CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0112

BULLETPROOF HOSTING SERVICES ESSENTIAL FOR CRIMINAL UNDERGROUND SECURITY AND ANONYMITY

Recorded Future analyzed current data from the Recorded Future® Platform, dark web, information security reporting, and other open-source intelligence (OSINT) sources to identify the use and prevalence of bulletproof hosting services advertised by threat actors within the criminal underground. This report expands upon findings addressed in the report "Automation and Commoditization in the Underground Economy," following reports on database breaches, checkers and brute forcers, loaders, and crypters, credit card sniffers, banking web injects, exploit kits, and forums, marketplaces and shops. This report will be of most interest to security researchers charged with security risk management and mitigation.

Executive Summary

Bulletproof hosting services (BPHS) provide secure hosting for malicious content and activity and assure anonymity to threat actors. This typically consists of activities commonly disallowed by legitimate hosting providers such as the hosting of malware or other stolen materials. BPHS offerings have continued to flourish across open and closed sources, providing a variety of features to aspiring actors interested in hosting a variety of potential services away from the attention of law enforcement. BPHS offerings are still consistently discussed on dark web forums and continue to be a critical tool for criminal actors attempting to anonymize both their digital footprint as well as that of their infrastructure.

Partnerships between organized cybercriminal entities such as ransomware cartels and bulletproof hosting services have persisted throughout 2020. This report provides a high-level overview of six providers offering varying degrees of services to cybercriminal entities. Unlike regular web hosting, these services are often lenient about what can be hosted on their servers, only restricting particular services if they are likely to generate abuse complaints from authorities within the country where they are hosted. Countries that continue to be popular locations for bulletproof hosting services include Russia, Ukraine, and other Commonwealth of Independent States (CIS) nations, though historically one of the largest hosting service providers, McColo, responsible for 60 percent of the world's spam when taken down, was based in the U.S.

Bulletproof hosting providers are presented with a number of options when confronted with a notification alleging abusive behavior at one of their IP addresses. The options typically include either ignoring the request altogether or providing early notification to customers so they have time to alter their operations and avoid downtime. A key process of avoiding legal ramifications is creating a process that drags out the complaint procedure to the point when the request is often abandoned by the third party.

Key Judgments

- Bulletproof hosting services have increasingly appealed to ransomware operators attempting to avoid the attention of law enforcement.
- Prominent bulletproof hosting services with an established reputation within the cybercriminal community such as Yalishanda continue to enable the dissemination of more advanced strains of malware.
- Despite the threat of arrests and seizures of malicious infrastructure by law enforcement, bulletproof hosting service providers have continued to actively promote their services within the criminal underground throughout 2020.
- While there are many features in demand by aspiring cybercriminals when selecting a BPHS, the most popular features are those that combine client anonymity and security against law enforcement efforts.
- Cybercriminals supplement their BPHS operations by purchasing already compromised network access and reselling them via dark web/underground sources.

Table of Contents

Section I. Background and Function of a BPHS

The term "bulletproof" refers to the ability of these services to enable criminal businesses to operate unhindered for extended periods of time while ignoring the many abuse requests likely to arrive from legitimate service providers or law enforcement entities. To keep their criminal enterprise running smoothly, threat actors can choose from a myriad of services providing bulletproof hosting and proxy services. This large volume of offerings has created a competitive landscape for bulletproof hosting providers attempting to draw attention to their specific service. There now exist several features that threat actors are very likely to consider essential when selecting a particular service, features primarily focused on enabling the actors to maintain a strong degree of anonymity and preventing their business operations from being disrupted.

To extend the longevity of their criminal enterprises, threat actors have turned to proxy and bulletproof hosting services to help obfuscate their activities and to keep them from being shut down by law enforcement. One of the greatest distinctions between bulletproof hosting service (BPHS) operations and the services offered by a "regular" web hosting provider is the leniency they grant toward the data they allow to be hosted on their servers. Previous Recorded Future research has shown that such services often use geo-spoofing techniques to create a wide pool of IPs and are commonly advertised on both entry-level and highly-technical underground sources.

Dedicated bulletproof hosting providers typically have three primary methods of creating the infrastructure that enables them to sell their hosting services to clients:

1. Developing a privately-owned, in-house/custom data center;
2. Leasing out commercial infrastructure for an extended period of time, or;
3. Compromising assets belonging to a different set of providers, typically for activities for a shorter period of time, such as the distribution of spam.

As to the third category and how criminals typically go about compromising exposed assets or servers, actors often use a combination of techniques and purchase direct access to server assets from the same underground sources they may advertise on subsequently. Advertisements for exploits that enable actors to compromise and eventually use exposed servers for hosting purposes have been observed throughout 2020 as well, albeit to a much lesser extent than advertisements for hosting services that are already available to purchase.

Hosting services are fundamental for most, if not all, of the cybercriminal operations reported on throughout 2020 as part of Recorded Future's automation and commoditization series studying the economy of the criminal underground. Hosting providers sell cybercriminals the means that enable them to covertly host the many forums or marketplaces that make up this underground economy in a stable and efficient manner with minimal disruption.

Since the beginning of 2020, Recorded Future has observed a consistent volume of references to actors within underground sources seeking recommendations for a new bulletproof hosting service, though analysts did observe that this was more of a tendency for actors on entry-level, English-language forums. It is likely that actors operating within high-tier forums that traditionally post content in other languages, particularly Russian, are less likely to openly recommend the hosting services they use unless incentivized, given the unnecessary risk or attention it may bring to the services they use in the long term.

Forums often devote entire sections specifically to the sale of these services or for buying compromised assets. The majority of bulletproof hosting providers indexed within the Recorded Future platform advertise on the high-tier Russian language criminal forum Exploit. The advertisements referenced in the visual below represent a sample of approximately 7,000 references to different hosting providers who have advertised on dark web and underground forums since the beginning of 2020. The market remains saturated with multiple brands, with some of the most frequently referenced services indexed within the Recorded Future platform detailed in the next section. However, this market can be differentiated between top-tier providers and low-tier ones, who mostly sell compromised RDP or SSH accesses with no guarantee that the access will last.

