The Hacker Infrastructure and Underground Hosting

An Overview of the Cybercriminal Market

Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin

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.

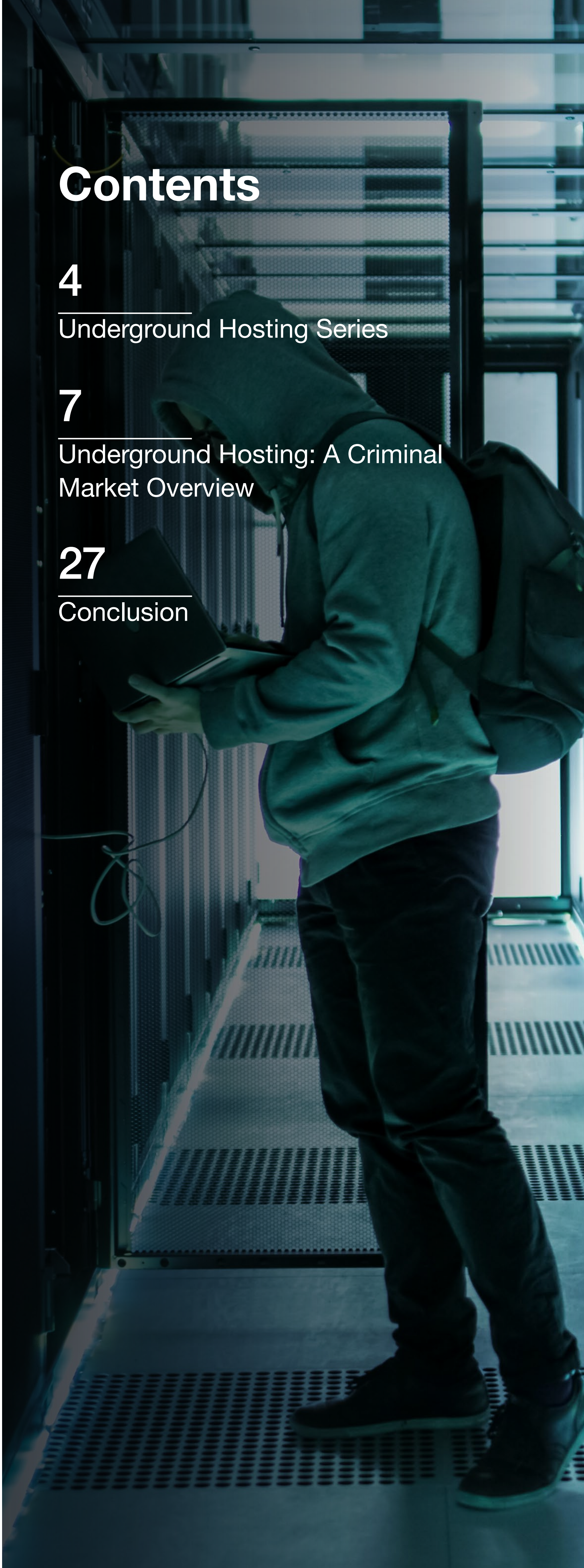
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is 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, and
Fyodor Yarochkin**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)



Contents

Cybercriminals are in the business of making money at their victims' expense. Unfortunately, this involves a great deal of money and countless victims. Criminals do this by stealing identities and credit card numbers, encrypting user data (and offering to restore it for a fee), and employing many other methods.

In the cybercrime underground, a criminal's hosting service and infrastructure serve as the backbone of every aspect of their business model. It hosts the command-and-control (C&C) servers that threat actors use to run their victims' machines, the forums and chat services used for interacting with fellow criminals, the anonymizing services for covering their tracks, and many more. At every level of these criminal enterprises, a reliable infrastructure is critical.

How do criminals host such content on the internet without a takedown or an arrest, and what makes them difficult to track down? The answer is that they use what the InfoSec community call underground hosting, or underground infrastructure.

Hosting services are the foundation of many, if not all, major cybercriminal operations. These hosting providers sell cybercriminals the means to host their C&C infrastructure, discussion forums, marketplaces, various malicious content, and other tools that enable them to be efficient and extremely difficult to disrupt.

This research paper details how criminal forums have evolved to adapt to the demands of the underground market and ways they have enabled easier access to underground hosting. We delve deep into this thriving cybercriminal market and reveal the full range of products and services it offers to threat actors, and the methods used to promote and sell them.

Underground Hosting Series

This paper is the first of a three-part series that aims to cover the broad topic of underground infrastructures. It has been over five years since we published an article on underground hosting,[1] and the situation regarding its infrastructure has changed significantly, as did the tools used by threat actors. We have noticed that a certain type of threat actor is now extensively using cloud services in their attack toolchain, along with widely abused "free" services such as free DNS domains, free content hosting abuse, and social networks.

The use and abuse of compromised assets have also become more significant. Acquisition, analysis, and resale of compromised assets formed a whole new market in the underground. Compromised asset analysis, wherein criminal experts examine the compromised assets and identify the best possible ways to monetize the system, is now an essential part of the attack chain.

This research series aims to be as comprehensive as possible, covering all major parts of the current criminal hosting infrastructure. We have divided it into three core parts, outlined below:

- **Part 1 - Underground Hosting: A Criminal Market Overview.** The first part of the series details the market element of the cybercrime underground: How are goods and services bought and sold? This part will be of particular interest to those looking to learn about the economy of the underground functions.
- **Part 2 - Underground Services and Infrastructure.** This part covers the major types of infrastructure that cybercriminals use — from compromised assets to dedicated hosting providers and more. It also provides practical insights for organizations on what to expect if some of their servers are compromised. This part will benefit those responsible for protecting networks and organizations from attacks, as well as those investigating cybercrime at a technical level.
- **Part 3 - Underground Hosting OpSec and Modus Operandi.** To conclude the series, part 3 will cover the business models and survival methods that cybercriminals deploy to advertise their criminal infrastructure. It will also include our insights on the future of the criminal infrastructure. This report intends to empower those investigating criminal actors (such as law enforcement), as well as those interested in the human element of cybercrime.

Each part of the series also includes an appendix of "Definitions and Concepts," serving as a glossary of terms that readers may not be familiar with. It is also worth noting that several screenshots used here were machine-translated.

One area that this series does not cover in-depth is the monetization and money laundering schemes used by criminals. As with traditional crime, the main goal of cybercrime is to make money; thus, moneymaking schemes and "cleaning" infrastructure or services account for a significant part of criminal business models. Cybercriminals need services that would allow them to legalize their funds, be those funds stolen from credit cards or other compromised resources. However, the ways criminals monetize their activities is a topic that is substantial enough for a separate research paper and outside of the scope of this project, which focuses on the technical infrastructure of cybercrime.

What is Underground Hosting?

We define underground hosting as any service provided to host components or infrastructure with the goal of conducting malicious and criminal activity. This is a very broad definition, but it also allows us to examine a wide range of underground activities involved in the provision of infrastructure components to criminals.

Such services include the provision of hosting infrastructures, virtual and dedicated servers, IP addresses, fast-flux infrastructures, compromised servers, compromised credentials used to create additional infrastructure components, domain name provisions, and crime-assisting infrastructures such as the provision of anonymizing services, virtual private networks (VPNs), or traffic accelerators. It also includes services such as distributed denial of service (DDoS) protection, which, while used by large legitimate websites, is also critical for many criminal services.

The Past of Underground Hosting

The hosting of hacker infrastructure has been an essential component of cybercrime from the very early days of the internet. Malicious software needed to communicate with its master, so hackers had to run systems that would receive those connections. These systems are commonly referred to as C&C systems.

From dedicated hostings to peer-to-peer and fast-flux, techniques used to effectively and securely organize such infrastructure have since evolved. Hackers used domain generation algorithms (DGAs) to ensure that malware C&C infrastructure could survive takedowns. In 2015, we released a paper documenting some of the bulletproof and fast-flux infrastructures[2] they used.

The hosting of C&C systems is not the only purpose of the infrastructure that threat actors use. Hosted infrastructures also serve other purposes, such as running forums and message boards and trading illegal materials via online shops. They're also used to host phishing content or send phishing emails and virtual private server (VPS) systems that threat actors use to launch attacks.

Traditionally, underground hosting mainly covers the hosting of systems used by criminals for malicious purposes. However, recent developments in cybercrime have increased the variety of offerings for hosting related services in the underground. The next section discusses the types of such services in detail.

Types of Services

We classified the types of services related to the provision of underground infrastructure based on the intended use of those services. This includes:

- **Dedicated and virtual hosting providers.** This includes bulletproof hosting, fast-flux networks, and other types of hosting provision.
- **Service protection and anonymization providers.** This includes VPNs, proxies, reverse proxy services, anonymization services, and traffic acceleration services. This category does not only include dedicated proxies, but includes those from compromised residential IP addresses, mobile, and internet of things (IoT) devices.
- **Additional infrastructure provision.** This includes uncommonly used infrastructure provisions such as telecommunication-related services (e.g., calling, call landing, SMS spamming), in-browser botnet services, and IoT hosting services.
- **Legitimate services/systems used and exploited for malicious purposes.** This includes free services such as free DNS hosting, dynamic DNS hosting, free SSL certificate provision, and cloud services.

How Hosting Is Used

Hosting is the core component that connects different cybercriminal components. Botnets require hosting to deploy their C&C infrastructure. Underground forums need it to host their communication platforms. Criminal groups require it to run their communication systems. Spam operators need it to host their spam distribution systems.

Threat actors design many of these hosting applications to meet a few common criteria, such as:

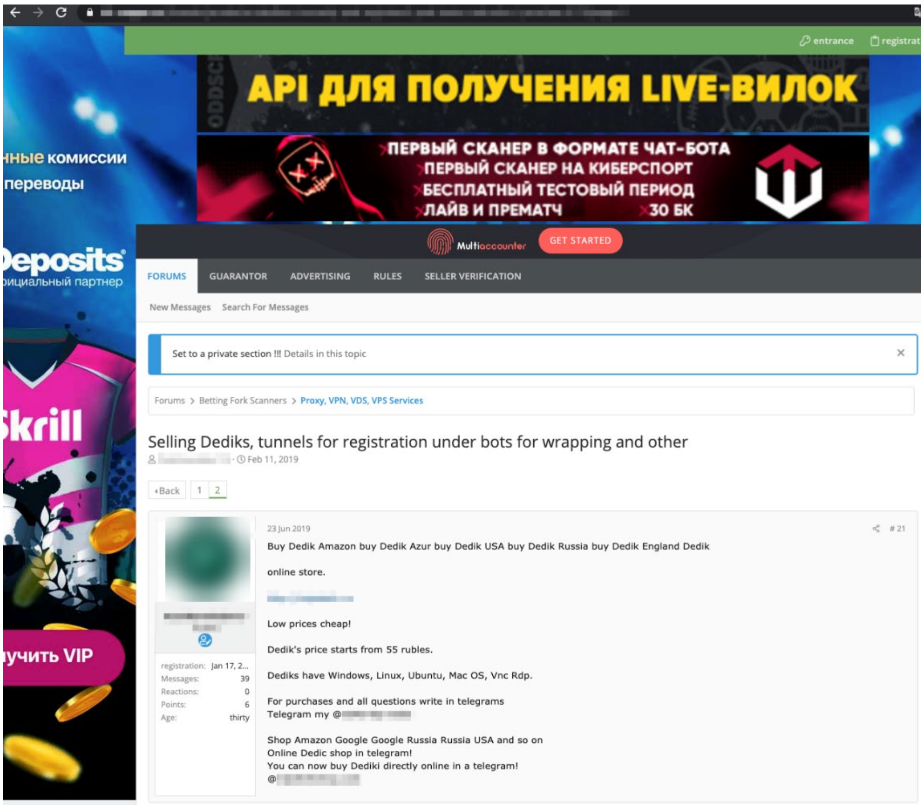
- To protect availability
- To maintain anonymity
- To prevent forensics or make forensic analysis difficult
- To obscure physical location
- To obscure jurisdiction
- To make IP spoofing possible
- To bypass internet restrictions

Underground Hosting: A Criminal Market Overview

Platforms Offering Underground Hosting

Multiple platforms offer information on how to buy hosting services — the most fundamental and important piece of infrastructure for criminal attackers. These platforms commonly cover offerings and prices for bulletproof hosting. The same platforms often have advertisements of proxies for sale and offerings of VPS and VPN. It comes as no surprise that criminal hackers widely use such services. Often, we can also observe shops dedicated to selling such services.

Another interesting fact is that the sale of such services could also be observed on forums related to online betting, search engine optimization (SEO), and online marketing. Proxies and services are widely used in those fields for the production of clicks to influence the behavior of a search engine or other purposes.



Set to a private section !!! Details in this topic

Selling Dediks, tunnels for registration under bots for wrapping and other

[redacted] · Feb 11, 2019

[redacted]

registration: Jan 17, 2...
Messages: 39
Reactions: 0
Points: 6
Age: thirty

23 Jun 2019

Buy Dedik Amazon buy Dedik Azur buy Dedik USA buy Dedik Russia buy Dedik England Dedik

online store.

[redacted]

Low prices cheap!

Dedik's price starts from 55 rubles.

Dediks have Windows, Linux, Ubuntu, Mac OS, Vnc Rdp.

For purchases and all questions write in telegrams
Telegram my @[redacted]

Shop Amazon Google Google Russia Russia USA and so on
Online Dedic shop in telegram!
You can now buy Dediki directly online in a telegram!
@[redacted]

Figure 1. An online shop that sells dedicated hosting servers

We can also observe the promotion of these services on social networks such as VK, as well as dedicated groups on online messenger platforms, such as Telegram and WhatsApp. We often observe the same actors advertising their services on both underground forums and online messenger chat groups. We can link those together because the threat actors use the same contact information.

