges belonging to the CDN used by this underground forum.

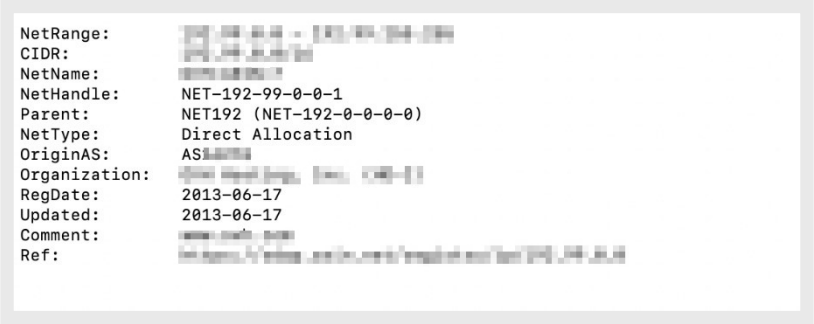


Figure 40. Underground forum hosted on an IP address located in another netblock

When accessed directly via this true hosting IP, the site was accessible without triggering the Captcha security mechanism provided by the CDN. This way, accessing the server should not be exposed in normal circumstances; it should only be accessible via the domain name.

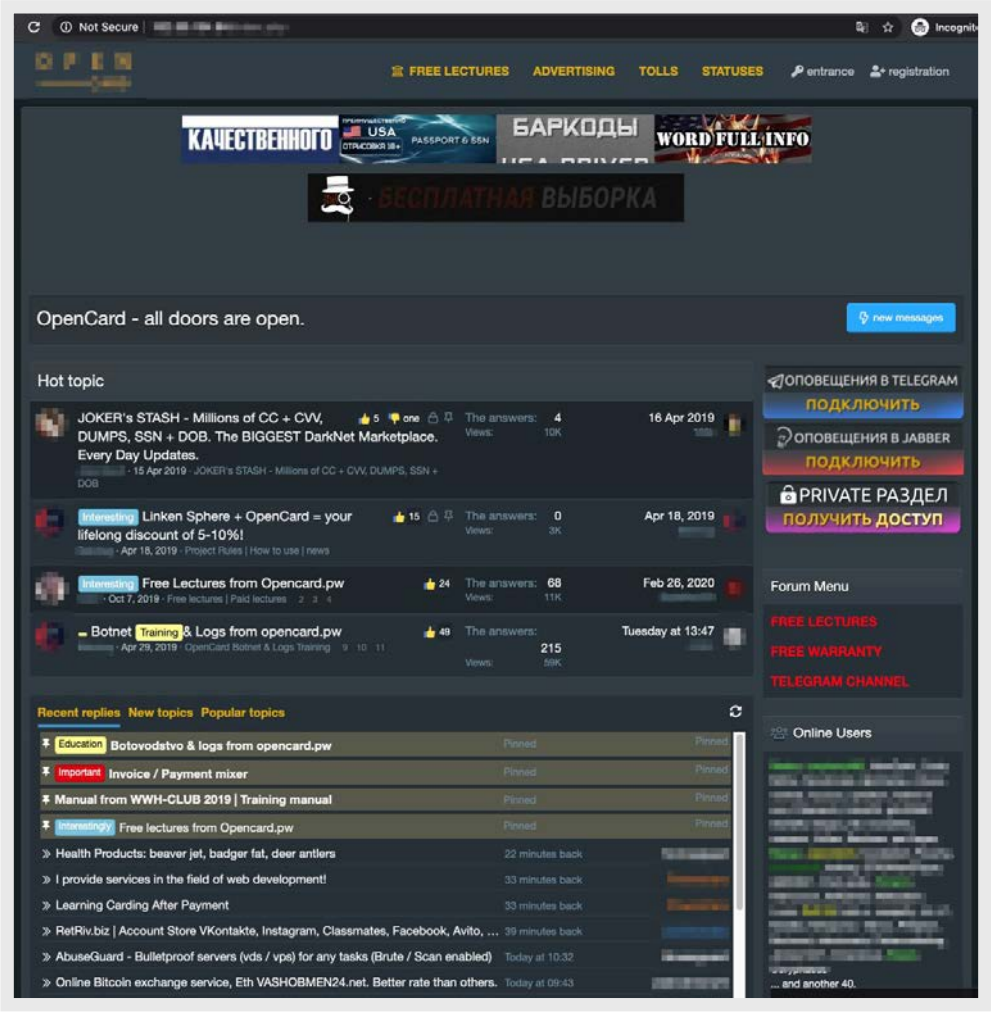


Figure 41. Access to the underground site by IP address does not require solving of the Captcha

From a threat actor's point of view, this kind of configuration error can lead to a variety of attacks on the website, including more effective DDoS attacks. For researchers and law enforcement, discovering the true IP address of a hosted malicious site opens up a range of extra chances to disrupt it, or at least makes it easier to do than when behind a CDN.

References

1 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Jul. 21, 2020). *Trend Micro.* "Hacker Infrastructure and Underground Hosting 101: Where Are Cybercriminal Platforms Offered?." Accessed on Aug. 22, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered.

2 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sep. 1, 2020). *Trend Micro.* "Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals." Accessed on Sep. 1, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals.

3 Colin Lecher. (Sep. 27, 2019). *The Verge.* "Police raid 'bulletproof' hosting company run out of former NATO bunker." Accessed on Aug. 22, 2020, at https://www.theverge.com/2019/9/27/20886971/german-nato-bunker-bulletproof-hosting-raid.