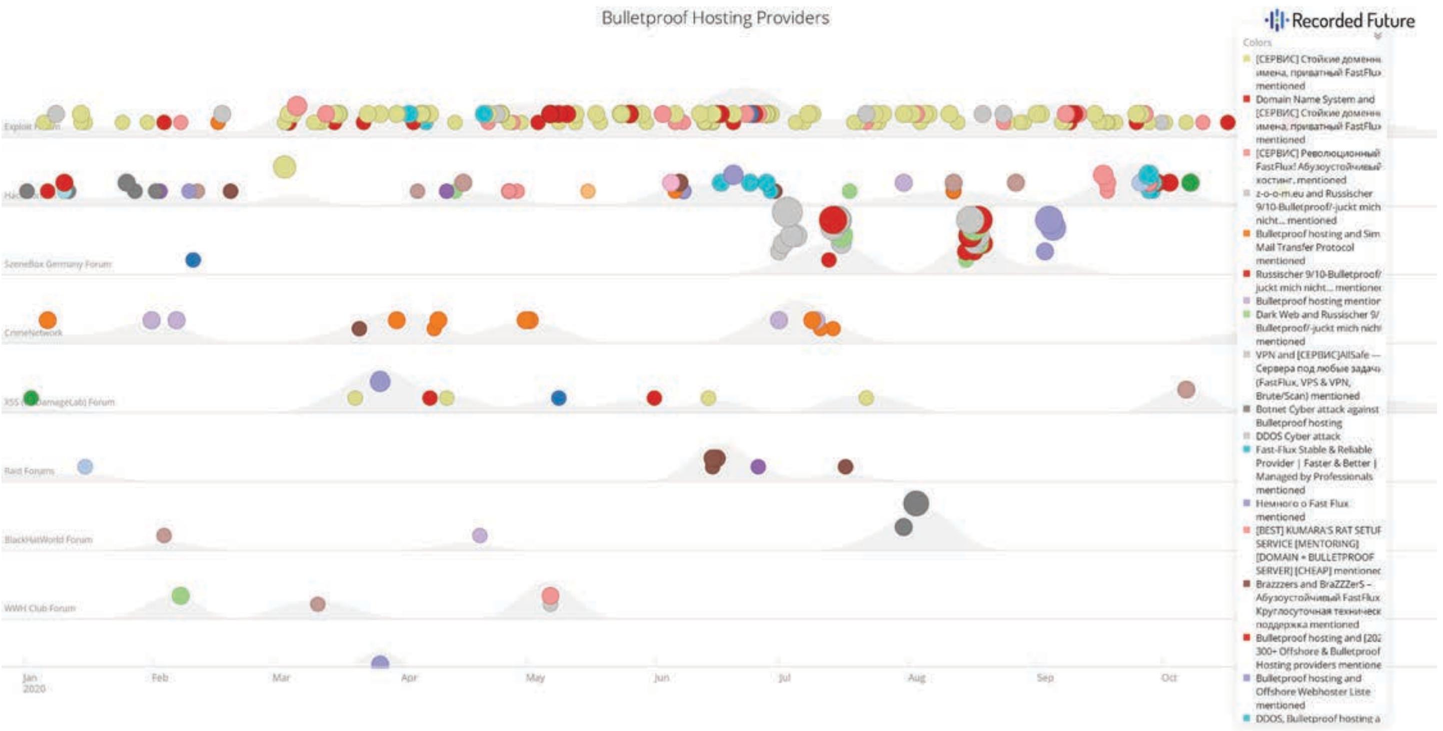


Figure 1: Bulletproof hosting providers on dark web and underground forums (Source: Recorded Future)

Threat actors know that these services are offered in jurisdictions outside the purview of many law enforcement agencies, relying on a model that promises not to comply with legal requests that would either disrupt their operations or result in arrests. Some countries offer a middle-ground option as well, allowing administrators of these potential services to establish legitimate businesses within the country in question and only requiring routine check-ins or disclosures of business operations to government officials. Criminal forums, Jabber servers, banking trojans, and other criminal operations could not exist without hosting, and individuals who use these services could not use them securely without some sort of network anonymity.

Bulletproof hosting via these underground advertisements serves a variety of purposes. Prominent examples of these services include the following:

- Ransomware blogs
- Malware C2s
- Child exploitation content (most of the top-tier services refuse to host such material)
- Shops selling personally identifiable information (PII)
- Dark web forums and marketplaces
- Chat services
- Brute-force attack tools
- Botnet infrastructure
- Exploit kits
- Spamming services

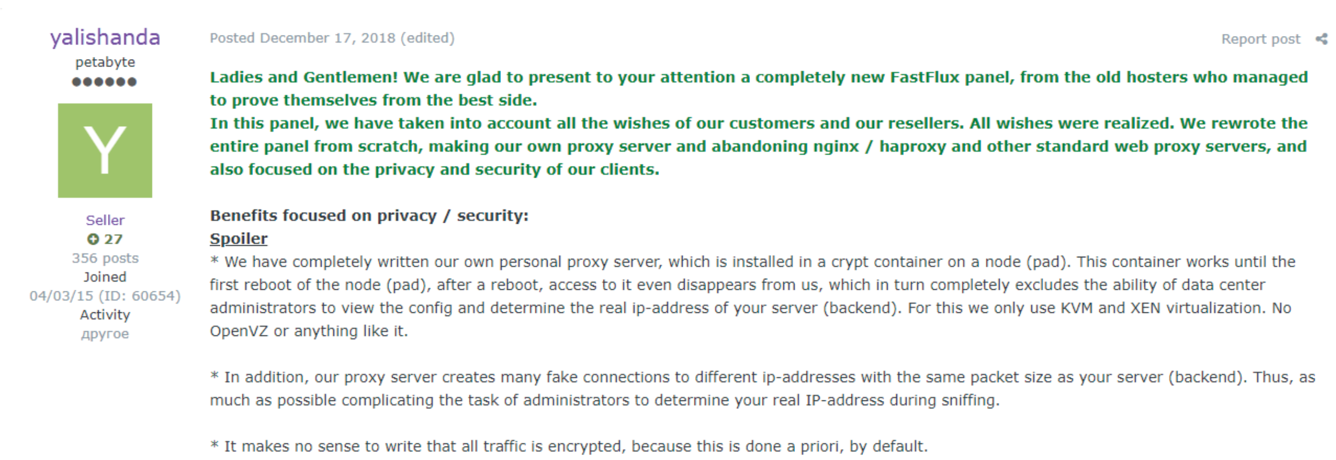
Section II. Sample List of Bulletproof Hosting Services

Yalishanda

Yalishanda is an underground actor known historically for advertising hosting services on Exploit and multiple other Russian-language forums since as early as December 2018. Using Fast-flux technology, the user has claimed to have their own proxy server that relies on Kernel-based virtual machines and XEN virtualization. Three domain registrars located in Europe, China, and Malaysia have been affiliated with the actor, representing a geographic diversity in locations that host their malicious infrastructure. The nickname Yalishanda means “Alexander” in Mandarin (亚历山大).

According to Brian Krebs, the domain names used in criminal infrastructure were attributed to “Aleksandr Volosovyk” and an email address, stas_vl@mail[.]ru, establishing that he resides in Vladivostok, a major Pacific port city in Russia close to the borders with China and North Korea.

In a talk given at the Black Hat security conference in 2017, researchers from Cisco and cyber intelligence firm Intel 471 labeled Yalishanda as one the “top tier” bulletproof hosting providers worldwide, noting that in just one 90-day period in 2017 its infrastructure was seen hosting sites tied to some of the most advanced malware strains at the time, including the Dridex and Zeus banking trojans.



yalishanda
petabyte
●●●●●●

Seller
⊕ 27
356 posts
Joined
04/03/15 (ID: 60654)
Activity
другое

Posted December 17, 2018 (edited)

Report post

Ladies and Gentlemen! We are glad to present to your attention a completely new FastFlux panel, from the old hosters who managed to prove themselves from the best side.
In this panel, we have taken into account all the wishes of our customers and our resellers. All wishes were realized. We rewrote the entire panel from scratch, making our own proxy server and abandoning nginx / haproxy and other standard web proxy servers, and also focused on the privacy and security of our clients.