One common perception is that all of the discussion takes place on the deep web or dark web. Those terms often cause a lot of confusion. The term “deep web” refers to any internet content not indexed by search engines (e.g., a private section of a forum, private social media posts). “Dark web” refers to the section of the internet that is only accessible via specific, additional software or means such as Tor (The Onion Router). Contrary to popular opinion, the criminal forums we describe here predominantly exist on the clear or surface web. We have previously written extensively on the dark web.[3, 4]

In general, there are three main levels of maturity in underground platforms:

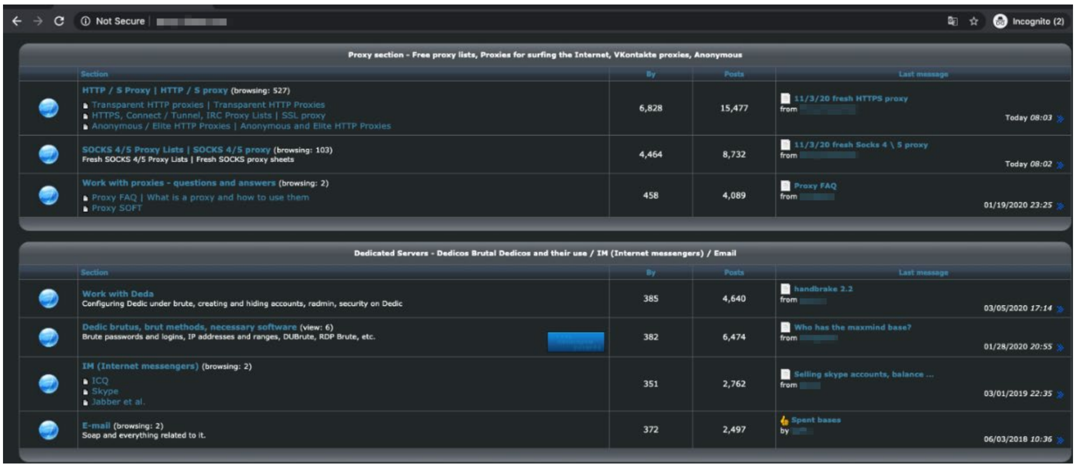
- Those that are open for users to join; these platforms have lower maturity in actors but have a larger volume of posts with content that are generally easy for anyone to read.
- Those that are publicly online, but are not available for free signup. Users would need to be vouched in some way, have some form of reference code, or pay for access. The main pages of these sites can be found, but not their content. These have medium to high maturity in criminal actors.
- Those that are private, invite-only for accessing platforms, shared in very limited and very trusted criminal communities. These generally have the highest maturity level in actors.

The following sections give an overview of the underground market offers and demands of hosting services. These sections include coverage of activity on online forums, dedicated shops, official reselling sites, online messengers, and media platforms.

Forums

Hosting and VPNs are hot topics in underground forums. Many of these forums have dedicated sections for buying and selling hosting services. These sections often have hundreds of topics.

In many cases, we observed threads promoting and advertising dedicated shops or Telegram channels and bots. The screenshot below shows one such forum, which has a hosting section that contains over 10,000 topics and 25,000 posts related to proxies and VPNs. It also contains over 1,000 topics and 15,000 posts related to hosting and dedicated servers.



Not Secure | [redacted]

Incognito (2)

Proxy section - Free proxy lists, Proxies for surfing the Internet, VKontakte proxies, Anonymous

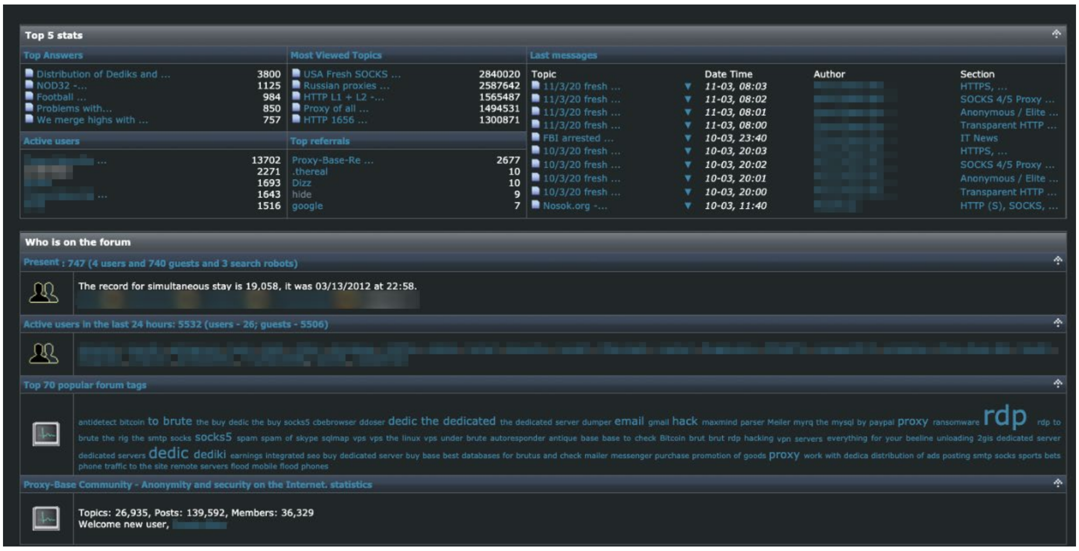
Section	By	Posts	Last message
HTTP / S Proxy | HTTP / S proxy (browsing: 527) Transparent HTTP proxies | Transparent HTTP Proxies HTTPS, Connect / Tunnel, IRC Proxy Lists | SSL proxy Anonymous / Elite HTTP Proxies | Anonymous and Elite HTTP Proxies	6,828	15,477	11/3/20 fresh HTTPS proxy from [redacted] Today *08:03*
SOCKS 4/5 Proxy Lists | SOCKS 4/5 proxy (browsing: 103) Fresh SOCKS 4/5 Proxy Lists | Fresh SOCKS proxy sheets	4,464	8,732	11/3/20 fresh Socks 4 \ 5 proxy from [redacted] Today *08:02*
Work with proxies - questions and answers (browsing: 2) Proxy FAQ | What is a proxy and how to use them Proxy SOFT	458	4,089	Proxy FAQ from [redacted] 01/19/2020 *23:25*

Dedicated Servers - Dedicos Brutal Dedicos and their use / IM (Internet messengers) / Email

Section	By	Posts	Last message
Work with Deda Configuring Dedic under brute, creating and hiding accounts, radmin, security on Dedic	385	4,640	handbrake 2.2 from [redacted] 03/05/2020 *17:14*
Dedic brutus, brut methods, necessary software (view: 6) Brute passwords and logins, IP addresses and ranges, DUBrute, RDP Brute, etc.	382	6,474	Who has the maxmind base? from [redacted] 01/28/2020 *20:55*
IM (Internet messengers) (browsing: 2) ICQ Skype Jabber et al.	351	2,762	Selling skype accounts, balance ... from [redacted] 03/01/2019 *22:35*
E-mail (browsing: 2) Soap and everything related to it.	372	2,497	Spent bases by [redacted] 06/03/2018 *10:36*

Figure 2. Underground forum sections related to hosting and VPNs

The statistics section of the same forum is very interesting. We observed that some topics were viewed over a million times. Popular topics include the sale of well-known malware-as-a-service tools, but some of the most discussed topics are related to law enforcement action against forum users. For example, the following screenshot shows a very popular thread related to recent FBI arrests.



Top 5 stats

Top Answers	
Distribution of Dediks and ...	3800
NOD32 -...	1125
Football ...	984
Problems with...	850
We merge highs with ...	757

Most Viewed Topics	
USA Fresh SOCKS ...	2840020
Russian proxies ...	2587642
HTTP L1 + L2 -...	1565487
Proxy of all ...	1494531
HTTP 1656 ...	1300871

Active users	
[redacted] ...	13702
[redacted]	2271
[redacted]	1693
[redacted] ...	1643
[redacted]	1516

Top referrals	
Proxy-Base-Re ...	2677
.thereal	10
Dizz	10
hide	9
google	7

Last messages

Topic		Date Time	Author	Section
11/3/20 fresh ...	▼	*11-03, 08:03*	[redacted]	HTTPS, ...
11/3/20 fresh ...	▼	*11-03, 08:02*	[redacted]	SOCKS 4/5 Proxy ...
11/3/20 fresh ...	▼	*11-03, 08:01*	[redacted]	Anonymous / Elite ...
11/3/20 fresh ...	▼	*11-03, 08:00*	[redacted]	Transparent HTTP ...
FBI arrested ...	▼	*10-03, 23:40*	[redacted]	IT News
10/3/20 fresh ...	▼	*10-03, 20:03*	[redacted]	HTTPS, ...
10/3/20 fresh ...	▼	*10-03, 20:02*	[redacted]	SOCKS 4/5 Proxy ...
10/3/20 fresh ...	▼	*10-03, 20:01*	[redacted]	Anonymous / Elite ...
10/3/20 fresh ...	▼	*10-03, 20:00*	[redacted]	Transparent HTTP ...
Nosok.org -...	▼	*10-03, 11:40*	[redacted]	HTTP (S), SOCKS, ...

Who is on the forum

Present : 747 (4 users and 740 guests and 3 search robots)

The record for simultaneous stay is 19,058, it was 03/13/2012 at 22:58.
[redacted]

Active users in the last 24 hours: 5532 (users - 26; guests - 5506)

[redacted]

Top 70 popular forum tags

antidetect bitcoin to brute the buy dedic the buy socks5 cbebrowser ddoser dedic the dedicated the dedicated server dumper email gmail hack maxmind parser Meiler myrq the mysql by paypal proxy ransomware rdp rdp to brute the rig the smtp socks socks5 spam spam of skype sqlmap vps vps the linux vps under brute autoresponder antique base base to check Bitcoin brut brut rdp hacking vpn servers everything for your beeline unloading 2gis dedicated server dedicated servers dedic dediki earnings integrated seo buy dedicated server buy base best databases for brutus and check mailer messenger purchase promotion of goods proxy work with dedica distribution of ads posting smtp socks sports bets phone traffic to the site remote servers flood mobile flood phones

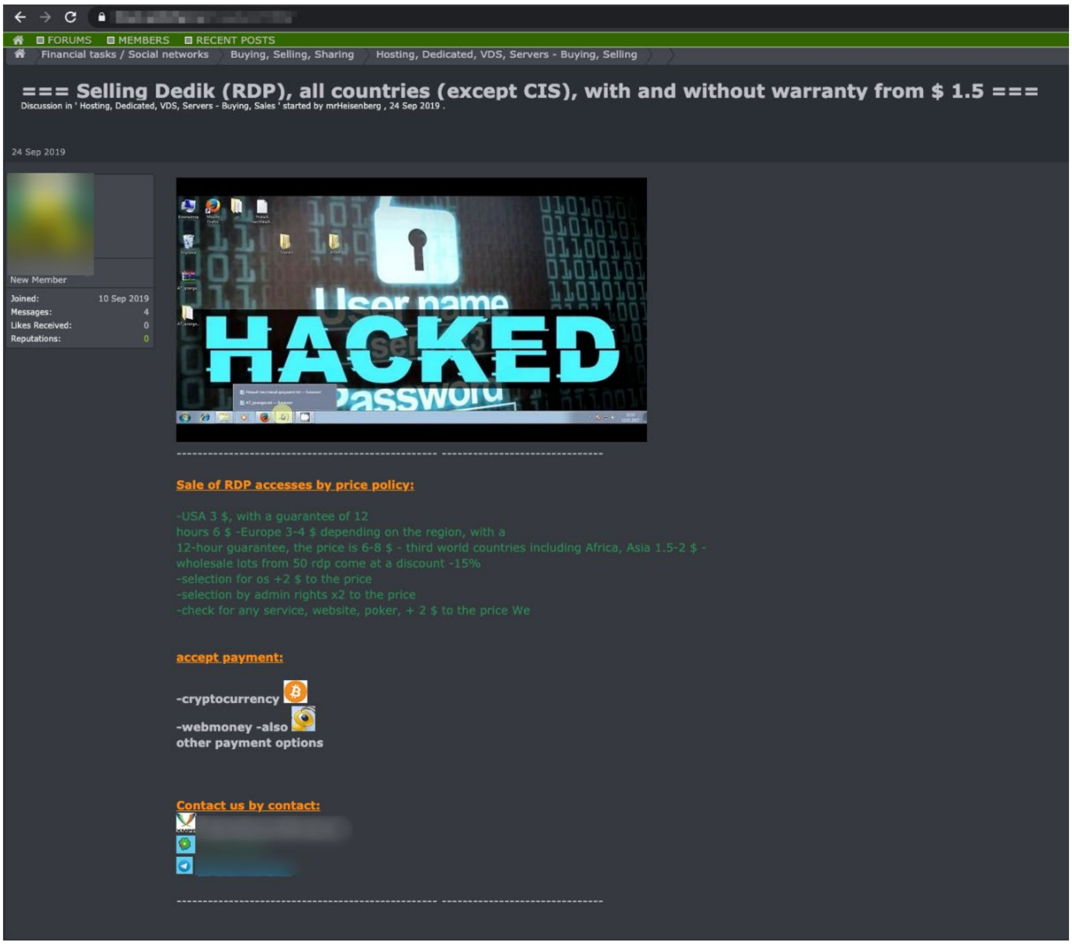
Proxy-Base Community - Anonymity and security on the Internet. statistics

Topics: 26,935, Posts: 139,592, Members: 36,329
Welcome new user, [redacted]

Figure 3. Statistics and prevalent tags at a hosting forum

Many of the advertisements on those forums provide the seller's contact information. Sellers often use communication methods that provide some anonymity, such as Jabber or Telegram. QQ, while being a relatively old service, is still being used as well.

