



Datum: 12 oktober 2022

Onderwerp: Waarschuwingslijst

Politie

Postbus 100, 0900-8844

Team Criminele Inlichtingen:

088-9647360

Beste digitale service provider,

Bij deze bieden wij een bijgewerkte lijst aan van hosting resellers die op het *surface web* openlijk worden besproken als de facilitators van cybercrime¹. Deze bedrijven afficheren zichzelf als bulletproof dienstverlener², al dan niet met een specificering van de verschillende misdrijven die zij mogelijk maken. De politie denkt dat de hosting resellers op de lijst de schakels kunnen zijn tussen uw bedrijf en individuen of groepen die het volgende slachtoffer al in het vizier hebben.

Reputatieschade

Op fora en ratingsites voor bulletproof hosting gebruiken deze bedrijven de Nederlandse, digitale infrastructuur vaak als verkoopargument. Ze weten dat Nederland doorgaans synoniem staat voor bulletproof. Dit negatieve profiel van Nederland als een accomoderende omgeving voor cybercriminele activiteiten geven de Nederlandse hostingsector een slechte naam.

De politie wil met u samenwerken om dit onderwerp te adresseren. Wij willen geen servers in beslag nemen, waardoor inkomsten onder druk komen, legitieme klanten last krijgen en werkdagen worden verstoord zonder ondernemingen de mogelijkheid te geven om hun bedrijfsvoering te wapenen. We adviseren het volgende als een van de personen of bedrijven tot uw klantenbestand hoort:

- Herzie uw overeenkomst met deze partijen,
- Doe een risicobeoordeling door een serie vragen te stellen, en
- Verzekert dat uw voorwaarden helder en consequent zijn.

Wij ondersteunen deze maatregelen graag en verzoeken om uw hulp bij de bestrijding van deze criminele entiteiten. Zij vormen een essentiële schakel voor cybercrime en zorgen voor significante reputatieschade voor Nederlandse digitale diensten.

Nieuwe lijst

In overleg met het Landelijk Parket van het Openbaar Ministerie is besloten tot een herhaling van deze actie. De brief en de lijst worden gedeeld met verschillende private partners. De wereld van het internet is volatiel, dus naast al bekende namen staan er nieuwe hosting resellers op de lijst. Daarnaast hebben wij de categorisering van deze partijen verder uitgewerkt. Om die reden delen we dit maal

¹ Deze lijst is te vinden als bijlage 1, op pagina 3 en 4 van deze brief. De tweede bijlage (p. 5) geeft achtergrondinformatie bij de lijst. De eerste keer dat wij een dergelijke lijst verstuurd hebben was op 17 november 2021.

² Bulletproof hosting (BPH) is technical infrastructure service provided by a web hosting provider that is resilient to complaints of illicit activities, which serves criminal actors as a basic building block for streamlining various cyberattacks (McCoy, Mi & Wang 2017, p. 805).



enkel de namen van bedrijven die *zichzelf* afficheren als bulletproof dienstverlener, al dan niet met hun eigen verduidelijking van de verschillende misdrijven die zij mogelijk maken. De lijst bevat bedrijfsnamen als *Abusehosting*, *Bulletproof web* en *Fuckservers*, om een idee te geven van de schaamteloosheid waarmee geadverteerd wordt voor de schadelijke dienstverlening.

Twee categorieën

Bijlage 2 biedt meer achtergrond bij de indicatoren en categorisering van hosting resellers. Omwille van de lengte wordt hier alleen nog het verschil benoemd tussen de twee categorieën van de lijst:

- 1) Deze hosters of resellers richten zich primair tot de cybercriminele gemeenschap. Zij adverteren in de regel op cybercriminele fora, zonder verwijzing naar een eigen website. Dit is een advertentie van een dergelijke hoster:

Origineel	Vertaling
Выделенные сервера под БРУТ и СКАН. Качественно! Доступно! Быстро! [...] Локация Нидерланды	Dedicated servers voor BRUTEFORCE en SCANNING. Goede kwaliteit! Betaalbaar! Snel! [...] Locatie: Nederland

Bron: <https://bhf.im/threads/592373/> (geraadpleegd: 16 mei 2022)

- 2) Deze bedrijven verklaren dat zij bulletproof hosting leveren, maar zij geven niet aan welke misdrijven zij faciliteren. Ze hintten wel op het plegen van delicten via hun onderverhuurde servers³.

Ter afsluiting

Pakketjes met schadelijke data kunnen vrijwel ongestoord via de Nederlandse haven het internet over. De 'Hollandse netwerken' van de infrastructuur staan bij criminelen, en binnen de cybersecurity-gemeenschap, bekend als een vrijhaven om slachtoffers te maken. Dit is niet acceptabel voor de Nederlandse politie. Het delen van de lijst is dan ook deel van een breed pallet aan acties om de Nederlandse infrastructuur te wapenen en samen met partners te werken aan de veiligheid van het internet.