Benefits focused on privacy / security:
Spoiler
* We have completely written our own personal proxy server, which is installed in a crypt container on a node (pad). This container works until the first reboot of the node (pad), after a reboot, access to it even disappears from us, which in turn completely excludes the ability of data center administrators to view the config and determine the real ip-address of your server (backend). For this we only use KVM and XEN virtualization. No OpenVZ or anything like it.

* In addition, our proxy server creates many fake connections to different ip-addresses with the same packet size as your server (backend). Thus, as much as possible complicating the task of administrators to determine your real IP-address during sniffing.

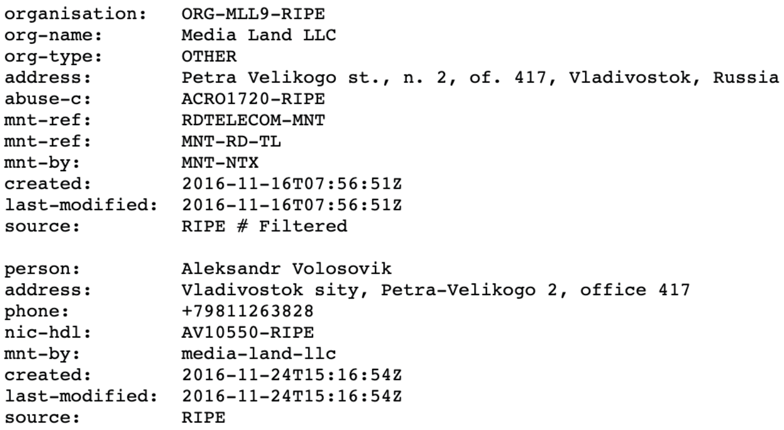
* It makes no sense to write that all traffic is encrypted, because this is done a priori, by default.

Figure 2: yalishanda advertisement (Source: Exploit Forum)

The benefits Yalishanda offers aimed at privacy and security are detailed in Figure 2 above, and include a personal proxy server, as well as the following:

- The ability to add or remove domains and subdomains
- Management of DNS records such as MX/XT/CNAME directly from the panel
- Three bulletproof public DNS and personal FastFlux DNS
- SSL certification provision
- Simple interface for changing the given proxy server as needed
- Unlimited backends (IP adding/removing)
- Support for all known crypto domains, such as .bit
- Three domain registrars spread out across multiple geographic regions including Europe, China, and Malaysia
- Addition of a checker for domains that are blocked or are on blocklists
- Support for the purchase of SSL certificates and VPS/dedicated servers

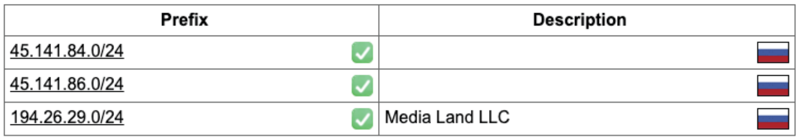
Yalishanda is currently using Media Land LLC AS206728 for their illegal activity. Russian business portal Zachestniybiznes[.]ru provides a record[1] that the business entity is founded and managed by "Volosovik, Aleksandr Aleksandrovich",[2] which is consistent with the allegations made by Brian Krebs in his research.



```
organisation:   ORG-MLL9-RIPE
org-name:       Media Land LLC
org-type:       OTHER
address:        Petra Velikogo st., n. 2, of. 417, Vladivostok, Russia
abuse-c:        ACRO1720-RIPE
mnt-ref:        RDTELECOM-MNT
mnt-ref:        MNT-RD-TL
mnt-by:         MNT-NTX
created:        2016-11-16T07:56:51Z
last-modified:  2016-11-16T07:56:51Z
source:         RIPE # Filtered

person:         Aleksandr Volosovik
address:        Vladivostok sity, Petra-Velikogo 2, office 417
phone:          +79811263828
nic-hdl:        AV10550-RIPE
mnt-by:         media-land-llc
created:        2016-11-24T15:16:54Z
last-modified:  2016-11-24T15:16:54Z
source:         RIPE
```

Figure 3: AS206728 Record — Media Land LLC (Source: Hurricane Electric Internet Services)



Prefix	Description
45.141.84.0/24 ✓	🇷🇺
45.141.86.0/24 ✓	🇷🇺
194.26.29.0/24 ✓	Media Land LLC 🇷🇺

Figure 4: AS206728 Media Land LLC prefixes (Source: Hurricane Electric Internet Services)

According to the Hurricane Electric Internet Services IPv4 route propagation diagram, AS206728 has two uplink providers: AS3216 PJSC "Vimpelcom" and AS9002 RETN Limited. From a technical standpoint, it is not difficult for the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) to "cut the wires" of an internet provider that hosts malicious content. The fact that it has not done so implies that the hosting's behavior materially benefits the Russian geopolitical agenda.

Examples of this hypothetical symbiotic relationship between Russian underground criminal elements and Russian law or intelligence services could include the exfiltration of strategic information or espionage via criminal ransomware, the destruction or disruption of critical assets of an adversarial government or organization by underground criminal elements,

[1] https://zachestnyibiznes[.]ru/company/ul/1152536009900_2536288610_OOO-MEDIA-LEND

[2] https://zachestnyibiznes[.]ru/fl/253609232850

or the provision of clandestine and underground market goods and services to friendly governments or organizations which would otherwise be illegal.

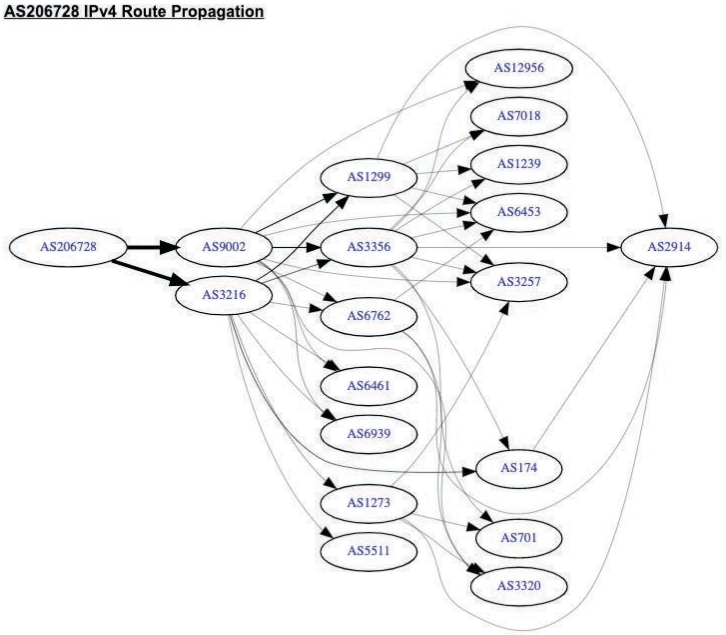
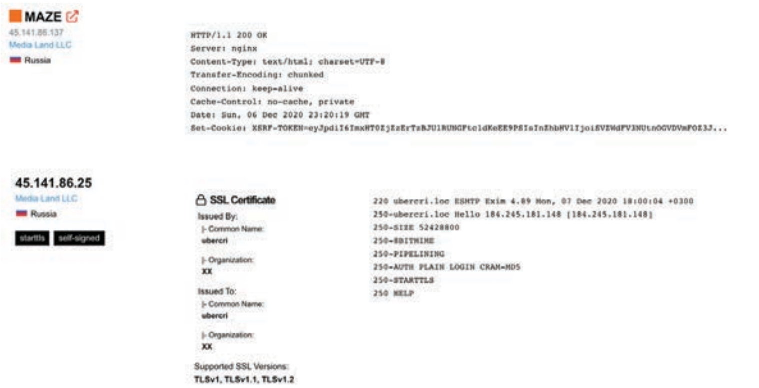