Below is another example of an advertisement for dedicated servers with remote desktop protocol (RDP) access (located across the world, except the Commonwealth of Independent States area). The prices in this advertisement for US-based hosts start from US$3. The cheapest servers come without a guarantee of further availability. The higher-priced hosts, which start at US$6, come with an additional guarantee of availability for the next 12 hours. The seller provides a 15% discount for buyers who purchase more than 50 hosts. This gives an idea of the volume of sales we regularly see on criminal forums, as well as the marketing savvy of the sellers involved.



[redacted]

FORUMS
MEMBERS
RECENT POSTS
Financial tasks / Social networks
Buying, Selling, Sharing
Hosting, Dedicated, VDS, Servers - Buying, Selling

=== Selling Dedik (RDP), all countries (except CIS), with and without warranty from $ 1.5 ===

Discussion in ' Hosting, Dedicated, VDS, Servers - Buying, Sales ' started by mrHeisenberg , 24 Sep 2019 .

24 Sep 2019

New Member

Joined: 10 Sep 2019
Messages: 4
Likes Received: 0
Reputations: 0

User name
HACKED
Password

--- ----------------------------

Sale of RDP accesses by price policy:

-USA 3 $, with a guarantee of 12
hours 6 $ -Europe 3-4 $ depending on the region, with a
12-hour guarantee, the price is 6-8 $ - third world countries including Africa, Asia 1.5-2 $ -
wholesale lots from 50 rdp come at a discount -15%
-selection for os +2 $ to the price
-selection by admin rights x2 to the price
-check for any service, website, poker, + 2 $ to the price We

accept payment:

-cryptocurrency
-webmoney -also
other payment options

Contact us by contact:

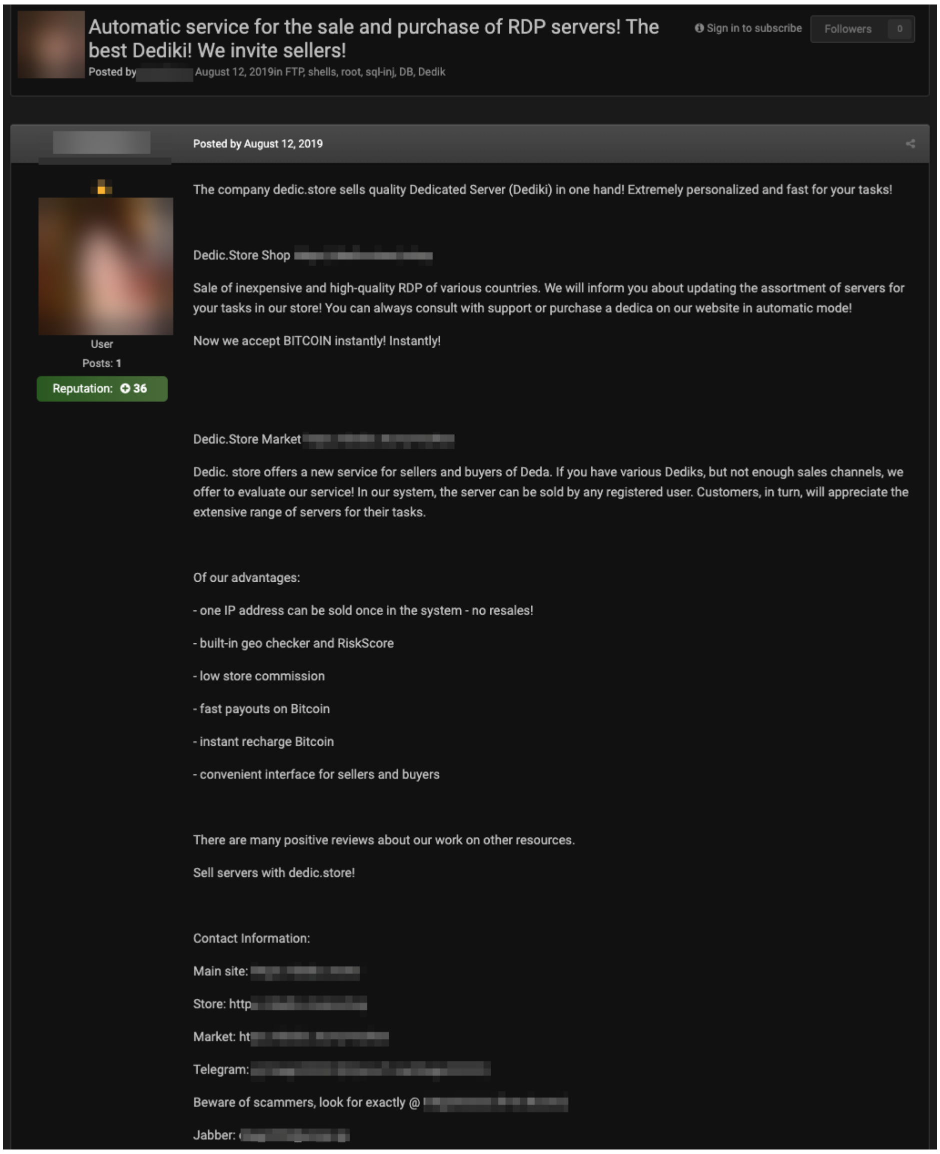
[redacted]

--- ----------------------------

Figure 4. An advertisement for compromised hosts in an underground forum

Dedicated shops and custom platforms are often advertised in underground forums. The posts often provide some brief information on available items, along with a URL of the shop, seller contact information, and supported means of payment.

In the screenshot below, the seller is advertising a platform for both buyers and sellers of RDP servers. This platform supports instant bitcoin payments.



Automatic service for the sale and purchase of RDP servers! The best Dediki! We invite sellers!

Posted by [redacted] August 12, 2019in FTP, shells, root, sql-inj, DB, Dedik

Posted by August 12, 2019

The company dedic.store sells quality Dedicated Server (Dediki) in one hand! Extremely personalized and fast for your tasks!

Dedic.Store Shop [redacted]

Sale of inexpensive and high-quality RDP of various countries. We will inform you about updating the assortment of servers for your tasks in our store! You can always consult with support or purchase a dedica on our website in automatic mode!

Now we accept BITCOIN instantly! Instantly!

Dedic.Store Market [redacted]

Dedic. store offers a new service for sellers and buyers of Deda. If you have various Dediks, but not enough sales channels, we offer to evaluate our service! In our system, the server can be sold by any registered user. Customers, in turn, will appreciate the extensive range of servers for their tasks.

Of our advantages:

- one IP address can be sold once in the system - no resales!
- built-in geo checker and RiskScore
- low store commission
- fast payouts on Bitcoin
- instant recharge Bitcoin
- convenient interface for sellers and buyers

There are many positive reviews about our work on other resources.

Sell servers with dedic.store!

Contact Information:

Main site: [redacted]

Store: http[redacted]

Market: ht[redacted]

Telegram: [redacted]

Beware of scammers, look for exactly @ [redacted]

Jabber: [redacted]

Figure 5. An advertisement for automatic platforms for sellers and buyers of dedicated servers

Dedicated Shops

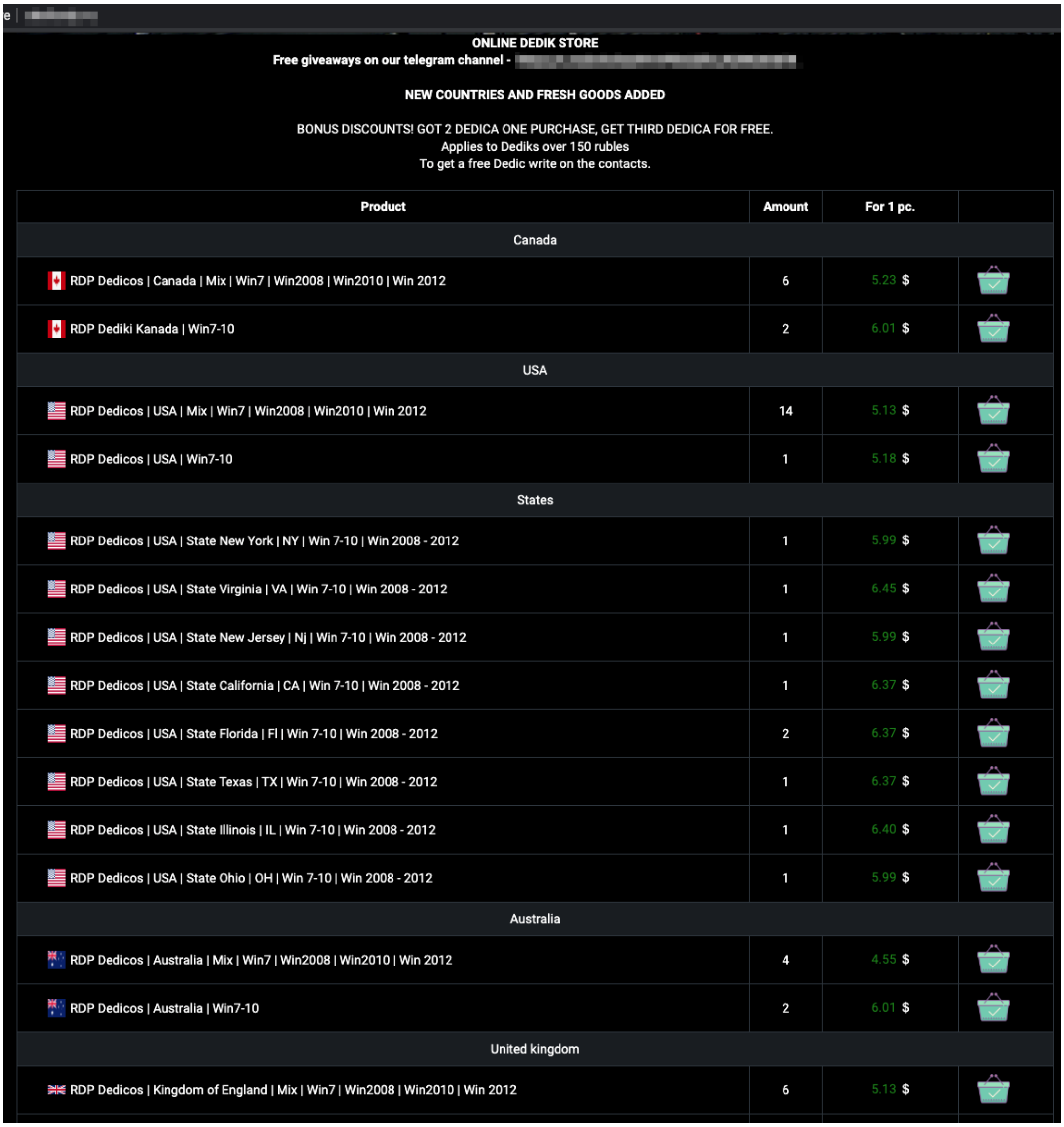
Hosting services are not only sold through forum threads and discussions. We often saw professional, dedicated shops advertising similar services. These shops are an important part of the underground hosting ecosystem.

Through our research, we have identified several types of shops that can be seen on the market.

First are the universal shops, which offer different assets. They could be selling credit card dumps and skimmers and would have a section related to underground hosting. This section offers a variety of services, including dedicated servers, VPS, SOCKS proxies, VPNs, and sometimes even DDoS protection services. Definitions of each of these services can be found in the appendix, but their inner workings will be explored in-depth later in this series.

Other shops focus mainly on a particular topic, for example, selling dedicated servers with RDP or virtual network computing (VNC) access.

Offers in these shops are often categorized by several criteria, such as country/location, hardware properties, network capabilities, and available access type.



e | [redacted]

ONLINE DEDIK STORE
Free giveaways on our telegram channel - [redacted]

NEW COUNTRIES AND FRESH GOODS ADDED

BONUS DISCOUNTS! GOT 2 DEDICA ONE PURCHASE, GET THIRD DEDICA FOR FREE.
Applies to Dediks over 150 rubles
To get a free Dedic write on the contacts.

Product	Amount	For 1 pc.	
Canada			
🇨🇦 RDP Dedicos | Canada | Mix | Win7 | Win2008 | Win2010 | Win 2012	6	5.23 $	🛒
🇨🇦 RDP Dediki Kanada | Win7-10	2	6.01 $	🛒
USA			
🇺🇸 RDP Dedicos | USA | Mix | Win7 | Win2008 | Win2010 | Win 2012	14	5.13 $	🛒
🇺🇸 RDP Dedicos | USA | Win7-10	1	5.18 $	🛒
States			
🇺🇸 RDP Dedicos | USA | State New York | NY | Win 7-10 | Win 2008 - 2012	1	5.99 $	🛒
🇺🇸 RDP Dedicos | USA | State Virginia | VA | Win 7-10 | Win 2008 - 2012	1	6.45 $	🛒
🇺🇸 RDP Dedicos | USA | State New Jersey | Nj | Win 7-10 | Win 2008 - 2012	1	5.99 $	🛒
🇺🇸 RDP Dedicos | USA | State California | CA | Win 7-10 | Win 2008 - 2012	1	6.37 $	🛒
🇺🇸 RDP Dedicos | USA | State Florida | Fl | Win 7-10 | Win 2008 - 2012	2	6.37 $	🛒
🇺🇸 RDP Dedicos | USA | State Texas | TX | Win 7-10 | Win 2008 - 2012	1	6.37 $	🛒
🇺🇸 RDP Dedicos | USA | State Illinois | IL | Win 7-10 | Win 2008 - 2012	1	6.40 $	🛒
🇺🇸 RDP Dedicos | USA | State Ohio | OH | Win 7-10 | Win 2008 - 2012	1	5.99 $	🛒
Australia			
🇦🇺 RDP Dedicos | Australia | Mix | Win7 | Win2008 | Win2010 | Win 2012	4	4.55 $	🛒
🇦🇺 RDP Dedicos | Australia | Win7-10	2	6.01 $	🛒
United kingdom			
🇬🇧 RDP Dedicos | Kingdom of England | Mix | Win7 | Win2008 | Win2010 | Win 2012	6	5.13 $	🛒

Figure 6. A dedicated server shop offering configurations and prices of sold assets

Shops accept different payment methods such as payment via credit card, Qiwi, WebMoney, and Bitcoin. Credit cards are accepted because criminals have the ability to maintain anonymity by monetizing stolen credit cards.