4 Latvian Public Broadcasting. (Sep. 13, 2018). *LSM.lv.* "Latvian hacker sentenced to 33 months in US federal prison." Accessed on Aug. 22, 2020, at https://eng.lsm.lv/article/society/crime/latvian-hacker-sentenced-to-33-months-in-us-federal-prison.a292202/.

5 Brian Krebs. (Jul. 19, 2016). *Krebs on Security.* "Meet the World's Biggest 'Bulletproof' Hoster." Accessed on Aug. 22, 2020, at https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/.

6 Vincent Hanna. (Nov. 17, 2008). *Spamhaus.* "Another one bytes the dust." Accessed on Aug. 22, 2020, at http://www.spamhaus.org/news/article/640/.

7 Jeff Stone. (Jul 16, 2019). *CyberScoop.* "Ukrainian hacker arrested after allegedly providing bulletproof hosting to Russian security." Accessed on Aug. 22, 2020 at https://www.cyberscoop.com/mikhail-rytikov-ukrainian-hacker-arrested-ivan-bakanov/.

8 Dhia Mahjoub. (Oct. 18, 2018). *RIPE Network Coordination Centre.* "Criminal Abuse in RIPE IP space." Accessed on Aug. 22, 2020, at https://ripe77.ripe.net/presentations/134-RIPE77_Anti_Abuse_WG.pdf.

9 Justin Nasseri. (Nov. 19, 2013). *McCarthy Tétrault LLP.* "'The digital and Internet age meets the law of search and seizure' as the SCC clarifies the law on search warrants and computers in R v. Vu." Accessed on Aug. 22, 2020, at https://www.mccarthy.ca/en/insights/blogs/canadian-appeals-monitor/digital-and-internet-age-meets-law-search-and-seizure-scc-clarifies-law-search-warrants-and-computers-r-v-vu.

10 Ernesto Van der Sar. (Mar. 7, 2014). *TorrentFreak.* "'Domains by Proxy' Hands Over Personal Details of "Pirate" Site Owner." Accessed on Aug. 22, 2020, at https://torrentfreak.com/domains-proxy-hands-personal-details-pirate-site-owner-140307/.

11 Brian Krebs. (May 20, 2013). *Krebs on Security.* "Conversations with a Bulletproof Hoster." Accessed on Aug. 22, 2020, at https://krebsonsecurity.com/2013/05/conversations-with-a-bulletproof-hoster/.

12 Robert Grill. (n.d.). *SANS Institute.* "Testing Web Applications for Malicious Input Attack Vulnerabilities." Accessed on Aug. 22, 2020, at https://pen-testing.sans.org/resources/papers/gcih/testing-web-applications-malicious-input-attack-vulnerabilities-100140.

13 Elena Korenévskaya. (Mar. 28, 2014). *Russia Beyond.* "4 Soviet films in a British boat" Accessed on Aug. 22, 2020, at https://www.rbth.com/arts/2014/03/28/four_soviet_films_in_a_british_boat_35445.html.

14 Hurricane Electric Internet Services. (Aug. 21, 2020). *Hurricane Electric.* "AS200936 TORAT Private Enterprise." Accessed on Aug. 22, 2020, at https://bgp.he.net/AS200936.

15 RIPE NCC. (n.d.). *RIPE Network Coordination Centre.* "IT-SOFTKOM Private Enterprise." Accessed on Aug. 22, 2020, at https://www.ripe.net/membership/indices/data/ua.it-softkom.html.

16 Scamalytics. (n.d.). *Scamalytics.* "TORAT Private Enterprise - Fraud Risk." Accessed on Aug. 22, 2020, at https://scamalytics.com/ip/isp/torat-private-enterprise.

17 GARANT. (2017). *Garant.ru.* "Решение Московского городского суда от 17 августа 2017 г. по делу N 3-0348/2017." Accessed on Aug. 22, 2020, at http://base.garant.ru/149139495/.

18 Spamhaus. (n.d.). *Spamhaus.* "The Spamhaus Don't Route Or Peer Lists." Accessed on Aug. 22, 2020, at https://www.spamhaus.org/drop/.

19 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Jul. 21, 2020). *Trend Micro.* "Hacker Infrastructure and Underground Hosting 101: Where Are Cybercriminal Platforms Offered?." Accessed on Aug. 22, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered.

20 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sep. 1, 2020). *Trend Micro.* "Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals." Accessed on Sep. 1, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals.

21 Max Goncharov. (Jul. 15, 2015). *Trend Micro.* "Bulletproof Hosting Services: Cybercriminal Hideouts for Lease." Accessed on Aug. 22, 2020, at https://www.trendmicro.no/media/wp/wp-criminal-hideouts-for-lease-en.pdf.

22 Maria Konte, Roberto Perdisci, and Nick Feamster. (Aug. 2015). *Association for Computing Machinery.* "ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes." Accessed on Aug. 22, 2020, at https://dl.acm.org/doi/abs/10.1145/2785956.2787494.

23 Arman Noroozian et al. (Aug. 2019). *USENIX.* "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting." Accessed on Aug. 22, 2020, at https://www.usenix.org/system/files/sec19-noroozian.pdf.

24 Arman Noroozian. (Feb. 10, 2020). *TU Delft Library*. "Evaluating Hosting Provider Security Through Abuse Data and the Creation of Metrics." Accessed on Aug. 22, 2020, at https://repository.tudelft.nl/islandora/object/uuid:8d2b0432-7ebe-42c0-b231-34f1a08bd779?collection=research.

25 Sumayah Alrwais et al. (n.d.). *Damon McCoy.* "Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks." Accessed on Aug. 22, 2020, at http://damonmccoy.com/papers/alrwais2017under.pdf.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research

©2020 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Smart Protection Network are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.