Figure 5: AS206728 Media Land LLC route propagation (Source: Hurricane Electric Internet Services)

According to information aggregated within Shodan, Media Land LLC has remained a hosting provider for multiple criminal underground services throughout 2020, including the following:

- Maze Ransomware operators as indicated in the visual below
- Multiple Cobalt Strike team servers
- Anubis infrastructure
  - An IP address identified to be affiliated with Yalishanda infrastructure, 45.141.84[.]85, hosted the domain lab8fc81.justinstalledpanel[.]com from July through September 2020. *.justinstalledpanel.com refers to the default admin panel for web servers managed via Ispsystem (ispsystem[.]com). *.justinstalledpanel[.]com has continued to appear in open-source reporting throughout 2020 in connection to reports of Media Land LLC's role in hosting criminal malware.
- SMTP server of "ubercri", the threat actor responsible for hacking into the Election Assistance Commission in 2016 and other government entities in 2017.



MAZE
45.141.86.137
Media Land LLC
Russia

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, private
Date: Sun, 06 Dec 2020 23:20:19 GMT
Set-Cookie: XSRF-TOKEN=eyJpdiI6ImxHT0ZjZzErTzBJU1RUNGFtcldKeEE9PSIsInZhbHVlIjoiSVZWdFV3NUtnOGVDVmFOZ3J...
```

45.141.86.25
Media Land LLC
Russia
starttls self-signed

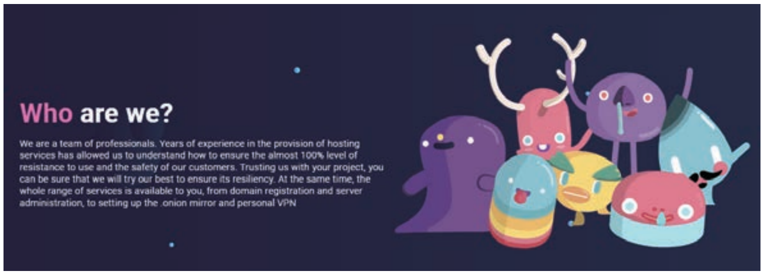
SSL Certificate
Issued By:
|- Common Name:
ubercri
|- Organization:
XX
Issued To:
|- Common Name:
ubercri
|- Organization:
XX
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
220 ubercri.loc ESMTP Exim 4.89 Mon, 07 Dec 2020 18:00:04 +0300
250-ubercri.loc Hello 184.245.181.148 [184.245.181.148]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN CRAM-MD5
250-STARTTLS
250 HELP
```

Figures 6 and 7: Notable clients hosted at Media Land LLC including Maze ransomware operators (Source: Shodan)

FLOWSPEC

The visuals below are taken from the FLOWSPEC[.]ru hosting service, representing recurring attempts by a BPHS attempting to appear as legitimate as possible. Services such as FLOWSPEC[.]ru aim to invoke a strong sense of professional web development to visitors. A service's reputation within the cybercriminal community plays a strong role in determining which BPHS is more likely to thrive over extended periods of time, with consistent posts from clients recommending the services on forums also contributing to the overall success of a BPHS.



Who are we?

We are a team of professionals. Years of experience in the provision of hosting services has allowed us to understand how to ensure the almost 100% level of resistance to use and the safety of our customers. Trusting us with your project, you can be sure that we will try our best to ensure its resiliency. At the same time, the whole range of services is available to you, from domain registration and server administration, to setting up the .onion mirror and personal VPN

Figure 8: FlowSpec[.]ru webpage

FlowSpec administrators advertise the following features for the service:

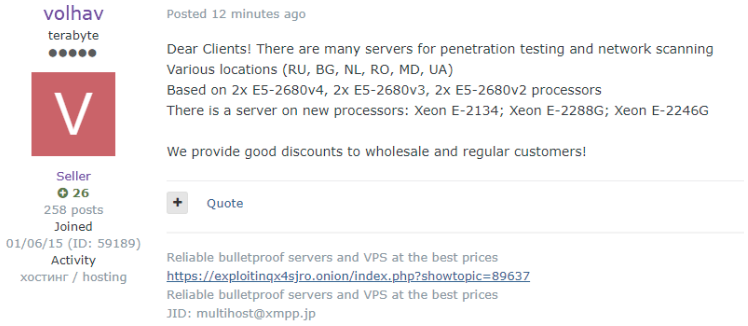
- A geo-distributed network of IP addresses and autonomous systems
- Equipment and server racks stored on privately owned property
- All client traffic is and must continue to be encrypted
- Custom infrastructure service offerings that include backup of files, databases, backup proxies, fault-tolerant domains, and DNS
- 24/7 customer support
- Dedicated or virtual servers ($150 or $50 USD respectively)

- Protection of .onion sites from distributed denial-of-service attacks
- Generating of permanent Tor domains
- Registration of bulletproof domains

Similar to Media Land LLC described previously, FLOWSPEC services are typically associated with another unique ASN, AS210138. Analysis of SSL certificate information associated with this ASN revealed its ongoing hosting of active criminal marketplaces including the Hydra Market, which predominantly sells narcotics, controlled substances, and counterfeit documents or currency to Russia-based buyers.

volhav

volhav is another service that provides bulletproof hosting and access to virtual (VPS/VDS) servers in data centers via the criminal underground. The threat actor behind the service, whose username is also "volhav," reportedly offers servers for almost any purpose (malware, spam, DDoS, port scanning, Spamhaus) with prices starting from $150 USD and an installation period of 12 to 48 hours. volhav also offers servers with IP spoofing for "testing" the network infrastructure for resistance to DDoS attacks and provides assistance in server administration and in resolving issues that may have arisen. volhav remains one of the leaders in the bulletproof hosting industry.



volhav
terabyte
●●●●●
Seller
26
258 posts
Joined
01/06/15 (ID: 59189)
Activity
хостинг / hosting

Posted 12 minutes ago

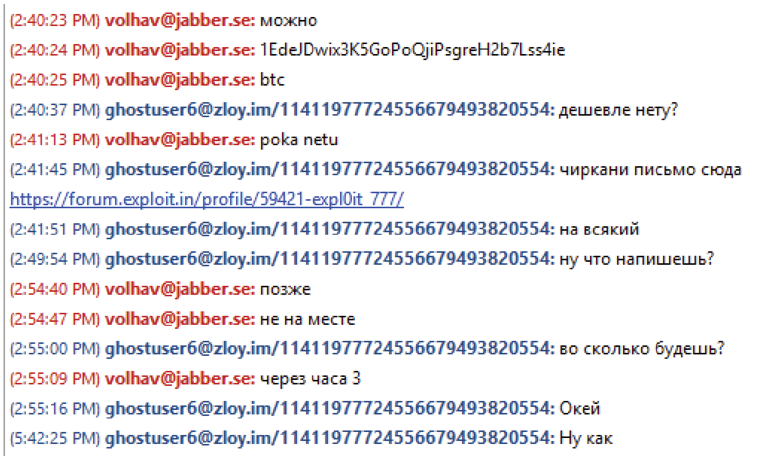
Dear Clients! There are many servers for penetration testing and network scanning
Various locations (RU, BG, NL, RO, MD, UA)
Based on 2x E5-2680v4, 2x E5-2680v3, 2x E5-2680v2 processors
There is a server on new processors: Xeon E-2134; Xeon E-2288G; Xeon E-2246G

We provide good discounts to wholesale and regular customers!