Official Resellers

When people think about criminal infrastructure providers, they likely think of purely criminal outfits that offer their servers and other infrastructure solely to a criminal clientele. In this thinking model, there are criminal infrastructure providers for cybercriminals. On the other side, there are the more household name infrastructure providers that help host all the other legitimate websites we interact with every day.

So one may find it strange that we link “official resellers” of such legitimate hosting providers with the criminal underground hosting market. However, we identified several official resellers of these more public hosting services, which also advertise in underground forums directly. These are hosting providers that have a legitimate clientele and advertise openly on the internet.

Several of their resellers sell exclusively to the criminal underground, either with or without the company’s knowledge. This should not be surprising; after all, some of these well-known hosting companies provide excellent services that criminals, just like their actual target clientele, would want to use.

As part of this trend, we have seen underground threat actors sharing their reference links from these hosting providers and earning referral money from the community. Hosts are often discussed, liked, and advertised by criminal actors in terms of their abuse-handling (or non-handling) policies and anonymity. Hostings with a high level of anonymity are also extremely popular among underground threat actors.

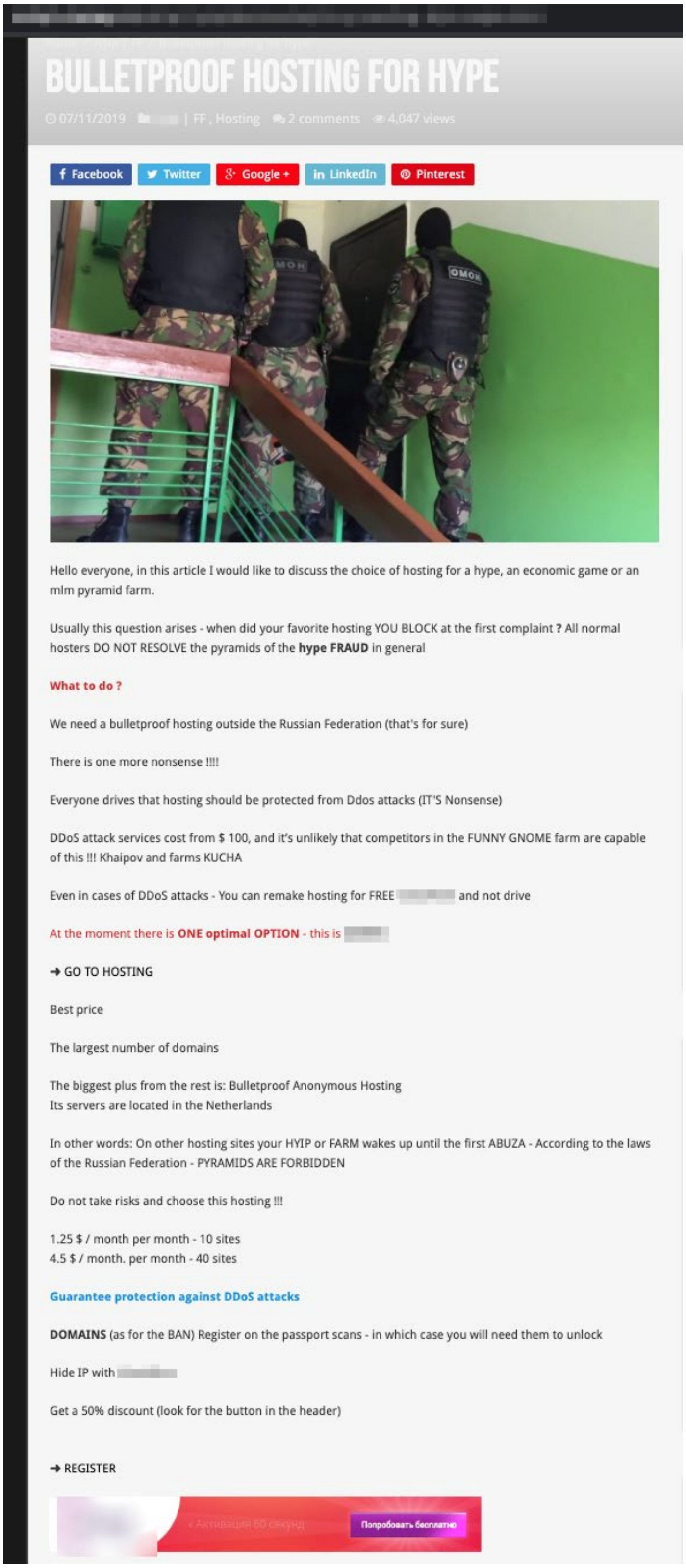
For example, free hosting providers and DNS providers that accept anonymous means of payment, such as bitcoin, are frequently used. The following sections show some of the advertisements of known official hosting providers found in underground forums.

Advertised as Bulletproof

Bulletproof hosting services are often advertised in the underground. The term “bulletproof” refers to several categories of hosting providers, including those who deliberately ignore and abuse legal requests, those who exist in countries with lax cybercrime laws, or even legitimate services with poor abuse-handling records. If you are running a cybercrime business, you need a hosting provider that will allow you to conduct cybercrime from their servers, or at least be slow to stop you when you do.

Most bulletproof hosts exist in a sort of gray market, as opposed to fully “black.” They are generally normal hosting providers that are trying to diversify their business to cater to customer needs to the absolute limit of what the law allows (and prosecutes) in their location, at a more premium price. Very few bulletproof providers attempt to truly allow any sort of content to survive for a long period. While they can charge even more for their services, historically, we have seen these providers have a short life span before they are shut down by successful law enforcement actions.

Some hosting providers try to fulfill both bulletproof and normal hosting markets. The screenshot below shows a company advertising bulletproof services:



[redacted]

BULLETPROOF HOSTING FOR HYPE

07/11/2019 [redacted] | FF , Hosting 2 comments 4,047 views

Hello everyone, in this article I would like to discuss the choice of hosting for a hype, an economic game or an mlm pyramid farm.

Usually this question arises - when did your favorite hosting YOU BLOCK at the first complaint ? All normal hosters DO NOT RESOLVE the pyramids of the **hype FRAUD** in general

What to do ?

We need a bulletproof hosting outside the Russian Federation (that's for sure)

There is one more nonsense !!!!

Everyone drives that hosting should be protected from Ddos attacks (IT'S Nonsense)

DDoS attack services cost from $ 100, and it's unlikely that competitors in the FUNNY GNOME farm are capable of this !!! Khaipov and farms KUCHA

Even in cases of DDoS attacks - You can remake hosting for FREE [redacted] and not drive

At the moment there is **ONE optimal OPTION** - this is [redacted]

➜ GO TO HOSTING

Best price

The largest number of domains

The biggest plus from the rest is: Bulletproof Anonymous Hosting
Its servers are located in the Netherlands

In other words: On other hosting sites your HYIP or FARM wakes up until the first ABUZA - According to the laws of the Russian Federation - PYRAMIDS ARE FORBIDDEN

Do not take risks and choose this hosting !!!

1.25 $ / month per month - 10 sites
4.5 $ / month. per month - 40 sites

Guarantee protection against DDoS attacks

DOMAINS (as for the BAN) Register on the passport scans - in which case you will need them to unlock

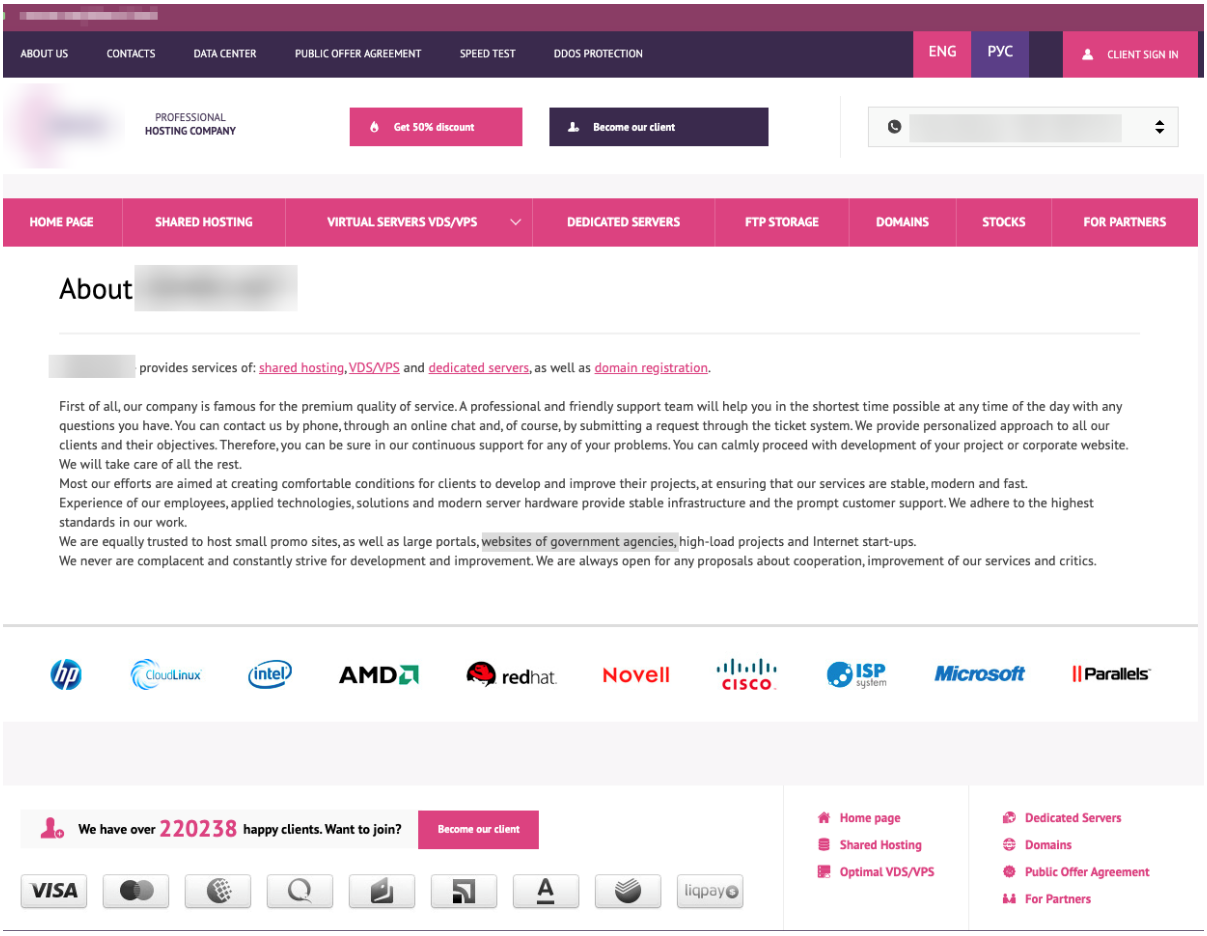
Hide IP with [redacted]

Get a 50% discount (look for the button in the header)

➜ REGISTER

Figure 7. An advertisement for a bulletproof hosting service provider

On the official site of the same company, we can see that it claims to provide hosting services for the websites of government agencies (as seen in the screenshot below). It is unusual to see something like it on the clear web; the company is trying to sound as legitimate as possible, leveraging on the perceived trustworthiness of working with governments. However, the same company markets its service in criminal forums based on their resistance to abuse requests.



About [redacted]

[redacted] provides services of: shared hosting, VDS/VPS and dedicated servers, as well as domain registration.