Wij vragen u en uw bedrijf om met ons samen te werken als deel van de oplossing.

Bij voorbaat dank,

Politie

³ Websites van de bedrijven zelf zijn bezocht waar mogelijk. Bedrijven zonder websites adverteren op een cybercrimineel forum, waarbij ze hun klanten vragen om contact op te nemen via Jabber of Telegram.



Bijlage 1: Waarschuwinglijst

Categorie 1:

- 4server
- AbuseGuard
- Abuzam.net
- AlphaDS
- Best-rdp
- Brazzzers
- Bulletproof Hosting
- Corona Hosting
- EliteVPS
- Fitserver
- Fuckservers
- G-Hosting
- GOHS
- Inferno
- Masscan
- PiratHost
- Quality Hosting
- Rincomhost
- SpideHost
- Yalishanda
- Zservers



Categorie 2:

- AbuseHosting
- AdelinaHost
- Antiddos
- Blitz-Host
- Bulletproof Serv
- Eurohoster
- Flowspec
- Free-www
- Go4Cloud
- Hostingblack[.]com
- HostSting
- Njal.la
- PowerVPS
- Shinjiru
- Vainet.biz
- VPSDedic
- Xhost24



Bijlage 2: Achtergrond lijst

Deze lijst biedt informatie over hosters en resellers die vermoedelijk aanbieders zijn van bulletproof hosting (BPH⁴), meestal in een (criminele) context van bulletproof hosting. Om deze hosters/resellers te identificeren zijn 'bulletproof hosting' en de Russische vertaling hiervan ingevoerd in de zoekmachines van Google en het Russische Yandex. Veel van de hosters/resellers staan gerangschikt als BPH-aanbieders op vergelijkingswebsites. Andere bedrijven adverteren op cybercriminele fora of zij worden genoemd in discussies op dit soort fora. Informatie over al deze hosters/resellers is verwerkt in een standaard formaat, waaronder:

- Of de hoster/reseller wordt genoemd op vergelijkingswebsites;
- Of de hoster/reseller een of meer advertenties op internetfora heeft waar cybercrimediensten worden verhandeld;
- Of de hoster/reseller open is over het aanbieden van BPH, en
- Of de hoster/reseller wordt genoemd als BPH door een externe partij (of partijen).

Hier moet worden benadrukt dat niet alle hosters/resellers in de onderliggende databank voor de lijst en de lijst zelf gezien moet worden als doelbewust illegaal handelende partijen. Het is verder mogelijk dat een partij illegaal handelde in het verleden, maar sindsdien zijn handelswijze heeft aangepast.

Wat is bulletproof hosting?

Over de jaren is bulletproof hosting een bekend concept geworden in de cybersecurity gemeenschap. Cybercriminelen en degenen die van het internet een veiliger omgeving willen maken zien een bulletproof hosting provider, of reseller, als een facilitator voor *abuse*. Deze bedrijven bieden 'een schild' aan voor criminelen die mogelijk worden onderzocht door de autoriteiten. Het is belangrijk om te melden dat bulletproof in de regel *badware* betekent, omdat er ook hostingbedrijven zijn die bijvoorbeeld anonimiteit bieden aan dissidenten van autocratische en dictatoriale regimes. Zij hebben hun eigen

⁴ Bulletproof hosting (BPH) is technical infrastructure service provided by a web hosting provider that is resilient to complaints of illicit activities, which serves criminal actors as a basic building block for streamlining various cyberattacks (McCoy, Mi & Wang 2017, p. 805).



ethische standaarden voor het aanbieden van hun diensten, terwijl een bulletproof hoster slechts geïnteresseerd is in geld verdienen, ongeacht wat de kosten zijn voor een samenleving. De zogenoemde ethische hosting providers gebruiken de term bulletproof niet. Zij refereren aan hun diensten als privacy-vriendelijk, bijvoorbeeld.

Tijdens ons onderzoek in open bronnen over cybercrime hebben wij, de politie, meer dan eens gelezen dat de digitale infrastructuur van ons land een vrijhaven is voor abuse. Nederland wordt zelfs gebruikt als synoniem voor de bulletproof netwerken van het internet. Onze 'welwillende' wetgeving is een uniek verkoopargument voor criminelen die zo veel mogelijk slachtoffers willen maken. De volgende quote is wat dat betreft relevant:

The Netherlands is to cybercrime what Switzerland is to money.

Antivirusbedrijf Norton geeft de volgende uitleg over BPH:

"Bulletproof hosting operations are similar to regular web hosting, however these companies are a lot more lenient about what can be hosted on their servers. [...] Bulletproof hosting services are often found in countries with more relaxed laws about what type content is hosted on these servers, and also have less strict extradition laws, therefore making it easier to evade law enforcement. Due to the different laws in different countries, this creates a huge grey area that allow the owners to claim immunity to what their customers host."