Reliable bulletproof servers and VPS at the best prices
https://exploitinqx4sjro.onion/index.php?showtopic=89637
Reliable bulletproof servers and VPS at the best prices
JID: multihost@xmpp.jp

Figure 9: volhav advertisement (Source: Exploit Forum)

On August 11, 2020, another threat actor, "Expl0it_777," shared a screenshot of their conversation with volhav where the bulletproof hosting operator provided a Bitcoin address for payment.



```
(2:40:23 PM) volhav@jabber.se: можно
(2:40:24 PM) volhav@jabber.se: 1EdeJDwix3K5GoPoQjiPsgreH2b7Lss4ie
(2:40:25 PM) volhav@jabber.se: btc
(2:40:37 PM) ghostuser6@zloy.im/11411977724556679493820554: дешевле нету?
(2:41:13 PM) volhav@jabber.se: poka netu
(2:41:45 PM) ghostuser6@zloy.im/11411977724556679493820554: чиркани письмо сюда
https://forum.exploit.in/profile/59421-expl0it_777/
(2:41:51 PM) ghostuser6@zloy.im/11411977724556679493820554: на всякий
(2:49:54 PM) ghostuser6@zloy.im/11411977724556679493820554: ну что напишешь?
(2:54:40 PM) volhav@jabber.se: позже
(2:54:47 PM) volhav@jabber.se: не на месте
(2:55:00 PM) ghostuser6@zloy.im/11411977724556679493820554: во сколько будешь?
(2:55:09 PM) volhav@jabber.se: через часа 3
(2:55:16 PM) ghostuser6@zloy.im/11411977724556679493820554: Окей
(5:42:25 PM) ghostuser6@zloy.im/11411977724556679493820554: Ну как
```

Figure 10: volhav conversation log with the customer Expl0it_777 (Source: Exploit Forum)

[Translated from the original Russian:
V: it's possible
V: 1EdeJDwix3K5GoPoQjiPsgreH2b7Lss4ie
V: btc
G: anything cheaper?
V: don't have anything right now
G: shoot me over a message here (link to Exploit forum profile used to validate that volhav is who they say they are)
G: just in case
G: so, are you going to write?
V: later
V: not around right now
G: when will you be?
V: in about 3 hours
G: Okay
G: So how's it going]

Using Chainalysis proprietary sources, we identified the root BTC address affiliated with the wallet (1EdeJDwix3K5GoPoQjiPsgreH2b7Lss4ie) provided in the conversation in Figure 10. According to the public ledger, this Bitcoin cluster received direct payments from multiple underground criminal sources, including ransomware operators tied to the Phobos and CrySiS (Dharma) strains. Operators associated with these ransomware strains likely used volhav as their preferred method of bulletproof hosting for a component of their malicious infrastructure. The information security community has historically reported on technical and operational similarities between two separate strains of ransomware, Phobos and CrySiS (Dharma), leading to speculation that operators of the malware were working together in some capacity. The co-hosting strengthens this theory.

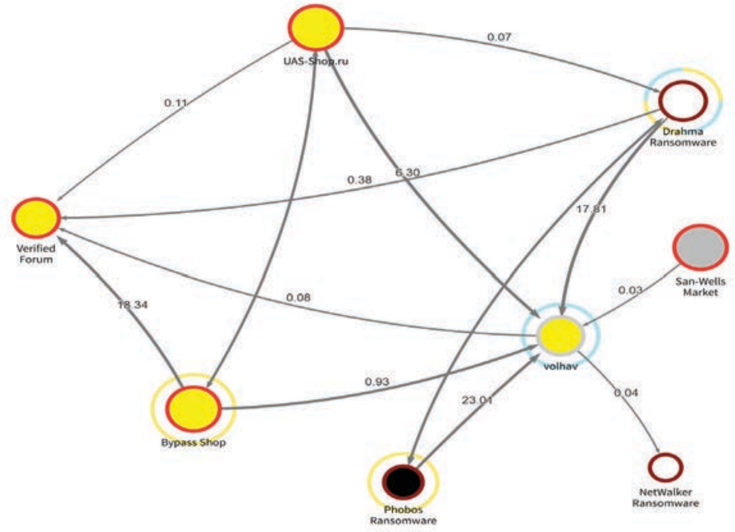


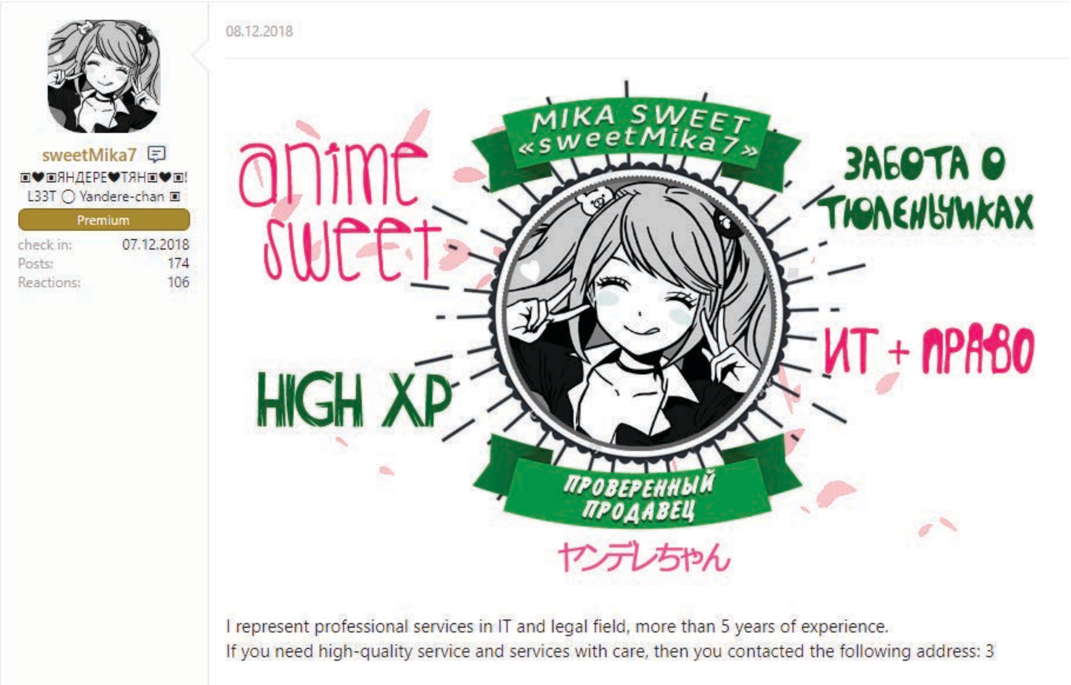
Figure 11: Bitcoin transfers tie ransomware strains to volhav wallet (Source: Chainalysis)