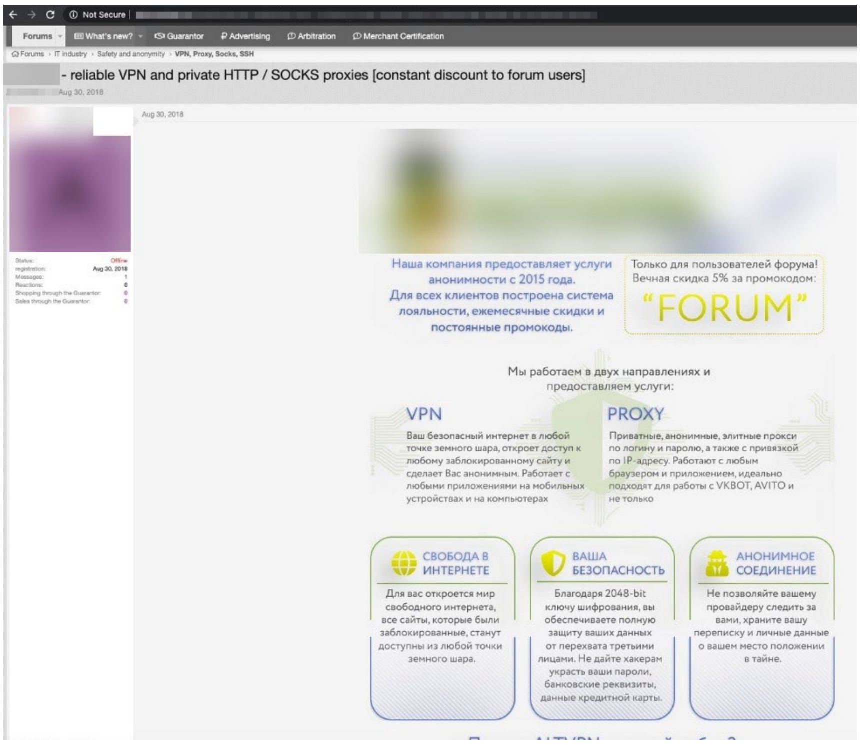
First of all, our company is famous for the premium quality of service. A professional and friendly support team will help you in the shortest time possible at any time of the day with any questions you have. You can contact us by phone, through an online chat and, of course, by submitting a request through the ticket system. We provide personalized approach to all our clients and their objectives. Therefore, you can be sure in our continuous support for any of your problems. You can calmly proceed with development of your project or corporate website. We will take care of all the rest.
Most our efforts are aimed at creating comfortable conditions for clients to develop and improve their projects, at ensuring that our services are stable, modern and fast.
Experience of our employees, applied technologies, solutions and modern server hardware provide stable infrastructure and the prompt customer support. We adhere to the highest standards in our work.
We are equally trusted to host small promo sites, as well as large portals, websites of government agencies, high-load projects and Internet start-ups.
We never are complacent and constantly strive for development and improvement. We are always open for any proposals about cooperation, improvement of our services and critics.

Figure 8. The same company provides hosting services for the websites of government agencies

Advertised as Anonymizers

VPNs and anonymizers are also easily found in underground forums. Such services allow criminals to hide their true location on the internet, which makes law enforcement investigation of their activities more difficult. They are also useful when looking to fool anti-fraud systems that expect compromised customers to access services from specific locations, such as the town they live in. Criminals favor VPN providers that are advertised as “no log,” meaning they claim not to keep any activity logs that law enforcement could request in the future.

The advertisers of these often sell compromised accounts and registration codes for well-known providers, purchased by stolen credit cards, gift cards, or other methods. In some cases, we witnessed that these “well-known” services directly advertised in underground forums. An example of a VPN service advertising directly is provided in the screenshot below.



[redacted] - reliable VPN and private HTTP / SOCKS proxies [constant discount to forum users]

Aug 30, 2018

Status: Offline
registration: Aug 30, 2018
Messages: 1
Reactions: 0
Shopping through the Guarantor: 0
Sales through the Guarantor: 0

Aug 30, 2018

Наша компания предоставляет услуги анонимности с 2015 года.
Для всех клиентов построена система лояльности, ежемесячные скидки и постоянные промокоды.

Только для пользователей форума!
Вечная скидка 5% за промокодом:
“FORUM”

Мы работаем в двух направлениях и предоставляем услуги:

VPN
Ваш безопасный интернет в любой точке земного шара, откроет доступ к любому заблокированному сайту и сделает Вас анонимным. Работает с любыми приложениями на мобильных устройствах и на компьютерах

PROXY
Приватные, анонимные, элитные прокси по логину и паролю, а также с привязкой по IP-адресу. Работают с любым браузером и приложением, идеально подходят для работы с VKBOT, AVITO и не только

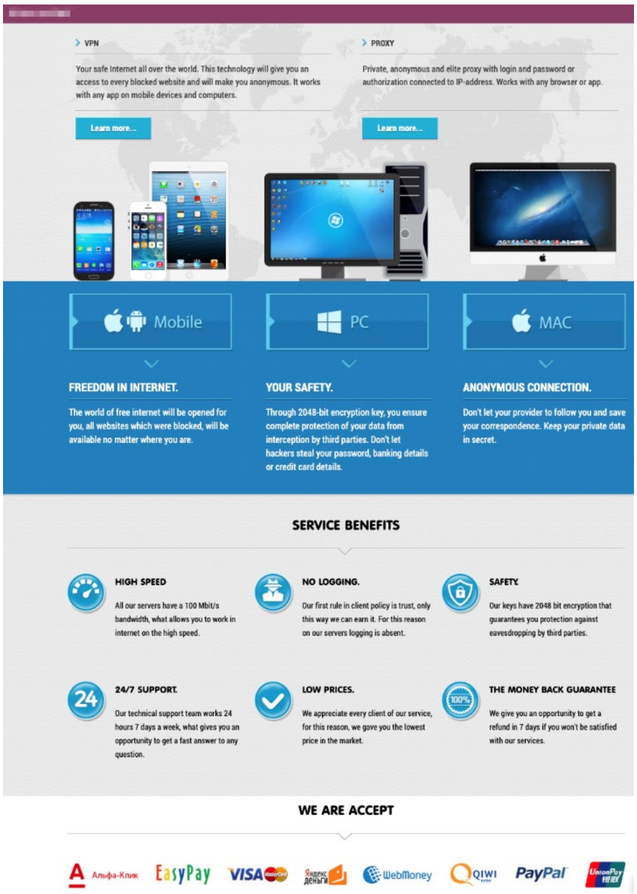
СВОБОДА В ИНТЕРНЕТЕ
Для вас откроется мир свободного интернета, все сайты, которые были заблокированные, станут доступны из любой точки земного шара.

ВАША БЕЗОПАСНОСТЬ
Благодаря 2048-bit ключу шифрования, вы обеспечиваете полную защиту ваших данных от перехвата третьими лицами. Не дайте хакерам украсть ваши пароли, банковские реквизиты, данные кредитной карты.

АНОНИМНОЕ СОЕДИНЕНИЕ
Не позволяйте вашему провайдеру следить за вами, храните вашу переписку и личные данные о вашем место положении в тайне.

Figure 9. An advertisement of a “well-known” VPN service in an underground forum

This VPN provider has a website available in several languages, including English, Ukrainian, and Russian. It accepts conventional means of payment, such as PayPal, Visa, and Mastercard.



[redacted]

VPN

Your safe Internet all over the world. This technology will give you an access to every blocked website and will make you anonymous. It works with any app on mobile devices and computers.

PROXY

Private, anonymous and elite proxy with login and password or authorization connected to IP-address. Works with any browser or app.

FREEDOM IN INTERNET.

The world of free internet will be opened for you, all websites which were blocked, will be available no matter where you are.

YOUR SAFETY.

Through 2048-bit encryption key, you ensure complete protection of your data from interception by third parties. Don't let hackers steal your password, banking details or credit card details.

ANONYMOUS CONNECTION.

Don't let your provider to follow you and save your correspondence. Keep your private data in secret.

SERVICE BENEFITS

HIGH SPEED

All our servers have a 100 Mbit/s bandwidth, what allows you to work in internet on the high speed.

NO LOGGING.

Our first rule in client policy is trust, only this way we can earn it. For this reason on our servers logging is absent.

SAFETY.

Our keys have 2048 bit encryption that guarantees you protection against eavesdropping by third parties.

24/7 SUPPORT.

Our technical support team works 24 hours 7 days a week, what gives you an opportunity to get a fast answer to any question.

LOW PRICES.

We appreciate every client of our service, for this reason, we gave you the lowest price in the market.

THE MONEY BACK GUARANTEE

We give you an opportunity to get a refund in 7 days if you won't be satisfied with our services.

WE ARE ACCEPT

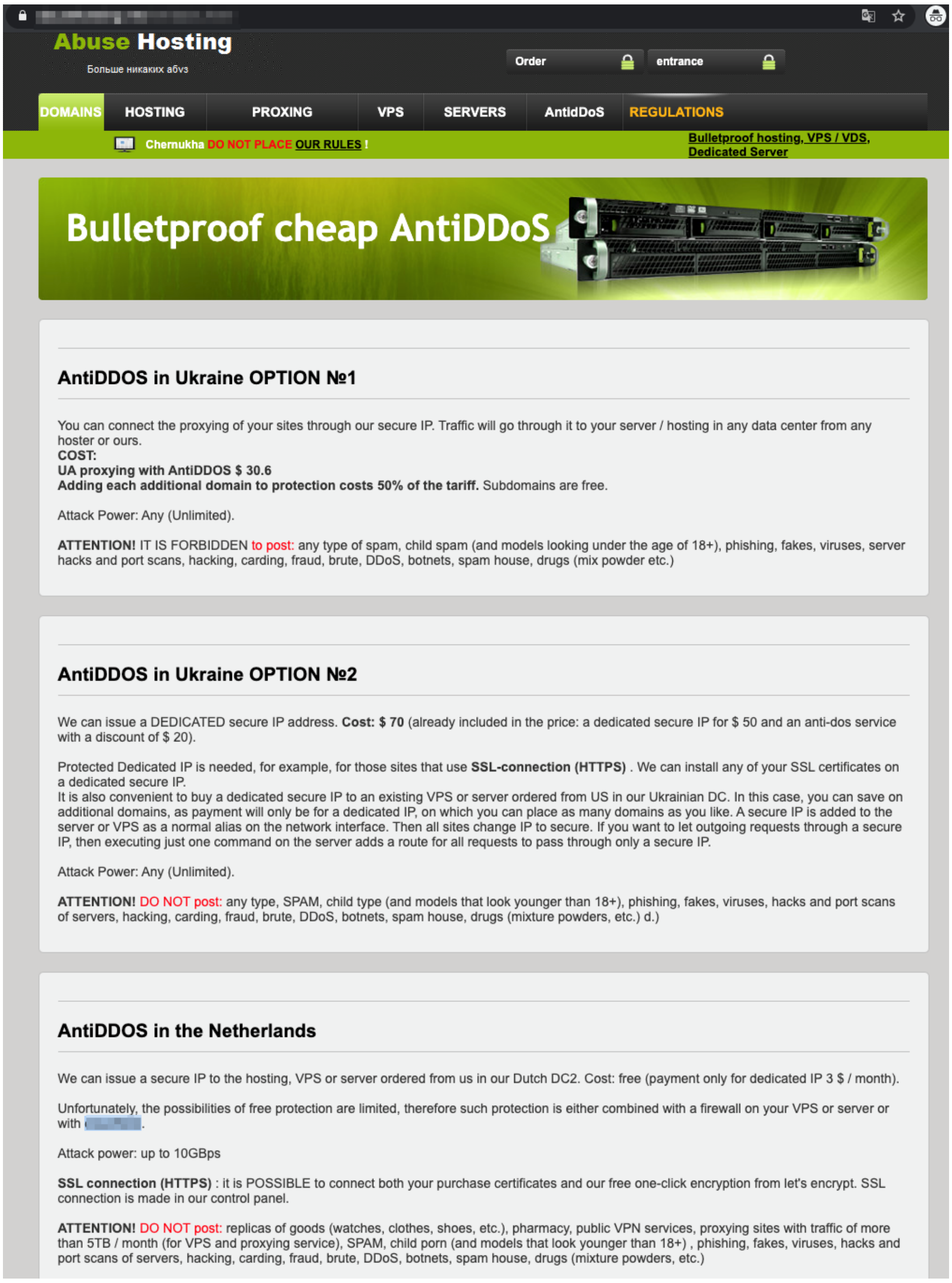
Figure 10. Website of a VPN provider that advertises its services in underground sites

Advertised as DDoS Protection Service, a Part of Bulletproof Hosting Services

When people think of DDoS, armies of compromised machines being taken advantage of by an attacker usually come to mind. Attackers extort resources from innocent victims' websites, which could be especially damaging to e-commerce businesses. One could expect that it is these victims that would require DDoS protection and not attackers themselves. However, there is no honor among thieves, and in some cases, criminals will use DDoS as a tool against their competitors to gain an advantage. This is why certain criminals find themselves in need of the same services.

The number of organizations and brand names in the DDoS protection business is much lower compared with hosting services. It is not the easiest business to operate (nor is it inexpensive), requiring the ability to handle massive fluctuations in bandwidth usage at a short notice.

It is unsurprising then that we were unable to find any advertisement of well-known, legitimate protection companies in underground forums. What we were able to find, however, is the use of such services by hosting providers that position themselves as bulletproof, often highlighted as a unique value proposition for their business. In the screenshot of the Anti-DDoS section of a bulletproof host below, we found that it uses one of the best-rated DDoS protection services.[5]



[redacted]

Abuse Hosting
Больше никаких абvз
Order
entrance
DOMAINS
HOSTING
PROXING
VPS
SERVERS
AntidDoS
REGULATIONS
Chernukha DO NOT PLACE OUR RULES !
Bulletproof hosting, VPS / VDS, Dedicated Server
Bulletproof cheap AntiDDoS

AntiDDOS in Ukraine OPTION №1

You can connect the proxying of your sites through our secure IP. Traffic will go through it to your server / hosting in any data center from any hoster or ours.
COST:
UA proxying with AntiDDOS $ 30.6
Adding each additional domain to protection costs 50% of the tariff. Subdomains are free.

Attack Power: Any (Unlimited).

ATTENTION! IT IS FORBIDDEN to post: any type of spam, child spam (and models looking under the age of 18+), phishing, fakes, viruses, server hacks and port scans, hacking, carding, fraud, brute, DDoS, botnets, spam house, drugs (mix powder etc.)

AntiDDOS in Ukraine OPTION №2

We can issue a DEDICATED secure IP address. **Cost: $ 70** (already included in the price: a dedicated secure IP for $ 50 and an anti-dos service with a discount of $ 20).