Indicaties van bulletproof hosting

De analyse van entiteiten die BPH aanbieden of genoemd worden in de een context van BPH hebben waardevolle inzichten geboden in het opereren van deze entiteiten. In het bijzonder: tijdens het proces om te komen tot deze lijst hebben wij geleerd dat (vermoedelijke) BPH-providers vaak specifieke boodschappen sturen naar klanten om te hinten dat zij BPH leveren:

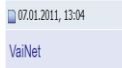
- Nederland heeft duidelijk een reputatie vanwege de tolerante jurisdictie voor digitale activiteiten. Van de (vermoedelijke) BPH-providers in categorie 1 en 2 laten de meesten expliciet weten dat hun servers in Nederland staan.



- Sommige, vermoedelijke BPH-providers, zoals in onderstaand voorbeeld⁵, beloven volledige anonimiteit aan klanten:

Анонимно. Мы не требуем от Вас каких либо персональных данных. Для регистрации необходима только электронная почта.	Anonymous. We don't ask any personal data from you. To register, you only need an e-mail address.
---	---

- Vermoedelijke BPH-providers melden vaak, zoals in het volgende voorbeeld⁶, dat zij hosten 'voor welk type project dan ook' (of een variatie van deze zin):

 07.01.2011, 13:04 Русский Реклама: СВТ - Принимаем и выплачиваем любые суммы. Работаем с 2014 VaiNet Абузостойчивый хостинг и выделенные сервера под любые проекты.	BPH and dedicated servers for whatever type of project
---	--

- Ter afsluiting, het ziet ernaar uit dat BPH-providers eerder dan reguliere providers kiezen voor communicatie met klanten via Jabber of Telegram in plaats van e-mail of telefoon.

Categorieën

Na de analyse van een brede populatie entiteiten die verklaren BPH te leveren, of worden genoemd in een context van BPH, kunnen we drie types onderscheiden:

1) Het eerste type hoster/reseller is open over het leveren van BPH en richt zich primair op de cybercrime gemeenschap. Deze hosters/resellers adverteren gebruikelijk op cybercrimefora en zij hebben geen reguliere website.

2) Het tweede type hoster/reseller biedt BPH openlijk aan, maar het specificeert niet het soort cybercrime dat het faciliteert. Van buiten af gezien verschilt dit type met de eerste categorie. De meeste

⁵ See <https://cvvboard.de/topic/2963-zserversru-vydelennye-i-virtualnye-servera-po-nizkim-tc/>

⁶ See <https://mmgp.ru/showthread.php?t=84858>

van deze bedrijven hebben een reguliere website, en de meeste van hen adverteren niet specifiek op cybercriminele fora. Veel van de hosters/resellers in deze categorie bieden servers aan in Nederland en impliceren aan potentiële klanten dat de Nederlandse wetgeving bepaalde vormen van digitale activiteit toelaat die in andere landen zijn begrensd. De hosting die zij aanbieden is bulletproof, vanuit hun perspectief, in die zin dat klachten van buiten Nederland genegeerd en verworpen kunnen worden. Voorbeelden van dit soort implicaties aan potentiële klanten zijn te vinden in de volgende fragmenten⁷:

АБУЗОУСТОЙЧИВОСТЬ Нашим клиентам мы гарантируем защиту от возможных поступающих жалоб. Учитывая расположение серверов в Нидерландах, мы ориентируемся на законы этой страны. Наша техподдержка будет игнорировать обращения надзорных органов других стран.	Bulletproof We guarantee protection to our customers from possible incoming complaints. Given the fact that our servers are located in the Netherlands, we are focused on the legislation of that country. Our tech support will ignore the appeals from supervisory bodies of other countries.
Наш хостинг выполняет требования закона в тех странах в которых находятся сервера - Германия, Голландия, Россия	Our hosting meets the legal requirements in those countries in which our servers are located – Germany, the Netherlands, Russia

3) **Het derde type** hoster/reseller maakt geen melding van BPH, maar hij wordt desalniettemin gerangschikt op vergelijkingswebsites vanwege de servers in tolerante jurisdicties zoals Nederland en mogelijk op basis van klantenervaringen. Deze categorie is niet gedeeld buiten de politie, omdat deze bedrijven niet van zichzelf zeggen dat zij BPH leveren. Wij hebben dit soort verklaringen niet gevonden.

De onderliggende databank voor de lijst is gestructureerd volgens deze drie categorieën van hosters/resellers.

⁷ See <https://hoststing.ru/> and <https://steadyhost.ru/lk/billing.php?do=faq&group=0&fgroup=0&item=3>