Both ransomware variants operate as a ransomware-as-a-service (RaaS) model wherein the attackers can generate their own versions of the ransomware to distribute to victims via phishing campaigns. As denoted in the visual in Figure 11 above, wallets associated with both strains of the ransomware were observed funnelling a combined total of over $250,000 USD in bitcoins to at least one wallet linked to volhav, dating back to 2018. Deposits from operators tied to the Dharma ransomware strain persisted for approximately two years, from Q2 2018 through Q2 2020. The last observed set of funds transferred to volhav service by a wallet associated with Dharma ransomware occurred in April 2020, just one month after open-source reporting detailed that an advertisement for the source code for Dharma had appeared within the criminal underground. The role of underground marketplaces seen transferring funds to volhav was less pronounced, with two marketplaces observed sending bitcoins to volhav, Bypass Shop and UAS-Shop[.]ru. Compromised Remote Desktop Protocol credentials purchased from sites such as Bypass Shop have long been a confirmed origin of ransomware attacks.

sweetMika7

sweetMika7 is a bulletproof hosting provider with a focus on customer service advertised across multiple tier-one forums. According to the threat actor, their service is simple to manage, also implying that they devote a maximum level of care for their clients in an attempt to portray themselves as a "legitimate" business entity. Services provided in connection with this emphasis on customer support include server selection, initial server configuration, server reconfiguration, assistance in installation, and the setting up of additional software. Prices are negotiated according to requirements with the possibility of substantial discounts off of list prices. The threat actor accepts Bitcoin and Monero, and is willing to pay for the escrow upon the request of certain (for example, ransomware) clients.

Similar to volhav, the ASN associated with the service offered by sweetMika7, AS47510, has attracted a string of ransomware operators over the duration of its lifespan. Information compiled[3] from Shodan revealed the ASN to be hosting the ransomware extortion sites, Egregor News and MountLocker Leaks as recently as November 2020.


sweetMika7
▣❤▣ЯНДЕРЕ❤ТЯН▣❤▣!
L33T ○ Yandere-chan ▣
Premium
check in: 07.12.2018
Posts: 174
Reactions: 106

08.12.2018

I represent professional services in IT and legal field, more than 5 years of experience.
If you need high-quality service and services with care, then you contacted the following address: 3

Figure 12: sweetMika7 profile and advertisement (Source: XSS Forum)

[3] A valid Shodan account is necessary to submit search queries. https://beta.shodan.io/search?query=org%3A%22Crex+Fex+Pex+Internet+System+Solutions+LLC%22+ssl%3A%22egregornews%22 https://beta.shodan.io/search?query=asn%3A%22AS47510%22+http.title%3A%22Mount+Locker+%7C+News+%26+Leaks%22

sweetMika7 offers the following services:

- Dedicated servers (DS)
- Virtual servers (VPS)
- Smart servers (SmartServer)
- Remote desktops based on Microsoft Windows (VDI)
- Virtual private networks (VPN)
- Custom configurations, for example for Jabber or Proxy
- Fast flux DNS

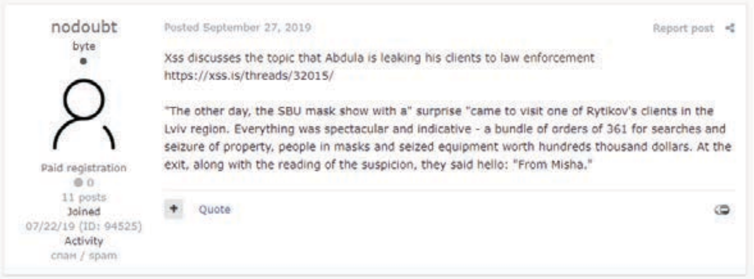
AbdAllah/Whost/WebHost

In 2013, a federal indictment in the District of New Jersey charged Mikhail Rytikov, also known as "AbdAllah," and four others with conspiring in a worldwide hacking scheme that targeted major corporate networks and stole over 160 million credit card numbers. It is estimated that hundreds of millions of dollars were stolen, making it the largest such scheme ever prosecuted in the U.S at the time.

Rytikov wasn't extradited to the United States because Ukraine doesn't allow extradition of its citizens. AbdAllah restarted the operation under the new monikers "WebHost" and "Whost," advertising bulletproof hosting services in Lebanon.

- On July 11, 2019, Security Service of Ukraine (SBU) officers in cooperation with U.S. law enforcement entities announced they'd conducted 29 searches and detained two individuals in connection with a sprawling bulletproof hosting operation. The arrests provided insight into the scale of a bulletproof hosting operation, with the group consisting of about 10 key participants, including Mikhail Rytikov and dozens of associates, intermediaries in a number of countries, as well as thousands of customers. According to the official release, the actors were worried about the fact that hundreds of terabytes of data were obtained by law enforcement partners that could provide evidence for hundreds of criminal cases all over the world. According to SBU estimates, the service offered by these actors encompassed "about 40 percent of the Russian-language DarkNet segment." Officials stated they found the data center to have 150 servers, providing critical insight into the composition of a BPHS of this scale.

Exploit[.]lm Jabber server was also down during the raid. Members accused Whost of concealing information and eventually another user on Exploit Forum, "nodoubt" accused Rytikov of working for the SBU.



nodoubt
byte

Paid registration
● 0
11 posts
Joined
07/22/19 (ID: 94525)
Activity
спам / spam

Posted September 27, 2019

Report post

Xss discusses the topic that Abdula is leaking his clients to law enforcement
https://xss.is/threads/32015/

"The other day, the SBU mask show with a" surprise "came to visit one of Rytikov's clients in the Lviv region. Everything was spectacular and indicative - a bundle of orders of 361 for searches and seizure of property, people in masks and seized equipment worth hundreds thousand dollars. At the exit, along with the reading of the suspicion, they said hello: "From Misha."