Protected Dedicated IP is needed, for example, for those sites that use **SSL-connection (HTTPS)** . We can install any of your SSL certificates on a dedicated secure IP.
It is also convenient to buy a dedicated secure IP to an existing VPS or server ordered from US in our Ukrainian DC. In this case, you can save on additional domains, as payment will only be for a dedicated IP, on which you can place as many domains as you like. A secure IP is added to the server or VPS as a normal alias on the network interface. Then all sites change IP to secure. If you want to let outgoing requests through a secure IP, then executing just one command on the server adds a route for all requests to pass through only a secure IP.

Attack Power: Any (Unlimited).

ATTENTION! DO NOT post: any type, SPAM, child type (and models that look younger than 18+), phishing, fakes, viruses, hacks and port scans of servers, hacking, carding, fraud, brute, DDoS, botnets, spam house, drugs (mixture powders, etc.) d.)

AntiDDOS in the Netherlands

We can issue a secure IP to the hosting, VPS or server ordered from us in our Dutch DC2. Cost: free (payment only for dedicated IP 3 $ / month).

Unfortunately, the possibilities of free protection are limited, therefore such protection is either combined with a firewall on your VPS or server or with [redacted].

Attack power: up to 10GBps

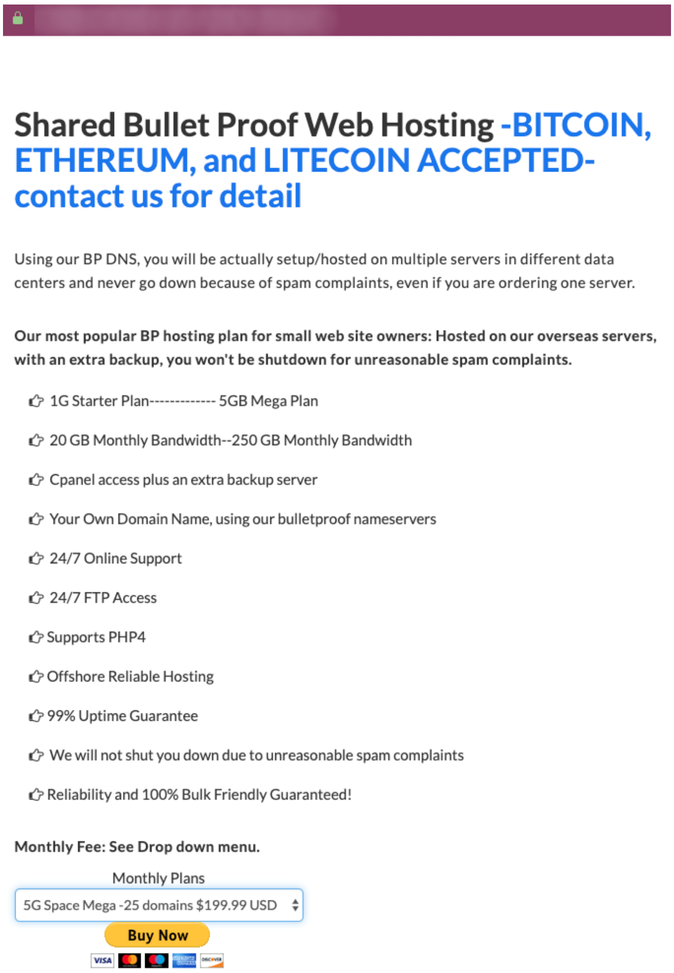
SSL connection (HTTPS) : it is POSSIBLE to connect both your purchase certificates and our free one-click encryption from let's encrypt. SSL connection is made in our control panel.

ATTENTION! DO NOT post: replicas of goods (watches, clothes, shoes, etc.), pharmacy, public VPN services, proxying sites with traffic of more than 5TB / month (for VPS and proxying service), SPAM, child porn (and models that look younger than 18+) , phishing, fakes, viruses, hacks and port scans of servers, hacking, carding, fraud, brute, DDoS, botnets, spam house, drugs (mixture powders, etc.)

Figure 11. A hosting advertised as bulletproof with DDoS protection from a well-known content delivery network (CDN)

Sale by Cryptocurrencies and Anonymous Payments

Many hostings that are advertised as bulletproof accept alternative means of payment. The most popular cryptocurrency used is Bitcoin, but it is possible to find many alternatives.



Shared Bullet Proof Web Hosting -BITCOIN, ETHEREUM, and LITECOIN ACCEPTED- contact us for detail

Using our BP DNS, you will be actually setup/hosted on multiple servers in different data centers and never go down because of spam complaints, even if you are ordering one server.

Our most popular BP hosting plan for small web site owners: Hosted on our overseas servers, with an extra backup, you won't be shutdown for unreasonable spam complaints.

☞ 1G Starter Plan------------ 5GB Mega Plan

☞ 20 GB Monthly Bandwidth--250 GB Monthly Bandwidth

☞ Cpanel access plus an extra backup server

☞ Your Own Domain Name, using our bulletproof nameservers

☞ 24/7 Online Support

☞ 24/7 FTP Access

☞ Supports PHP4

☞ Offshore Reliable Hosting

☞ 99% Uptime Guarantee

☞ We will not shut you down due to unreasonable spam complaints

☞ Reliability and 100% Bulk Friendly Guaranteed!

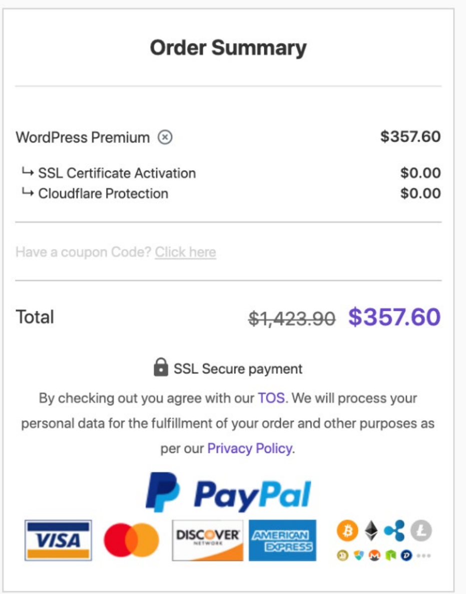
Monthly Fee: See Drop down menu.

Monthly Plans

5G Space Mega -25 domains $199.99 USD

Figure 12. A hosting accepting several cryptocurrencies

Hosting services that advertise as bulletproof aren’t the only ones that accept cryptocurrencies. Well-known hostings accept cryptocurrencies as a payment method. The screenshot below shows a known hosting provider accepting over half a dozen cryptocurrencies. The list of accepted coins includes Bitcoin, Ethereum, Ripple, Litecoin, and Monero.



Order Summary

WordPress Premium ⊗	$357.60
↳ SSL Certificate Activation	$0.00
↳ Cloudflare Protection	$0.00

Have a coupon Code? Click here

Total	~~$1,423.90~~ $357.60

SSL Secure payment

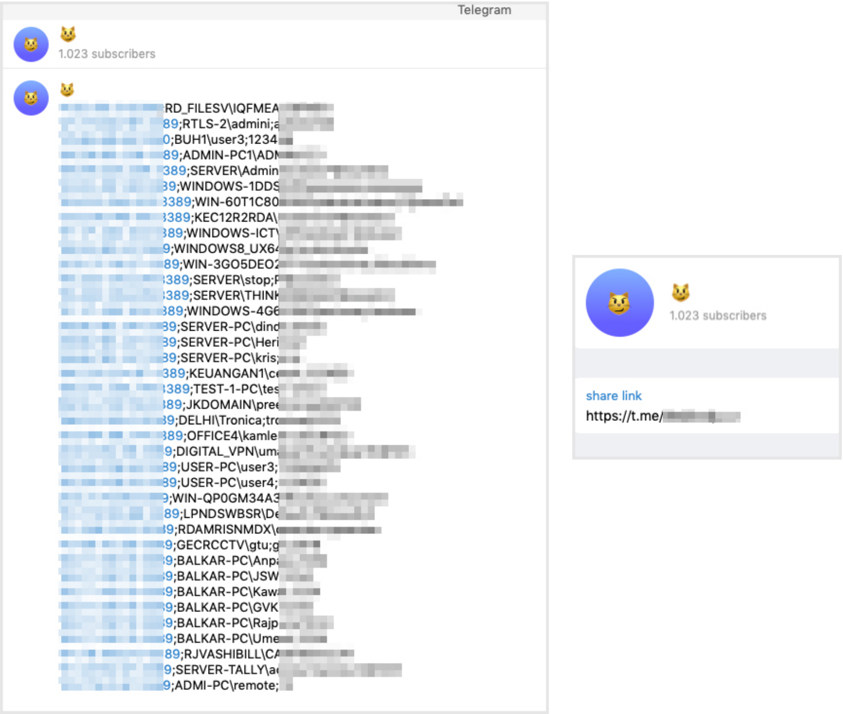
By checking out you agree with our TOS. We will process your personal data for the fulfillment of your order and other purposes as per our Privacy Policy.

Figure 13. Accepted means of payment

Messenger and Social Media Platforms

Telegram

There are several options for how underground actors use and abuse the Telegram chat platform. The most obvious use is providing Telegram as a point of contact in advertisements in underground forums. The second option is using Telegram as an advertising platform. The screenshot below is an example of a channel that exposes part of the details of a compromised asset for selling other hosts.

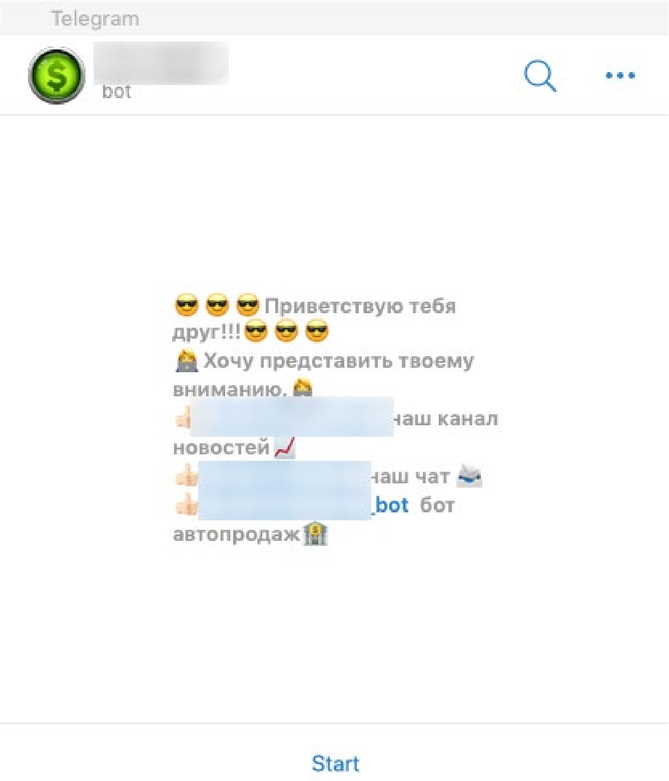


```
[redacted]
RD_FILESV\IQFMEA
89;RTLS-2\admini;a
0;BUH1\user3;1234
89;ADMIN-PC1\ADM
389;SERVER\Admin
39;WINDOWS-1DDS
3389;WIN-60T1C80
3389;KEC12R2RDA\
389;WINDOWS-ICT\
9;WINDOWS8_UX64
89;WIN-3GO5DEO2
3389;SERVER\stop;F
3389;SERVER\THINK
389;WINDOWS-4G6
39;SERVER-PC\dind
39;SERVER-PC\Heri
39;SERVER-PC\kris;
389;KEUANGAN1\ce
3389;TEST-1-PC\tes
389;JKDOMAIN\pree
39;DELHI\Tronica;tro
389;OFFICE4\kamle
9;DIGITAL_VPN\uma
39;USER-PC\user3;
39;USER-PC\user4;
9;WIN-QP0GM34A3
89;LPNDSWBSR\De
39;RDAMRISNMDX\c
9;GECRCCTV\gtu;g
9;BALKAR-PC\Anpa
9;BALKAR-PC\JSW
9;BALKAR-PC\Kaw
9;BALKAR-PC\GVK
9;BALKAR-PC\Rajp
9;BALKAR-PC\Ume
89;RJVASHIBILL\CA
9;SERVER-TALLY\ac
9;ADMI-PC\remote;
```

https://t.me/[redacted]

Figure 14. A Telegram channel that uses exposure of compromised assets to advertise their services

The third option is using Telegram for dedicated chats and bots, which are used to sell dedicated servers and other compromised assets.

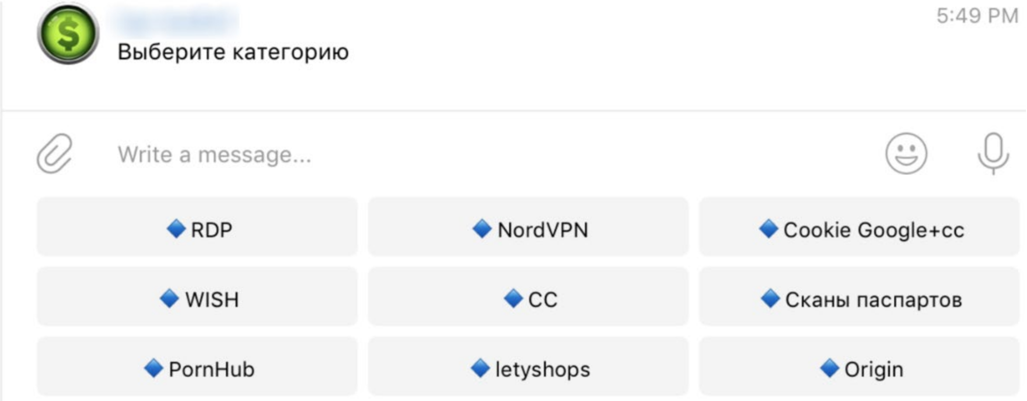


[redacted] bot

😎😎😎 Приветствую тебя друг!!!😎😎😎
🧑‍💻 Хочу представить твоему вниманию. 🧑‍💻
👍[redacted]наш канал новостей📈
👍[redacted]наш чат 📩
👍[redacted]bot бот автопродаж🏦

Figure 15. A Telegram bot used to sell dedicated servers

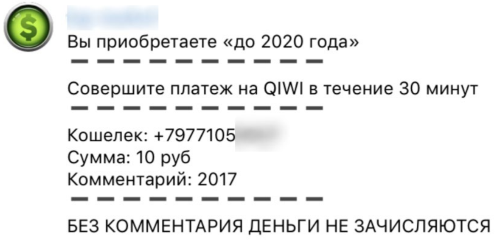
This bot offers several service categories that include cookies for Google accounts, hosts with RDP access, VPNs, and others.