Figure 13: Underground forum post claiming Abdula was leaking client info to law enforcement (Source: Exploit Forum)

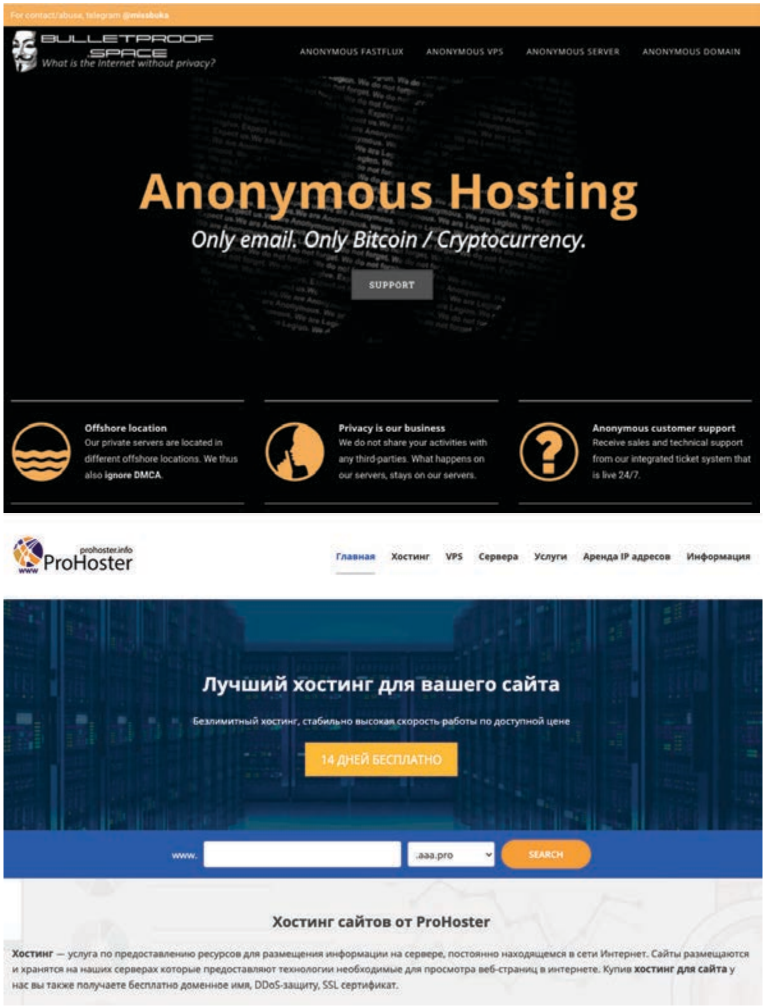
According to the investigation conducted by the Ukrainian media outlet Liga[.]Net, Rytikov again was eventually able to avoid prosecution. He even attempted to mislead his clients that the raid, conducted by the SBU, wasn't against the Whost/WebHost, and that the data center would be operational within days. Currently, the Whost service appears to be down, so if Rytikov returned to providing BPHs it has been branded under a new name, though there is no indication that this is the case.

Figures 14 and 15: WebHost underground data center and Mikhail Rytikov (Source: SBU.gov.ua)

ProHoster

On January 17, 2020, as part of measures to combat cybercrime, the SBU identified and stopped the activities of another hacker group that specialized in providing "abuse-resistant" bulletproof hosting services. During the investigation, law enforcement authorities detained the unnamed organizer of the group in Vinnytsia (Ukraine), who provided server equipment for hosting, administration, and distribution of malicious software, botnets, and cyberattacks since 2011. These services were reportedly used for a variety of other specific criminal purposes including DDoS attacks on strategic targets within Ukraine as well as against international banking institutions. The bulletproof hosting service and the threat actor behind it was known on the Dark Web as "ProHoster" and "Bulletproof[.]space".

Figures 16 and 17: Datacenter and organizer detained during SBU raid (Source: SBU.gov.ua)



For contact/abuse, telegram @missbuka

BULLETPROOF .SPACE

What is the Internet without privacy?

Anonymous Hosting

Only email. Only Bitcoin / Cryptocurrency.

Offshore location
Our private servers are located in different offshore locations. We thus also **ignore DMCA**.

Privacy is our business
We do not share your activities with any third-parties. What happens on our servers, stays on our servers.

Anonymous customer support
Receive sales and technical support from our integrated ticket system that is live 24/7.

prohoster.info ProHoster

Лучший хостинг для вашего сайта

Безлимитный хостинг, стабильно высокая скорость работы по доступной цене

Хостинг сайтов от ProHoster

Хостинг — услуга по предоставлению ресурсов для размещения информации на сервере, постоянно находящемся в сети Интернет. Сайты размещаются и хранятся на наших серверах которые предоставляют технологии необходимые для просмотра веб-страниц в интернете. Купив **хостинг для сайта** у нас вы также получаете бесплатно доменное имя, DDoS-защиту, SSL сертификат.

Figures 18 and 19: Bulletproof[.]space and ProHoster[.]info websites

However, 10 months after the raid, the bulletproof[.]space and prohoster[.]info domains were still active. In the months following the arrests, the ProHoster service has continued operations through to as recently as November 2020. This trend of bulletproof services continuing to operate within select countries despite the intervention of law enforcement officials is very likely to encourage aspiring cybercriminals to operate within more lenient countries and remains one of the most desired features among criminals actively seeking a BPHS.

Section III. Key BPHS Features

The following section details several features that many modern bulletproof hosting services commonly advertise and consider staples for a reliable BPHS capable of supporting long-term criminal activity. The following features are often designed to reliably achieve a variety of goals. This typically includes features that either obfuscate the buyers' information or infrastructure from law enforcement entities or ensure that the service continues to operate even in the event that a portion of the infrastructure is disrupted or seized.

Fast-Flux DNS

Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. Fast-flux hosting services continue to hinder takedown efforts against nefarious storage services related to malware storage or underground marketplaces, allowing infrastructure like C2 domains to be constantly cycled through an ever-changing series of IP addresses. Fast flux-backed services are traditionally more expensive than those that do not offer the feature, and they support threat actors across a variety of use cases, such as serving exploit kits. Members of high-tier Russian-language forums, such as Exploit[.]in, have consistently continued to advertise fast-flux hosting services over VPN configurations, and servers located in every corner of the globe continue to remain a vital commodity within underground communities. Providers of fast flux-based infrastructure also regularly rely upon a number of cloud services to procure their infrastructure, including common services such as Microsoft Azure and Google Cloud.

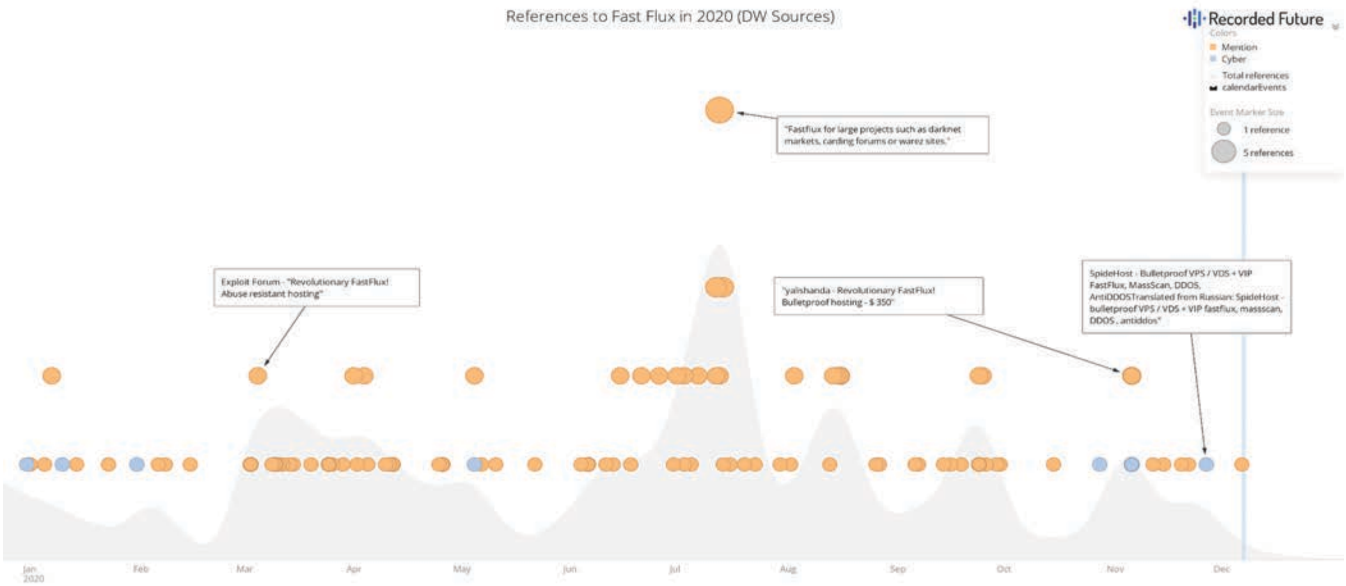


Figure 20: References to fast flux offerings within the dark web in 2020 (Source: Recorded Future)

Border Gateway Protocol

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. BGP route hijacking is an attack vector that temporarily spreads incorrect routing information as a way of intercepting network traffic in transit. Such attacks pose a risk to the ability of a network service provider to guarantee the safe delivery of content and data.

BGP targeting has positioned ISPs, or any hosting provider, as a target for both fraudsters and espionage operators. Most BGP routing incidents occur due to operator error, with any instance of BGP misrouting likely to have consequences for the traffic attempting to reach the victim AS. The misrouting can effectively "blackhole" traffic, or prevent a group of users from reaching a particular service. This is detrimental in the case of underground bulletproof providers offering a service to their customers whose financial success is contingent on maintaining operations. If the traffic is not blackholed by the offending AS, it may be intercepted and read, in a very noisy, but effective, surveillance operation. This could theoretically provide security or law enforcement professional's insight into the ownership of a particular criminal BPHS. Short-term leases of hosting resources from hosting providers remain common, with the providers reselling said resources from providers they consider to be suitable for their business purposes.

Privacy and Anonymity

Customer privacy, particularly the ability to submit anonymous payments, remains another critical feature criminals expect from any bulletproof hosting provider that claims to provide reliable services for illegal activity. Other unique service offerings within the criminal underground can provide a strong degree of privacy or anonymity support to a particular bulletproof hosting provider, including advertisements tied to the sale of SOCKS proxies or paid censorship bypassing services. Cryptocurrencies continue to be a major form of payment to hosting or DNS service providers including those who do not advertise their services as "bulletproof." The adoption of cryptocurrencies by hosting providers includes legitimate providers that offer their services to journalists or whistleblowers attempting to protect their identities. While Bitcoin remains the predominant cryptocurrency used to pay for criminal bulletproof hosting services, Recorded Future has observed advertisements accepting other forms of the digital currency including Ethereum and Monero among other currencies.

In addition to the anonymization of payments submitted to the providers, another layer of privacy highly desired by aspiring criminals within the underground when selecting a bulletproof hosting service is its capability to anonymize traffic. Many threat actors use either a VPN, VPS, or a bulletproof hosting provider to not only obfuscate their geographical location but also change originating IPs as needed. Custom services that rely on a combination of network connections distributed around the globe with other anonymized platforms such as Tor are highly desired for their ability to hinder efforts by law enforcement investigators. The speed of connection can be another factor in driving the price of a particular bulletproof hosting service and is likely to be highly desired by actors conducting other specific forms of threat activity reliant on a faster connection such as a brute-force attack. In some cases, the need for anonymity has to be counterbalanced with the need for speed as infrastructure in some of the safer regions may not be up to the level needed for operations.

Custom Data Centers

Not every hosting provider manages data centers that they are in direct control or ownership of, opting instead to act as resellers of systems leased from other internet service providers or hosting services. Custom infrastructure developed in-house by criminal providers is likely to continue to be more popular in countries where hosting certain criminal content is not a priority for law enforcement entities. In-house servers or data centers are distinct from other infrastructure that may be owned by another entity but were compromised by criminal actors to use within a bulletproof hosting service they offer. Custom data centers typically refer to servers or systems located on the privately owned property of individual actors offering to sell services administered through these systems to criminal entities. This setup can range from a rack of servers in a home to a private military bunker, as demonstrated by admins affiliated with the dark web marketplace Wall Street Market who were arrested in 2019.

Resistant to Law Enforcement or Abuse Requests

Bulletproof hosting providers are presented with a number of options when confronted with allegations of abusive behavior at one of their IP addresses. The options typically include either ignoring the request altogether or providing early notification to customers so they have time to alter their operations and avoid downtime. A key process of avoiding legal ramifications is creating a process that drags out the complaint procedure to the point where the request is often abandoned by the third party. It is in the face of such requests that the more credible bulletproof hosting providers are ultimately tested on many of their claims to be resistant to the efforts of law enforcement and capable of ensuring abuse requests are unable to result in prolonged periods of downtime. One critical aspect that can differentiate which providers are truly immune to such requests is those who have a strong understanding or working legal relationship with legitimate hosting providers in the countries related to the origin of the abuse request. Bulletproof hosting providers have historically evaded prosecution or jail time as a direct result of a working relationship with a combination of personnel within government or law enforcement agencies directly responsible for investigating their crimes. In attempts to avoid this scenario, some bulletproof hosting providers will refuse to allow the sale or promotion of certain services if they know it to be a priority for law enforcement investigators within a particular country. For example, investigative reports detailed by Trend Micro mention that Yalishanda was likely operating their infrastructure out of China, a country more tolerant of certain spamming operations than political content or satire directed at domestic officials.

Section IV. Outlook and Mitigation Strategies

There has been, and is likely to continue to be, a trend of ransomware operators purchasing already compromised network access from cybercriminals. Cybercriminals are likely to continue purchasing already compromised network access and reselling them via dark web/underground sources to supplement BPHS operations. Common cases for using bulletproof hosting services are likely to continue to include the hosting of command and control infrastructure, the distribution of phishing or spam messaging, and the hosting of other online fraud activities. As noted previously, ransomware operators affiliated with the Dharma and Phobos strains of malware that operate around a RaaS service model have already been observed using the volhav provider in 2020.

Bulletproof hosting services will often advertise the capability to migrate infrastructure as a key component of their service, enabling interested parties to choose and register their own subnet of IP addresses. Though full mitigation of malicious services hosted within countries more inclined to allow criminal actors to conduct their underground business is virtually impossible without the intervention of regulatory or law enforcement agencies, the Recorded Future Platform can assist in the monitoring of malicious service providers likely disseminating data linked to these businesses (regardless of whether the traffic is unintentional). The crux of this monitoring is often contingent on entire network allocations and the high volumes of malicious services they become affiliated with becoming unilaterally blocklisted. Recorded Future recognizes that this is not always a viable option, particularly as criminal actors have grown reliant on renting rather than owning this hosting infrastructure.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.