[redacted] 5:49 PM
Выберите категорию

Figure 16. Categories sold by a Telegram bot

Once the category is selected, the bot provides payment information. Payment should be made using the Qiwi system to an account linked to a phone number and comment provided by the bot. In the screenshot below, we can see payment details for the VPN category. The payment of 10 Russian Rubles should be sent during the next 30 minutes to wallet ID:+7977710*****, with the comment ”2017”.

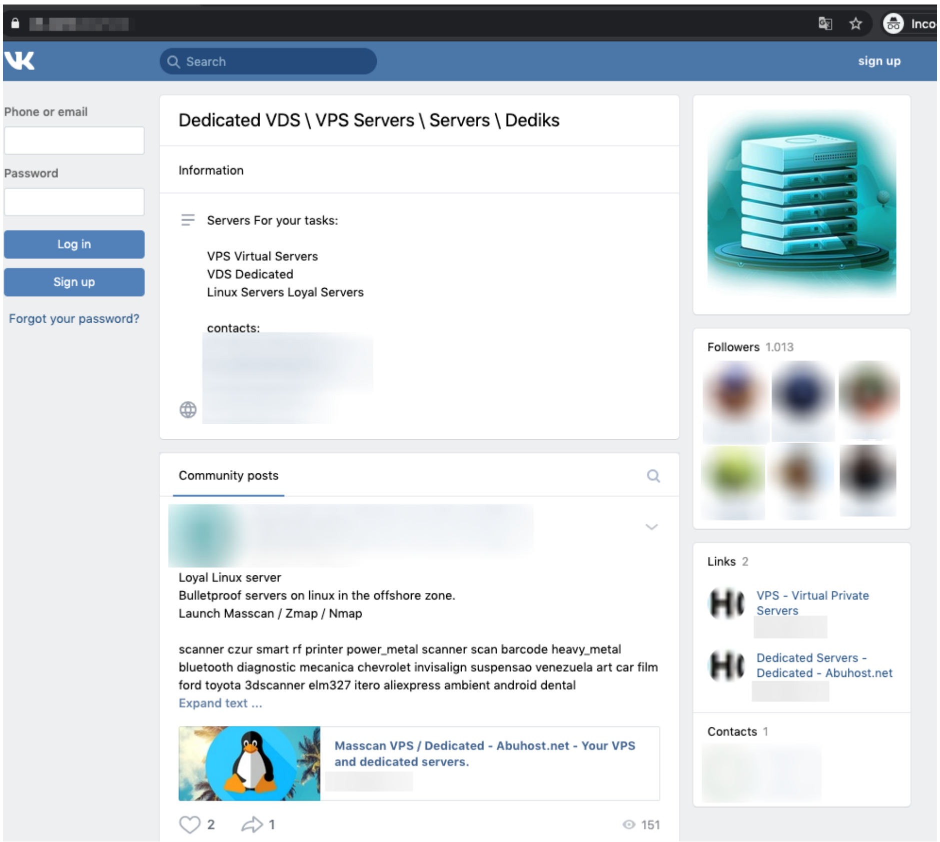


[redacted]
Вы приобретаете «до 2020 года»
— — — — — — — — — — —
Совершите платеж на QIWI в течение 30 минут
— — — — — — — — — — —
Кошелек: +7977105[redacted]
Сумма: 10 руб
Комментарий: 2017
— — — — — — — — — — —
БЕЗ КОММЕНТАРИЯ ДЕНЬГИ НЕ ЗАЧИСЛЯЮТСЯ

Figure 17. Payment information for VPN category

VK

VK is one of the biggest social media platforms for the Russian-speaking community. It is widely used to promote different kinds of small businesses. Underground actors often try to abuse VK’s advertisement capabilities to promote their bulletproof services. The screenshot below shows a hosting advertisement with contacts linked to the well-known underground forum exploit[.]im.



Dedicated VDS \ VPS Servers \ Servers \ Dediks

Information

Servers For your tasks:

VPS Virtual Servers
VDS Dedicated
Linux Servers Loyal Servers

contacts:
[redacted]

Community posts

[redacted]

Loyal Linux server
Bulletproof servers on linux in the offshore zone.
Launch Masscan / Zmap / Nmap

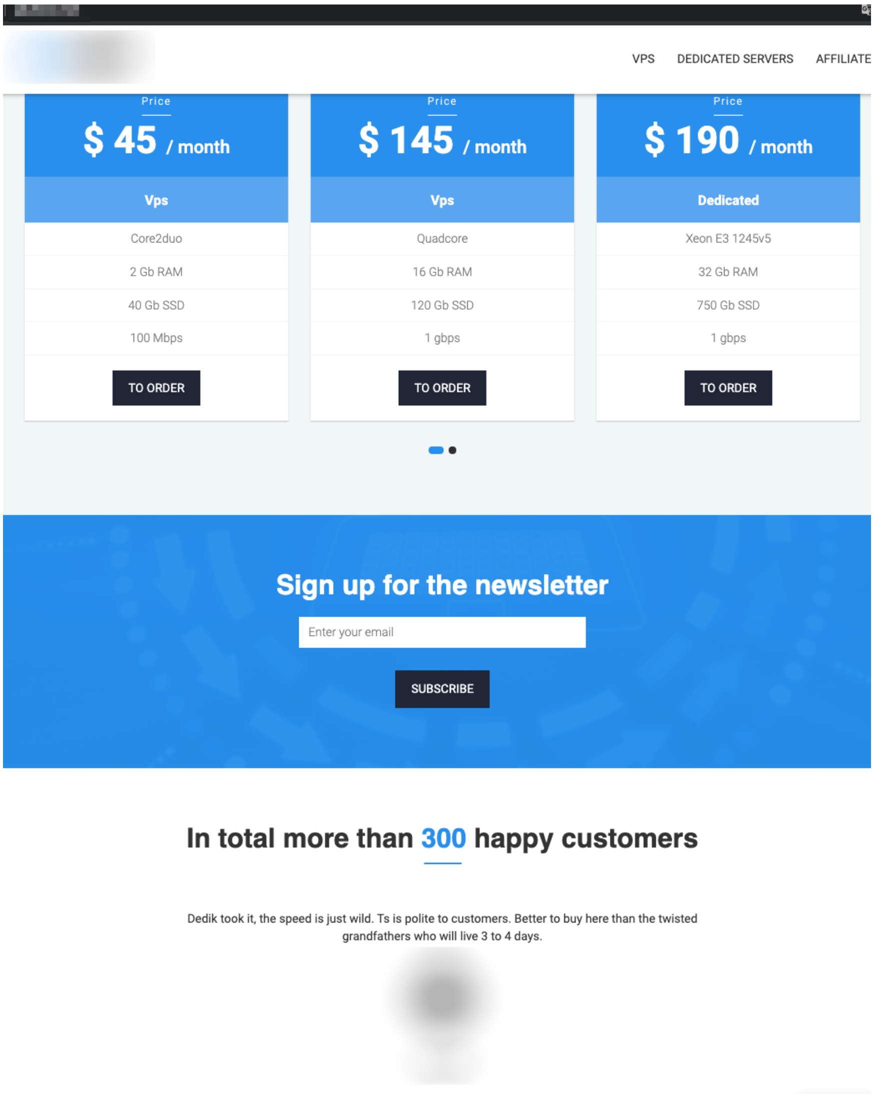
scanner czur smart rf printer power_metal scanner scan barcode heavy_metal bluetooth diagnostic mecanica chevrolet invisalign suspensao venezuela art car film ford toyota 3dscanner elm327 itero aliexpress ambient android dental
Expand text ...

Masscan VPS / Dedicated - Abuhost.net - Your VPS and dedicated servers.

2
1
151
Followers 1.013
Links 2
VPS - Virtual Private Servers
Dedicated Servers - Dedicated - Abuhost.net
Contacts 1

Figure 18. An advertisement of a hosting service on the VK social network with Jabber at exploit[.]jim domain

The name of the official website of this hosting provider suggests that the hosting is abuse-proof. Interestingly, the website also provides customer feedback on underground actors. The screenshot below shows feedback provided by the actor from the well-known underground forum BHF, also known as the "Best Hack Forum."



Price $ 45 / month	Price $ 145 / month	Price $ 190 / month
Vps	Vps	Dedicated
Core2duo	Quadcore	Xeon E3 1245v5
2 Gb RAM	16 Gb RAM	32 Gb RAM
40 Gb SSD	120 Gb SSD	750 Gb SSD
100 Mbps	1 gbps	1 gbps
TO ORDER	TO ORDER	TO ORDER

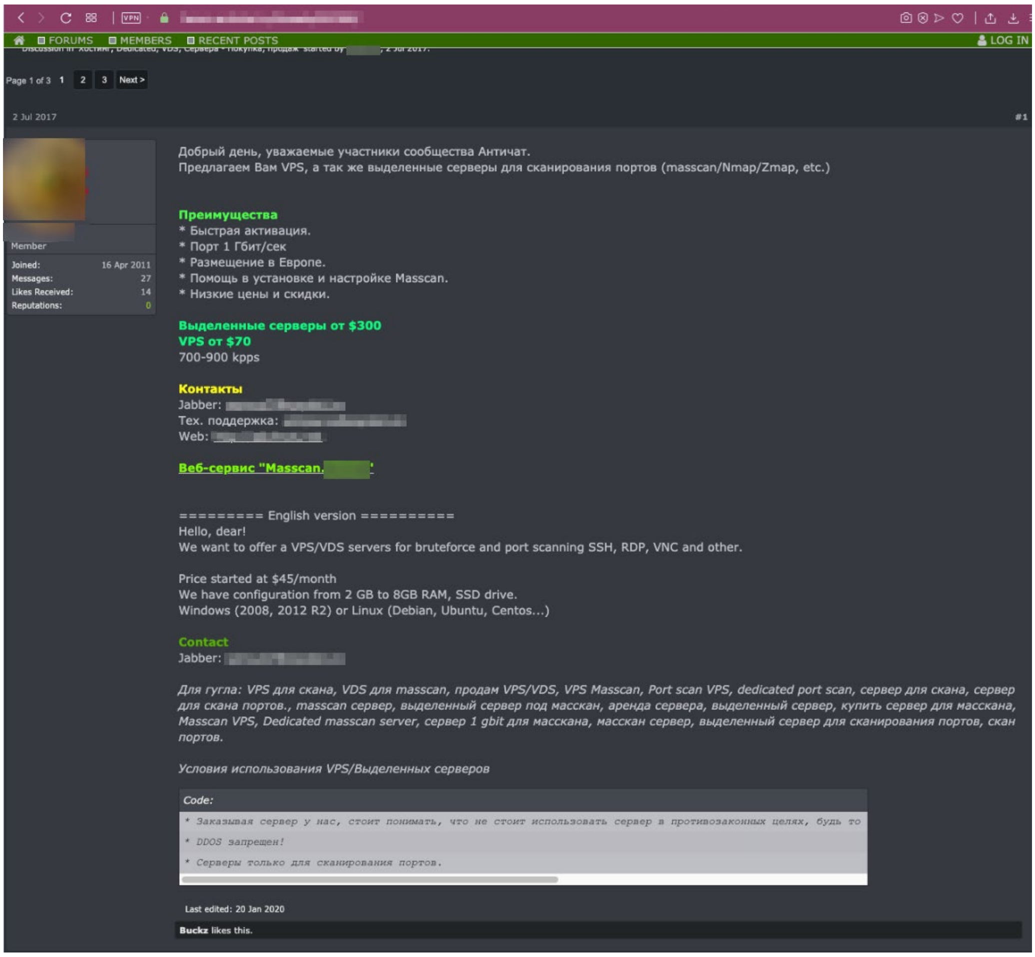
Sign up for the newsletter

In total more than 300 happy customers

Dedik took it, the speed is just wild. Ts is polite to customers. Better to buy here than the twisted grandfathers who will live 3 to 4 days.

Figure 19. Price list and feedback from an actor from well-known BHF underground forum

The same service is advertised in an underground forum called "Antichat." The service is positioned as suitable to run mass internet scans and brute-force attacks that use tools such as Masscan, Nmap, and ZMap.



Discussion in 'Хостинг, Dedicated, VDS, Сервера - покупка, продажа' started by [redacted], 2 Jul 2017.

2 Jul 2017 #1

[redacted]

Member

Joined: 16 Apr 2011
Messages: 27
Likes Received: 14
Reputations: 0

Добрый день, уважаемые участники сообщества Античат.
Предлагаем Вам VPS, а так же выделенные серверы для сканирования портов (masscan/Nmap/Zmap, etc.)

Преимущества
* Быстрая активация.
* Порт 1 Гбит/сек
* Размещение в Европе.
* Помощь в установке и настройке Masscan.
* Низкие цены и скидки.

Выделенные серверы от $300
VPS от $70
700-900 kpps

Контакты
Jabber: [redacted]
Тех. поддержка: [redacted]
Web: [redacted]

Веб-сервис "Masscan.[redacted]'

========= English version ==========
Hello, dear!
We want to offer a VPS/VDS servers for bruteforce and port scanning SSH, RDP, VNC and other.

Price started at $45/month
We have configuration from 2 GB to 8GB RAM, SSD drive.
Windows (2008, 2012 R2) or Linux (Debian, Ubuntu, Centos...)

Contact
Jabber: [redacted]

Для гугла: VPS для скана, VDS для masscan, продам VPS/VDS, VPS Masscan, Port scan VPS, dedicated port scan, сервер для скана, сервер для скана портов., masscan сервер, выделенный сервер под масскан, аренда сервера, выделенный сервер, купить сервер для масскана, Masscan VPS, Dedicated masscan server, сервер 1 gbit для масскана, масскан сервер, выделенный сервер для сканирования портов, скан портов.

Условия использования VPS/Выделенных серверов

Code:

```
* Заказывая сервер у нас, стоит понимать, что не стоит использовать сервер в противозаконных целях, будь то
* DDOS запрещен!
* Серверы только для сканирования портов.
```

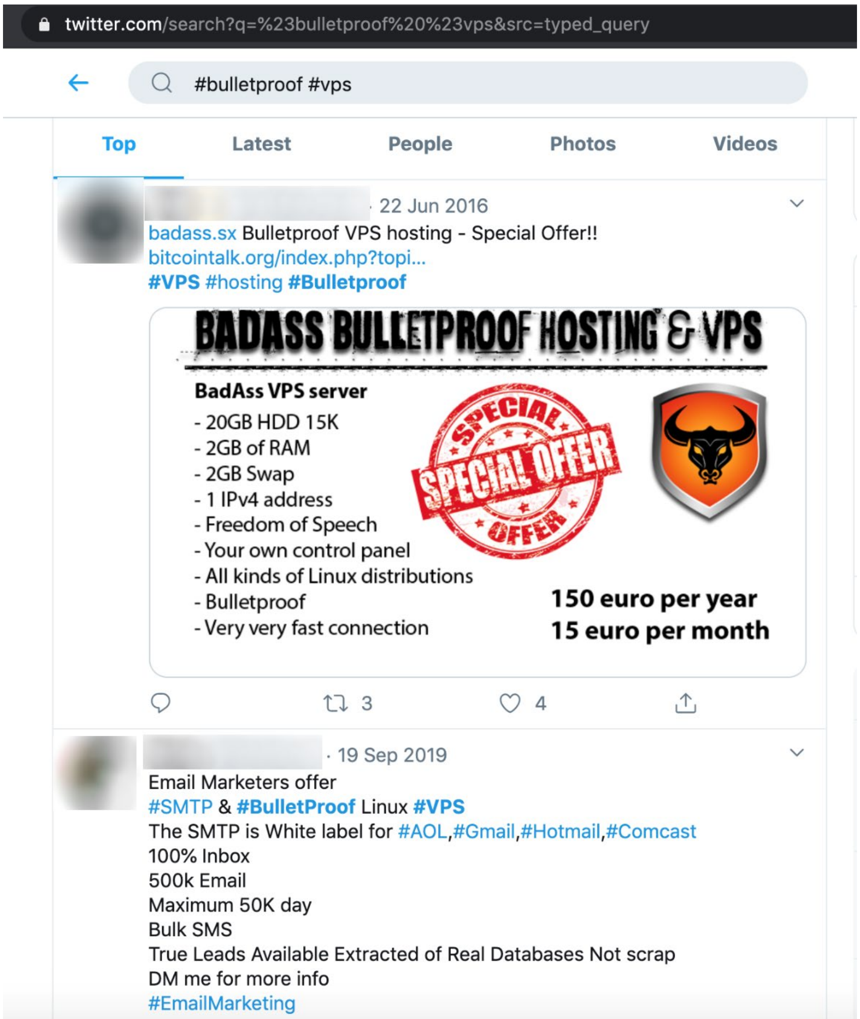
Last edited: 20 Jan 2020

Buckz likes this.

Figure 20. An advertisement of a hosting service in an underground forum

Twitter

Hashtags like #VPS or #bulletproof and their analogues in other languages can be used to find advertisements for bulletproof services on Twitter.



twitter.com/search?q=%23bulletproof%20%23vps&src=typed_query

#bulletproof #vps

· 22 Jun 2016

badass.sx Bulletproof VPS hosting - Special Offer!!
bitcointalk.org/index.php?topi...
#VPS #hosting #Bulletproof

BADASS BULLETPROOF HOSTING & VPS

BadAss VPS server

- 20GB HDD 15K
- 2GB of RAM
- 2GB Swap
- 1 IPv4 address
- Freedom of Speech
- Your own control panel
- All kinds of Linux distributions
- Bulletproof
- Very very fast connection

150 euro per year
15 euro per month

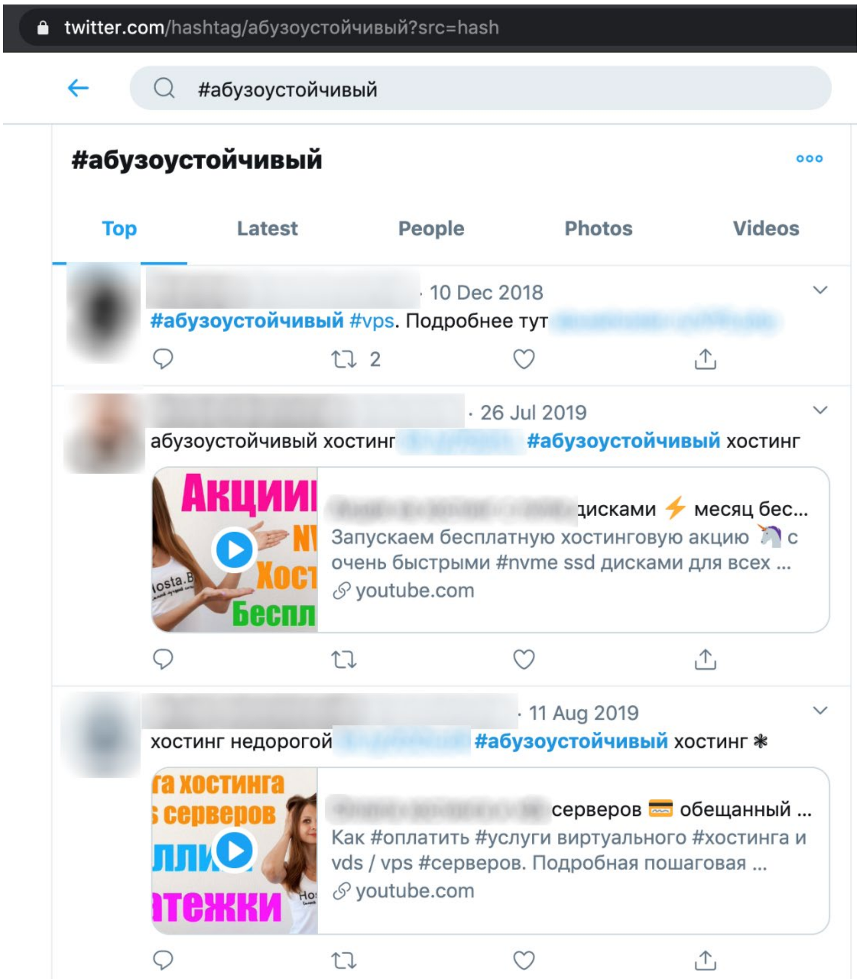
· 19 Sep 2019

Email Marketers offer
#SMTP & #BulletProof Linux #VPS
The SMTP is White label for #AOL,#Gmail,#Hotmail,#Comcast
100% Inbox
500k Email
Maximum 50K day
Bulk SMS
True Leads Available Extracted of Real Databases Not scrap
DM me for more info
#EmailMarketing

Figure 21. Advertisements of bulletproof services on Twitter using English hashtags

The advertisement is on Twitter, but these hashtags are not widespread or trending.

Using the Russian equivalent of the bulletproof tag reveals similar advertisements. We can find advertisements and links to promotion videos hosted on YouTube.



twitter.com/hashtag/абузоустойчивый?src=hash

#абузоустойчивый

#абузоустойчивый

[redacted] · 10 Dec 2018

#абузоустойчивый #vps. Подробнее тут [redacted]

[redacted] · 26 Jul 2019

абузоустойчивый хостинг [redacted] #абузоустойчивый хостинг

[redacted] дисками ⚡ месяц бес...

Запускаем бесплатную хостинговую акцию 🦄 с очень быстрыми #nvme ssd дисками для всех ...

youtube.com

[redacted] · 11 Aug 2019

хостинг недорогой [redacted] #абузоустойчивый хостинг ✱

[redacted] серверов 💳 обещанный ...

Как #оплатить #услуги виртуального #хостинга и vds / vps #серверов. Подробная пошаговая ...

youtube.com

Figure 22. Advertisements of bulletproof services on Twitter using Russian hashtags for bulletproof hosting

Conclusion

As highlighted at the introduction of this series, the infrastructure element of cybercrime is certainly critical to the successful business models of almost every form of cybercrime we see today. It should not come as a surprise that in such a successful criminal ecosystem, the market for buying and selling such services only continues to mature — and we see no reason for this trend to abate.

When we took a deep dive into the underground five years ago, criminal forums were still the primary means of communication, advertisement, and sale of services. From criminals advertising on social networks with a blatant disregard for the likelihood of an arrest to highly professional dedicated shops with filters and in-built rating systems, the first part of our series highlights that criminal forums have evolved. We have also seen that the areas where criminal infrastructure and legitimate internet infrastructure meet have become a deepening gray zone in terms of usage — something that will be dissected further in the series.

So how can knowledge of the way criminals sell their hosting solutions help us when it comes to disrupting their activities? First, it is important to note that stopping all cybercrime is likely impossible. The goal is much more on reducing the risks as much as possible. One way to do that is to drive up the cost of business for the threat actors. If you can disrupt the ability of a seller to reach their buyers, you can have a very major impact on both sides of the criminal divide.

This paper was published during the Covid-19 pandemic in 2020, when you did not need to look far to see the effects on economies where consumers could no longer reach the provider. In many cases, the providers fail to stay afloat, and in extreme cases, crucial parts of the economy fail. In cybercrime, understanding where and how these services are sold and using the collective resources of the InfoSec community and law enforcement will help to disrupt and undermine criminals wherever possible. This is arguably the best strategy for making a lasting and repeatable dent in cybercrime.

In the next part of the series, we will delve deeper into each of the major types of infrastructure leveraged by cybercriminals, and how each is used and acquired. It will discuss the costs of underground services like the ones mentioned above. We will also cover the different uses of compromised assets and dedicated hosting providers. In particular, we will take the reader through the lifecycle of such a compromised asset and how its monetization changes at different periods after its initial victimization.

Finally, we will conclude the series by looking into the modus operandi of criminals behind these services and how some of the longer-term career criminal providers have survived as long as they have.

To understand cybercrime, you need to understand its motives, driving factors, trends, and setups. By the end of this series, we hope to shed light upon all of these areas.

Appendix

Definitions and Concepts

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

- **Bulletproof hosting** refers to several categories of hosting providers, including those who deliberately ignore and abuse 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** is a type of internet hosting whereby the client leases an entire server not shared with anyone else.
- **Domain generation algorithm (DGA)** is a computer program that generates domains to contact systematically or programmatically.
- **Fast flux** is a domain name service (DNS) obfuscation technique used by botnets to hide their servers behind an ever-changing network of compromised machines or proxies (See proxy.).
- **Internet service provider (ISP)** is 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. This is often seen in VPN setups.
- **Proxy** is a computer that functions as a relay between a client and a server, offering a degree of obfuscation to the true location of the client. One well-known type uses a protocol known as SOCKS.
- **Remote desktop protocol (RDP)** is a protocol developed by Microsoft, which provides a user with a graphical interface for a computer being connected across a network. VNC is a similar standard.
- **Traffic direction system (TDS)** 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 as geographic location, operating system, browser, and language.
- **Virtual private network (VPN)** is a private network overlaid virtually on top of a public network such as the internet.
- **Virtual private server (VPS)** is a virtual machine sold as a service by an internet hosting provider.

References

1 Max Goncharov. (15 July 2015). *Trend Micro Security News*. “Bulletproof Hosting Services: Cybercriminal Hideouts for Lease.” Last accessed on 5 June 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bulletproof-hosting-services-cybercriminal-hideouts-for-lease.

2 Max Goncharov. (15 July 2015). *Trend Micro Security News*. “Bulletproof Hosting Services: Cybercriminal Hideouts for Lease.” Last accessed on 5 June 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bulletproof-hosting-services-cybercriminal-hideouts-for-lease.

3 Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler. (22 June 2015). *Trend Micro Security News*. “Going Deeper: Exploring the Deep Web.” Last accessed on 5 June 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploring-the-deep-web.

4 Trend Micro Research. (1 March 2016). *Trend Micro Security News*. “Going Deeper: Exploring the Deep Web.” Last accessed on 5 June 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercrime-and-the-deep-web.

5 Nate Drake. (30 May 2020). *TechRadar*. “Best DDoS protection of 2020.” Last accessed on 5 June 2020 at https://www.techradar.com/news/best-ddos-protection.

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 threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research